

# Contents

<b>Enhancements in firmware version 1.40 .....</b>	<b>1</b>
DNS .....	1
What does a DNS server do? .....	1
Setting up the DNS server .....	2
The DNS menu .....	4
<i>ELSA CAPI Faxmodem</i> .....	7
Installation .....	7
Faxing with the <i>ELSA CAPI Faxmodem</i> .....	7
Channel bundling with BACP .....	7
Microsoft CHAP .....	7
SNMP Base MIB II .....	7
Connection controltime-dependent .....	8
General notes .....	8
Changes in the menu .....	8
<b>Enhancements in firmware version 1.50 .....</b>	<b>11</b>
NetBIOS-Proxy .....	11
To the point: What is NetBIOS? .....	11
Handling of NetBIOS packets .....	12
Which preconditions must be fulfilled? .....	12
Linking two Microsoft Networks via ISDN .....	15
Dial-up procedure for a remote access station .....	16
Search and Find: the Network Neighborhood .....	17
The NetBIOS menu .....	18
<b>Enhancements in firmware version 1.70 .....</b>	<b>23</b>
Send network configuration over ISDN .....	23
Obtain DHCP information from the remote network .....	23
Adapt DHCP information.....	24
Obtain boot images from the remote network .....	24
Standard and expert mode for <i>ELSA LANconfig</i> .....	25
Time controller for the default route .....	25
Reserving B channels.....	25
Index.....	27



# Enhancements in firmware version 1.40

## DNS

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

### What does a DNS server do?

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

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

- An *ELSA LANCOM Office* router can automatically distribute IP addresses for the computers in the local network when in DHCP server mode. In other words, the DHCP server already knows the names and IP addresses of all of the computers in its own network that were assigned IP addresses via DHCP. With the dynamic address assignments of a DHCP server, an external DNS server might have difficulties in keeping the associations between the names and IP addresses current.
- When routing Microsoft Networks via NetBIOS, the *ELSA LANCOM Office* router also knows the computer names and IP addresses in the other connected NetBIOS networks. In addition, computers with fixed IP addresses can also enter themselves in the NetBIOS table and thus be known by their names and addresses.
- The DNS server in the *ELSA LANCOM Office* router can also be used as an extremely convenient filter mechanism. Requests for domains can be prohibited throughout the LAN, for subnetworks, or even for individual computers—simply by specifying the domain name.

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

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

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

## Setting up the DNS server

Proceed as follows to set up the DNS server:

- ① Switch the DNS server on.

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

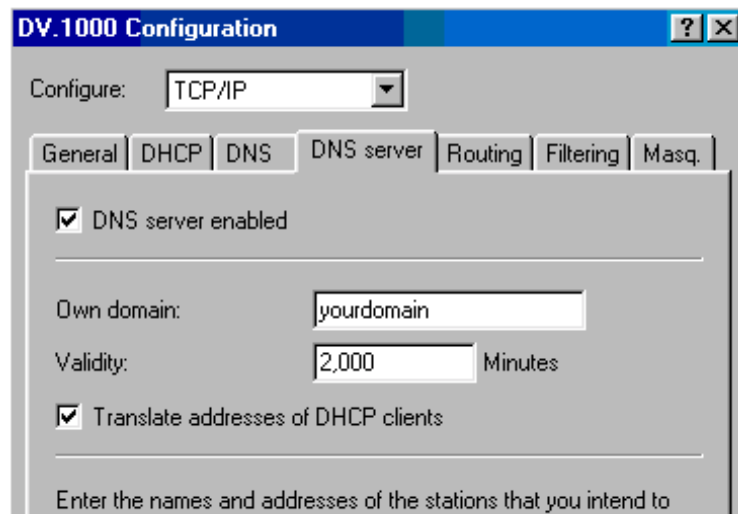
- ② Enter the domain in which the DNS server is located. The DNS server uses this domain to determine whether the requested name is located in the LAN. Entering the domain is optional.

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

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

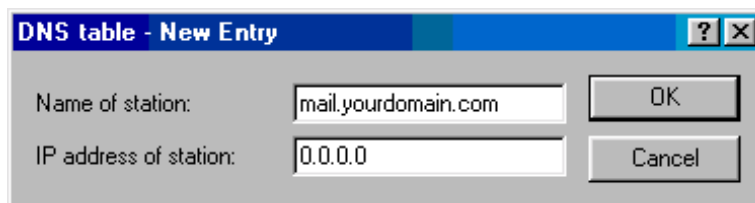
```
set setup/dns-module/dhcp-usage yes
```

```
set setup/dns-module/NetBIOS-usage yes
```



- ④ The main task of the DNS server is to distinguish requests for names in the Internet from those for other remote stations. Therefore, enter all computers into the DNS table
- for which you know the name and IP address,
  - that are not located in your own LAN,
  - that are not on the Internet and
  - that are accessible via the router.

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



```
cd setup/dns-module/dns-table
```

```
set mail.yourdomain.com 10.0.0.99
```

Stating the domain is optional but recommended.

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

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

```
cd setup/dns-module/filter-list
```

```
set 001 www.offlimits-domain.com 0.0.0.0 0.0.0.0
```

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

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







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

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

## The DNS menu

### Setup/DNS module

The settings for the DNS server can be modified here as required. The menu contains the following items (incl. their default settings):

Operating		On (default) or off
Domain		Own domain, optional, 32 characters max.
DHCP-usage		Yes (default) or no
NetBIOS-usage		Yes (default) or no
DNS-table		Static DNS table for the manual association of IP addresses to names, 64 entries
Filter-list		Filter list for the exclusion of prohibited domains, 64 entries

Leasetime



Specifies the name validity information to be given to a requesting computer. Default: 2000

*DNS-table*

The DNS table contains a simple association of local names to IP addresses. The table is sorted alphabetically by names.

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

Host name	IP-Address
HOST10	10.0.0.10

The name is restricted to a maximum of 32 characters. Longer names are not necessarily practical in a local network.

*Filter-list*

The filter list contains the entries for prohibited domains. In addition, it is possible to specify for whom a given domain will be prohibited. This is set using an IP address/net-mask pair. An IP address of 0.0.0.0 prohibits this domain for all computers. A subnet mask of 0.0.0.0 prohibits the domain for all networks. The table has the following structure:

Idx.	Domain	IP-Address	Netmask
F001	*xxx*	0.0.0.0	0.0.0.0

Clear IDs can be freely selected and assigned to the filters in the 'Idx.' field.

Enter the name of the domain to be prohibited in the 'Domain' field. Wildcards such as '?' and '\*' may be used. The wildcard '?' replaces exactly one character, while '\*' can stand for a random number of characters. Multiple instances of the wildcard '\*' can be used. For example, \*xxx\* filters all names containing the letters xxx in any position within the name.











The IP address and subnet mask fields can be used to specify the subnet for which the domain will be prohibited.

The filter table is sorted according to the subnet masks in descending order (the longest at the top); entries with identical subnet masks are sorted according to the IP addresses in ascending order. In the event of identical IP addresses, the entries are sorted in ascending order according to the domain to be prohibited.

The table is searched from top to bottom and an error message is returned to the requesting computer in the event of a match.

### Status/TCP-IP/DNS-statistics

The DNS statistics provide supplementary information about the DNS module. This menu has the following structure:

LAN-Rx		Number of DNS packets received by the LAN
LAN-Tx		Number of DNS packets sent on the LAN
WAN-Rx		Number of DNS packets received by the WAN
WAN-Tx		Number of DNS packets sent on the WAN
Forwarded		Number of requests that could not be fulfilled and were thus forwarded
Errors		Number of invalid requests
DNS-access		Indicates the number of names that were looked up from the DNS table
DHCP-access		Indicates the number of names that were looked up from the DHCP table
NetBIOS-access		Indicates the number of names that were looked up from the Net-BIOS tables
Hit-list		This table contains the 16 most popular requests. These may then be prohibited via the filter list if desired.

The hit list has the following structure:

Domain	Requests	Time	IP-Address
www.elsa.com	1	00.00.0000 00:00:29	10.0.0.123

The individual fields of this list have the following significance:

Domain	Name of the requested computer
Requests	Total number of requests for this name since its appearance in the table
Time	Time of the last request
IP-Address	Address of the computer that last requested this name

This list is sorted according to the frequency of requests. When the table is full, the names that have not been requested for the longest period will be deleted to make room for new entries.



## ELSA CAPI Faxmodem

The *ELSA CAPI Faxmodem* provides a Windows fax driver (Fax Class 1) as an interface between the *ELSA LANCAP*i and applications, permitting the use of standard fax programs with an *ELSA LANCOM Office* router.

### Installation

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

### Faxing with the *ELSA CAPI Faxmodem*

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



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

## Channel bundling with BACP

Channel bundling with BACP is also supported starting with firmware version 1.40.

The BAP (Bandwidth Allocation Protocol) and BACP (Bandwidth Allocation Control Protocol) control the channel assignments of multilink connections. The BACP negotiates the enabling thereof. The actual control activity is then carried out by the BAP. A variety of messages for channel bundling control are available in the second protocol, BAP.

## Microsoft CHAP

The verification of the remote station in accordance with Microsoft CHAP is also supported as of firmware version 1.40. No changes have been made that affect the function or operation of the remote station verification.

## SNMP Base MIB II

The configuration via SNMP also supports MIB II as of firmware version 1.40.

## Connection controltime-dependent

### General notes

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

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

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

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



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



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











*Only the router functions are protected by the charge and time monitoring functions! Connections via LANCAPI or the a/b ports are not affected.*

### Changes in the menu

The Setup/Charges-module menu item contains the configuration menus for monitoring online time and connect charges, as well as for controlling call establishment.

Day(s)/period		Length of a period in days
Budget-units		Units available for each period

Spare-units		Remaining number of available units
Router-units		Number of units used by the router modules
Total-units		Total number of units used by the device
Minutes-budget		Minutes available for each period
Spare-minutes		Remaining number of available minutes
Router-minutes		Number of minutes used by the router modules
Table-budget		Itemization of the local charge budgets for the individual interfaces
Time-table		Itemization of the local time budgets for the individual interfaces

**Day(s)/period** This item defines the number of days after which the remaining charge and time budgets are reset to their full values. In other words, the duration of the monitoring period in days can be specified here. The calling charges reported via the D channel and the connection times of the router are both monitored.

**Budget-units**  
**Minutes-budget** Use this item to set the number of charge units or online minutes that can be used in a monitoring period before the router is locked to prevent the establishment of further connections. Connections that are open when the charge lock is activated will be closed. The active lock is signaled by the blinking power LED on the front panel of the unit. Setting any of these values to zero will disable the associated monitoring function!

**Spare-units**  
**Spare-minutes** These values indicate the number of units or online minutes still available in the current monitoring period. The first value to reach zero will lock the router.

**Router-units**  
**Router-minutes** These values log the total number of units or online minutes used by the router for all monitoring periods. These two values are not recorded by the monitoring system.

**Total-units** This value represents the total number of charge units reported by the D channel. The following functions are included in this value: the router, the *LANCAPI*, the time module, and (for the *LANCOM 2000 Office*) the a/b ports.

**Table-budget**  
**Time-table** The following two tables provide detailed time and charge information for the individual modules (router, *LANCAPI*, time module and a/b ports). Only the router has a budget and a value for remaining units, being the only module protected by the charge monitor. The online times of the *LANCAPI*, the time module and the a/b ports are not recorded for this reason.

Ifc	Budget-units	Spare-budget	Total-units
Router	830	830	0
LANCAPI	0	0	0
ab-1	0	0	0
ab-2	0	0	0
ab-3	0	0	0

lfc	Budget-units	Spare-budget	Total-units
ab-4	0	0	0
Time module	0	0	0

lfc	Budget minutes	Spare-minutes	Total-minutes
Router	210	12	465
LANCAPI	0	0	0
ab-1	0	0	0
ab-2	0	0	0
ab-3	0	0	0
ab-4	0	0	0
Time module	0	0	0

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

# Enhancements in firmware version 1.50

## NetBIOS-Proxy

Starting with firmware version 1.50, a *ELSA LANCOM Office* router can also route NetBIOS packets or answer them locally as a proxy. As a result, it is now possible to economically link Microsoft Networks using the router function.

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

### To the point: What is NetBIOS?

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

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

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

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

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

## Handling of NetBIOS packets

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

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

- In the NetBIOS module, it is possible to specify the remote stations to which the name information should be transferred via NetBIOS to ensure the routing of those packets that are actually required. After the NetBIOS module has been switched on and an unspecified waiting time has elapsed, a connection is established to the NetBIOS remote stations (insofar as these are not individual Remote Access workstations). The duration of the waiting period will be increased if the connection cannot be established. The following exchange of NetBIOS information then fills the billboard for the first time.
- In its proxy function, the unit answers queries to computers already known in the NetBIOS module (on the billboard) by proxy for those computers. After the initial exchange of information, no new connections are established as a result of queries to workstations in the local network, or to known workstations in the remote network.

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

## Which preconditions must be fulfilled?

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

### Installed components

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

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



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

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

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

#### ■ Client

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

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

#### ■ Service

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

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

### Microsoft Network settings

#### ■ Name and group designation

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

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

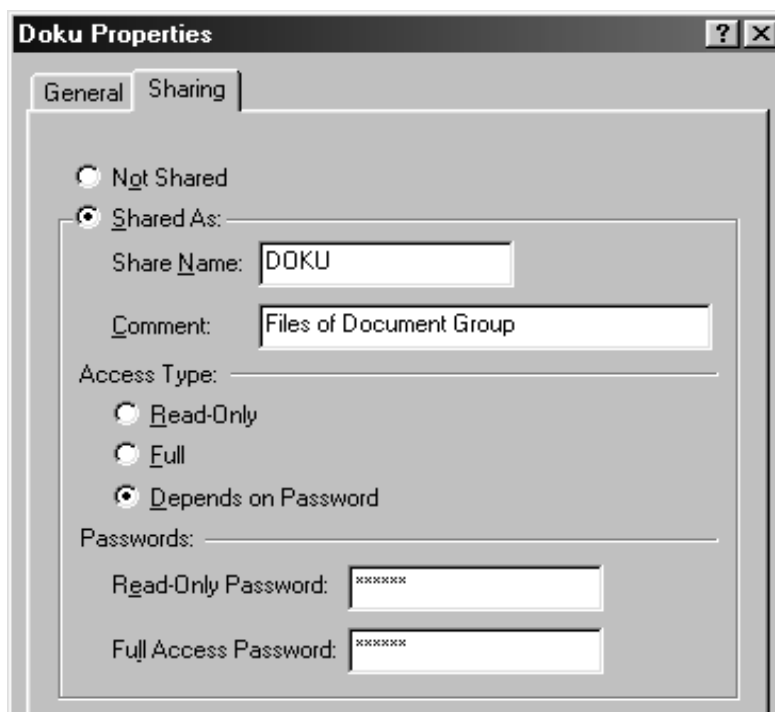
■ File and printer sharing

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



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

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



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



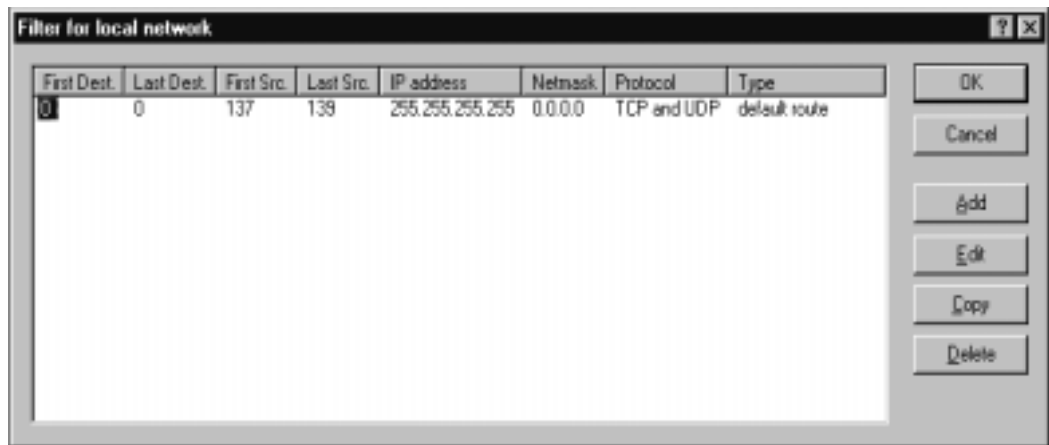


*It's easy to check whether the Microsoft Network settings have been made correctly: the local computer must appear with its name in the Network Neighborhood.*

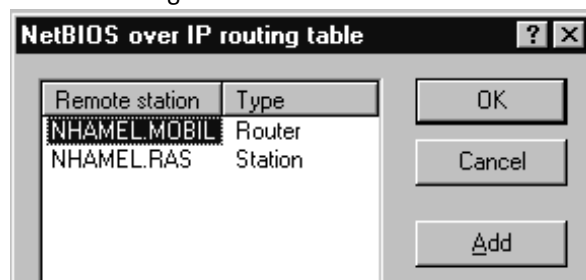
## Linking two Microsoft Networks via ISDN

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

- ① Set up both networks for a LAN-LAN interconnection via TCP/IP as described in the Workshop. We recommend using the convenient *ELSA LANconfig* wizard.
- ② Check the settings of the IP filter. This filter must capture all NetBIOS packets to be sent over the DEFAULT route to ensure that they do not lead the establishment of a connection on the DEFAULT route. This has been preset in the unit's factory defaults.



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



Alternatively, enter the following when configuring via telnet:

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

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



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

- ④ Once all remote stations have been entered, activate the NetBIOS function.

```
cd /Setup/NetBIOS-module
```

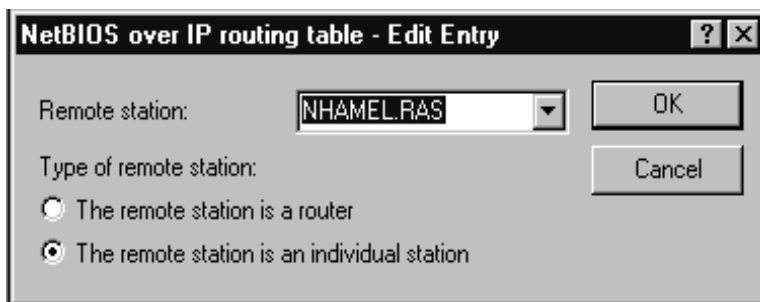
```
set operating on
```

After switching the module on, a connection is established after an unspecified waiting time to all remote stations not identified as dial-up nodes. The required information regarding the other computers in the networks is then exchanged during this initial connection. Computers on the remote side cannot be accessed until this operation is complete.

## Dial-up procedure for a remote access station

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

- ① The *ELSA LANCOM Office* router and the remote access computer must be prepared for network access as described in the Workshop. The IP filters in the *ELSA LANCOM Office* router must also be checked in this case (see 'Linking two Microsoft Networks via ISDN', page 15).
- ② Also create an entry for the remote stations in the NetBIOS IP routing table.



```
cd /Setup/NetBIOS-module/Remote-table
```

```
set nhamel.ras workstation
```



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

## Search and find: the network neighborhood

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

## NetBIOS routing via LAN-LAN interconnections

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

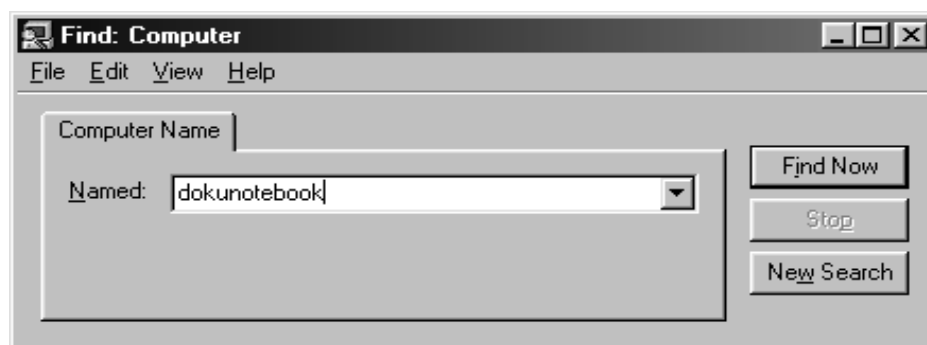
```
dir /Setup/NetBIOS-module/Host-list
```

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

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

This table shows, for example, that the computer named 'DOKUNOTEBOOK' with the IP address '10.10.0.53' is available via the remote station 'NHAMEL.MOBIL'. The further parameters are covered in the description of the menus ('The NetBIOS menu', page 18).

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



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

## NetBIOS routing via RAS

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








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

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

## The NetBIOS menu

### Setup/NetBIOS

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

Operating		On or off
Scope-ID		NetBIOS scope in which the router is located.
NT-Domain		Workgroup/domain in which the router is located.
Remote-table		All remote stations must be entered in the remote-station table together with their NetBIOS information.
Group-list		All workgroups known to NetBIOS are recorded in the group list.
Host-list		All computer names known to NetBIOS are recorded in the host list.
Server-list		All servers that have logged onto the network are recorded in the server list.

#### Scope-ID

The Scope-ID menu item can be used to specify the NetBIOS scope in which the device is located. It then sees only those NetBIOS packets originating in the same NetBIOS scope; all other packets are automatically rejected. The scope ID is only used in conjunction with Windows name servers (WINS). This entry can generally be left blank.

#### NT-Domain

A workgroup/domain can be specified in the NT domain item to trigger the search procedure when starting the NetBIOS module. This is required if the network does not contain any computers running Windows 95 or Windows 98.

#### Remote-table

All remote stations that are to provide or receive NetBIOS information must be entered in the remote-table. When the NetBIOS module is switched on, NetBIOS packets from

remote stations other than those specified will be rejected automatically. The remote-table has the following structure:

Idx.	Type
Glasgow	Router or workstation

#### Type

The 'Type' field specifies whether the remote station is a router or a workstation. In the case of a workstation, all of the known names and servers in the local network and all other connected routers are logged off and deleted from their respective tables as soon as the connection to the remote station is closed.

#### Host table

The host table has the following structure:

Idx.	Type	IP-Address	Remote-station	Timeout	Flags
REMOTE	00	10.0.1.100	Glasgow	5000	xx20
WORKSTATION	00	10.0.0.10		5000	xx00

#### Group table

The group table thus looks like this:

Group/Domain	Type	IP-Address	Remote-station	Timeout	Flags
WORKGROUP	1e	10.0.0.10		5000	xx00
WORKGROUP	1e	10.0.1.100	Glasgow	5000	xx20

The fields of the table have the following significance:

Idx.	Name of the host in the host table.
Group/Domain	Name of the group or domain in the group list. Groups and NT domains are handled in the same manner from the NetBIOS point of view.
Type	WINS type of the host. The type is not relevant for NetBIOS, but Microsoft Networks assign certain properties to the name on the basis of the type.
IP-Address	IP address of the owner of the name. The same name can be assigned to multiple IP addresses in the group list.
Remote-station	Name of the remote station for which the name became known.
Timeout	Time until the name is no longer valid. The time-out is also associated with an aging counter in the flags.
Flags	The flags contain additional information pertaining to the name.

*Flags*

The flags have the following significance:

0x0003	This counter increments up each time the validity expires. The entry will be deleted if the name is not refreshed after the second expiration at the latest.
0x0004	This identifies an entry that still needs to be transferred.
0x0008	This identifies an entry that is queued for deletion, i.e. the name has not yet been refreshed after the establishment of a connection.
0x0010	Reserved
0x0020	This identifies a remote station.
0x0040	Reserved
0x0080	Reserved

The server list has the following structure:

Host	Group/ Domain	UPD	IP- Address	OS- Ver	SMB- Ver	Server- type	Remote -station	Timeout	Flags
REMOTE	WORKGROUP	00	10.0.1.100	0400	010f	0004140b	Glasgow	13	0020
WORKSTATION	WORKGROUP	07	10.0.0.10	0400	0415	00452003		31	0000












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

The individual fields have the following significance:

Host	Name of the server
Group/Domain	Workgroup or domain in which the server is located
UPD	Update counter: indicates the number of times that the server has already propagated itself
IP-Address	Address of the server
OS- Ver	Operating system version number
SMB- Ver	Version number of the SMB protocol used
Server- type	Bit mask in which the services of the server are coded
Remote-station	Name of the remote station from which the server was announced
Timeout	Time until the entry loses its validity (for entries from the LAN) or time until the router propagates a remote entry
Flags	Corresponds to the flags in the host or group tables

## Status/TCP-IP-statistics/NetBIOS

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

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

- B-Nodes* Broadcast nodes. A B node performs name negotiations exclusively via broadcasts. Such a computer is not visible over a router connection, since broadcasts may not be routed.
- P-Nodes* Point-to-point nodes. For name negotiations, a P node requires a NetBIOS nameserver (NBNS) as well as a NetBIOS datagram distribution server (NBDD) to transfer datagrams over a router.
- M-Nodes* Mixed nodes. This type is a mixture of B and P nodes. It acts as a B node in the local network; if the required partner can't be found in the local network, it attempts to locate it using an NBNS query (P node behavior).
- W-Nodes* This type of node is not permissible according to RFC, but was introduced nevertheless by Microsoft as a hybrid node.





# Enhancements in firmware version 1.70

## Send network configuration over ISDN

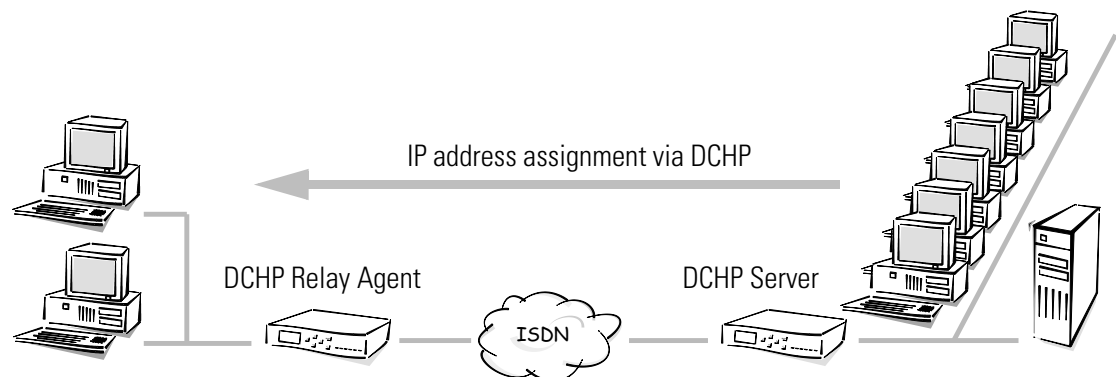
Generally the Proxy ARP function is used to link individual workstations to the LAN of a central office via IP. For this purpose a previously specified IP address from the address range of the central office is assigned to the dialing-in computer.

If an entire branch IP network with a number of computers is to be linked to a central office LAN, a LAN-LAN coupling is implemented. Here, however, the two networks will be in different IP address groups.

While all addresses and other network information can easily be assigned via DHCP within the central office LANs, the LAN-LAN coupling is not so simple.

## Obtain DHCP information from the remote network

The "DHCP Relay Agent" function also enables DHCP information to be sent over ISDN lines. This also makes it possible to link a number of computers in a network into the central office IP address group over an ISDN line.



To enable this the DHCP server is integrated into the branch network in the relay agent mode. The DHCP queries will then be forwarded to another server, whose address will be fixed. The connection to the network is implemented with an appropriate entry in the IP routing table.

If a computer that requests an IP address from a DHCP server is started now in the central office network, the DHCP relay agent will forward this request to the DHCP server in the central office network over the ISDN line. This server then gives the requesting computer a previously specified IP address based on the transmitted MAC address.

The preceding has covered all required settings:

- ① The DHCP server in the router of the branch network is set to forward the DHCP queries. The IP address of the DHCP servers is set in the central office LAN for this purpose.

- ② In addition, this router must have all information for establishing a connection with the central office network (standard LAN-LAN coupling).
- ③ As well the standard routing information, the DHCP server in the central office will have the MAC addresses and the IP addresses that are to be assigned to all the remote stations. The name of the corresponding computer for which the DNS server is to be used will be entered for this purpose.

## Adapt DHCP information

Now all DHCP information is brought to the DHCP server in the central office. However, this results in the router in the central office acting as the gateway for the branch. If a computer in the branch wishes to access the Internet, the query will be forwarded to the gateway in the central office. The Internet connection is therefore via the central office network. To avoid this detour, the DHCP relay agent can use a function that allows the responses from the remote DHCP servers to be adapted to the requirements of their own LANs. Network mask, broadcast address and gateway will then no longer be taken from the central office network.

## Obtain boot images from the remote network

To link branch networks that do not have full workstations but only terminals without bootable hard disks, the DHCP server also provides the capacity of obtaining a complete boot image over the ISDN line. This enables the entire terminal configuration to be maintained and serviced at one central point.

The DHCP relay agent in the branch network is configured for this. In the central office network, in addition to the IP address entries for the specific MAC address, the boot image that must be used is specified. The boot image is input via a symbolic name. The symbolic name is assigned to a server in an image table with information on the directory and files with which the boot image can be found.

If a terminal in the branch network is started, it automatically establishes a connection to the central office network via the router and obtains the current boot image from there.

You can find the settings for the DHCP relay agent, the associated server and the boot images in *ELSA LANconfig* in the 'TCP/IP' configuration area on the 'DHCP' and 'DHCP/BOOTP' registry tabs or in the case of configuration via Telnet in `setup/DHCP-module`.

## Standard and expert mode for *ELSA LANconfig*

The configuration program *ELSA LANconfig* has two different display modes:

- The standard display of the configuration shows only the settings required for standard applications.
- The complete configuration display shows all available settings. Only experienced users should change some of them.

Toggle between the two display modes with **View ► Options**.

## Time controller for the default route

Similar to the least cost routing (LCR), the time controller for the default route is a function that automatically selects the provider with the best rate depending on the time.

As soon as an IP packet requires a connection over the default route, the remote station entered in the default route is not dialled until the remote station that is to be used has been checked in the time controller table.

You enter the days of the week and the times of the day on which a specific provider must be used into this time controller table. As soon as an IP packet requests the default route, a check is first made in the time controller table of whether its use is enabled. Then a search for an entry that covers the current day and time is made in the table. If a relevant entry is found, the router establishes a connection to the remote stations found there. If there is no appropriate entry in the time controller table, the router returns to the IP routing table and uses the remote station entered there.

You can find the settings for the default route time controller in *ELSA LANconfig* in the 'IP router' configuration section on the 'Routing' registry tabs and for configuration via Telnet in `setup/IP-router-module`. The days are entered in the same syntax as with the LCR. The definition of the holidays is also taken from the LCR module.

## Reserving B channels

The reserving of B channels is intended to enable incoming and outgoing calls at any time and therefore to be available for external remote stations at any time or to be able to make calls at any time.

To enable this, the maximum number of connections that can be made simultaneously on one interface divided into incoming and outgoing calls is specified for every  $S_0$  interface.

*The limit on the number of connections is based on all operating modes of the device, i.e. on router, LANCAP, any available a/b ports etc.*



The values for B-channel reserving are entered in the interface table as maximum value for incoming and outgoing connections:

- By default both values are set to 2. This enables two parallel outgoing connections to be established and also two incoming calls to be answered.
- If the value for the maximum number of incoming calls is set to 1, the device can only answer one call in this interface. If another call comes in, it will be rejected, even though a B-channel may still be free. However, this channel will then be reserved for outgoing calls. This principal also applies to the maximum number of outgoing calls.
- If the value for the maximum number of incoming calls is set to 0, no calls can be answered at this interface. Only the maximum number of allowable outgoing connections can be established.



*If both values are 0, a connection can no longer be established at this interface at all.*

You can find the settings for the B-channel reserving in *ELSA LANconfig* in the 'Management' configuration section on the 'Interfaces' registry tabs and for configuration via Telnet in `setup/WAN-module/Interface-list`.

# Index

## A

Access Type .....	14
Available workstations .....	17

## B

BACP .....	7
Bandwidth Allocation Control Protocol .....	7
Bandwidth Allocation Protocol .....	7
BAP .....	7
B-channel reserving .....	26
Boot images .....	24

## C

Call establishment .....	12
CAPI Faxmodem .....	7
Channel bundling .....	7
Charge units .....	8
Charges .....	8
Computer names .....	1, 11
Connect charges .....	12
Connection control .....	8

## D

Default route .....	25
DHCP .....	23
DHCP Relay Agent .....	23
DHCP Server .....	23
Display .....	25
DNS .....	1
DNS forwarding mechanism .....	2
DNS server .....	1
available information .....	2
filter list .....	4
filter mechanism .....	1
Domain name service .....	1
Domains .....	1

## E

Expert mode .....	25
-------------------	----

## F

Fax .....	7
Fax Class 1 .....	7

Fax driver .....	7
Fax transmission .....	7
Faxmodem .....	
LANCAPI .....	7
File and printer sharing .....	13
firmware version 1.40 .....	11

## G

Gateway .....	24
Group table .....	19
Groups .....	11

## H

High telephone charges .....	8
Host .....	1
Host table .....	19

## I

Identifikation .....	13
IP filter .....	12
ISDN dial-up connections .....	8

## L

LCR .....	25
Least-cost router .....	25
Limiting charges .....	8

## M

MAC address .....	23
Mail server .....	3
MIB II .....	7
Microsoft Network .....	11
Microsoft Network client .....	13
Microsoft Networking .....	17
MS-CHAP .....	7
Multilink connections .....	7

## N

Name and group designation .....	13
Name information .....	12
Names .....	11
NBNS .....	11
NetBIOS .....	1
IP filter .....	15
LAN-LAN interconnection .....	15
network protocol .....	12

remote access .....	16
remote station .....	15
TCP/IP .....	13
NetBIOS nameserver .....	11
NetBIOS networks .....	1
NetBIOS ports .....	12
NetBIOS remote stations .....	12
NetBIOS-Proxy .....	11
Network names .....	1
Network Neighborhood .....	17
No charge information .....	8
NT domain .....	18

**P**

Passwords .....	14
Period .....	8
Prohibiting domains .....	4
Provider .....	25
Proxy ARP .....	23

**R**

Remote Access .....	12
Remote station verification .....	7
Remote-table .....	18
Reserving .....	25
Routing .....	12
Routing Microsoft Networks .....	11

**S**

S0 interface .....	25
Scope ID .....	18
Scopes .....	11
Server list .....	20
Service .....	1
Shared resources .....	14
SNMP .....	7
Standard fax programs .....	7
Standard mode .....	25

**T**

TCP/IP networks .....	1
Terminal .....	24
Time budget .....	8
Time controller .....	25
Time controller table .....	25
Time-dependent connection control .....	8

**V**

Verification of the remote station .....	7
--	---

**W**

Wildcards .....	4
Windows Internet Name Service server .....	11
WINS server .....	11