

# Technical basics

This chapter gives a short introduction to the technology behind your new ELSA device. Pros in network technology will breeze through this part. If you are new to networks, you will find this section very helpful for understanding the technical terms and concepts.

This reference section describes the following devices:

- *ELSA LANCOM Wireless IL-11*
- *ELSA LANCOM Wireless L-11*
- *ELSA LANCOM Wireless devices with DSL firmware*

## Wireless networks, IEEE 802.11 standard

The *ELSA LANCOM Wireless* series devices conform to the IEEE 802.11 standard. This standard is a supplement to the previous IEEE standards for LANs, with IEEE 802.3 for Ethernet being the best known. In fact, wireless networks that comply with 802.11 can easily be connected to existing Ethernet networks. This is the most important function of the *ELSA LANCOM Wireless* devices. With the exception of a few additional parameters, a wireless adapter that complies with 802.11 is seen by the computer as a normal Ethernet card. This means that you can use any protocol that you would otherwise use for a wired Ethernet (IP, IPX, NetBIOS,...) on an 802.11 wireless network. The only difference is that there are no wires between the computers.

The range of wireless LAN systems is limited, the IEEE standard only covers the definition of LANs. A typical line-of-sight range would be under 300 meters, with considerable reductions in range due to walls and floors of buildings. The group of wireless LAN stations directly within range of each other is generally called a cell.

### Ad hoc mode

The IEEE standard provides for two operating forms that differ with regard to the security and range of these wireless LANs.

A wireless LAN in ad hoc mode consists of a single cell, which is seen by the Ethernet as 'closed', i.e. an external connection is only possible by routing superordinate protocols. An example for such an element would be an *ELSA LANCOM Wireless IL-11*, that serves as an Internet access router for all other stations via its ISDN port. Ad hoc networks tend to spring up spontaneously. For example, a workgroup might like to network its workstations for data exchange. Workstations can enter and leave the network as required. There is no special node that must be present at all times. Authentication cannot be a requirement for participation, since there is no central station to monitor the participants.

But what happens when a workgroup in a neighboring office has the same idea, and also sets up a network? While two normal Ethernets would consist of two wired physical structures without connections between them, it's harder to block radio waves to prevent interference. To prevent this, every IEEE wireless LAN has a specific parameter - the name of a WLAN domain. The users choose a string of up to 32 characters for the WLAN domain name. At the wireless level, this name is converted to an additional addressing component that associates data packets with a specific cell. To enter an existing wireless LAN, the name of the WLAN domain must be entered in the advanced settings for the network adapter driver. Upon starting, the driver will look for an existing wireless network with this identification. If it finds one, it will then establish a connection, permitting you to communicate with the computers in that wireless network. If it does not find an existing network, it will establish a new cell.

Even if the cells are logically separated in this manner, they can still interfere with one another physically, since only one station can transmit at a time. In other words, none of the cells would be able to take advantage of the full bandwidth in the event of an overlap. This can be prevented by also assigning different radio channels to the individual networks. Just as two radio transmitters can transmit simultaneously on different frequencies, two wireless LANs can work simultaneously on different channels without interference. If two cells are very close to one another, there should be a difference of 4 to 5 channels between the channels used, because the cells also partially use the neighboring channels.



*Not all of the channels included in the IEEE standard are permitted in all countries!*

## Infrastructure mode

The big advantage of wireless networks based on the IEEE 802.11 standard is the ease of coupling with existing Ethernet networks. A wireless network can be used to connect mobile stations to an existing wired network. Existing networks can also be used to link multiple cells, thus increasing the range of the wireless network. This requires all participants to operate in a different mode, the infrastructure mode.

In addition to the mobile stations, infrastructure mode uses a base station, also known as an access point or distribution system. The *ELSA LANCOM Wireless* devices were designed to serve as access points. The access point handles monitoring functions in the infrastructure mode. Domain names and radio channels are still required, and stations entering a network still search for an existing cell. Unlike the ad hoc mode, however, the cell is always established by the access point, and each station entering the network must log on to the access point, before being permitted to exchange data in the cell. The access point generally also fulfills the function of a "relay station" for data. While this reduces the achievable data rate, careful positioning of the access point can increase the area of a cell. Still, the main role of an access point is to connect a wireless cell to a wired Ethernet. If the access point receives a data packet for a computer that is not logged on to it, it forwards the packet to the Ethernet. Conversely, it continuously monitors the

Ethernet for data directed to stations logged on to it, and forwards the packets within the radio cell. The logon requirement ensures that the access point always knows which stations are available on the wireless side. It then knows how to direct each data packet. This process is known as bridging. Important: Because it is not necessary to log on in ad hoc mode, this bridging (which is fully automatic for the users) is only possible in infrastructure mode. Therefore, you would only operate a *ELSA LANCOM Wireless* in ad hoc mode if you do not want to use the Ethernet interface.

As mentioned earlier, an Ethernet backbone can also be used to extend the range of a wireless LAN. In this case, multiple access points can be incorporated in the same LAN, and configured to the same WLAN domain. When a mobile station wants to establish a connection with the network, it seeks out and logs on to the access point with the strongest signal. Two mobile stations logged on to different access points can thus communicate with one another, even though they are not within direct radio range. The Ethernet, linking the access points, closes the gap.

If a station continues to monitor the radio situation after logging on, it can determine the relative signal strengths of the access points, and automatically switch over to the strongest access point at any given time without user intervention. This process is known as roaming.

## Interchangeability with other devices

*ELSA LANCOM Wireless* devices based on the IEEE-802.11 standard are, in principle, interoperable with devices based on 802.11 from other manufacturers. But because the 802.11 standard is still quite new, and many manufacturers are only now converting from proprietary wireless LAN solutions to 802.11, interoperability is not always possible. At the very latest, interoperability can fail due to the modulation process used: *ELSA LANCOM Wireless* devices use the direct sequenced spread spectrum (DSSS) process, while some other manufacturers use the frequency hopping spread spectrum (FHSS) process. The exchange of data between devices based on the different processes is never possible.

## Network technology



*This section gives a brief introduction to the basics of network technology. These descriptions do **not** cover all possible techniques, processes and terms associated with network technology. Their purpose is to help you understand your device and its product information.*

### The network and its components

*Network,  
Transmission  
medium,  
Interfaces*

Whenever several computers communicate with one another, they make up a "network". For computers to be able to communicate, they need a physical medium through which the information can be transmitted. This can be a wired or radio link, for example, that is connected to the computers using special interfaces (e.g. network adapters).



*The term network cable (or simply wire) in the following text is meant to include any other physical medium functioning as a cable, such as wireless links.*

*Packets  
Cells*

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



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

*Host*

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

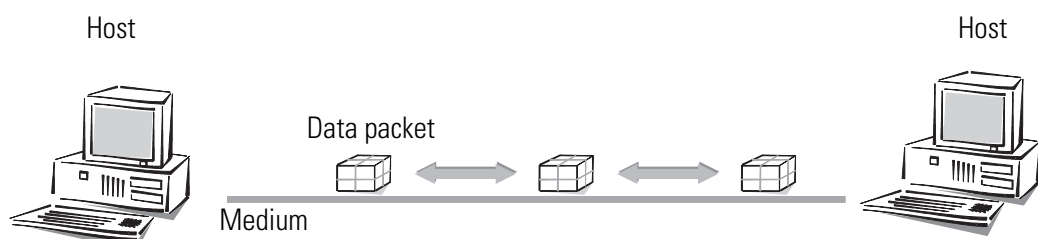
*Router*

The transport of packets between two hosts occurs indirectly through exchanges that pass packets on to the destination computer. These exchanges are called routers. A router has at least two interfaces, one to receive the data from a sender, one to transmit data to a destination. Apart from the exchange function, the router is also a host. It can also be the destination of data packets (e.g. for its own configuration).

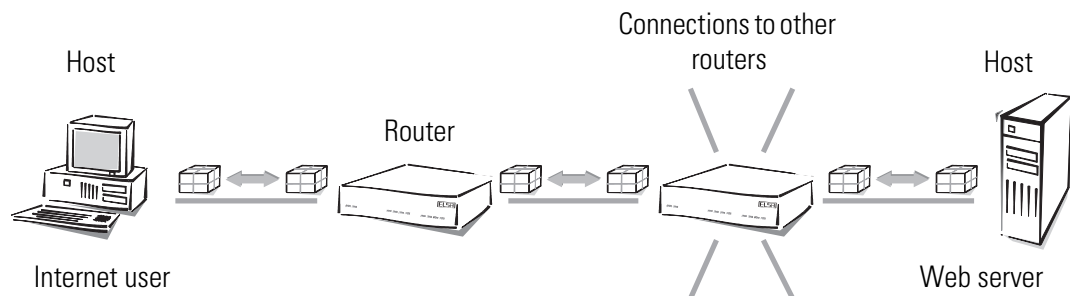
### Connection modes

*Point-to-point  
Connection*

When exactly two hosts are connected via a medium, this is referred to as a point-to-point connection. One host transmits packets that can be received by exactly **one** recipient (unambiguous connection).



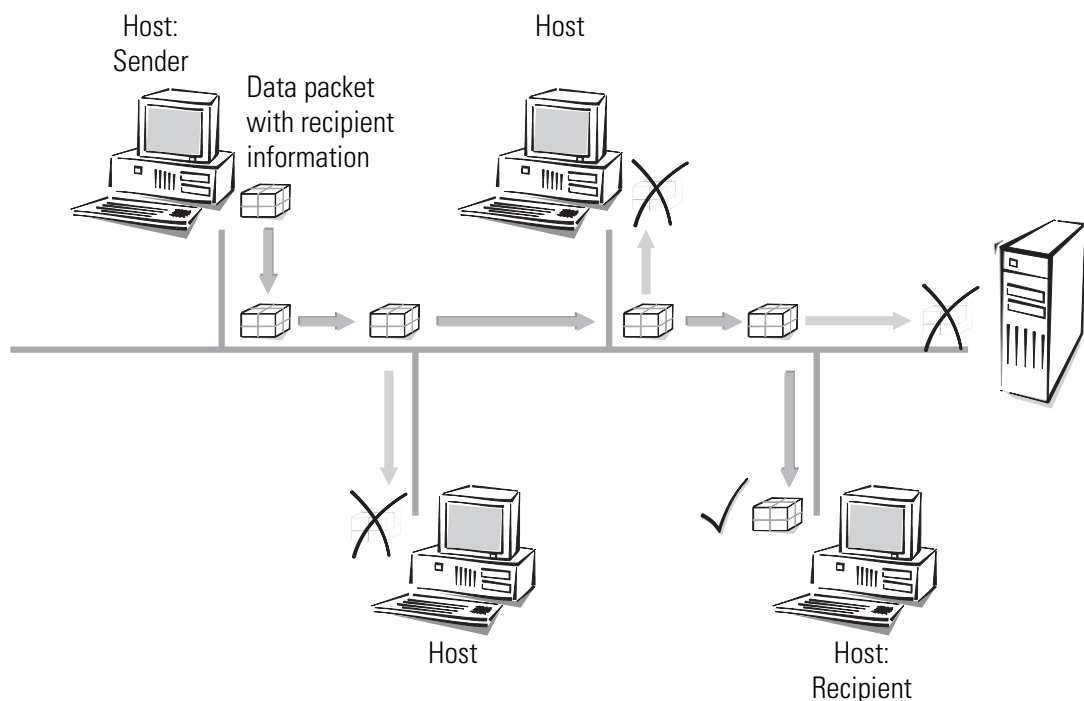
Access to the Internet is also a point-to-point connection. Even though the data packets are sent from the Internet user host to the Internet provider host (server) via several routers, each data packet still has its own specific destination. The routers will forward each data packet to exactly one recipient. Therefore, this connection is also called unambiguous.



#### Point-to-multipoint connection

*The term "point-to-point connection" is not quite correct. However, it is useful to distinguish this kind of connection from the following "point-to-multipoint connections".*


It is generally considered to be uneconomical to connect all computers in a network directly, via point-to-point wired connections. The computers would then require multiple interfaces. Computers in a network are therefore plugged into a joint medium shared by all hosts. The sender simply sends its packet to the medium to which other hosts are connected, specifying the recipient. The data packet arrives at **every** host in the network. Each host then decides whether or not it is the recipient of the packet. If the packet is addressed to a host, it will then accept it. If not, the host will ignore (discard) it. This is a point-to-multipoint connection, since the connection is not to one point only.



## Network types

<i>Protocol</i>	An important prerequisite for communications between computers is a common language among the hosts. In network technology, this language is called "network protocol" or simply "protocol".
<i>TCP/IP</i>	The most widely used network protocol is TCP/IP ( <b>T</b> ransmission <b>C</b> ontrol <b>P</b> rotocol/ <b>I</b> nternet <b>P</b> rotocol). It is used mainly in the Internet, although many company intranets now also use it. Other network protocols include IPX and Apple Talk. Because it is so widely used, this chapter deals mainly with TCP/IP.
<i>IP network</i>	Hosts wanting to communicate with each other using the TCP/IP protocol must be plugged into the same network, and must have the TCP/IP protocol (also called TCP/IP stack) installed. This is called an IP network.
<i>Internetwork Internet</i>	A number of networks connected using the IP protocol is referred to as an internetwork. The largest union of many small, public IP networks is the Internet.
<i>Local network (LAN)</i>	A network covering a limited area, with hosts on the same hierarchical level, and using the same medium (shared medium) is called a local network ( <b>L</b> ocal <b>A</b> rea <b>N</b> etwork, LAN).

## IP addressing

<i>Packet-oriented transfer</i>	In IP networks, the communication between computers is packet oriented. This means that data or messages are packed together in packets of variable length, and sent as a unit from the source computer to the destination computer. Apart from the actual information to be transmitted (useful data), the data packet also contains address and control information.
<i>IP address</i>	IP addresses are used in IP networks for communication between various devices. Every host has its unique address, which identifies it unambiguously. What does an IP address look like? It consists of four bytes separated by dots, making a total of 32 bits. Each of the four bytes can take on values from 0 to 255, e.g. 192.168.130.124.
	<i>To be precise, the IP address refers to the interface, and not the host itself. A terminal device with more than one interface (such as a router) needs an IP address for every interface. This is why ISDN routers from ELSA for example, have an IP address for communication with the hosts in their own network, as well as a second IP address for communication with the "outside world" using the ISDN network. Likewise, ELSA cable modems have an IP address for their own network, and another IP address for the exchange of data with the cable network.</i>
<i>Network address</i>	An IP address contains the address of the network, as well as that of the host. The network address is the same for all hosts on one network. The address of the host is unique within the network. A router can have several IP addresses, each unique within the network.

*Net mask*

How do you see which part indicates the network, and which part identifies the host? From the network mask. A mask is a familiar thing. It covers one part of something, and only leaves the other part visible. This is exactly how a network mask operates. It is a number, which is identical in structure to the IP address, i.e. 32 zeros or ones. The network mask usually starts with ones at the beginning and ends with zeros. The zeros at the end cover the part of the IP address, which does not belong to the network address.

Examples:

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

The same IP address, this time with another netmask:

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

From this you see that an IP address alone is not enough. A host can be identified unambiguously only in combination with a netmask.

And you can also see that there are more bits available to identify the individual hosts in a connected network, if there are fewer bits in a netmask that contain a '1'. While only 254 different addresses could be allocated in the first example with the netmask 255.255.255.0, the second example has  $254 \times 254 = 64516$  different addresses available. The first and the last digit of an address space are reserved for the network address and the broadcast address (addresses for packets to all hosts in an IP network). In the netmask 255.255.255.0 this is the '0' for the network address and the '255' for the broadcast address.

A new notation of the netmask simply attaches the number of bits available for the network address to the IP address: 137.226.4.101/24. The number after the slash tells us that the first 24 bits indicate the network address. This notation reduces the length of the entries in the routing tables.

*IP address management*

The IP addresses must be unique within a specific network in order to avoid confusion. Since the Internet is based on TCP/IP and thus uses IP addresses for its millions of connected computers, all Internet addresses must also be unique. Supervisory groups manage and distribute these publicly-accessible addresses. Since the number of IP addresses theoretically available is limited, these distributing authorities charge high rates for the addresses.

*Private address spaces*

Certain ranges of IP addresses are reserved for use free of charge (private address spaces) so that companies with intranets do not have to purchase individual IP addresses for every workstation. In a closed network (e.g. a private network or intranet), these addresses can be used as desired. The same address can be used in other closed networks (e.g. in different companies), but the addresses within one network must be unique.

However, these reserved IP addresses must **not** be made public (on the Internet). Only **those** devices in a network that are connected to a public network (e.g. the router at the interface to the Internet) must have a registered IP address.

IANA (Internet **A**ssigned **N**umbers **A**uthority) has allocated the following four address ranges for private use:

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

There are two considerations when using these IP addresses:

- The IP addresses used in a private network should not leave the network. An Internet connection is possible only when using IP masquerading, for example.
- The packets for these IP addresses will not be routed in the Internet. Backbone routers will simply discard such IP packets. Depending on the provider, penalties may result if such IP packets are released on the Internet.

## IP routing and hierarchical IP addressing

*Routing*

Every IP packet contains the IP addresses of the source and destination. A router receives IP packets at its interfaces, interprets the destination address and forwards the packets to one of its interfaces that is "on the way" to the destination. Finding the appropriate path is called routing.

*Routing table*

Every router manages a routing table. This table indicates, for every host in the network, the quickest interface connection to that host. You can imagine that, as they grow, these



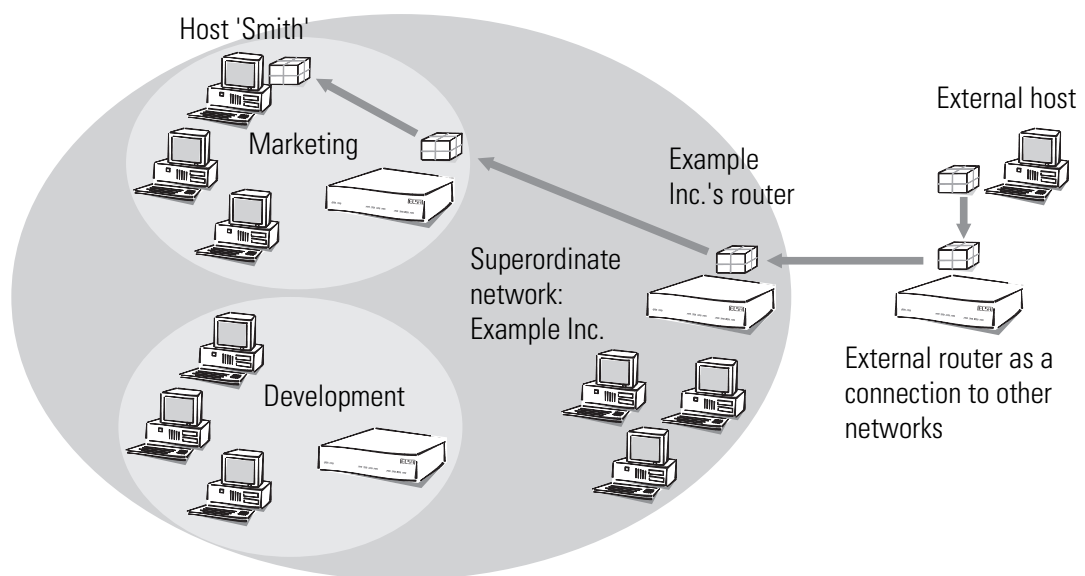
tables may exceed the capacity of the router. The Internet, as a worldwide collection of publicly accessible IP computers, contains several million hosts.

#### *Hierarchical IP addresses*

For this reason, hierarchical IP addresses were introduced. This means dividing the IP network into subnets, in which IP addresses are distributed from an unbroken numerical range. With several hierarchy levels, different subnets can be merged into larger subnets. The principle is similar to the hierarchical address used by postal systems, consisting of a country, a city, a street and a house number.

The consequences of this hierarchical IP addressing are:

- Since all hosts within one network have the same network address, the host address is sufficient for the hosts within this network to communicate with one another.
- A router has to know both the addresses of the hosts that are directly connected to it, and the addresses of all networks and subnets that are reachable via adjacent routers.
- It is **not** necessary for a router to know **all** other possible IP addresses.



As an example, think of a company with one large network, with small subnets for its different divisions. The address of the network for the marketing division is made up hierarchically from the address of the company and that of the department.

Whenever a host external to the company network sends a packet to a host in Example Inc., this is what happens:

- ① The sender gives the packet the destination address "host 'Smith' - Marketing - Example Inc.".
- ② An external router that establishes the connections to other networks has to know how to reach Example Inc. As soon as it receives a packet with the address for Example Inc., it passes the packet on to the router responsible for Example Inc.

- ③ The router in Example Inc. receives the packet and extracts from the address the information that it is destined for Example Inc. Since it is part of Example Inc., it takes a closer look at the address to find the name of the division. It then forwards the packet to the router in the marketing division.
- ④ The router in the marketing division receives the packet and extracts from the address the information that it is directed at the marketing division of Example Inc. Since it is part of this division, it takes a closer look at the address to find the name of the host. It then forwards the packet to the host of the employee Sam 'Smith'.

Now we shall take a look at the example using proper IP addresses. The network of Example Inc. has the numerical space '192.168.100.0' to '192.168.100.255' at its disposal, with the '0' for the network address and the '255' for the broadcast address.

All the router has to remember is that every address beginning with '192.168.100' is located within the network of Example Inc.

Imagine a router that is connected to the network of Example Inc. through an interface. If it receives a packet with destination address '192.168.100.4' and netmask '255.255.255.0', it will compare this with every network address it knows. In doing so it carries out a logical AND with the netmask, and compares the results with the network address: '192.168.100.4' AND '255.255.255.0' produces '192.168.100.0'. This is the network address of the Example Inc. network. The router recognizes that the recipient is located within Example Inc. and passes the packet on to the interface that is "on the way" to Example Inc. Within Example Inc. the packet is then passed on to the appropriate subnet.

The same procedure is used for the transfer of IP packets within a network:

- ① If a host in the subnet of the development department wants to send a data packet to Mr. 'Smith', the sender attaches the destination address "Host 'Smith' - Marketing - Example Inc.".
- ② The router in the development division receives the packet, and extracts from the address the information that it is destined for the marketing division of Example Inc. Since it is part of Example Inc., but not of the marketing division, it passes the packet on to the router in the superordinate network.
- ③ The router in Example Inc. receives the packet and extracts from the address the information that it is destined for Example Inc. Since it is part of Example Inc., it takes a closer look at the address to find the name of the division. It then forwards the packet to the router in the marketing division, where the packet is forwarded to the recipient.

## Expansion through local networks

### *Media access control*

So far, we have only considered the point-to-point connections. However, many computer networks are based on multipoint cabling, e.g. Ethernet. All computers connected to the same network can then receive the signals of all other computers (broadcast transfer to a shared medium). If several computers are sending simultaneously, the superimposed signals are destroyed. For the avoidance and resolution of such collisions, an access protocol, **Media Access Control**, is implemented.

### *LAN and IP network*

The connection of all computers communicating through a shared medium using a MAC protocol is called a LAN (local area network). A LAN forms an independent network and is logically subordinate to the IP network. IP networks can use the physical connections of the LAN to establish connections between hosts and routers. A LAN - Local Area Network - is, as the name indicates, spatially limited.

### *MAC address*

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

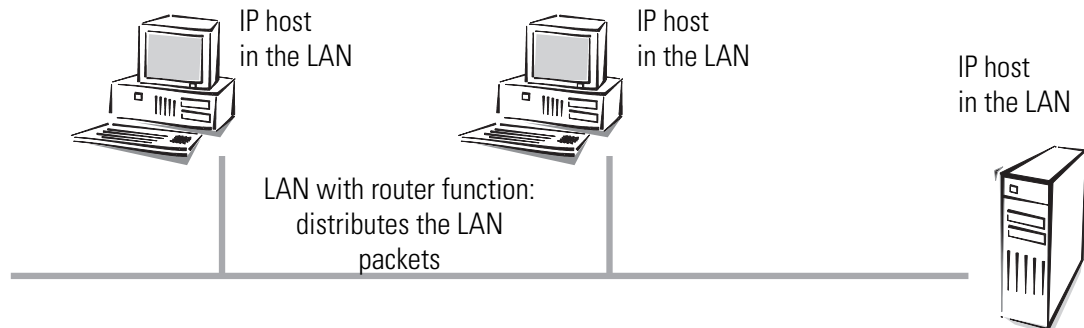
MAC addresses are independent of IP addresses. An IP host whose interface works via a LAN, has an IP and a MAC address. Whereas the structure of IP addresses, with its similarity to postal addresses, is designed to simplify routing in enormous IP networks, the fingerprint-like MAC addresses are designed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

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

### *IP in the LAN*

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

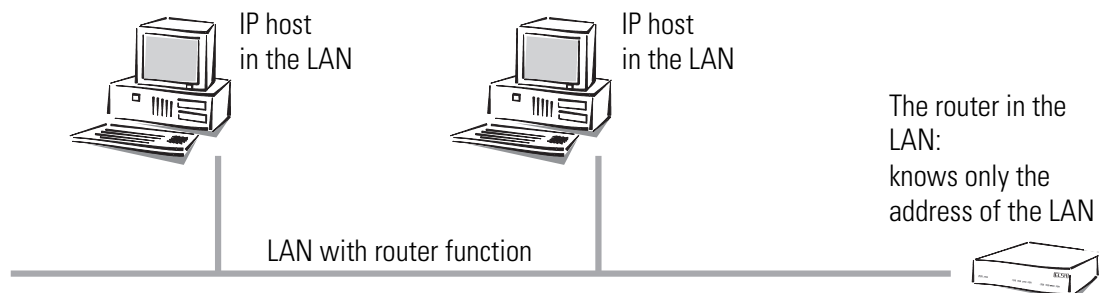
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts give the packets to the LAN, which handles the further distribution of the data packet. Therefore, for internal communication of LAN hosts via the IP protocol, only IP addresses from the numerical space of the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



To a router in the LAN, a host in its own LAN seems to be located behind another router. So the task for the router is very simple: all it has to know for operating in the IP network are the IP addresses

- of the directly connected hosts and
- of the available networks and subnets.

So all it has to remember are the network addresses and the netmasks of the subnets in the LAN.



In contrast, the host is confronted with a more difficult task than the router. In case of a wired point-to-point interface, the host knows that all packets that it sends through the interface automatically arrive at its router, for example. With point-to-multipoint connection to the LAN, it has to distinguish two cases.

- A packet with an address outside the LAN is passed on by a sending host to a router in the LAN, which takes care of the further processing of the packet.
- A packet with an address within the LAN has to be sent directly to the destination host, since the router in the network does not know the addresses of all the different hosts.

## Data transfer within the LAN

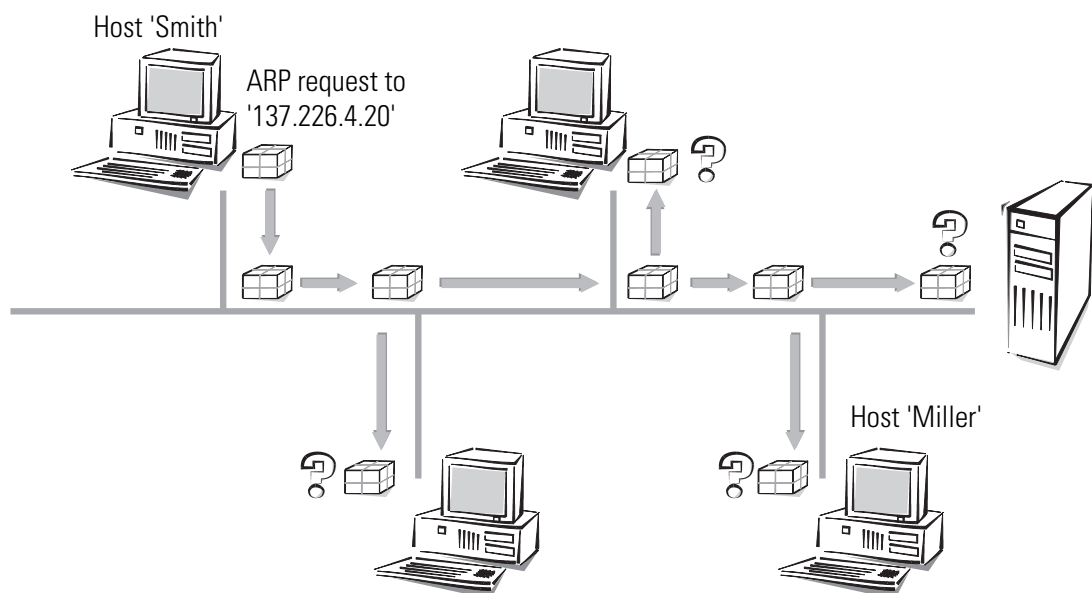
Let's use an example to explain this. Imagine the hosts of the subnet in the marketing division are linked via a LAN. The hosts have IP addresses from the numerical space '137.226.4.1' to '137.226.4.254' (the addresses '137.226.4.0' and '137.226.4.255' are reserved), the network address is '137.226.4.0' and the netmask is '255.255.255.0'. A router connected to the LAN provides access to the outside world of the Internet. Its LAN interface has the IP address '137.226.4.1' and the MAC address '00-80-C7-6D-A4-6E'.

Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). From the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located in a subnet of the same LAN. It therefore has to send the packet through the LAN, directly to host 'Miller'. Unfortunately he cannot tell the LAN interface: "Send the IP packet to IP address 137.226.4.20", because the LAN interface only understands MAC addresses.

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

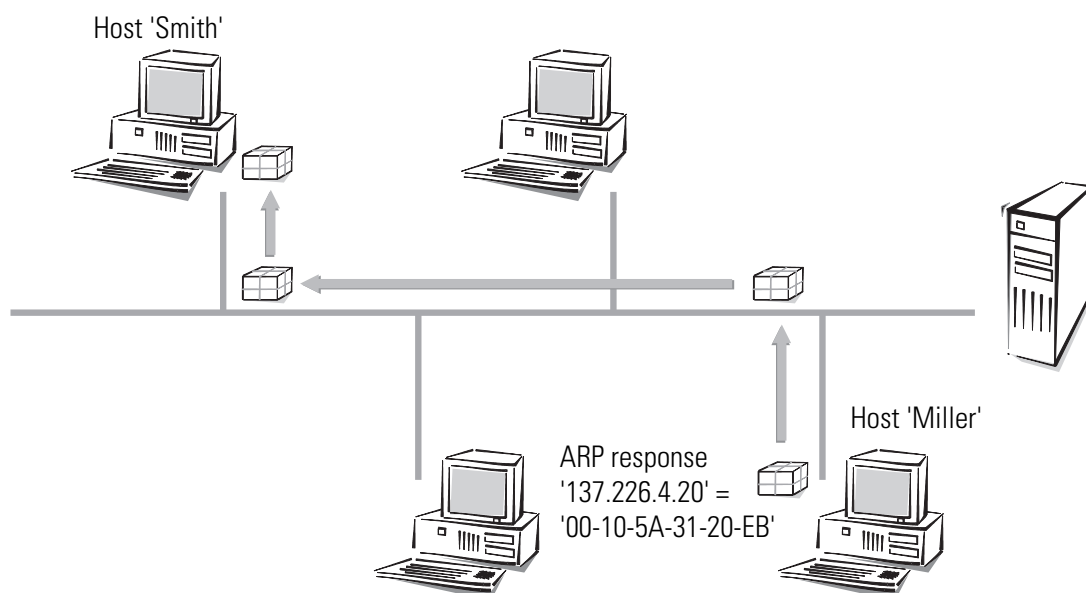
ARP

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



This ARP request packet is simply a question to all hosts listening to the IP address '137.226.4.20'. Host 'Miller' receives the packet, detects that it is addressed to him, and responds with an ARP response packet, which it sends directly to host 'Smith' (it takes

the MAC address '00-10-5A-31-20-DF' of host 'Smith' from the sender field in the ARP request packet). Host 'Smith' recognizes this as an answer to its request, extracts the MAC address '00-10-5A-31-20-EB' from the ARP response packet and enters it into his ARP table.



Then it can finally turn to its original task: sending the IP packet to host 'Miller'. It now finds the entry "IP address 137.226.4.20 corresponds to MAC address '00-10-5A-31-20-EB'" in the ARP table, and tells his LAN interface: "Send this IP packet to the computer with the MAC address '00-10-5A-31-20-EB'".

### Data transfer from the LAN to the Internet

Imagine the second task, that of sending an IP packet from host 'Smith' to the remote host 'External' with IP address 151.189.12.43. Host 'Smith' compares the IP address with his network address and realizes that host 'External' is located outside the LAN. So host 'External' can only be reached through the router. He discovers the MAC address of router '00-80-C7-6D-A4-6E' from its IP address by searching the ARP table. (If necessary, another ARP request is made first.) So host 'Smith' tells its LAN interface: "Send this IP packet to the computer with the LAN address '00-80-C7-6D-A4-6E'". The router extracts the IP packet from the LAN packet, and reads the IP address of host 'External'. In the routing table, the router then looks under the network address of this host, and finds the interface through which to forward the IP packet.

### LAN coupling on MAC basis

You know that LANs greatly simplify connecting computers to a local network. Nearly all house networks are thus LAN based. In some cases a LAN covers such a large area that the physical characteristics of the wiring inhibit connecting more computers. So it is sometimes very useful to combine several LANs. They remain, electrically and in terms of the MAC protocol, independent LANs, but for the IP protocol, they look like one big LAN.

This coupling of LANs is carried out using bridges. A bridge works somewhat like a router, but uses only MAC addresses for routing, not IP addresses. Since MAC addresses do not give any information on the structure of the network the way IP addresses do, every bridge has to know all MAC addresses in the whole LAN.

And so we encounter the same problem that we had with the routers before the introduction of subnets: As the LAN expands, it will at some point exceed the capacity of the address tables of the bridges. So one cannot use bridges to connect an extremely large number of LAN's. On the other hand, the unstructured MAC addresses allow the bridges to learn automatically about the location of computers in the network, using the received packets. This is called an "intelligent bridge".





# Menu command description

The configuration menu is divided into status information, setup parameters, firmware information and 'Other'.

For ease of orientation, we will first show you an overview of the menu structure.

In the complete list of all menu commands, you will find an exact description of all displays, menus, and commands with their parameters, default values, and valid entries.

You can access the configuration menus via Telnet or terminal programs, as well as via SNMP (see also 'Configuration modes').

If using a *ELSA LANconfig* configuration, you can use an integrated help system, that contains descriptions of the various parameters.

## Table descriptions

<b>Menu</b>	indicates the presence of a submenu.
<b>Info</b>	indicates a value that cannot be changed.
<b>Value</b>	indicates a value that can be changed.
<b>Table</b>	indicates a table, whose entries can be changed.
<b>Info table</b>	indicates a table, whose entries cannot be changed.
<b>Command</b>	executes a command.

## Menu overview

<b>MENU</b>	<b>Setup</b>	
	<b>VALUE</b>	Name
	<b>MENU</b>	WAN module
	<b>MENU</b>	Accounting module
	<b>MENU</b>	Charges module
	<b>MENU</b>	LAN module
	<b>MENU</b>	IPX module
	<b>MENU</b>	TCP-IP module
	<b>MENU</b>	IP router module
	<b>MENU</b>	SNMP module
	<b>MENU</b>	DHCP module
	<b>MENU</b>	DNS module
	<b>MENU</b>	NetBIOS module
	<b>MENU</b>	Config module
	<b>MENU</b>	WLAN module
	<b>MENU</b>	LANCAPi module
	<b>MENU</b>	LCR module
	<b>MENU</b>	Time module

<b>MENU</b>	<b>Firmware</b>	
	<b>INFO TABLE</b>	Version table
	<b>INFO TABLE</b>	FirmSafe table
	<b>VALUE</b>	FirmSafe mode
	<b>VALUE</b>	FirmSafe timeout
	<b>COMMAND</b>	Firmware test
	<b>COMMAND</b>	Firmware upload

<b>MENU</b>	<b>Status</b>	
	<b>INFO</b>	Connection
	<b>INFO</b>	Current time
	<b>INFO</b>	Operating time
	<b>MENU</b>	WLAN statistics
	<b>MENU</b>	WAN statistics
	<b>MENU</b>	LAN statistics
	<b>MENU</b>	PPP statistics
	<b>MENU</b>	IPX statistics

<b>MENU</b>	TCP-IP statistics
<b>MENU</b>	IP router statistics
<b>MENU</b>	Config statistics
<b>MENU</b>	Queue statistics
<b>INFO TABLE</b>	Connection statistics
<b>INFO TABLE</b>	Info. connection
<b>INFO TABLE</b>	Layer connection
<b>INFO TABLE</b>	Call info. table
<b>INFO TABLE</b>	Remote connection statistics
<b>MENU</b>	S <sub>0</sub> bus
<b>INFO TABLE</b>	Channel statistics
<b>MENU</b>	Time statistics
<b>MENU</b>	LCR statistics
<b>INFO TABLE</b>	Charge statistics
<b>MENU</b>	PCMCIA status
<b>COMMAND</b>	Delete values
<b>MENU</b>	LAN management statistics
<b>MENU</b>	<b>Other</b>
<b>MENU</b>	Manual dialing
<b>COMMAND</b>	System boot
<b>COMMAND</b>	System reset
<b>COMMAND</b>	System upload

## Status

The "status" menu contains information about the current status, and about internal LAN and WAN processes that could affect the data transmission link (e.g. dialing or connection) or statistics (e.g. number of data packets received or sent). The statistical displays are an important aid for verifying correct functioning, and for optimizing parameter settings. In addition, they provide valuable information for error analysis when malfunctions occur.

Most status displays are continually updated. The menus contain a **Delete values** command that sets the display to 0.

The menu has the following structure:

Status	Running status displays	
Connection	<b>INFO</b>	Status of the WAN link
Current time	<b>INFO</b>	Current time in device
Operating time	<b>INFO</b>	Operating time of device since last switched on
WAN statistics	<b>MENU</b>	WAN statistics display
LAN statistics	<b>MENU</b>	Network area statistics
WLAN statistics	<b>MENU</b>	Wireless network area statistics
PPP statistics	<b>MENU</b>	Point-to-point protocol statistics
IPX statistics	<b>MENU</b>	IPX area Statistics
Bridge statistics	<b>MENU</b>	Bridge area statistics
TCP-IP statistics	<b>MENU</b>	TCP/IP area statistics
IP router statistics	<b>MENU</b>	IP router statistics
Config statistics	<b>MENU</b>	Remote configuration statistics
Queue statistics	<b>MENU</b>	Individual module queue packet statistics
Connection statistics	<b>INFO TABLE</b>	Connection information for each interface
Info. connection	<b>INFO TABLE</b>	Information about last connection for each Interface
Layer connection	<b>INFO TABLE</b>	Information about the B-channel protocol used for each interface
Call info. table	<b>INFO TABLE</b>	Information about the last 100 calls received
Remote connection statistics	<b>INFO TABLE</b>	Statistics for the last 100 connections
S <sub>0</sub> bus	<b>MENU</b>	Status of the S <sub>0</sub> interface
Channel statistics	<b>INFO TABLE</b>	Individual channel status information.
Time statistics	<b>MENU</b>	Time module information
LCR statistics	<b>MENU</b>	Least-cost router information
PCMCIA status	<b>INFO TABLE</b>	PCMCIA status information

Status	Running status displays	
Charge statistics	<b>MENU</b>	Charges module information
Delete values	<b>COMMAND</b>	Delete all values except for tables with subordinate statistics
LAN management statistics	<b>MENU</b>	Address table for the local network

## Status/Connection

The menu command **Status/Connection** displays the status reports for the individual channels.

/Connection	Running status displays	
Connection	<b>INFO</b>	DSL1: Ready; CH01: Ready; CH02: Ready

## Status/Current time

This displays the current device time, as used for such things as least-cost router calculations, or for certain statistics. This time can either be read from the ISDN network (ISDN time, see also Setup/time module) or manually set (with the “time” command).

## Status/Operating time

This displays the router’s operating time since last being switched on, in days, hours, minutes and seconds.

## Status/WLAN statistics

This describes the instantaneous status of the WLAN interface.

LAN Rx packets	<b>INFO</b>	Number of data packets received
LAN Tx packets	<b>INFO</b>	Number of data packets sent
LAN Rx error	<b>INFO</b>	Number of data packets incorrectly received
LAN Tx errors	<b>INFO</b>	Number of data packets incorrectly sent
LAN stack errors	<b>INFO</b>	Number of packets without a suitable receive module (bridge/router)
LAN queue packets	<b>INFO</b>	Number of buffers in use
LAN queue errors	<b>INFO</b>	Number of packets discarded due to buffer limitations
LAN Rx bytes	<b>INFO</b>	Number of bytes received from the LAN
LAN Tx bytes	<b>INFO</b>	Number of bytes sent to the LAN
LAN Rx broadcasts	<b>INFO</b>	Number of broadcast packets received from the LAN
LAN Rx multicasts	<b>INFO</b>	Number of multicast packets received from the LAN

LAN Rx unicasts	<b>INFO</b>	Number of directly addressed packets received from the LAN
LAN Tx broadcasts	<b>INFO</b>	Number of broadcasts received from the WAN
LAN Tx multicasts	<b>INFO</b>	Number of multicasts received from the WAN
LAN Tx unicasts	<b>INFO</b>	Number of unicasts received from the WAN
LAN Tx discarded	<b>INFO</b>	Number of packets discarded by the LAN
LAN repeats	<b>INFO</b>	Number of packets that were repeated, before being successfully received
LAN multiple repeats	<b>INFO</b>	Number of packets that were repeated several times, before being successfully received
LAN ready	<b>INFO</b>	Successful initialization of the wireless network adapter
Station table	<b>INFO TABLE</b>	Display of currently logged-on mobile stations.
WLAN parameters	<b>MENU</b>	Wireless network parameters
Interpoint statistics	<b>MENU</b>	Point-to-point status tables are here. Network coupling with two or more base stations.
IAPP table	<b>INFO TABLE</b>	Displays all base stations found by means of the IAP protocol. IAPP is used for point-to-point connections, as well as for roaming between base stations.

*Station table*

This table displays individual mobile station information:

Channel	B channel identification.
Index	displays the order of entries in the table.
Age	Age of the station: Time since last data packet was transferred
Phy signal	Average signal strength of the data packets received from this station.
Node ID	Station address. Depending on availability, either a MAC address, IP address or a symbolic name, if this station uses DHCP.
LAN Tx bytes and LAN Rx bytes	data volume transmitted from/to this station
Status	Can be either "none", "auth" or "assoc". When logging on, a station first authenticates itself, then "associates" itself, i.e. makes itself available for data communication. The base port status must first be 'Assoc' for data transfer to be allowed! 'Auth' indicates whether or not the station replies to a base port request for authentication.
Encaps	In WLAN, ethernet frames can be packed into a WLAN frame in various ways. In the 'IEEE' method, a new header is added to the entire Ethernet packet. Another method uses a more intelligent process that transforms headers into other headers, and that uses 'LLC-SNAP' coding to identify the protocol. The base port automatically recognizes both coding forms. Given the choice, SNAP coding should be used, because the overhead per frame is 6 bytes smaller.

## WLAN Parameter

This table displays the current wireless network parameters:

BSSID	Displays the coding currently being used for the wireless cell. In the infrastructure mode, the MAC address is always the base station, and in ad-hoc mode, it is an arbitrary number agreed on by the stations. It contains the following points:
	<i>Access point list</i> - all currently known remote stations, with address, signal strength and data rate of the last packet received.
	<i>Routing list</i> – computers recognized in adjacent LANs, with MAC addresses, transfer statistics and the number of base stations, over which they can be reached. This number corresponds to their position in the access point list. Numbering begins with 0.
	<i>Broadcast</i> – number of broadcasts over the wireless bridge, and the quantity of data transmitted through them. Because broadcasts are not directed to a specific station, and are therefore not in the routing list, there are two extra parameters.
PHY channel	The channel in current use. In the infrastructure mode, this is given by the base port, in ad-hoc mode, given by the station.
Regulatory domain	Licensed jurisdiction of the installed wireless network adapter.
PHY type	The modulation process DSSS ( <b>D</b> irect <b>S</b> equences <b>S</b> pread <b>S</b> pectrum) used by the WLAN card.
WEP support	Indicates whether or not the wireless network adapter in use supports WEP encoding. The WEP points in the WLAN setup only have an effect if this support is indicated.

## Status/WLAN statistics

This command displays various statistical parameters of the WAN port. Many transmitted data volume statistics yield useful information about the load on the WAN port, errors that have occurred, and the internal resources of the devices available in the current operating state.

The WAN statistics are tracked by interface, i.e. each interface has its own statistics on transmitted data and errors. The **Status/WAN statistics** menu has the following structure:

/WAN statistics	Running status displays	
Byte transport statistics	<b>INFO TABLE</b>	Statistics on bytes transferred
Packet transport statistics	<b>INFO TABLE</b>	Statistics on data packets transferred
Error statistics	<b>INFO TABLE</b>	Statistics on transmission errors that have occurred
WAN Tx discarded	<b>INFO</b>	Number of packets discarded due to error/lack of resources
WAN heap packets	<b>INFO</b>	Number of buffers in use
WAN queue packets	<b>INFO</b>	Number of available buffers
WAN queue errors	<b>INFO</b>	Number of packets discarded due to insufficient buffers
Throughput statistics	<b>INFO TABLE</b>	Statistics for bytes transferred on every channel
Delete values	<b>COMMAND</b>	Delete WAN statistics

*Byte transport statistics*

For each available interface, the **Status/WAN statistics/byte transport statistics** menu item contains statistics on the bytes transmitted via this interface. This table has the following form:

lfc	CRx bytes	Rx bytes	Tx bytes	CTx bytes
Ch01	0	0	0	0
Ch02	0	0	0	0

A description of the fields is given below:

lfc	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** command provides statistics on the packets transferred via this interface. This table has the following form:

lfc	Rx	Tx total	Tx normal	Tx secured	Tx urgent
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

A description of the fields is given below:

lfc	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 secured	Number of secured data packets sent
Tx urgent	Number of data packets sent with priority handling (urgent queue)

*Error statistics*

For each available interface, the **Status/WAN statistics/error stat.** command contains statistics on the transmission errors that have occurred for the interface. This table has the following form:

lfc	Rx-L1-F.	Rx-L2-F.	Rx-L3-F.	Stack F.	Tx errors
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0



A description of the fields is given below:

lfc	designates the associated channel.
Rx-L3-F.	Number of layer 3 errors in data received (i.e. the protocol header of layer 3 is incorrect)
Rx-L2-F.	Number of layer 2 errors in data received (i.e. similar to layer 3 errors, e.g. defective PPP header)
Rx-L1-F.	Number of layer 1 errors in data received (similar to layer 3 errors)
Tx errors	Number of transmission errors when sending
Stack F.	Number of stack errors in data received. Stack errors are caused when frames that cannot be associated with any internal processing are received (e.g. IP routers).

#### Throughput statistics

For both channels, the **Status/WAN statistics/throughput statistics** command provides statistics on the bytes transferred via this interface. This table has the following form:

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

A description of the fields is given below:

lfc	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 transmitting direction
Rx/s average	Average throughput on the channel, in the receiving direction
Tx/s average	Average throughput on the channel, in the transmitting direction

## Status/LAN statistics

Analogous to the previous commands, relevant LAN port statistics are displayed here. The **Status/LAN statistics** menu has the following structure:

/LAN statistics	Running status displays	
LAN Rx packets	INFO	Number of data packets received
LAN Tx packets	INFO	Number of data packets sent
LAN Rx error	INFO	Number of data packets incorrectly received
LAN Tx errors	INFO	Number of data packets incorrectly sent
LAN stack errors	INFO	Number of packets without a suitable receive module (bridge/router)
LAN NIC errors	INFO	Number of packets discarded by the NIC

/LAN statistics	Running status displays	
LAN heap packets	<b>INFO</b>	Number of available buffers
LAN queue packets	<b>INFO</b>	Number of buffers in use
LAN queue errors	<b>INFO</b>	Number of packets discarded due to buffer limitations
LAN collisions	<b>INFO</b>	Number of collisions during the send procedure
Connection - established	<b>INFO</b>	Displays the number of correct Ethernet connections (data transfer possible). Corresponds to the 'Link' LED on the device.
Negotiation completed	<b>INFO</b>	
Connection	<b>INFO</b>	
LAN Rx bytes	<b>INFO</b>	Number of bytes received from the LAN
LAN Tx bytes	<b>INFO</b>	Number of bytes sent to the LAN
LAN Rx broadcasts	<b>INFO</b>	Number of broadcast packets received from the LAN
LAN Rx multicasts	<b>INFO</b>	Number of multicast packets received from the LAN
LAN Rx unicasts	<b>INFO</b>	Number of directly addressed packets received from the LAN
WAN Rx broadcasts	<b>INFO</b>	Number of broadcasts received from the WAN
WAN Rx multicasts	<b>INFO</b>	Number of multicasts received from the WAN
WAN Rx unicasts	<b>INFO</b>	Number of unicasts received from the WAN
Delete values	<b>COMMAND</b>	Delete LAN statistics

## Status/PPP statistics

Within the PPP statistics, separate statistics are maintained for the status of individual PPP sub-protocols for each interface. However, statistics on transmitted frames for the individual sub-protocols are maintained only within common statistics. The **Status/PPP statistics** menu therefore has the following structure:

/PPP statistics	Running status displays	
PPP phases	<b>INFO TABLE</b>	Statistics relating to PPP protocol negotiation status for each interface
LCP statistics	<b>MENU</b>	PPP/LCP statistics display
PAP statistics	<b>MENU</b>	PPP/PAP statistics display
CHAP statistics	<b>MENU</b>	PPP/CHAP statistics display
CBCP statistics	<b>MENU</b>	PPP/CBCP statistics display
IPXCP statistics	<b>MENU</b>	PPP/IPXCP statistics display
IPCP statistics	<b>MENU</b>	PPP/IPCP statistics display
CCP statistics	<b>MENU</b>	PPP/CCP statistics display
ML statistics	<b>MENU</b>	PPP/ML statistics display
BACP statistics	<b>MENU</b>	PPP/BACP statistics display

/PPP statistics	Running status displays	
Rx options	<b>MENU</b>	Display of LCP, IPCP and IPXCP information received
Tx options	<b>MENU</b>	Display of LCP, IPCP and IPXCP information sent
Delete values	<b>COMMAND</b>	Deletes PPP statistics

PPP statistics give a detailed breakdown of a PPP negotiation, especially for connection problems involving external products. They contain critical diagnostic error information.

#### PPP phases

For each available interface, the **Status/PPP statistics/PPP phases** command provides a list of the current states of PPP protocol negotiation. This table has the following form:

lfc	Phase	LCP	IPXCP	IPCP	CCP
Ch01	DEAD	Initial	Initial	Initial	Initial
Ch02	DEAD	Initial	Initial	Initial	Initial

A description of the fields is given below:

lfc	designates the associated channel.
Phase	indicates the current phase of the PPP. Possible values are <b>AUTHENTICAT</b> , <b>NETWORK</b> and <b>TERMINATE</b> .
LCP	Status of the 'Link Control Protocol' sub-protocol. Possible values are: <b>Initial</b> , <b>Startng</b> , <b>Stoppng</b> , <b>Stopped</b> , <b>Closing</b> , <b>Closed</b> , <b>ReqSent</b> , <b>AckRcvd</b> , <b>AckSent</b> and <b>Opened</b> .
IPCP	Similar to 'LCP', the status of the 'IP Control Protocol' sub-protocol is displayed here.
CCP	Similar to 'LCP', the status of the 'Compression Control Protocol' sub-protocol is displayed here.

**Status/PPP Statistics/PPP phases** displays the current PPP phase. As specified above, these phases are; idle (Dead), ready (Establish), verifying access parameters (Authenticate) and network phase (Network). In the sub-statistics, the exchanged frames are separately encrypted by type and quantity.

#### Status/PPP statistics/LCP statistics

The **LCP** (Link Control Protocol) negotiates the basic characteristics of the PPP connections. The LCP frames exchanged during PPP negotiation are statistically analyzed and displayed by type and quantity. If the LCP does not change to the OPEN state for a connection, these statistical values provide information about errors that occurred during

the initial phase of PPP negotiation. The parameters in these statistics are described below:

Rx errors	Number of PPP packets incorrectly 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 nack.	Number of configure negative acknowledge packets received
Rx config reject	Number of configure reject packets received for LCP
Rx term request	Number of terminate request packets received for LCP
Rx term 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 nack.	Number of configure negative acknowledge packets sent
Tx config reject	Number of configure reject packets sent for LCP
Tx term request	Number of terminate request packets sent for LCP
Tx term 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	Delete LCP statistics

### Status/PPP statistics/PAP statistics

The **PAP** (Password Authentication Protocol) is one of two common procedures for verifying remote stations in PPP. When a connection is established, it checks the remote station password once, and enables the connection only if the password exchange is successful (see also Point-to-Point Protocol). The parameters in these statistics are described below:

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 are 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	Delete PAP statistics

### Status/PPP statistics/CHAP statistics

The **CHAP** (Challenge Authentication Protocol) is the second option for verifying remote stations under PPP. The password is checked as the connection is established, and again at adjustable intervals during the connection (see also 'Point-to-Point Protocol'). The parameters in these statistics are described below:

Rx discarded	Number of CHAP packets discarded
Rx challenges	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 retries	Number of times the CHAP challenge packets were resent
Tx challenges	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	Delete CHAP statistics

### Status/PPP statistics/IPCP statistics

When IP is in use, the **IPCP** (Internet Protocol Control Protocol) displays the status of the protocol, and the packets exchanged during negotiation.

Rx rejected	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 nack.	Number of configure negative acknowledge packets received
Rx config reject	Number of configure reject packets received for IPCP
Rx term request	Number of terminate request packets received for IPCP
Rx term 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 nack.	Number of configure negative acknowledge packets sent
Tx config reject	Number of configure reject packets sent for IPCP
Tx term request	Number of terminate request packets sent for IPCP
Tx term ack.	Number of terminate acknowledge packets sent for IPCP
Tx code reject	Number of code reject packets sent for IPCP
Delete values	Delete IPCP statistics

### Status/PPP statistics/CBCP statistics

When IP is in use, the **CBCP** (Callback Control Protocol) displays the status of the protocol, and the packets exchanged during negotiation.

Rx request	Number of CBCP request packets received
Rx response	Number of CBCP response packets received
Rx discarded	Number of CBCP packets discarded
Rx ack	Number of CBCP acknowledge packets received
Tx request	Number of CBCP request packets sent
Tx response	Number of CBCP response packets sent
Tx ack	Number of CBCP acknowledge packets sent
Delete values	Delete IPCP statistics

### Status/PPP statistics/CCP statistics

The CCP (Compression Control Protocol) statistics show the packets exchanged for data compression during 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 nack.	Number of CCP queries rejected because query parameters were not accepted.
Rx config reject	Number of CCP queries rejected for other reasons.
Rx termination request	Number of CCP queries after decompression.
Rx term ack	Number of confirmed CCP queries after decompression.
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 nack.	Number of CCP queries rejected by the remote station because parameters were not accepted.
Tx config reject	Number of CCP queries rejected by the remote station for other reasons.
Tx termination request	Number of CCP queries sent after decompression.
Tx term ack.	Number of CCP confirmations sent for decompression.
Tx code reject	Number of CCP queries rejected because the <i>ELSA LANCOM</i> does not want to use compression (via layer list setting).
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	Delete CCP statistics

### Status/PPP statistics/ML statistics

MLPPP statistics mostly provide information about how the remote station handles individual packets within a bundled PPP connection.

Bundle conn.	Number of connections that used MLPPP
Rx seq loss	Number of packets with an error in the sequential numbering order.
Rx seq repeat	Number of packets, whose sequence numbers arrived late.
Rx Mrru exceeded	Number of packets that (after reassembly) exceeded the MRRU (maximum received reassembled unit) limit specified in the PPP negotiation.
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 set 'start' flag (first part of a fragmented packet).
Rx frag mid	Number of packets with a set 'mid' flag (middle part of a fragmented packet).
Rx frag end	Number of packets with a set 'end' flag (last part of a fragmented packet).
Rx unfragmented	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 via LCP, IPCP, and IPXCP during negotiation.

*Rx options* This provides information on what the remote station requested (LCP), or what was assigned to the router (IPCP and IPXCP).

*Tx options* This provides information on what the router requested from the remote station (LCP), or what it was assigned (IPCP and IPXCP).

The two submenus have the same structure:

/Rx and Tx options	Display	
LCP	<b>INFO TABLE</b>	Information on packet sizes, control characters, security procedures and callback
IPCP	<b>INFO TABLE</b>	Information on IP network addresses

The LCP table has separate listings for each channel:

MRU	<b>M</b> aximum <b>R</b> ecieve <b>U</b> nit specifies the maximum packet size that the remote station can receive
ACCM	<b>A</b> synchronous <b>C</b> ontrol <b>C</b> haracter <b>M</b> ap specifies the characters in the asynchronous data flow that are interpreted as control characters
Authent.	Authentication procedure used (PAP/CHAP)
Callback	Callback negotiation type

Finally, IPCP contains the negotiated IP options, once again separated according to channel:

IP address	Once again, the Rx options contain the addresses assigned by the remote station, and the Tx options contain those that the <i>ELSA LANCOM</i> assigns to the remote station. (You can then easily find information like the IP address of the Internet provider dial-up node in the Tx options.)
DNS server	
NBNS server	

## Status/IPX statistics

The statistics from the IPX area are collected here, and are classified as type, socket, and router information. The IPX statistics contain the following parameters:

/IPX statistics	Statistics from the IPX and IPX router areas	
MAC statistics	<b>MENU</b>	Statistics from the Media Access Control of IPX packets
Watchdog statistics	<b>MENU</b>	Statistics on watchdog packets
Propagate statistics	<b>MENU</b>	Statistics on IPX propagated packets (IPX type 20)
RIP statistics	<b>MENU</b>	Statistics for RIP network
SAP statistics	<b>MENU</b>	Statistics for SAP network
IPX router statistics	<b>MENU</b>	Remote IPX router statistics
Delete values	<b>COMMAND</b>	Delete IP statistics

The substatistics then provide you with further parameters for the individual menus.



**Status/IPX statistics/MAC statistics**

These statistics contain 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	Delete MAC statistics

**Status/IPX statistics/Watchdog statistics**

These statistics contain 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	Delete watchdog statistics

**Status/IPX statistics/Propagate statistics**

These statistics contain the following values:

Propagate LAN Rx	Number of IPX propagated packets received from the LAN
Propagate LAN Filter	Number of IPX propagated packets received/filtered from the LAN
Propagate LAN Tx	Number of IPX propagated packets sent to the LAN
Propagate LAN socket errors	Number of IPX propagated packets filtered from the LAN by socket filters
Propagate LAN hop errors	Number of IPX propagated packets filtered from the LAN by hop count

Propagate LAN backroute errors	Number of IPX propagated packets from the LAN that are to be routed back
Propagate LAN contention	Number of packets to be routed from the LAN in the event of a bad connection
Propagate WAN Rx	Number of IPX propagated packets received from the WAN
Propagate WAN filters	Number of IPX propagated packets received/filtered from the WAN
Propagate WAN Tx	Number of IPX watchdog packets sent to the WAN
Propagate WAN socket errors	Number of IPX propagated packets filtered from the WAN by socket filters
Delete values	Delete IPX propagated packet statistics

### Status/IPX statistics/RIP statistics

These statistics contain the following values:

RIP LAN Rx	Number of RIP packets received from the LAN
RIP LAN errors	Number of RIP packets with corrupted 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 corrupted content received from the WAN
RIP WAN Tx	Number of RIP packets sent to the WAN
Delete values	Delete RIP statistics
RIP table	RIP table display

#### RIP table

There are 256 entries in the **RIP table** with RIP information. The table is structured as follows:

Network	Hops	Tics	Node ID	Time	Flags
Network address	Number of routers to pass on the way to the other network	Time required for this route in tics	MAC server address	Number of table updates before the entry is removed	local, remote, loop or down

### Status/IPX statistics/SAP statistics

These statistics contain the following values:

SAP LAN Rx	Number of SAP packets received from the LAN
SAP LAN errors	Number of SAP packets with corrupted 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 corrupted content received from the WAN

SAP WAN Tx	Number of SAP packets sent to the WAN
Delete values	Delete SAP statistics
SAP table	Number of SAP packets received from the LAN

*SAP table*

There are 512 entries in the **SAP table** with SAP information. The table is structured as follows:

Type	Server name	Network	Node ID	Socket	Hops	Time	Flags
Service SAP no.	Computer name of the server	Network address	Server MAC address	Socket for the service	Number of routers to target network	Number of table updates before the entry is removed	local, remote, loop or down

**Status/IPX statistics/IPX router statistics**

These statistics contain 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 network errors	Number of packets to be routed from the LAN 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 in the event of a bad 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 network errors	Number of packets to be routed from the WAN 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 Int Rx	Number of packets from internal modules to the IPX router

Networks	Network table in the IPX routing table with node IDs
Delete values	Delete IPX router statistics
Establish table	Table of the last 20 packets that required a connection

*Establish table* The **Establish table** is another subordinate component of the router statistics. It contains the last 20 entries, with information about the system time, the IPX target address, and the IPX source address of the data packets that led to the establishing of a connection.

An IPX establish table can have the following structure:

System time	Target address	Source address
1T; 16:45:01	00000081 ffffffff 0453	00000001 00a05702000a 0453
1T; 10:45:10	00000081 ffffffff 0452	00000001 00a05702000a 0452

The 'System time' is displayed as either the device operating time, or the real time of the ISDN (if provided by the ISDN terminal). The target address 'fffffff' indicates, for example, a broadcast packet. The target and source addresses consist of the network number, MAC address, and the socket number (all hexadecimal).

*Networks* The **Network statistics** are also a subordinate component of the IPX router statistics. This table displays more detailed information about a static route (remote station). The table is structured as follows:

Remote ID	Network	Binding	Propagate	Backoff	Time	Node ID
Logical remote	Network address	Binding	Route /Filter	Establish counter	Wait time until next connect attempt	Remote node ID

The entries have the following meanings:

Remote ID	Logical remote name, as shown in the routing table. An entry for the LAN link is also given. It is first in the table, and has the name "LAN".
Network	Address of the network where the remote station is located. For WAN remotes, this is the entry shown in the routing table. If the autodetect function is enabled in the IPX routing table (/SETUP/IPX-MODUL/LAN-EINSTELLUNG/NETZWERK), then this entry can show which network has been identified.
Binding	Ethernet binding, to which the remote is bound. For WAN remotes, this is the entry shown in the routing table. If the autodetect function is enabled in the IPX routing table (/SETUP/IPX-MODUL/LAN-EINSTELLUNG/NETZWERK), then this entry can show which binding has been identified.
Propagate	Filter flag for IPX type 20 (propagated) frames. For WAN remotes, this is the entry shown in the routing table. For the LAN, the route is always entered here.

Backoff	'Establish' counter for the exponential backoff algorithm. When the establish counter reaches 16, no new attempt is made. The route is then inactive (also possible with LAN).
Time	Wait time (in seconds) until the next exponential backoff algorithm connection attempt. When a successful connection is made, the wait time is set to zero. Then the route is active.
Node ID	Node ID of the relevant router in the WAN network For the LAN, the router node ID is always entered here.

## Status/TCP IP statistics

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

/TCP IP statistics	TCP/IP area statistics	
ARP statistics	<b>MENU</b>	Statistics from the ARP area
IP statistics	<b>MENU</b>	Statistics from the IP area
ICMP statistics	<b>MENU</b>	Statistics for ICMP packets
TCP statistics	<b>MENU</b>	Statistics for TCP packets from TCP sessions to the router
TFTP statistics	<b>MENU</b>	Statistics for TFTP operations
DHCP statistics	<b>MENU</b>	Statistics from the DHCP server
NetBIOS statistics	<b>MENU</b>	NetBIOS module statistics
DNS statistics	<b>MENU</b>	Statistics from the DNS server
Delete values	<b>COMMAND</b>	Delete TCP/IP statistics

The substatistics then provide you with further parameters for the individual menus.

### Status/TCP IP statistics/ARP statistics

These statistics contain the following values:

ARP LAN Rx	Number of ARP queries and responses received from the LAN
ARP LAN Tx	Number of ARP queries and responses sent to the LAN
ARP LAN errors	Number of ARP queries incorrectly received from the LAN
ARP WAN Rx	Number of ARP queries and responses received from the WAN
ARP WAN Tx	Number of ARP queries and responses sent to the WAN
ARP WAN errors	Number of ARP queries incorrectly received from the WAN
Delete values	Delete ARP statistics
ARP table	ARP table display

*ARP table*

There are 128 entries with ARP information in the **ARP table**. The table is structured as follows:

IP address	Node ID	Last access	Connection
IP address that has been previously found by an ARP query	Associated MAC address	Time since the last access in tics	Local or remote

**Status/TCP IP statistics/IP statistics**

These statistics contain 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 fragmentation errors	Number of fragmentations incorrectly received from the LAN
IP LAN fragmentations	Number of fragmentations received from the LAN
IP LAN fragmentation - forced	Number of forced fragmentations 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 fragmentation errors	Number of fragmentations incorrectly received from the WAN
IP WAN fragmentations	Number of fragmentations received from the WAN
IP WAN fragmentation - forced	Number of forced fragmentations from the WAN
IP WAN service errors	Number of IP packets received from the WAN for an incorrect service
IP WAN Rx discarded	Number of packets from the WAN discarded by time-out management
Delete values	Delete IP statistics

**Status/TCP IP statistics/ICMP statistics**

These statistics contain 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	Delete ICMP statistics

### Status/TCP IP statistics/TCP statistics

These statistics contain 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 Rpt	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	Number of current TCP LAN connections
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	Number of current TCP WAN connections
Delete values	Delete TCP statistics

### Status/TCP IP statistics/TFTP statistics

These statistics contain the following values:

TFTPX 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
TFTPX LAN Rx data	Number of TFTP data packets received from the LAN
TFTPX 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 unk.	Number of unknown TFTP packets received from the LAN
TFTP LAN Tx	Number of TFTP packets sent to the LAN
TFTPX LAN Tx data	Number of TFTP data packets sent to the LAN
TFTPX 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 error	Number of TFTP error packets received from the WAN
TFTP WAN Rx unk.	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 error	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	Delete TFTP statistics

### Status/TCP IP statistics/DHCP statistics

These statistics contain 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 discarded	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 Nack	Number of DHCP packets not acknowledged
DHCP server errors	Number of DHCP packets received that were not intended for this server
DHCP-assigned	Number of currently assigned addresses
DHCP MAC conflicts	Number of assignments rejected because IP addresses were in use



DHCP table	Table with assignments of IP addresses to MAC addresses
Server flags	On/off switching of server flags
Delete values	Delete DHCP statistics

*DHCP table*

There are entries with DHCP information in the **DHCP table**. It contains 16 entries (or multiples of 16). The table dynamically adjusts to the requirements, and grows or shrinks accordingly. The table is structured as follows:

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

**Status/TCP IP statistics/NetBIOS**

Additional information about the NetBIOS module can be obtained from the /Status/TCP IP statistics/NetBIOS menu. This menu is structured as follows:

LAN-Rx, WAN Rx	<b>INFO</b>	Number of NetBIOS packets received by the LAN or WAN
LAN Tx, WAN Tx	<b>INFO</b>	Number of NetBIOS packets sent to the LAN or WAN
Registrations	<b>INFO</b>	Number of name registrations performed
Conflicts	<b>INFO</b>	Number of detected name conflicts. Since the NetBIOS module is only a bulletin board (where each computer places its name), the module does not check the data for consistency. Therefore, the counter is only increased if a host itself notices a conflict, and broadcasts this fact over the network.
Releases	<b>INFO</b>	Number of successful name shares
Refreshes	<b>INFO</b>	Number of successful name refreshes
Timeouts	<b>INFO</b>	Number of expired names
B nodes	<b>INFO</b>	Number of currently active B nodes (broadcast) in the network
P nodes	<b>INFO</b>	Number of currently active P nodes (peer-to-peer) in the network
M nodes	<b>INFO</b>	Number of currently active M nodes (mixed-mode) in the network
W nodes	<b>INFO</b>	Number of currently active W nodes (hybrid) in the network

*B nodes*

Broadcast nodes A B node carries out name negotiation exclusively via broadcasts. Such a computer cannot be seen in a router connection, since broadcasts cannot be routed.

*P nodes*

Point-to-point nodes For name negotiation, a P node requires a NetBIOS name server (NBNS). And for datagram transmission via a router, it also requires a NetBIOS datagram distribution server (NBDD).

*M nodes*

Mixed nodes This node type is a mix of the B and P nodes. In a local network, it behaves as a B node. If the desired communication partner is not to be found in the local network, it then tries to find the partner with an NBNS query (P node behavior).

W nodes

This type of node is not allowed by the RFC. Despite this, Microsoft introduced it as a hybrid node.

### Status/TCP IP statistics/DNS statistics

The DNS statistics provide supplementary information about the DNS module. This menu is structured as follows:

LAN Rx	<b>INFO</b>	Number of DNS packets received by the LAN
LAN Tx	<b>INFO</b>	Number of DNS packets sent to the LAN
WAN Rx	<b>INFO</b>	Number of DNS packets received from the WAN
WAN Tx	<b>INFO</b>	Number of DNS packets sent to the WAN
Forwarded	<b>INFO</b>	Number of queries that could not be answered, and which are therefore being forwarded
Errors	<b>INFO</b>	Number of invalid requests
DNS accesses	<b>INFO</b>	Indicates the number of names that were looked up from the DNS table
DHCP accesses	<b>INFO</b>	Indicates the number of names that were looked up from the DHCP table
NetBIOS accesses	<b>INFO</b>	Indicates the number of names that were looked up from the NetBIOS tables
Filter	<b>INFO TABLE</b>	Number of DNS packets filtered by the filter table
Hit list	<b>INFO TABLE</b>	This table contains the 16 most popular queries. If desired, they can be blocked via the filter list.

The hit list is structured as follows:

Name	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 meanings:

Name	Name of the computer queried
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 asked about this name

This list is sorted by the number of requests. When the table is full, the names that have not been requested for the longest period are deleted, to make room for new entries.

## Status/IP router statistics

Statistics from the IP router module are maintained here.

/IP router statistics	Statistics from the IP router area	
IPr LAN Rx	<b>INFO</b>	Number of data packets to be routed from the LAN
lpr LAN Tx	<b>INFO</b>	Number of data packets routed to the LAN
lpr LAN local routings	<b>INFO</b>	Number of packets received from the LAN and routed to the LAN
lpr LAN network errors	<b>INFO</b>	Number of LAN packets that were not routed
lpr LAN routing errors	<b>INFO</b>	Number of LAN packets that must be sent to another router
IPr LAN TTL errors	<b>INFO</b>	Number of LAN packets with an expired time-to-live value
lpr LAN filters	<b>INFO</b>	Number of LAN packets filtered by the filter table
lpr LAN discarded	<b>INFO</b>	Number of LAN packets discarded
IPr WAN Rx	<b>INFO</b>	Number of data packets to be routed from the WAN
lpr WAN Tx	<b>INFO</b>	Number of data packets routed to the WAN
lpr WAN network errors	<b>INFO</b>	Number of WAN packets that were not routed
lpr WAN TTL errors	<b>INFO</b>	Number of WAN packets with an expired time-to-live value
lpr WAN filters	<b>INFO</b>	Number of WAN packets filtered by the filter table
lpr WAN discarded	<b>INFO</b>	Number of WAN packets discarded
lpr WAN type errors	<b>INFO</b>	Number of packets from the WAN without an IP router ID
lpr ARP errors	<b>INFO</b>	Number of unsuccessful attempts to access the ARP cache
Establish table	<b>INFO TABLE</b>	Table of the last 20 packets that required a connection
Protocol table	<b>INFO TABLE</b>	Table of routed packets sorted by protocol
RIP statistics	<b>MENU</b>	Statistics from the IP/RIP area
Delete values	<b>COMMAND</b>	Delete IP router statistics

*Establish table* The **establish table** contains the last 20 entries, which provide information on the system time, target and source addresses, IP protocol, destination port and source port of the data packets that should have led to the establishing of a connection.

An IP router establish table can be structured as follows:

System time	Destination address	Source address	Protocol	D port	S port
1T; 16:45:01	192.120.131.40	192.120.130.10	tcp	23	4711
1T; 10:45:10	192.120.131.50	192.120.130.10	udp	53	8123

The 'System 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 to tcp, udp, while the destination and source ports provide more detail about services (e.g. Telnet via TCP and D port 23, name server via UDP and D port 53).

#### Protocol Table

The protocol table also supplies valuable information on the volume of packets transferred to the LAN or WAN. These values are encrypted by the various IP protocols, such as ICMP, TCP, UDP.

A protocol table can be structured as follows:

Protocol	LAN Tx	WAN Tx
tcp	14	30
udp	15	50
icmp	60	40

#### Status/IP router statistics/RIP statistics

This displays the IP RIP packets received from the device. These subordinate statistics include 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 discarded	Number of IP RIP packets discarded
RIP errors	Number of corrupted IP RIP packets
RIP entry errors	Number of corrupted entries in IP RIP packets
RIP Tx	Number of IP RIP packets sent
RIP table	Routing table of routes discovered through RIP broadcast
Delete values	Delete IP RIP statistics

#### RIP table

The corresponding RIP table contains all routes discovered from the network. The router maintains this table - it cannot be manually modified.

An IP RIP table can have the following structure:

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 displays 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	INFO	Current number of active configuration connections from the LAN
LAN total connections	INFO	Total number of configuration connections to date from the LAN
WAN active connections	INFO	Current number of active configuration connections from the WAN
WAN total connections	INFO	Total number of configuration connections to date from the WAN
Outband active connections	INFO	Current number of active outband configuration connections
Outband total connections	INFO	Total number of outband configuration connections to date
Outband bit rate	INFO	Bit rate of the last outband configuration session
Logon errors	INFO	Total number of defective logon attempts
Logon locks	INFO	Number of logon locks
Rejections while logging on	INFO	Number of logon attempts, while the logon lock was active
Delete values	COMMAND	Delete 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	INFO	Number of available buffers
LAN queue packets	INFO	Number of buffers in use
WAN heap packets	INFO	Number of available buffers
WAN queue packets	INFO	Number of buffers in use
ARP query queue packets	INFO	Number of ARP packets in the query queue
ARP queue packets	INFO	Number of ARP packets in the normal queue
IP queue packets	INFO	Number of IP packets in the normal queue
IP urgent queue packets	INFO	Number of IP packets in the secured queue
ICMP queue packets	INFO	Number of ICMP packets
TCP queue packets	INFO	Number of TCP packets
TFTP queue packets	INFO	Number of TFTP packets

/Queue statistics	Statistics on the queue	
SNMP queue packets	<b>INFO</b>	Number of SNMP packets
Prot heap packets	<b>INFO</b>	Number of prot heap packets
IPR queue packets	<b>INFO</b>	Number of packets remaining to be processed by the IP router.
DHCP server queue packets	<b>INFO</b>	Number of packets in the receive queue of the DHCP server.
IPR RIP queue packets	<b>INFO</b>	Number of packets in the receive queue of the IP RIP module (for RIP queries, RIP propagations ...).
DNS Tx queue packets	<b>INFO</b>	Number of packets to be forwarded to DNS or NBNS servers.
DNS Rx queue packets	<b>INFO</b>	Number of packets that come from DNS or NBNS servers and are to be forwarded to the host.
IP Masq. Tx queue packets	<b>INFO</b>	Number of masked packets to be sent (to the Internet).
IP Masq. Rx queue	<b>INFO</b>	Number of packets received from the Internet that must be demasked.
WAN management heap packets	<b>INFO</b>	Number of packets available in buffers

## 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** command provides statistics on the connections established via this interface. This table has the following form:

lfc	Connection	Active	Passive	Errors	Connection time	Charge
Ch01	0	0	0	0	No connection	0
Ch02	0	0	0	0	No connection	0

A description of the fields is given below:

lfc	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.
Connection time	Indicates the period of time the current connection has existed. If no connection exists, "No connection" is output.
Charge	Indicates the amount charged 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 (see also **Setup/Charges module**).

## Status/Info. connection

For every available interface, the **Status/Info. connection** command provides additional information on the current connection status (logical remote station, etc.). This table has the following form:

lfc	Status	Mode	Dialup remote	Device name	B1 HZ	B2 HZ
Ch01	Ready				0	0
Ch02	Ready				0	0

A description of the fields is given below:

lfc	designates the associated channel.
Status	Indicates the status of the particular connection. Possible values are: <b>Init</b> , <b>Setup WAN</b> , <b>Ready</b> , <b>Dial</b> , <b>Incoming call</b> , <b>Protocol</b> , <b>Connection</b> , <b>Callback</b> , <b>Bundle</b> and <b>Reserved</b> . The <b>Bundle</b> status is indicated in the display (only for <i>ELSA LANCOM Wireless</i> ) by the addition of a "/2" in columns 15 and 16 of the associated display line. <b>Bundle</b> is displayed for the second interface, either when a bundle connection has been established via the first interface, or when a leased-line connection with two B channels has been set. <b>Reserved</b> is displayed for the second interface, when a connection exists to the first B channel, and the Y connection has been closed.
Mode	Reflects the type of establishment. The following are possible: <b>Act.</b> (active call establishment = dialing) <b>Passive</b> (passive call establishment = incoming call) <b>CB</b> (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 HZ	Indicates the timeout for the connection.
B2 HZ	Indicates the timeout for bundled channels for this connection.

## Status/Layer connection

For every available interface, the **Status/Layer connection** command provides information on the B channel protocol used on that 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. This menu has the following structure:

lfc	WAN layer	Encaps.	Lay 3	Lay 2	L2 Opt.	Lay 1
Ch01 Ch02	DEFAULT PPPHDL	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	lfc	CLIP caller	Dial caller	Capab.	B chan.
0T; 00:20:57	S <sub>0</sub>	5678	1234	HDLC64K	2
0T; 00:20:46	S <sub>0</sub>	4321	1234	HDLC64K	1
0T; 00:19:47	S <sub>0</sub>	4321	1234	HDLC64K	1
0T; 00:11:33	S <sub>0</sub>	5678	1234	HDLC64K	1
0T; 00:01:13	S <sub>0</sub>	4321	1234	HDLC64K	2
0T; 00:01:02	S <sub>0</sub>	4321	1234	HDLC64K	1
0T; 00:00:06	S <sub>0</sub>	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).
lfc	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 is entered here. Possible values are HDLC64K, HDLC56K and unknown. An analog call is displayed here as unknown. <i>LANCOM Office Router</i> can also display the values A-3 kHz (analog 3 kHz), language (for normal speech transmission) and fax G2/3 (for group 2 or 3 analog fax transmission).
B chan.	The B channel used is entered here. A value of 0 means that all channels are already in use, i.e. call waiting is on.



*A tip for those using a router in a PBX: after a call to any ISDN device under the ISDN bus number, the MSN/EAZ displayed under 'Dial caller' is exactly what 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, with information on the remote station.

The table has the following layout:

Conn. start	Remote ID	Mode	Ifc	Conn. time	Charge
OT; 00:20:57	BERLIN	Act.	Ch01	50	5
OT; 00:20:46	CHEMNITZ	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 Passive - 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 adds to the table, from top to bottom. If an existing connection is the lowest entry in the table, then an already released connection will be deleted from the table instead.

## Status/S<sub>0</sub> bus

This command allows you to display the current status of the S<sub>0</sub> interface. The statistics are structured as follows:

/S <sub>0</sub> bus	Running status displays	
D info	<b>INFO TABLE</b>	Overview of the D channel status
D2 statistics	<b>INFO TABLE</b>	Encoding of the D channel layer 2 information 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	Enabling of layer 2 of the D channel ('Yes' or 'No')
TEI	TEI assigned ('Yes' or 'No')
S <sub>0</sub> enabling	Displays enabling status ('Yes' or 'No')

### D2 statistics

This table shows layer 2 information for the individual B channels:

Channel	B channel identification.
TEI	<b>T</b> erminal <b>E</b> quipment <b>I</b> dentifier assigned by the switching center.
L2 enabling	Enabling of layer 2 of the D channel ('Yes' or 'No').
Connections	Number of connections made over the displayed TEI.

## Status/Channel statistics

This table provides information on the current status of the two B channels. For *ELSA LANCOM Wireless*, a/b port information is also shown. The information from this table is primarily used for output via *ELSA LANmonitor*. Therefore, some values are shown simply as bits, with no further explanation.

The table has the following form:

Channel	State	App	Mode	Cause	Dialup remote	Sub-address	Charge	Conn. time	Extra	ISDN display
S <sub>0</sub> ERR	00000000	Router	active	0000	0241123456	00000000	3	0		
S <sub>0</sub> B1	00000000	a/b	active	0000	0241123457	00000000	2	20		
S <sub>0</sub> B2	00000000	LANCAP	passive	0000	0241123458	00000000	4	180		

Channel	State	App	Mode	Cause	Dialup remote	Sub-address	Charge	Conn. time	Extra
DSL ERR	00000000	none	active	0000	0241123456	00000000	3	0	
DSL line	00000000	Router	wired	0000	0241123456	00000000	2	20	
S <sub>0</sub> 1 ERR	00000000	none	unk.	0000	0241123456	00000000			
S <sub>0</sub> 1 B1	00000000	none	unk.	0000	0241123456	00000000			
S <sub>0</sub> 1 B2	00000000	none	unk.	0000	0241123456	00000000			

A description of the fields is given below:

Channel	Channel for the entry is valid. Only the latest status of a channel is displayed. A dedicated "channel" is maintained for channel error messages.
State	The status of a channel is shown here (e.g. 'ready').
App	Application that occupies the channel: Router <i>LANCAPI</i>
Mode	Type of last connection establishment: Active Passive
Cause	Last error
Dialup remote	Remote station call number: with active establishment, the number dialed; and with incoming calls, the caller number.
Sub-address	Application add-on that, among other things, indicates the logical channel for the router. Or for the <i>LANCAPI</i> , the IP address of the client using the CAPI.
Charge	Number of charge units incurred for this connection.
Conn. time	Duration of the last connection on this channel
Extra	Additional connection information (e.g. the name of the remote station for router connections).
ISDN display	Information from the switching center (e.g. error messages), or, if connected to the PBX, possibly also the caller's name, etc.

## Status/Time statistics

This menu provides information on the current time in the device, and on the path by which the *ELSA LANCOM Wireless* obtained the time.

The menu has the following form:

/Time statistics		Time module statistics
Current time	<b>INFO</b>	Current device time
Source	<b>INFO</b>	Time output source. Possible values are: 'ISDN' for time taken from the ISDN, 'Manual' for the manual time setting with the 'time' command, 'RAM' for time imported from the device RAM after booting.
Setup	<b>INFO</b>	Number of time imports from one of the above sources
ISDN	<b>MENU</b>	Additional information on time importing from the ISDN

### Status/Time statistics/ISDN

These statistics contain the following values:

Connection	Number of attempts at reading 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	

### Status/LCR statistics

This menu provides information on the current time in the device, and on the path by which the *ELSA LANCOM Wireless* obtained the time.

The menu has the following form:

/LCR statistics		Least-cost router statistics
Total calls	<b>INFO</b>	Total number of LCR calls
Successes	<b>INFO</b>	Number of calls, for which the router found a suitable rule in its tables, and successfully rerouted the connection.
Not-found errors	<b>INFO</b>	Number of calls, for which the router did not find a suitable rule in its tables, and thus could not reroute the connection.
No-time errors	<b>INFO</b>	Number of calls, for which the LCR could not become active, due to a lack of time
Provider statistics	<b>INFO TABLE</b>	A table with all providers used (or their area codes), and the number of successful and unsuccessful calls
Delete values	<b>COMMAND</b>	Delete LCR statistics

## Status/PCMCIA status

General information on the inserted card can be found here:

LAN card present	<b>INFO</b>	Indicates whether or not card is inserted (this does not necessarily mean that the card is working, just that something is in the PCMCIA slot!)
Card ID	<b>INFO</b>	The card name read from the PCMCIA Config Space, i.e. the device name, for which Windows requests a driver when the card is first inserted.
Firmware version	<b>INFO</b>	Information about the firmware of the WLAN card, provided that the card initialized correctly.

## Status/Charge statistics

This menu displays the current values from the charges module:

Days remain.	<b>INFO</b>	Number of days remaining in monitoring period.
Remain. budget	<b>INFO</b>	Remainder of budget for current monitoring period.
Router units	<b>INFO</b>	Number of units used by router modules in the current monitoring period.
Total units	<b>INFO</b>	Total number of units used in the current monitoring period.
Budget table	<b>INFO TABLE</b>	Detailed list of charge units for the ISDN from the individual modules (Router/LANCAPI/Time module).
Remaining ISDN minutes	<b>INFO</b>	Remainder of budget for current monitoring period.
Router ISDN minutes	<b>INFO</b>	Total online time on the ISDN interface since device was last switched on.
Remaining DSL minutes	<b>INFO</b>	Remainder of budget for current monitoring period.
Router DSL minutes	<b>INFO</b>	Total online time on the ISDN interface since device was last switched on.
Time table	<b>INFO TABLE</b>	Detailed list of online time for the individual modules (Router (ISDN)/Router (DSL)/LANCAP (ISDN)/Time module (ISDN)) on the respective interfaces.
Delete values	<b>COMMAND</b>	Delete charge statistics

## Delete status/values

With the exception of the tables, this command allows you to delete all the values in the sub-statistics. 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 for device functioning.

/Setup	System configuration	
Name	<b>Value</b>	Enter the device name
WAN module	<b>MENU</b>	WAN settings
Accounting module	<b>MENU</b>	Charge management settings
Charges module	<b>MENU</b>	Charge management settings
LAN module	<b>MENU</b>	LAN settings
WLAN module	<b>MENU</b>	WLAN settings
IPX module	<b>MENU</b>	IPX module settings
TCP IP module	<b>MENU</b>	TCP/IP module settings
IP router module	<b>MENU</b>	IP router module settings
SNMP module	<b>MENU</b>	Settings for configuration via SNMP
DHCP module	<b>MENU</b>	DHCP server settings
NetBIOS module	<b>MENU</b>	NetBIOS proxy settings
Config module	<b>MENU</b>	Configuration module settings
DNS module	<b>MENU</b>	DNS server settings
LANCAPi module	<b>MENU</b>	ELSA LANCAPI settings
LCR module	<b>MENU</b>	Least-cost router settings
Time module	<b>MENU</b>	Time module settings

### Name

Here you can enter the device name (maximum 16 characters). The character set 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. It 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 verification by PAP or CHAP.

Because the router permits only uppercase letters in the device name list, the name is transferred in uppercase letters (in the case of ELSA protocol verification). Special

characters should not be used in device names, unless the remote station can process them.

In addition, the device names you assign must be unique. For example, you might match the device names to the location (e.g. Buffalo, Berlin, Provider, etc.).

## Setup/Accounting module

In the accounting module, you can select whether or not the user data will be flagged and stored in flash-ROM. The menu has the following form: (incl. default values):

/Accounting module		Charge management settings
State	VALUE	Indicates whether or not the accounting data should be flagged. The possible values are 'on' or 'off'.
Save in flash-ROM	VALUE	Indicates whether or not the summation tables should be saved in flash-ROM. Possible values are 'yes' or 'no'.
Sort by	VALUE	Indicates how the summation table will be sorted. The possible values are time (sorted by online time) or data (sorted by transfer volume).
Current user	INFO TABLE	The data for the current connections are maintained in this table. This table is quasi-dynamic. It begins with 16 entries, and when these are filled, another 16 are added.
Accounting list	INFO TABLE	The summation table is stored here. This table contains 512 user entries, for either users who had the longest online time, or those who had the largest transfer volume.
Delete accounting list	COMMAND	Deletes the values in the accounting list

The accounting table has the following structure:

User name	Remote ID	Connection type	Rx kbytes	Tx kbytes	Total time	Connections
User 1	Internet	DSL connection	234	45	43	4
User 2	0	unknown	34	453	23	34

The summation table and the current connection table have the same table fields:

<i>User name</i>	The user's name. If this cannot be looked up, his layer 3 address (IP, IPX, or MAC address).
<i>Remote ID</i>	Name of the remote station, to which the user sent data, or from which the user received data.
<i>Connection type</i>	Type of connection established with the remote station. Possible values are: unknown, dial-up, leased line, and DSL connection.
<i>Rx, Tx bytes</i>	Data volume on the interface (64-bit counter).
<i>Total time</i>	Total online time for the user.

Connections

Number of connections established, counted for the user.

## Setup/Charges module

With this command, necessary charge protection settings may be made.

The individual commands have the following meaning:



Days/Period	Number of days in a monitoring period.
Budget units	Charge unit budget that may be used within a monitoring period. If the value is 0, the monitoring is disabled.
Remain. units	Remainder of budget for current monitoring period.
ISDN minute budget	Online time on the ISDN interface, that may be used within a monitoring period. If the value is 0, the monitoring is disabled.
Remaining ISDN minutes	Remainder of budget for current monitoring period.
Router ISDN minutes	Total online time on the ISDN interface since the device was last switched on.
DSL minute budget	Online time on the DSL interface, that may be used within a monitoring period. If the value is 0, the monitoring is disabled.
Remaining DSL minutes	Remainder of budget for current monitoring period.
Reserve DSL budget	Additional budget that may be used on the DSL interface within the monitoring period, if the normal DSL budget has been used up. This additional budget must be manually selected.
Router DSL minutes	Total online time on the ISDN interface since the device was last switched on.
Budget table	Detailed list of charge units for the ISDN from the individual modules (Router/ <i>LANCAP</i> /Time module).
Time table	Detailed list of online time for the individual modules (Router (ISDN)/Router (DSL)/ <i>LANCAP</i> (ISDN)/Time module (ISDN)) on the respective interfaces.
Enable reserve	This command makes the additional budget become available.

When a budget is depleted, the device automatically breaks the connection with the error message "Charge lockout". Another connection may only be established after the monitoring period is over, or by switching the device off and on. In addition, a new budget can be entered. This also resets the charge lockout.



## Setup/WAN module

This menu groups together all the settings necessary for starting up the WAN interface, and for controlling connections to logical remote stations.

/WAN module	WAN settings	
Interface list	<b>TABLE</b>	S <sub>0</sub> interface settings
Router interface list	<b>TABLE</b>	Router module interface settings
ISDN name list	<b>TABLE</b>	Remote station settings
Round-robin list	<b>TABLE</b>	Settings for different remote station numbers
Layer list	<b>TABLE</b>	Settings for the layer combinations used
DSL name list	<b>TABLE</b>	Remote station settings
PPP list	<b>TABLE</b>	Parameter settings for PPP connections
Number list	<b>TABLE</b>	Settings for call numbers with access authorization
Script list	<b>TABLE</b>	Dialup script settings
Protect	<b>VALUE</b>	Protection for answering incoming calls
CB attempts	<b>VALUE</b>	Number of callback attempts when the remote station is busy
Manual dialing	<b>MENU</b>	Settings for manual connection control

### Interface list

This table contains the interface settings, which apply to all operating modes (modules) of the devices.

lfc	Protocol	FV B chan.	Dial prefix
S0	Auto	1	0

lfc	Protocol	Dial prefix	Max. pass. connections	Max. act. connections
S0	Auto	0	2	2

Additional special interface settings are also available for individual modules (e.g. the call numbers to which a module should respond. See also

Setup/WAN module/Router interface list

setup/lancapi module

A description of the fields is given below:

Ifc	Designates the associated interface.
Protocol	D channel protocol setting. Possible values are: <b>Auto</b> : automatic detection of the D channel protocol <b>DSS1</b> : Euro ISDN <b>1TR6</b> : national ISDN <b>GRP0</b> : Leased-line connection group 0 <b>GRP2</b> : Leased-line connection group 2 <b>P2P DSS1</b> : Point-to-point connection
FV B chan.	B channel settings for a leased-line connection. Possible values are: <b>none</b> : Leased-line connection not assigned to a specific channel. <b>1</b> or <b>2</b> : Leased-line connection operates over the assigned B channel. Please refer to the information on setting these parameters in the leased-line connection description. The leased-line connection function is not a standard feature of <i>ELSA LANCOM Wireless</i> .
Dial prefix	Global dialing prefix for all device modules. The digits entered (maximum 8) are automatically prefixed to the selected call number for every call. Use this prefix when, for example, the router is connected to a PBX.
Max. pass. connections	Maximum number of possible concurrent passive connections
Max. act. connections	Maximum number of possible concurrent active connections

*Router interface list* This table contains the interface settings that apply to the router modules.

Ifc	MSN/EAZ	YV.	CLIP
S0	123456	Off	On

A description of the fields is given below:

Ifc	Designates the associated interface.
-----	--------------------------------------

MSN EAZ	<p>If your device is connected to an ISDN port with 1TR6, enter the EAZ to which the interface is to respond.</p> <p>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.</p> <p>For outgoing calls, the first MSN in this list will be reported to the remote station. If no MSN is entered, the switching center sends the main terminal MSN.</p>
YV.	<p>This entry can be used to control the interface's ability to establish Y connections. Possible settings are:</p> <p><b>On:</b> 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 needs to be established.</p> <p>Refer also to the settings for the availability of the <i>LANCAP</i>.</p> <p><b>Off:</b> Y connection not supported; only one connection can be established. The second connection is blocked. If a connection to an additional remote station is to be established, this establishment is rejected. A channel bundling connection is not affected.</p>
CLIP	<p>Calling Line Identification Protocol: Suppresses the outgoing MSNs.</p> <p>Possible values:</p> <p><b>Yes:</b> Enable CLIR, do not send MSN.</p> <p><b>No:</b> Disable CLIR, send MSN to remote station.</p> <p>Please note: The "selective suppression of call number transmission" may be a service feature that has to be obtained from the phone company.</p>

#### ISDN Name list

The device names entered in the name list are needed by the router, in order to determine the correct remote station and corresponding layer name. The name list is also used for the callback function.

The ISDN name list can contain 64 different device names. It may have the following appearance:

Device name	Dialup remote	B1 HZ	B2 HZ	WAN layer	Callback
AACHEN	875463	180	0	PPPHDL	On
BERLIN	040785647	20	20	DEFAULT	Off

A description of the fields is given below:

Device name	In the <b>Device name</b> column, you can enter an individual remote station name, which you must then assign to the relevant remote station via the <b>Name</b> command in the <b>Setup</b> menu.
Dialup remote	In this column, you can store the number to be called, and (if applicable) supplement it with special dialing characters (see Default: None).
B1 HZ	<p>In this column, you can define appropriate connection timeouts (in seconds) for the first B channel.</p> <p>If no data is being transmitted when this time expires, the connection on this channel is closed (default: 20).</p> <p>If charge information is transmitted over the ISDN network during the connection, the <i>ELSA LANCOM</i> will make full use of every charge unit, and will only terminate the connection just before the beginning of the next unit. This function is also referred to as dynamic short-hold.</p>

B2 HZ	In this column, you can define appropriate connection timeouts for the second B channel (same as B1 HZ, default: 20). The B2 timeout controls the bundling behavior during a channel bundling. Values of 0 or 9999 identify static bundling, values in between identify dynamic bundling.
WAN layer	This column stores a name that must also be entered in the layer list. This establishes the transfer protocol setting required for this connection.
Callback	In this column, you can define whether or not 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 within 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 by means of the number list. A callback can also 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 outside line access, the use of a semipermanent leased-line connection or they determine the interface to be used for the connection:

#	Outside line access (only with some PBXs).
F	The remote station can be reached via the leased-line connection. Syntax: F[channel:][call number] The channel and call 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 call number indicates whether or not a dynamic channel bundling, or a backup line is to occur over the dial-up connection.

When **S** or **S2** is appended to the call number, the semipermanent connection (SPV) is enabled for the D channel protocol 1TR6.



*Obtain a fixed price SPV through your telephone company.*



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 would then charge you the fixed price, and the dial-up line charges incurred during the line usage time.

*Round-robin list* The round-robin list enables a remote station to be reached with several call numbers. It has the following layout:

Device name	Round-robin	Head
AACHEN	4321-5555-6666	Last

A description of the fields is given below:

Device name	In the device name column, you can enter a remote device name from the name list. If one line in the round-robin list is insufficient for all desired call numbers, the line can be extended as shown below: The # character and a unique index are added to the device name (e.g. AACHEN#1), and it is entered on the next line.
Round-robin	The DDI numbers of all possible remote stations are entered here under their corresponding device names. The individual DDI numbers must be separated by hyphens.
Head	In the <b>Head</b> column, the following entries are possible: <b>Last:</b> The next connection to be established will begin with the DDI that was successfully used for establishing the last connection (default). <b>First:</b> 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 <b>first</b> 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 with devices from other manufacturers that use different B-channel protocols.

The following standard settings are valid for *LANCOM Office Router*:

WAN layer	Encaps.	Lay 3	Lay 2	L2 Opt.	Lay 1
DEFAULT	TRANS	PPP	TRANS	bnd+compr.	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	none	HDLC64K
MLPPP	TRANS	PPP	TRANS	bnd+compr.	HDLC64K
RAWHDL	TRANS	TRANS	TRANS	none	HDLC64K

A description of the fields is given below:

WAN layer	<p>In this column, you can enter a specific name designating the layer combination that you use. These names can then be used in the 'layer name' column of the name list, to set the protocol.</p> <p>If an entry with the name <b>DEFAULT</b> is defined in this column, the settings stored there will be 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 <b>DEFAULT</b> 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.</p>	
Encaps.	<p>Additional information regarding the data to be transmitted may be specified in the <b>Encaps</b> column. The following entries are possible:</p>	
	ETHER	The data is provided with an Ethernet header. This setting is required for communication with older <i>ELSA LANCOM</i> devices, or in bridge operation.
	ETHER	The data is provided with an Ethernet header. This setting is required for communication with older <i>ELSA LANCOM</i> devices.
	TRANS	No Ethernet header is sent with this setting. Only "pure" IP data packets are transferred, for example. This setting provides the greatest possible effective data throughput.
Lay 3	<p>In the lay 3 column, you can define additional headers for ISDN data transmission in. You can select from among the following settings:</p>	
	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).
	ELSA	The data is provided with an ELSA header. In addition, when a connection is established, protocol negotiation is performed, in which the remote stations exchange names. Incoming-call protection by name is possible only if this setting is selected. Without an ELSA setting, incoming-call protection can only be based on call number. This setting is required for communication with older <i>ELSA LANCOM</i> devices, or with the workstation drivers.
	PPP	Point-to-point protocol negotiation is performed.
	APPP	Asynchronous PPP negotiation is performed. APPP is used whenever synchronous PPP is not possible, because the connection may not permit synchronous transmission (e.g. for analog modem operation).
	SCPPP	Following completion of script processing, synchronous PPP negotiation is initiated.
	SCAPPP	Following completion of script processing, asynchronous PPP negotiation is initiated.
	SCTTRANS	Following completion of script processing, a connection exists to the remote station. No further protocol negotiation is performed.
Lay 2	<p>In this column, you can select the protocol for ISDN layer 2:</p>	
	TRANS	The data is packed directly into 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.	<p>The L2 opt. column enables the setting of a data transfer option under Lay 2 with an additional <i>ELSA LANCOM</i>.</p>	

	none	No data compression or channel bundling is performed.
	Compr.	V.42bis ( <i>ELSA LANCOM Wireless</i> ) or Stac data compression is used. V.42bis data compression is possible only in connection with X.75ELSA or X.75LAPB. Stac (Hi/fn) compression 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 'PPP' Lay 2 settings. Static or dynamic channel bundling depends on the B2 connection timeout. A B2 timeout of '0' or '9999' will set static channel bundling, in which both channels are always used. In dynamic channel bundling with other B2 timeouts, the second channel is only enabled when the data throughput exceeds a specified threshold.
	bnd+cmpr	Channel bundling and data compression takes place over two B channels.
Lay 1		The lay 1 column allows you to define the speed at which the data is sent in ISDN.
	HDLC64K	The data is transmitted at 64,000 bps.
	HDLC56K	The data is transmitted at 56,000 bps. This setting is especially important for connections in the USA.



*In order for the device to function correctly as a bridge, **ETHER** must always be entered in the **Encaps** field. If *ELSA LANCOM* is used as a router, any entry may be made, which should be adapted to the remote station.*

To link to devices from other manufacturers, please check with the manufacturer for the data format used (PPP is almost universally supported).

For Internet and remote access, PPP is generally specified.

#### DSL name list

The devices names entered in the DSL name list are needed by the router, in order to determine the correct remote station and corresponding layer name.

The name list can contain 16 different device names, and might (for example) have the following appearance:

Device name	SH time	AC name	Service name
AACHEN	180		
BERLIN	20		

A description of the fields is given below:

Device name	In the <b>Device name</b> column, you can enter an individual remote station name, which you must then assign to the relevant remote station via the <b>Name</b> command in the <b>Setup</b> menu.
SH time	In this column, you can define appropriate connection timeouts (in seconds) for the DSL connections. If no data is being transmitted when this time expires, the connection on this channel is closed (default: 20).
AC name	Name of the desired access concentrator. If nothing is entered here, the LANCOM will accept any AC with a matching service.
Service name	Name of the desired service. With no entry, the LANCOM will accept any service offered.

#### 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	Retry	Conf	Fail	Term	User name
AACHEN	CHAP	*****	0	5	10	5	2	ELSA

Not all parameters can be reached via the Telnet configuration. Use *ELSA LANconfig* if possible.

A description of the fields is given below:

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 "User name". For remote access via the data transmission network, the 'User name' field (see below) has no effect. Entries are also 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 require authentication from the router. This is the case when connecting to an ISP, for example.
	PAP	The remote station is checked using the Password Authentication Protocol.
	CHAP	The remote station is checked with the Challenge Handshake Authentication Protocol.
Key	A password may be entered in this column. Its presence is indicated by the symbol *, and it is used to check the remote station. It may consist of 95 characters (7-bit ASCII, including spaces). Default: none. The <code>set ?</code> command shows the list of allowed characters.	



Time	In this column, you can enter the period of time between two remote station verifications (in minutes). The CHAP protocol must be set here. Default: 0
Retry	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 can 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. However, the default values 10, 5, 2 are still used. These parameters can only be changed via SNMP or TFTP (using the <i>ELSA LANconfig</i> configuration program)!
User name	User name (max. 64 characters) transmitted to the remote station during PPP negotiation. In this way, the router identifies itself to the remote station. If no user name is entered, the device name serves as the user name. Entries are case-sensitive here.

*Number list*

Under this command, a number list is maintained, in which you can enter 64 different call numbers, along with their associated device names. This list can be used to assign the call numbers (CLI) transferred from the remote stations to the remote station names.

The number list entries for the two calling devices 'AACHEN' and 'BERLIN' might appear as in the table below. This would thus permit the derivation of the name from the supplied call number, and (if desired) also permit a callback to be initiated via the name list:

Dialup remote	Device name
875463	AACHEN
040785647	BERLIN

This number list is required for passive connection establishment. The remote station call numbers must be entered without leading zeros.

The currently active D-channel protocol 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 number or 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 protocol (PPP) negotiation.

#### Script list

Some Internet providers (e.g. CompuServe) conduct a script-controlled logon procedure before PPP negotiation. In order to be able to establish this type of connection as well, a simple script processing procedure is also implemented in *ELSA LANCOM* (see 'Script processing').

In this table, the scripts are defined, and are assigned to the remote stations. The table has the following layout:

Device name	Script
CSSERVE	<>[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. Should the required command sequence be longer, an additional entry for the logical remote station may be added (similar to 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 command can be used for manual connection control, for testing purposes.

/Manual dialing	Settings for manual connection control	
Connect	<b>COMMAND</b>	Establishes a connection.
Disconnect	<b>COMMAND</b>	Termination of connections
Status	<b>INFO</b>	Displays the current connection status.

#### Connect

Parameter: Remote station device name (via remote configuration only).

You can use the

Do /Setup/WAN module/Manual dialing/Connect to remote station

command to initiate manual connection establishment via remote configuration. The remote station device name specified as a parameter must also be entered in the name list, along with a call number.

#### Disconnect

This command allows you to terminate an existing connection. If a connection is terminated manually, the name of a remote station can also be entered in the remote configuration. In this case, only the connection to the specified remote station specified is terminated. If there is no connection to the specified remote station, then there is no

further response. However, if a remote station name is not entered, all existing connections will be terminated.

### 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 protection 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 'Number/Name' setting allows you to select combined protection, using a name list and a number list. First, the existence of a number list entry is verified. 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 between 3 and 5, in order to optimize the callback functionality. The default setting is 3.

### Setup/LAN module

This command allows you to select the settings needed for the local network. The menu has the following layout:

/LAN module	LAN settings	
Connection	VALUE	Selection of the network connection
Node ID	INFO	MAC layer address of the device
Spare heap	VALUE	Buffers that receive data packets from the local network

*Node ID*

This command allows you to display the router's own Ethernet address. The value displayed here was factory set, 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 four Telnet sessions (for example) can be enabled via the local network at any time.

## Setup/IPX module

This menu allows you to enter settings for the IPX module, and especially for the IPX router. The menu has the following layout:

/IPX module	IPX module settings (IPX router)	
State	<b>VALUE</b>	Enables/disables IPX module
IPX router	<b>VALUE</b>	Enables/disables the IPX router
LAN config	<b>MENU</b>	LAN-side settings
WAN config	<b>MENU</b>	WAN-side settings
RIP config	<b>MENU</b>	RIP settings
SAP settings	<b>MENU</b>	SAP settings

### State

This option allows you to enable or disable the IPX module. In the default configuration, the IPX module is enabled.



*Remote configuration via DOS/IPX and the IPX router is possible only if the IPX module is enabled. For local configuration via LAN, it is not necessary for the router to be enabled.*

### IPX router

This command allows you to enable or disable the IPX router. In the default configuration, the IPX module is disabled.



*When the IPX router is enabled, the IPX module is also enabled. The IPX router can only be enabled if the LAN and WAN setting contain different, allowable network addresses.*

## Setup/IPX module/LAN setting

The settings for the LAN data packets may be entered here. The menu has the following layout:

/LAN config	LAN-side settings	
Network	<b>VALUE</b>	Logical IPX network number of the LAN connection
Binding	<b>VALUE</b>	Ethernet frame type settings for the LAN connection
IPX watch	<b>VALUE</b>	Settings for IPX Watchdog management
SPX watch	<b>VALUE</b>	Settings for SPX Watchdog management
NetBIOS watch	<b>VALUE</b>	Settings for NetBIOS Watchdog management
Socket filter	<b>TABLE</b>	Filter table for destination socket filtering
Loc. routing	<b>VALUE</b>	Local routing enabled/disabled
RIP SAP scal.	<b>VALUE</b>	RIP SAP scaling enabled/disabled
LOOP propagation	<b>VALUE</b>	Redundant routing propagation enabled/disabled

<i>Network</i>	<p>The IPX network number for the Netware network is entered here (8digits, hexadecimal). This network is connected to the LAN connection binding (see below). If a NetWare Server is present in the local network, then the router can automatically determine the network number and the binding.</p> <p>The default value is "00000000", which means that the router should automatically determine the network number.</p>
<i>Binding</i>	<p>The Ethernet packet format (Auto, II, 802.3, 802.2, SNAP) for the LAN connection may be entered here. This format must be compatible with the Ethernet format bound in the local network, under the aforementioned network number.</p> <p>The default is 'Auto', and means that the router should automatically determine the binding (only when a NetWare server is present in the local network).</p>
<i>IPX watch</i>	<p>This sets the IPX watchdog packet management type.</p> <ul style="list-style-type: none"> <li>● <b>Filt.</b> means that the IPX watchdog packets are neither locally answered nor transmitted. Therefore, a user will always be logged off after the time set in the NetWare server.</li> <li>● <b>Route</b> means that the watchdog packets are transmitted, and that connections are established at regular intervals by server watchdog packets.</li> <li>● <b>Spoof</b> (default) ensures that IPX watchdog packets are answered locally by the router. Users are no longer automatically logged off. This setting is especially cost-effective. However, provisions may have to be made in the server to log off users at certain times, to prevent too many user licenses from being used.</li> </ul>
<i>SPX watch</i>	<p>This sets the SPX watchdog packet management type.</p> <ul style="list-style-type: none"> <li>● <b>Route</b> means that the SPX watchdog packets are transmitted, and that connections are established at regular intervals by server SPX watchdog packets.</li> <li>● <b>Spoof</b> (default) ensures that SPX watchdog packets are answered locally. This setting is especially cost-effective.</li> </ul>
<i>NetBIOS watch</i>	<p>This command displays how NetBIOS watchdog packets will be handled. NetBIOS watchdog packets appear when Windows networks are bound to IPX, for example. The settings are the same as for IPX or SPX watchdog packets (Filter, Route, Spoof).</p>
<i>Socket filter</i>	<p>The socket filter table enables specific filtering of LAN packets to certain destination socket areas. The filtering happens for simple IPX packets, as well as for propagated IPX packets. The following sockets that are periodically transmitted in the network (therefore</p>

frequently leading to connection establishment), are included in the LAN filter table by default (see also FAQs on 'IPX routers').

Start socket	End socket
0455	0457
0550	0555
1401	1402
1480	1481
83ba	83ba
900f	9010

#### *Loc. routing*

This setting enables support for the scaling of several routes in a local network. When all of a router's channels are already in use, and more packets arrive for the router, other routers in the LAN may actually still have free channels.

If 'Local routing' is enabled, then the router transfers the packets on the local network to another router, which has propagated a route to the desired destination remote station. The router saved this route (although it was worse than its own), and flagged it with a 'Reserve' flag in the RIP table.

The default setting for this is 'Off', because an IPX client that sends an RIP request for the desired route (after a timeout), will automatically find other routers, over which the destination network is reachable.

#### *RIP SAP scal.*

Another way to support scaling is to propagate every route that has an open connection, with a somewhat better Tic count than the current. This leads clients to send their packets for this route to the router with the open connection. Furthermore, if all channels are being used, the route that is no longer reachable can be propagated as 'DOWN'. Because this functionality results in at least one LAN broadcast for every connection established or terminated (which could cause other routers to broadcast, thus overloading the network), this feature can be switched enabled and disabled. The default setting is 'Off'.

#### *LOOP propagation*

Redundant routes, i.e. routes with the same Tic and hop count, are only passed on to remote stations, from which routes were not received (split horizon). The setting of the 'LOOP propagation' command also allows the propagation of these routes. Redundant routes are flagged in the RIP table with the 'LOOP' flag.

Since Novell specifications discourage the communication of redundant routes (without expressly forbidding it), the default setting is 'Off'.

## Setup/IPX module/WAN setting

The settings for the WAN connection data packets may be entered here. The menu has the following layout:

/WAN config	WAN-side settings	
Routing table	<b>TABLE</b>	Router table for IPX network and remote station assignment
Socket filter	<b>TABLE</b>	Filter table for destination socket filtering

### Routing table

The routing table can contain a maximum of 16 remote station and destination network entries. The table has 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 meaning:

- **Remote ID:** Name of the logical remote station (as given in the /Setup/WAN module/name list).
- **Network:** The address of the WAN-side network. A stand-alone network must be used; the same for both routers involved.
- **Binding:** Ethernet binding to be used on the ISDN route. This setting will only have an effect if Ethernet encapsulation is set in the utilized layer. If no binding is set, 802.3 will be assumed.
- **Propagate:** This command shows how type 20 IPX packets (NetBIOS propagated frames) will be handled. The possible settings are Route or Filter. If the entry is **Filter**, then no propagated frames will be transferred to this remote station. If the entry is **Route**, then the packets will be transferred to all currently reachable remote stations. In other words, there must be a connection to these stations, or at least a channel available for establishing a connection.

If no connection exists and no channel is available, the packet will be discarded. Therefore, the number of frames propagated to remote stations, cannot exceed the number of simultaneous possible connections. The default setting is 'Filter'.

- **Backoff:** The IPX router uses a special algorithm (exponential backoff), to keep connection costs to a minimum for incorrect configurations (see below).

If there is no server in the remote network (e.g. remote access from a workstation), the router cannot recognize this, and the remote station will be set inactive after a (maximum of a) day. To prevent this, the exponential backoff algorithm can be disabled for these remote stations.

The default setting is 'On'.

*Socket filter*

The socket filter table enables specific filtering of WAN packets to certain destination socket areas. The filtering happens for simple IPX packets, as well as for propagated IPX packets.

**Setup/IPX module/RIP setting**

The settings for the RIP data packets (router information) may be entered here. The menu has the following layout:

/RIP settings	RIP settings	
RIP table	<b>INFO TABLE</b>	Display RIP table
LAN filter table	<b>TABLE</b>	Filter areas for IPX network addresses (LAN)
WAN filter table	<b>TABLE</b>	Filter areas for IPX network addresses (WAN)
Routes/Frm	<b>VALUE</b>	Max. # RIP entries per transmitted RIP frame
Aging	<b>VALUE</b>	Aging period in update units
Spoofing	<b>VALUE</b>	Set RIP spoofing procedure
WAN update time	<b>VALUE</b>	RIP update period, depending on spoofing

*RIP table*

This command displays the entries in the current RIP table. This table can have a maximum of 256 entries.

The entries in the RIP table can be as follows, given networks 00000001, 00000002, 00000010, 00000081 that can be accessed by various routers. Flags indicate where these networks are located, relative to the different routers (**local** or **remote**). The word **direct** indicates that this particular network is either the local or the remote network. **DOWN** refers to a network that is known, but that is not reachable at the moment. The table is sorted by network number.

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 enables specific filtering of routes that were “learned” via the local network. Filtered routes do not appear in the IPX RIP table.

A LAN filter table for filtering routes in the area 00001000 to 00001fff may look like the following:

Start network	Destination network
00001000	00001fff



*WAN filter table* The WAN filter table enables specific filtering of routes that were "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 area 00002000 to 00002fff may look like the following:

Start network	Destination network
00002000	00002fff

*Routes/FRM* This parameter sets the maximum number of routes that can be contained within an RIP frame. The value originally set by Novell is 50. Currently, a higher number of routes is regularly packed in every frame, since this reduces the network load. If supported by all network devices, this value can be raised to 182.

*Aging* The number of times a RIP table entry can be updated before it "ages" can be set here. After this number, the route is flagged as "not reachable (down)". Valid numbers are from 1 to 60; the default is 3.

*Spoofing* This sets the way in which the router handles RIP packets.

- The setting **Without** means that RIP packets are handled the same way on the WAN, as on local networks. If there is new information and/or in one minute intervals, RIP data are sent to the remote side, and a connection is established.
- The **Trig** setting means that RIP data are sent to the remote side, whenever changes occur.
- The **Time** setting means that RIP data are sent to the remote side at a frequency given by the selected time interval (see below).
- **pBack** (default) is the least costly setting. RIP data are only sent to the remote side when a connection is active.



*With the spoofing set at **pBack**, entries in the RIP table only age when a new connection is made, and an entry is flagged as "unreachable".*

*WAN update time* A transmission period is set here for the Spoofing time control. Within this period, RIP data are transmitted to the remote side. Valid numbers are from 1 to 60 minutes; the default is 5.

### Setup/IPX module/SAP setting

The settings for the SAP data packets (server information) may be entered here.

/SAP settings		Settings for the SAP
SAP table	<b>INFO TABLE</b>	SAP table displays
LAN filter table	<b>TABLE</b>	Filter areas for IPX service addresses (LAN)
WAN filter table	<b>TABLE</b>	Filter areas for IPX service addresses (WAN)

/SAP settings		Settings for the SAP
Server/Frm	VALUE	Max. # SAP entries per transmitted SAP frame
Aging	VALUE	Aging period in update units
Spoofing	VALUE	Set SAP spoofing procedure
WAN update time	VALUE	SAP update period, depending on spoofing

*SAP table*

This command displays the entries in the current SAP table. This table can have a maximum of 512 entries. The table is sorted by service type, and for the same type, by server name. An SAP table could be structured as follows:

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

Various SAP types are listed there. Information includes the server name, the relevant network, the MAC address of the server (for internal server networks 000000000001), the socket number, and information on the location of the server.

*LAN filter table*

Through LAN filter table entries, it is possible to exclude certain service information areas of a Novell network from being entered in the SAP table, making better use of the resources of the IPX router. In addition, undesired connections are prevented by these SAPs (services).

All service information inside the LAN filter table filter area is not exported by the local network into the IPX router SAP table. It is also not transmitted to the remote station of the IPX router, and is also not available there.

Frequently, the service information for (as an example) the printer server is not necessary for the remote station of the IPX router. If the LAN filter table is to exclude this information from the SAP table, the following entry is necessary:

Start service	End service
030c	030c

A list of SAP services and their descriptions can be found in the 'Novell SAP numbers' section.

*WAN filter table* As with a LAN filter table, it is also possible with a WAN filter table to exclude areas of WAN service information from being entered into the SAP tables.

However, the blocked services will have already caused a connection to be established to the remote station, before the destination router could filter them from the WAN side.

In structure and function, the WAN filter table is completely analogous to the LAN filter table. A WAN filter table for filtering file services may look like the following:

Start service	End service
0004	0004

#### Server/FRM

This parameter sets the maximum number of services that can be contained within an SAP frame. The value originally set by Novell is 7. Currently, a higher number of services is regularly packed in every frame, since this reduces the network load. If supported by all network devices, this value can be raised to 22.

#### Aging

The number of times a SAP table entry can be updated before it "ages" can be set here. After this number, the service is flagged as "not reachable (down)". Valid numbers are from 1 to 60; the default is 3.

#### Spoofing

This sets the way in which the router handles SAP packets.

- The setting **Without** means that SAP packets are handled the same way on the WAN, as on local networks. If there is new information and/or in one minute intervals, SAP data are sent to the remote side, and a connection is established.
- The **Trig** setting means that SAP data are sent to the remote side, whenever changes occur.
- The **Time** setting means that SAP data are sent to the remote side at a frequency given by the selected time interval (see below).
- **pBack** (default) is the least costly setting. SAP data are only sent to the remote side when a connection is active.



*With the spoofing set at **pBack**, entries in the RIP table only age when a new connection is made, and an entry is flagged as "unreachable".*

#### WAN update time

A transmission period is set here for the Spoofing time control. Within this period, SAP data are transmitted to the remote side. Valid numbers are from 1 to 60 minutes; the default 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	
State	VALUE	Enables/disables the TCP/IP module
IP address	VALUE	Local IP address
IP netmask	VALUE	Local network's matching IP network mask
Intranet address	VALUE	Local Intranet address

/TCP IP module	TCP/IP module settings	
Intranet mask	<b>VALUE</b>	Local network's matching Intranet network mask
Access list	<b>TABLE</b>	Restricts access to internal functions via TCP/IP
DNS default	<b>VALUE</b>	Domain name server
DNS backup	<b>VALUE</b>	Backup domain name server
NBNS default	<b>VALUE</b>	NetBIOS name server
NBNS backup	<b>VALUE</b>	Backup NetBIOS name server
ARP table	<b>TABLE</b>	ARP table for mapping an IP address to a MAC address
ARP aging min.	<b>VALUE</b>	Dwell time for entries in the ARP table
TCP aging min.	<b>VALUE</b>	Time limit for configuration connections that are inactive
TCP max. conn.	<b>INFO</b>	Max. number of simultaneous configuration connections to <i>ELSA LANCOM</i>

*State*

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



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

*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 (using PPP), all computers linked by IP address and IP network mask within the network, are normally routed. These computers can then also be accessed directly from the Internet.

*IP network mask* 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 instead 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 second IP address enables the device to be used as a router for two logical IP networks. This address also has a specific meaning when using IP masquerading:

In this case, all computers that are linked in the network by Intranet address and Intranet mask, are hidden behind the address assigned by the provider (or the IP address).

*Intranet mask* The network mask belonging to the IP address of the local network must be entered here. The default setting is 255.255.255.0 (class C network).



*If neither an IP nor an Intranet address has been specified, the device responds to a default IP address, the first three digits of which are identical to the first three digits of the sending device XXX.XXX.XXX.YYY. The device can then be reached by dialing the IP address XXX.XXX.XXX.254.*



*If such an IP address already exists in the network, a different address must be entered via the keyboard (ELSA LANCOM Wireless only), or via outband configuration (terminal program).*



*If both an IP address and an Intranet address have been entered, the network defined by an IP address and IP network mask must contain only workstations (i.e. no routers).*

*Access list* The access to "internal functions" of the router can be controlled by an access list in TCP/IP applications.



*The device configuration data are password protected. However, this password is always transferred in plain text, making it possible, in principle, to detect this, and from 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, 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 TFTP protocol.
- SNMP: the configuration interface based on the SNMP.

Each of the maximum 16 entries in the access list has the following structure:

IP address	IP network mask
IP address of the authorized user (or user workgroup)	IP network mask of the user workgroup

Once an IP workstation with its IP address and the network mask 255.255.255.255 is entered in the list, then 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*, then this can be done as follows for a class C network:

IP address	IP network mask
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, so that computers that have direct access via PPP to the router can identify the name server responsible for their network.

If the router is configured for access to the Internet via an Internet Service Provider, then the DNS server is usually given by the provider. There are thus 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. It then uses the DNS information from the provider, not only for its own local network, but also forwards this information (DNS forwarding). Remote stations (e.g. 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** (NetBIOS Name Server) is required, so that computers that have direct access via PPP to the router can identify the NBNS responsible for their network.

*NBNS backup*

With the entry **NBNS backup**, a second server can be named, which is used if the NBNS fails.

*ARP table*

This command displays the ARP table (ARP cache), which is managed automatically for 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 could be as per the following, assuming that devices with IP addresses (192.168.139.20, 192.168.130.30) have communicated with the router:

IP address	Node ID	Last access	Connection
192.168.130.20	0000c0717860	6780443 tics	local
192.168.130.30	0800091eebf4	6214514 tics	local

*ARP aging min.*

A time (from 1 to 99 minutes) can be entered here, after which the ARP table is automatically updated. In other words, 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 stops entering data during the remote configuration), it will automatically terminate the TCP connection, when the time entered here expires. Possible settings are from 1 to 99 minutes. The default setting is 15 minutes.

*TCP max.  
connections*

The maximum number of allowable simultaneous possible connections can be set here. DEFAULT setting is '0', which means the same as "as many as desired".

## Setup/IP router module

The IP router module settings are entered via this menu. The menu has the following layout:

/IP router module	IP router module settings	
State	VALUE	Enables/disables the IP router module
IP routing table	TABLE	Router table for IP network and remote station assignment
Default time table	TABLE	Router table for IP network and remote station assignment
Usage default lists	VALUE	Router table for IP network and remote station assignment
LAN filter table	TABLE	Negative/conn. filter table for the TCP/UDP destination ports of LAN packets
WAN filter table	TABLE	Negative filter table for the TCP/UDP destination ports of WAN packets
Proxy ARP	VALUE	Enables/disables the proxy ARP function
Loc. routing	VALUE	Enables/disables local routing
Routing method	MENU	Routing method for IP packets
RIP settings	MENU	Settings for IP-RIP operation
Masquerading	MENU	Settings for IP masquerading

*State*

This command enables/disables the IP router module. In the default configuration, the IP router module is enabled.



*Enabling the IP router module on also enables 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 net masks, and the names or IP addresses of other local routers. Alternatively, you can enter a setting, such that 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 or not the route should be masked. The following options are offered here:

- **On:** IP masquerading is enabled, and functions by 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 disabled.

- **Static:** IP masquerading is enabled, and functions with the 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 as an example, and also shows the default settings:

IP address	IP network mask	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 (as an 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 devices 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* 'Dresden'.
  - Two destination networks 192.120.131.0 and 192.120.132.0 can be accessed by the remote stations 'AACHEN' and 'BERLIN'.
  - Data packets for the destination network 193.140.300.0 are to be sent to another local router with the IP address 192.120.130.200.
  - Absolutely nothing is to be transmitted to the destination network 193.140.200.0.



- All other non-local data packets must be sent to the router 'PROVIDER' at the Internet service provider.

In this example, the router table would contain the following entries:

IP address	IP network mask	Router name	Distance	Masquerade
192.120.130.10	255.255.255.255	DRESDEN	0	Off
192.120.130.11	255.255.255.255	DRESDEN	0	Off
192.120.130.12	255.255.255.255	DRESDEN	0	Off
192.120.131.0	255.255.255.0	AACHEN	0	Off
192.120.132.0	255.255.255.0	BERLIN	0	Off
193.140.200.0	255.255.255.0	0.0.0.0	0	Off
193.140.300.0	255.255.255.0	192.120.130.200	0	Off
255.255.255.255	0.0.0.0	PROVIDER	0	On



*If the connection to the selected remote station occurs 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 always works, 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 everything from a WAN terminal that is not local to the router at the provider.

#### Default time table

Similar to least-cost routing (LCR), time control for the default route is a function that automatically selects the provider with the lowest rate for the particular time of day.

When an IP packet would initiate a connection via the default route, the remote station entered as the default route is not selected. Instead, the time control table is checked for the desired remote station.

In this table, enter the days of the week, and hours of the day that each provider is to be used. Now, when an IP packet would initiate a connection via the default route, the time control table is first checked, to see if it is enabled for use. If it is, the table is then searched for an entry for the current hour and day. If a matching entry is found, the router establishes a connection to that remote station. If no entry is found, the router returns to the IP routing table, and uses the remote station entered there.

#### Usage default lists

Enables/disables the use of default lists.

#### 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 either not be forwarded (always filter); only if a

connection is currently in place (connect filter); or only if they can be routed over a route 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	Source address	Src net mask	Prot	Type
WIN	0	0	137	139	255.255.255.255	0.0.0.0	TCP and UDP	Always filt.

The table fields have the following meaning:

- **Idx.**  
Unique index. This entry is required to enable the filters to be distinguished. The index may be four characters long, and can be 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 unwanted and cost-intensive Windows network connections on IP. These networks regularly send items such as DNS queries to the local network. They would be 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	Destination 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 difference:

- 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 largest IP address is placed on top.

Network masks and IP addresses of 0.0.0.0 can be used as "wildcards". Certain computers and networks may be specifically filtered, while others, at the same time, 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 enable or disable 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. Local routing is necessary if the router, as the default gateway for the workstations, receives packets for destination networks, to which it cannot itself establish a connection. 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 increases network load in the LAN, the default setting is 'Off'.

### 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 selected in the 'Type of service' field in the IP header.

The menu has the following layout:

/Routing method	Routing method settings	
Routing method	VALUE	Routing method for IP packets
ICMP routing method	VALUE	Routing method for ICMP packets

*Routing method*

This setting defines the routing method used for IP packets:

- If you select 'Normal', all IP packets are handled in the same way, following the Internet protocol routing specifications.
- With the 'Type of service' setting, IP packets are placed in the urgent queue or the protected queue, depending on the 'Type-of-service' field entry. 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 setting defines the routing method used for ICMP packets:

- If you select 'Normal', the ICMP packets are handled like any other IP packets, following the Internet protocol routing specifications.
- If you select 'protected', all ICMP packets received are placed in the protected queue.

### Setup/IP router module/RIP settings

This option allows you to enter settings for the management of IP-RIP packets. The menu has the following layout:

/RIP settings	Settings for IP-RIP operation	
Type	VALUE	RIP compatibility switch
R1 mask	VALUE	Management of network masks
RIP table	INFO TABLE	Dynamic IP routing table

*Type*

This option allows you to select the method to be used for handling the IP-RIP packets. The settings have the following meanings:

- **Off:** IP RIP is not supported (default).
- **RIP 1:** RIP 1 and RIP 2 packets are received, but only RIP 1 packets are transmitted.
- **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*

The **RIP 1** setting influences network mask management. Therefore, these settings are required only for subnetting under **RIP 1**. The settings have the following meanings:

- **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 of the IP address entry. This and all higher-order bits within the network mask are set. For example, the IP address 127.128.128.64 yields the IP network mask 255.255.255.192.
- **Cl+Addr:** The network mask is derived in part from the IP address class, and from an added address procedure portion. For example, the preceding address and the network mask 255.255.0.0 yield the IP network mask 255.128.0.0.

*RIP table*

This command displays the entries in the current dynamic IP routing table.

An IP RIP routing table might, for example, have the following appearance:

IP address	IP network mask	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

Specify here if RIP packets will be sent to the LAN, or to the cable network.

### 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	VALUE	Time in seconds, after which a TCP masking becomes invalid
UDP aging	VALUE	Time in seconds, after which a UDP masking becomes invalid
ICMP aging	VALUE	Time in seconds, after which an ICMP masking becomes invalid
Service table	TABLE	Static masquerading table
Table masquerading	INFO TABLE	Dynamic masquerading table

*Service table*

The use of inverse masquerading (entering specified ports in the service table in the IP network) makes 'services' (e.g. a file server) selectively visible in the Internet. At the same time, all other services and computers remain invisible outside of 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 address
20	10.1.1.10
21	10.1.1.10

The 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

By means of this assignment, it is possible to access a service directly (e.g. via Telnet). Enter the IP address of the router, and attach the port number (separated by a colon) to the address.

You can use the command

```
telnet 192.38.50.100:27
```

to connect directly to a news server, which can be reached via a router with the IP address 192.38.50.100.

*Table  
Masquerade*

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 local network IP addresses that the router is currently masking. The dynamic masquerading table can contain up to 2048 entries, and has the following layout:

Intranet address	S port	Protocol	Time
10.1.1.10	1234	TCP	10

The 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 device via SNMP. The menu has the following layout:

/SNMP module	SNMP module settings	
Send traps	VALUE	Switch for issuing SNMP traps
IP trap table	TABLE	Table with 20 destination addresses for trap messages
Administrator	VALUE	Device administrator
Location	VALUE	Device location
Register monitor	COMMAND	Command to log on to a destination address, to which the traps are to be sent
Delete monitor	COMMAND	Command to delete an address that was set with 'Register monitor'
Monitor table	INFO 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 name

*Location* Device location

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

*Register monitor* With this command, applications log on to the router to get specific trap information. The *ELSA LANmonitor*, for example, compiles channel statistics in this way, and converts them to a Windows graphics display.

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 timeout, the address will be automatically deleted from the table. A timeout 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	
State	<b>VALUE</b>	Switch for enabling the DHCP module
Start address pool	<b>VALUE</b>	Start address for the address pool
End address pool	<b>VALUE</b>	End address for the address pool
Net mask	<b>VALUE</b>	Network mask for the address pool
Broadcast address	<b>VALUE</b>	Broadcast address for the LAN
Gateway address	<b>VALUE</b>	Gateway address for the LAN
Max. validity (minutes)	<b>VALUE</b>	Maximum period of validity for the address assignment via DHCP
Default validity (minutes)	<b>VALUE</b>	Default period of validity for the address assignment via DHCP
DHCP table	<b>INFO TABLE</b>	Table of current assignments via DHCP

*State*

On: The device operates as a DHCP server

Off: The device does not operate as a DHCP server

Auto: The device regularly checks if 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), then the router (in auto mode) will issue IP addresses from the address range 10.0.0.2 – 10.0.0.253 to all DHCP clients.*

*Start address pool*  
*End address pool*

The IP address assigned is taken from the address pool selected (entries from '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 in 'Setup/TCP module'. The procedure is as follows:

- If only the IP address or only the Intranet address is entered, then 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, then it will request this same address. The DHCP server will attempt to reassign this address to the computer, if the address has not already been assigned to another computer.

The DHCP server also checks that the address which is to be assigned to the computer is unique in the local network. It performs this check 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 querying computer is assigned the address found.

#### *Net mask*

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 of the local network (read 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 of the local network (read during address assignment).

#### *Max. validity (minutes)*

Here you can enter the maximum period of validity, for which the DHCP server assigns a host.

The default value of 6000 minutes is about 4 days.

#### *Default validity (minutes)*

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

The default value of 500 minutes is about 8 hours.

#### *DHCP table*

In the DHCP module, the 'Table DHCP' command may be used to look up the IP addresses assigned to computers. This table has the following layout:

IP address	MAC address	Timeout	Host name	Type
10.1.1.10	00a0570308e1	500	ELSA	new

- IP address: IP address assigned
- MAC address: Computer Ethernet address
- Timeout: Time remaining in validity period
- Host name: Descriptive computer name, if it accompanies the query
- Type: This field contains additional information on the assignment.  
The 'Type' field specifies how the address was assigned. In this field, the following values are possible:
  - **new**: First query by the computer. The DHCP server verifies the uniqueness of the address to be assigned to the computer.

- **unkn.:** A uniqueness check shows that the address is already 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 assigns an address to the computer.

## Setup/NetBIOS module

The Setup/NetBIOS menu contains the settings for the NetBIOS module. The menu has the following layout:

State	<b>VALUE</b>	On or off
Scope ID	<b>VALUE</b>	NetBIOS scope of the router.
NT domain	<b>VALUE</b>	Workgroup/domain of the router.
Remote table	<b>TABLE</b>	All remote stations, with whom NetBIOS information is exchanged, are listed in the remote-station table.
Group list	<b>INFO TABLE</b>	All workgroups known via NetBIOS are recorded in the group list.
Host list	<b>INFO TABLE</b>	All computer names known via NetBIOS are recorded in the host list.
Server list	<b>INFO TABLE</b>	All servers that have logged onto the network are recorded in the server list.
Watchdogs	<b>INFO TABLE</b>	Specifies how watchdog packets are handled
Alignment	<b>INFO TABLE</b>	Type of routing information alignment
WAN update min	<b>INFO TABLE</b>	Duration of alignment in minutes

### *Scope ID*

The Scope ID command can be used to specify the current device NetBIOS scope. It then sees only those NetBIOS packets originating from 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 command, in order to initiate 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 are listed in the remote table. When the NetBIOS module is enabled, NetBIOS packets from remote stations other than those specified will be automatically rejected. The remote-table has the following structure:

Name	Type
AACHEN	Router or workstation



*If the connection to the selected remote station is to occur via a PPP connection, the NetBIOS rights must be enabled for its entry in the PPP table.*

*Type* The 'Type' field specifies if the remote station is a router or a workstation. If it is a workstation, all the names and servers in the local network (and in all other connected routers known to the workstation) are logged off and deleted from the respective tables, as soon as the connection to the workstation is terminated.

*Host table* The host table has the following structure:

Name	Type	IP address	Remote ID	Timeout	Flags
REMOTE	00	10.0.1.100	AACHEN	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 ID	Timeout	Flags
WORKGROUP	1e	10.0.0.10		5000	xx00
WORKGROUP	1e	10.0.1.100	AACHEN	5000	xx20

The table fields have the following meaning:

Name	Host name in the host table
Group/Domain	Name of the group or domain in the group list. NetBIOS handles groups and NT domains in the same way.
Type	WINS host type. The type is not relevant for NetBIOS, but Windows networks assign certain properties to the name, on the basis of the type.
IP address	IP address of the name owner. The same name can be assigned to multiple IP addresses in the group list.
Remote ID	Name of the remote station, from which the name became known.
Timeout	Duration until the name is no longer valid. The timeout 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 meaning:

0x0003	This counter increases each time the validity expires. If the name is not renewed by the second expiry, it will be deleted.
0x0004	This identifies an entry that still needs to be transmitted.
0x0008	This identifies an entry that is queued for deletion. The name has not 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 ID	Timeout	Flags
REMOTE	WORKGROUP	00	10.0.1.100	0400	010f	0004140b	AACHEN	13	0020
WORKSTATION	WORKGROUP	07	10.0.0.10	0400	0415	00452003		31	0000

Unlike the host and group lists, this table fills gradually, because the NetBIOS module depends on messages from the servers themselves.

The individual fields have the following meaning:

Host	Name of the server
Group/Domain	Workgroup or domain of the server
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 server services are coded
Remote ID	Name of the remote station, from which the server was found
Timeout	The time until the entry loses its validity (for entries from the LAN), or the time until the router propagates a remote entry.
Flags	The flags in the host or group tables.

## Setup/Config module

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

/Config module	Configuration module settings	
LAN config	VALUE	Switch for configuring from the LAN-side
WAN config	VALUE	Switch for configuring from the WAN-side
Password required	VALUE	Password required on/off (if there is no password)
Maximum connections	VALUE	Maximum number of simultaneous connections
Farconfig (EAS-MSN)	VALUE	Call number for remote configuration via PPP
Config timeout (minutes)	VALUE	Time limit for remote configuration connections
Logon errors	VALUE	Number of unsuccessful logon attempts, before the logon block is activated
Block (minutes)	VALUE	Duration of block, and period until old logon errors are forgotten
Language	VALUE	Configuration language

*LAN config* This setting determines if a remote configuration from the LAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting is **On**.

*WAN config* This setting determines if a 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 determines if, when no password is present, 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 is **Off**.

*Farconfig (EAS-MSN)* This call number permits remote configuration via PPP. If no number is specified here, remote configuration calls will be accepted on all numbers.

*Config timeout (minutes)* If data transmission halts during a remote configuration session (e.g. because the user is no longer entering data), the device automatically terminates the connection at the end of the time period specified here. Possible settings are from 1 to 99 minutes. The default setting is 15 minutes.

*Logon errors* This entry specifies the number of unsuccessful attempts allowed, before the logon block is activated. An empty password (given by 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 logon block to be activated with only one access on an older ELSA LANconfig. In this case, obtain an updated ELSA LANconfig version from our online media.*

*Block (minutes)* This entry has two meanings. It indicates how long the access is blocked, if the logon block has been activated. It also sets the period, after which the device forgets all prior logon errors.

*Language* Here is where you select the German or English version of the software for performing the configuration.

## Setup/LANCAPI-module

The configuring of *LANCAPI* basically involves answering the following questions:

- To which call numbers from the telephone network should *LANCAPI* respond?
- 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	<b>TABLE</b>	List of computers allowed to use the <i>LANCAPI</i>
LANCAPI UDP port	<b>VALUE</b>	UDP port for communication between the <i>LANCAPI</i> server and clients
EAZ-MSN(s)	<b>VALUE</b>	EAZ or MSN to which the <i>LANCAPI</i> should respond
Prio out	<b>VALUE</b>	Priority for the <i>LANCAPI</i> versus router connections

- **State:** 'on', 'off' or 'outgoing'. With the last setting, the *LANCAPI* will not accept incoming calls.
- **Access list:** Here you can 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*.
- **LANCAPI UDP port:** In the default configuration, this option is set to '75'. Change this setting only if other devices in your network are already using this port.



*When you change the port, all current connections via the LANCAPI are lost!*

- **EAZ/MSN(s):** Here you enter the call numbers, to which the *LANCAPI* is to respond. If you wish to enter more than one number, separate them by a semicolon.
- **Prio out:** This priority controls the ability of outgoing router connections to be broken via the *LANCAPI*. A value of '1' means that no router connections are broken, '2' means that only auxiliary channels of a router connection with channel bundling are broken, and '3' means that router connection main channels are also broken.

## Setup/WLAN module

The WLAN module is configured using this menu:

WLAN domain	VALUE	The WLAN domain is entered here, i.e. the symbolic name that the mobile stations use to find the base port. An ASCII string with a maximum of 32 characters. The default setting is 'ELSA'.
Phy channel	VALUE	The wireless channel to be used by the base port. The possible values are 1 to 14. However, the channels overlap due to the spread-spectrum process, so that the entire radio band offers a maximum of 3 completely independent channels. <i>Not all channels are permitted in all countries (please see the table of radio channels in the Appendix).</i>
Packet size	VALUE	A value between 600 and 1600; that indicates the maximum size of WLAN packets in bytes. Default: 1550.
Access list	TABLE	This list can be used to exclude WLAN stations explicitly from data communications with the LAN/base port. Alternatively, it can be used to list only authorized stations. Enter the MAC addresses of stations in this list (the 12-character hexadecimal numbers printed on the cards), but without separators. For example, 00-60-B3-1F-02-11 would become 0060B31F0211. <i>This only denies the stations access to the LAN or WAN. Data communications between stations in the WLAN via the base port, which typically serves as a relay, is not affected.</i>
Access mode	VALUE	This positive/negative switch determines if the list is to serve as an authorization or an exclusion list. By default, the mode is set to negative, and the access list is empty, i.e. no stations are excluded from data communications.
Protocol list	TABLE	This list permits data packets to be blocked or permitted (depending on the positive/negative setting of the switch) on the basis of their protocol. Every Ethernet frame contains a 16-bit identifier that states the layer 3 protocol, in which it transmits data. These can be entered in the list as hexadecimal numbers. Common protocols include: 0800 = IP 0806 = IP/ARP 8137 = IPX FOF0, E0E0 = IPX 809B and 80F3 = Appletalk 6001 to 6007 = Decnet 80D5 and 0808 to 0D0D = IBM SNA <i>In this case as well, traffic is blocked between WLAN stations and the LAN (or WAN), but not between WLAN stations.</i>
Protocol mode	VALUE	Positive/negative switch for the protocol list
Interpoint traffic	VALUE	Allows the base station to be used for point-to-point communication, to connect two or more LANs wirelessly.
Access point list	TABLE	For point-to-point connections, it is necessary to enter here the MAC addresses of the remote access points (base stations). There can be six at most.
WEP encoding	VALUE	Enables WLAN data packet encoding. As soon as this setting is enabled, stations can log on only with a valid key.
WEP standard key	VALUE	The key used for transmitted packets.

WEP key	<b>TABLE</b>	The key used for coding. Internally, this key is a 40-bit number. Either a hexadecimal or a 5-digit ASCII string may be entered.
Node ID	<b>INFO</b>	MAC layer address of the device
Spare heap	<b>VALUE</b>	Buffers that receive data packets from the local network
IAPP protocol	<b>VALUE</b>	On/Off roaming switch For roaming, all base stations must use the same WLAN domain and the same radio channel.
IAPP announce interval	<b>VALUE</b>	For roaming, the time interval, within which a base station announces itself to all others over the cable-bound LAN.
IAPP handover timeout	<b>VALUE</b>	Maximum length of time, during which the base station waits for confirmation from the mobile station.

## 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 forwarded, when, and via which call-by-call provider?

The LCR module has the following layout:

/LCR module	Least-cost router settings	
Router usage	<b>VALUE</b>	Switch LCR for the router modules, <b>On</b> or <b>Off</b>
Lancapi usage	<b>VALUE</b>	Switch LCR for the <i>LANCAPI</i> , <b>On</b> or <b>Off</b>
Time table	<b>TABLE</b>	Call forwarding table
Holiday table	<b>TABLE</b>	List of holidays that affect the time table.

*Time table*

This table of 256 entries has the following structure:

Index	Prefix	Days	Start	Stop	Number list	Fallback
1	0171	192	0:00	23:59	01013;01070	On

The entries have the following meaning:

Index	Running index of table entries
Prefix	Area code to be forwarded
Days	Validity of the entry for weekdays and holidays shown in an 8-bit mask: Bit 0 represents Monday, bit 7 holidays. The entry '31' designates all business days, '192' Sundays and holidays
Start	Beginning time for the validity of the entry on the defined days.
Stop	Termination time for the validity of the entry on the defined days.
Number list	Network identification number of the call-by-call provider.
Fallback	Automatic fallback to your telephone company, if all call-by-call 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.

*Holiday table*

The holiday table, with 256 entries, has the following structure:

Index	Date
1	01010000
2	01050000
3	03100000
4	25120000
5	26120000
6	02041999
7	13051999

The entries have the following meaning:

Index	Running index of table entries.
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 fixed annual holidays.

## Setup/DNS module

The settings for the DNS server can be modified here. The menu contains the following commands (with default settings):

State	<b>VALUE</b>	On (default) or off
Domain	<b>VALUE</b>	Own domain, optional, 32 characters max.
DHCP usage	<b>VALUE</b>	Yes (default) or no
NetBIOS usage	<b>VALUE</b>	Yes (default) or no
DNS table	<b>TABLE</b>	Static DNS table for manually assigning IP addresses and names, 64 entries
Filter list	<b>TABLE</b>	Filter list for the exclusion of prohibited domains, 64 entries
Validity	<b>VALUE</b>	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 name.

The table is restricted to 64 entries, since larger networks are configured more effectively using the DHCP server, which can also be used to handle name requests. The table has the following layout:

Host name	IP address
Host10	10.0.0.10

The name is restricted to a maximum of 32 characters. Longer names are not 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/net mask pair. An IP address of 0.0.0.0 prohibits this domain for all computers. Likewise, a net mask of 0.0.0.0 prohibits the domain for all networks. The table has the following layout:

Name	Domain	IP address	Net mask
F001	*xxx*	0.0.0.0	0.0.0.0

Unique IDs can be freely selected and assigned to the filters in the 'Name' field.

Enter the name of the domain to be prohibited in the 'Domain' field. Wildcards (like '?' and '\*') may be used. The wildcard '?' replaces exactly one character, while '\*' replaces any string of any number of characters. The wildcard '\*' can be used more than once. 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 net masks in descending order (longest at the top); and entries with identical net masks are sorted according to IP addresses in ascending order. For identical IP addresses, the entries are sorted in ascending order according to the domain to be prohibited.

The tables are searched from top to bottom. As soon as a matching filter is found, an error message is sent to the requesting computer.

## Setup/Time module

The least-cost router in the device requires correct time information to calculate the call-by-call provider forwarding. Precise time information is also desirable for some statistics.

The time can either be set manually (with the 'time' command), or it can be automatically read from the ISDN network.

For automatic time comparison when the module is enabled, a pre-specified remote station is immediately called, and the time information is taken from the ISDN network. While the time module is enabled, the time from the ISDN will be refreshed every time the router establishes a connection.

The time module has the following layout:

/Time module	Time module settings	
State	<b>VALUE</b>	Switching the module: <b>On, Off</b>
Current time	<b>INFO</b>	Displays the current device time
Time EAZ-MSN	<b>VALUE</b>	Call number, to which a connection should be established, in order to receive time information from the ISDN
Dialing attempts	<b>VALUE</b>	Number of allowed attempts to receive time information

## Firmware

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

/Firmware	Display and keyboard settings	
Version table	<b>INFO TABLE</b>	Displays hardware releases and serial numbers for the router
FirmSafe table	<b>INFO TABLE</b>	Information about the two firmware versions stored in the device, and about the bootloader.
FirmSafe mode	<b>VALUE</b>	Firmware activation mode
FirmSafe timeout	<b>VALUE</b>	Time in minutes for a new firmware test
Test firmware	<b>COMMAND</b>	Tests inactive firmware
Firmware upload	<b>COMMAND</b>	Initiates a firmware upload

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

*FirmSafe table* 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.
```

*FirmSafe mode* 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 immediately activate it. The following situations can result:
  - The new firmware is successfully loaded and then operates as desired. Everything is OK.
  - 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.
- 'logged on': To prevent problems caused by defective firmware, there is a second way to load the firmware, and start it immediately.
  - In contrast to the first option, Firmsafe will wait until the device has successfully logged on over outband or inband (by Telnet). The new firmware will only be permanently activated when the computer was logged on successfully within the time set under 'Timeout firmsafe'.
  - If the device no longer responds, and it is therefore impossible to log on, the firmware automatically loads the previous firmware version, and reboots the device.
- 'manual': With the third option, you can also set a period (Firmsafe timeout) in advance 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	<b>COMMAND</b>	Tests a connection
System boot	<b>COMMAND</b>	Restarts the device
System reset	<b>COMMAND</b>	Resets to factory settings
Upload system	<b>COMMAND</b>	Loads new firmware

## Other/Manual dialing

This command can be used for manual connection control, for testing.

### System boot

This command allows you to reboot the device.



*Before executing the command, all open connections (ISDN or TCP) will be terminated or closed.*

### System reset

This option resets all the settings that have been entered. The device is reset to the delivery version.

For safety, 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 `System boot` command. If no password has been assigned, press Enter a second time.

### Upload system

This command starts a firmware upload (refer to the 'How to set up new software' section).

Flash ROM technology permits flexible and service-friendly handling of the system software, by allowing different firmware versions to be read in. Devices can also be retrofitted with future versions.



# TCP/IP Ports

Service.	Port no.	Protocol
echo	7	tcp
echo	7	udp
discard	9	tcp
discard	9	udp
systat	11	tcp
systat	11	tcp
daytime	13	tcp
daytime	13	udp
netstat	15	tcp
qotd	17	tcp
qotd	17	udp
chargen	19	tcp
chargen	19	udp
ftp data	20	tcp
ftp	21	tcp
Telnet	23	tcp
smtp	25	tcp
time	37	tcp
time	37	udp
rlp	39	udp
name	42	tcp
name	42	udp
whois	43	tcp
domain	53	tcp
domain	53	udp
name server	53	tcp
name server	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

Service.	Port no.	Protocol
supdup	95	tcp
host names	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
nnntp	119	tcp
ntp	123	udp
nbname	137	udp
nbdatagram	138	udp
nbssession	139	tcp
NeWS	144	tcp
sgmp	153	udp
tcprepo	158	tcp
snmp	161	udp
snmp-trap	162	udp
print-srv	170	tcp
vmnet	175	tcp
load	315	udp
vmnet0	400	tcp
sytek	500	udp
biff	512	udp
exec	512	tcp
logon	513	tcp

Service.	Port no.	Protocol
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
rxd control	531	udp
netnews	532	tcp
netwall	533	udp
uucp	540	tcp
klogon	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
acctlogon	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctslave2	706	udp
acctdisk	707	udp
kerberos	750	tcp
kerberos	750	udp

Service.	Port no.	Protocol
kerberos_master	751	tcp
kerberos_master	751	udp
passwd_server	752	udp
userreg_server	753	udp
krb_prop	754	tcp
erlogon	888	tcp
kpop	1109	tcp
phone	1167	udp
ingreslock	1524	tcp
maze	1666	udp
nfs	2049	udp
knetd	2053	tcp
eklogon	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



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

