

■ ***ELSA LANCOM™ Business***

Handbuch

© 1999 ELSA AG, Aachen (Germany)

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. ELSA haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von ELSA gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Marken

Windows®, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Das ELSA-Logo ist eine eingetragene Marke der ELSA AG.

ELSA behält sich vor, die genannten Daten ohne Ankündigung zu ändern, und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

ELSA AG

Sonnenweg 11

D-52070 Aachen

www.elsa.de

Aachen, Juli 1999

Art.-Nr. 20856/0799

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Mit dem *ELSA LANCOM Business* haben Sie sich für einen Router entschieden, mit dem Sie lokale Netzwerke oder einzelne Arbeitsplatzrechner mit anderen Netzwerken über ISDN-Verbindungen koppeln können.

Höchste Qualitätsanforderungen in der Fertigung und eine enggefaßte Qualitätskontrolle bilden die Basis für den hohen Produktstandard und sind Voraussetzung für gleichbleibende Qualität der ELSA-Produkte.

Dokumentation

Die beiliegende Dokumentation besteht aus:

- Installation Guide
Hardware-Installation und erste Konfigurationsbeispiele
- Handbuch
Ausführliche Beschreibung der Router-Funktionen und -Betriebsarten
- elektronischer Dokumentation auf CD
Referenzteil zum Nachschlagen, vollständige Beschreibung der Menüs

An der Erstellung dieser Dokumentation haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres ELSA-Produktes anzubieten.

Sollten Sie dennoch einen Fehler finden, oder Sie möchten einfach eine Kritik oder Anregung zu dieser Dokumentation äußern, senden Sie bitte eine E-Mail direkt an:



Lancom.doku@elsa.de



Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, stehen Ihnen unsere Online-Dienste (Internet-Server www.elsa.de und ELSA LocalWeb) rund um die Uhr zur Verfügung. Hier finden Sie im Dateibereich 'Support' unter 'Know-how' viele Antworten auf „häufig gestellte Fragen“. Darüber hinaus bietet Ihnen die Wissensdatenbank (KnowledgeBase) einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Handbücher stehen Ihnen jederzeit zum Download bereit.

Die KnowledgeBase ist auch auf der CD enthalten. Starten Sie dazu die Datei \Misc\Support\MISC\ELASIDE\index.htm

Inhalt

Einleitung	1
Was macht ein Router überhaupt?	1
Was bietet ein <i>ELSA LANCOM Business</i> ?	3
Wie sieht das Gerät aus?	8
Power/Msg.	8
Node oder Hub?	10
CE-Konformität	10
Konfigurationsmöglichkeiten	13
Viele Wege führen zum <i>ELSA LANCOM</i>	13
Der direkte Weg: Outband	13
Voraussetzungen für die Outband-Konfiguration	14
Outband-Konfiguration mit <i>ELSA LANconfig</i>	14
Outband-Konfiguration mit Terminalprogramm	14
Der komfortable Weg: Inband	15
Voraussetzungen für die Inband-Konfiguration	15
Alternativ: Adreßverwaltung mit dem DHCP-Server	15
Starten der Inband-Konfiguration über <i>ELSA LANconfig</i>	15
Starten der Inband-Konfiguration über Telnet	16
Der Fernzugang: Konfiguration über DFÜ-Netzwerk	16
Das brauchen Sie für die Fernkonfiguration	17
So bereiten Sie die Fernkonfiguration vor	17
Die erste Fernverbindung mit DFÜ-Netzwerk (<i>ELSA LANconfig</i>)	17
Die erste Fernverbindung mit PPP-Client und Telnet	17
Fernkonfiguration einschränken	18
Befehle für die Konfiguration	20
Neue Firmware mit FirmSafe	21
So funktioniert FirmSafe	21
So spielen Sie eine neue Software ein	22
Konfiguration über SNMP	25
Allgemeines	25
Zugriff auf Tabellen und Parameter über SNMP	25
Die Management-Information-Base (MIB)	27
Was ist los auf der Leitung?	29
Trace-Ausgaben	29
<i>ELSA LANmonitor</i>	31
.....	33
Funktionen und Betriebsarten	35
Sicherheit für Ihre Konfiguration	35

Paßwortschutz.....	36
Die Login-Sperre	36
Zugangskontrolle über TCP/IP.....	36
Sicherheit für Ihr LAN	37
Die Kontrolle	37
Der Rückruf.....	38
Das Versteck – IP-Masquerading (NAT, PAT).....	39
Gebührenmanagement	39
Gebührenabhängige Verbindungsbegrenzung.....	39
Zeitabhängige Verbindungsbegrenzung	40
Einstellungen im Gebührenmodul.....	40
ISDN-Verbindungen	41
Namenliste.....	41
Interface-Einstellungen.....	42
Router-Interface-Einstellungen.....	43
LANCAPI-Interface-Einstellungen.....	43
Layer-Liste.....	44
Round-Robin-Liste.....	45
Kanal-Liste	45
PPP-Liste.....	46
Script	47
Rufannahme	47
Nummernliste.....	48
Festverbindungen und Backup.....	48
So stellen Sie die Festverbindung ein	48
Einwahl über GSM.....	51
Point-to-Point Protocol.....	51
Das Protokoll	51
Die PPP-Liste	53
Alles o.k.? Leitungsüberprüfung mit LCP	54
Zuweisung von IP-Adressen über PPP	55
Rückruf-Funktionen	56
Schneller Rückruf nach ELSA.....	59
Rückruf nach RFC 1570 (PPP LCP Extensions).....	59
Kanalbündelung mit MLPPP	60
IPX-Routing	62
IPX-Adressierung.....	62
Informationen über das LAN.....	62
IPX-Routing-Tabelle	63
Was passiert bei der Datenübertragung im IPX-Netz?.....	64
RIP- und SAP-Tabellen	64
So viele Router hier	65
Redundante Routen.....	65

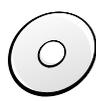
Exponential-Backoff	65
Filter für die IPX-Pakete	66
IP-Routing.....	68
Die IP-Routing-Tabelle	68
Filter für die TCP/IP-Pakete.....	71
Proxy-ARP	71
Lokales Routing.....	72
Dynamisches Routing mit IP-RIP.....	73
IP-Masquerading (NAT, PAT)	75
DNS-Forwarding.....	77
Policy Based Routing.....	78
Automatische Adreßverwaltung mit DHCP	78
Der Router als DHCP-Server	79
DHCP – 'Ein', 'Aus' oder 'Auto'?.....	79
So werden die Adressen zugewiesen.....	80
Konfiguration der Router als DHCP-Server	83
DNS.....	86
Was macht ein DNS-Server?	86
So stellen Sie den DNS-Server ein.....	87
NetBIOS-Proxy	89
Kurz und bündig: Was ist NetBIOS?	89
Behandlung von NetBIOS-Paketen	90
Welche Voraussetzungen müssen erfüllt sein?.....	91
So verbinden Sie zwei Windows-Netze über ISDN.....	94
So wählt sich ein Remote-Access-Rechner ein.....	95
Gesucht - Gefunden: Die Netzwerkumgebung	96
IP-Pooling für Einwahlzugänge	97
Bürokommunikation und <i>ELSA LANCAPI</i>	97
<i>ELSA LANCAPI</i>	98
<i>ELSA CAPI Faxmodem</i>	102
Installation	102
Faxen über <i>ELSA CAPI Faxmodem</i>	102
Der Least-Cost-Router	102
Workshop	109
Internet-Anwendungen.....	110
Internet für alle PCs im LAN	111
Intranet mit eigenem Web-Server im Internet	115
LAN-LAN-Kopplungen.....	120
Netze verbinden mit dem IP-Router.....	121
Netze verbinden mit dem IPX-Router	127
Remote-Access	131
Least-Cost-Router	138

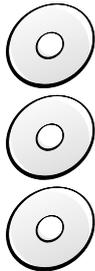
Anhang	143
Technische Daten	143
Steckerbelegungen:	144
Allgemeine Garantiebedingungen vom 01.06.1998	145
Konformitätserklärung	147

Glossar	149
----------------------	------------

Index	157
--------------------	------------

Beschreibung der Menüpunkte (nur auf CD)	R-1
Status	R-3
Display und Tastatur	R-4
Status/Verbindung	R-5
Status/Aktuelle-Zeit	R-6
Status/Betriebszeit	R-6
Status/S0-Bus	R-6
Status/WAN-Statistik	R-6
Status/LAN-Statistik	R-9
Status/PPP-Statistik	R-10
Status/IPX-Statistik	R-18
Status/TCP-IP-Statistik	R-22
Status/IP-Router-Statistik	R-28
Status/Config-Statistik	R-30
Status/Queue-Statistik	R-31
Status/Verbindungs-Statistik	R-32
Status/Info-Verbindung	R-33
Status/Layer-Verbindung	R-33
Status/Ruf-Info-Tabelle	R-34
Status/Gegenstellen-Statistik	R-34
Status/Kanal-Statistik	R-35
Status/Zeit-Statistik	R-36
Status/LCR-Statistik	R-37
Status/Werte löschen	R-37
Setup	R-38
Setup/WAN-Modul	R-39
Setup/LAN-Modul	R-50
Setup/IPX-Modul	R-51
Setup/TCP-IP-Modul	R-60
Setup/IP-Router-Modul	R-63
Setup/SNMP-Modul	R-71
Setup/DHCP-Server-Modul	R-72
Setup/NetBIOS	R-75
Setup/Config-Modul	R-77





Setup/LANCAPI-Modul	R-78
Setup/LCR-Modul.....	R-80
Setup/DNS-Modul	R-81
Setup/Zeit-Modul.....	R-82
Firmware	R-83
Sonstiges	R-85
<hr/>	
Novell SAP-Nummern	R-87
<hr/>	
TCP/IP-Ports	R-91
<hr/>	
ELSA LANCOM Business intern	R-95
Script-Verarbeitung.....	R-95
Allgemeines	R-95
Die Script-Liste.....	R-96
Compuserve-Anwahl.....	R-96
Online-Trace-Ausgaben	R-97
Allgemeines	R-97
Bedienung der Trace-Ausgaben.....	R-98
Beispiele zur Bedienung der Trace-Ausgaben.....	R-99
Unterstützte Protokolle und Funktionen.....	R-99
Policy Based Routing	R-110
Allgemeines	R-110
Beispiele.....	R-111

Einleitung

Mit den heutigen Mitteln moderner Kommunikation werden Internet- und Intranet-Anwendungen für Unternehmen aus verschiedenen Branchen immer wichtiger. Online-Dienste werden mehr und mehr professionell genutzt. Filialen sind miteinander verbunden, damit eine schnelle Kommunikation zwischen den unterschiedlichen Standorten möglich ist, und auch Telearbeit gewinnt immer mehr an Bedeutung.

All diese Anwendungen machen den Einsatz von ISDN-Routerlösungen attraktiver denn je. ISDN-Router von ELSA verbinden lokale Netze mit dem Internet und bilden in kleinen und mittleren Unternehmen die Kommunikations-Zentrale, über die Aufgaben wie Fax und Anrufbeantworter erledigt werden.

Außerdem verbinden die Router die lokalen Netze mit anderen LANs (Local Area Networks) und ermöglichen den Zugang zu den Firmendaten über Remote-Access.

Was macht ein Router überhaupt?

Mit einem Router werden lokale Netzwerke (LANs) und Einzel-PCs verbunden und bilden so gemeinsam ein Wide Area Network (WAN). Jeder Rechner in diesem WAN kann dann je nach Berechtigung auf die Rechner und Dienste im gesamten Netz zugreifen. Der Router sucht dabei einen Weg, über den die Daten zwischen den Rechnern ausgetauscht werden können. Dieser Weg steht in Form einer ISDN-Verbindung bereit.

Eine besonders weit verbreitete Form der Netzwerk-Verbindung stellt der Anschluß an das Internet dar. Wenn das lokale Netz in einer Firma mit dem Netz eines Internet-Service-Providers verbunden wird, können alle Rechner im LAN auf die Dienste und Angebote im World Wide Web zugreifen.

Aber die Router können noch mehr. Über eine spezielle Schnittstelle, die *ELSA LANCAPI*, können moderne Bürokommunikationsfunktionen wie Fax, Anrufbeantworter, Online-Banking etc. im gesamten lokalen Netz angeboten werden. Die entsprechenden Kommunikationsprogramme geben die Daten dabei über die *LANCAPI* an den Router weiter, der dann für die Datenübertragung sorgt. Eine kostspielige und wartungsintensive Ausstattung der einzelnen Arbeitsplätze mit eigenen Datenübertragungsendgeräten entfällt dadurch völlig.

Der Router wird wie ein normaler PC in das lokale Netz eingebunden. Alle Daten, die über die Verkabelung des Netzwerkes fließen, kommen damit auch beim Router an. Er entscheidet dann selbständig, ob Daten in ein anderes Netzwerk übertragen werden müssen. Bei Bedarf stellt er automatisch die Verbindung zur Gegenstelle her. Bei der Verwendung von Standleitungen entfällt natürlich der Verbindungsaufbau.

Wann setzen Sie Router nun ganz konkret ein?

Eigentlich immer dann, wenn Rechner miteinander verbunden werden sollen und ein reiner Modem-Betrieb nicht mehr ausreicht. Das sind z.B. die folgenden Anwendungen:

■ Internet im LAN

In vielen Unternehmen wächst die Forderung nach dem Zugriff auf das Internet von allen Arbeitsplätzen im LAN. Online-Recherchen, Filetransfer und E-Mail sind nur einige der Anwendungen, die den Anwendern am PC die Arbeit erleichtern sollen.

Ein Router verbindet alle Arbeitsplatzrechner in Ihrem lokalen Netz mit dem globalen Internet. Sicherheitsfunktionen wie IP-Masquerading sparen dabei nicht nur Kosten, sondern schirmen Ihr Netz auch gegen Zugriff von außen ab.

■ LAN-LAN-Kopplung

Wenn die Geschäfte so richtig laufen, wird es langsam Zeit für eine Tochtergesellschaft oder eine Niederlassung in den globalen Märkten. Auch die Filiale hat natürlich ihr eigenes Netz und möchte immer auf dem laufenden sein.

Die LAN-LAN-Kopplung verbindet die einzelnen LANs zu einem großen Netzwerk, wenn es sein muß, über Kontinente hinweg. Bei Verbindungen über Wählleitungen sorgt eine intelligentes Line-Management im Zusammenspiel mit ausgefeilten Filtermechanismen für geringe Verbindungskosten. Natürlich ist auch der Betrieb über Festverbindungen, auch in Kombination mit Wählleitungen, möglich.

■ Teleworking mit Remote-Access

Die Arbeit vieler Mitarbeiter in modernen Organisationen wird immer unabhängiger von bestimmten Orten – wichtig ist vor allem der ständige Zugriff auf gemeinsame, frei verfügbare Informationen.

Remote-Access heißt hier das Zauberwort. Teleworking für die Kollegen im Home-Office oder Kontakt zur Zentrale für Außendienst-Mitarbeiter von unterwegs werden über den Router im lokalen Netz der Zentrale ermöglicht. Auch beim Remote-Access tut ein *ELSA LANCOM* natürlich alles für den Schutz der firmeneigenen Datenbestände: Die Rückruffunktion über eingetragene Namen und Rufnummern gibt nur bestimmten Personen den Sesam-öffne-dich-Schlüssel. Und für die leichtere Abrechnung werden damit die Telefonkosten in der Firma zentral erfaßt.

■ Bürokommunikation über *LANCAPI*

Faxen direkt aus den Anwendungen heraus, Anrufbeantworter mit unterschiedlichen Ansagetexten je nach Tageszeit und Bankgeschäfte erledigen, ohne das Büro zu verlassen: Diese Funktionen werden ermöglicht durch den Einsatz der *LANCAPI*.

Die *LANCAPI* ist eine spezielle Form der CAPI-2.0-Schnittstelle, über die Anwendungsprogramme wie *ELSA-RVS-COM* oder *ELSA-ZOC* auf den Router zugreifen können.

- Einwahlknoten für Internet-Provider
Mit den vier verfügbaren S_0 -Anschlüssen, also acht B-Kanälen bietet sich ein *ELSA LANCOM Business* auch als Einwahl-Gerät für Provider an. Mit der Funktion des IP-Pooling wird auch die Verwaltung von vielen remoten Gegenstellen, die sich beim Router einwählen können, zur komfortablen Angelegenheit.

Was bietet ein *ELSA LANCOM Business*?

Um Ihnen einen kleinen Überblick über die Leistungsfähigkeit Ihres Geräts zu geben, sind im folgenden die wesentlichen Eigenschaften aufgeführt.

Einfache Installation

- *ELSA LANCOM* mit Spannung versorgen
- Verbindung zum LAN herstellen
- ISDN-Kabel einstecken
- Einschalten
- Loslegen

LAN-Anschluß

ISDN-Router von ELSA arbeiten im Ethernet. Ein *ELSA LANCOM Business* wird über den 10/100Base-TX-Anschluß an ein (Fast-)Ethernet angeschlossen.

WAN-Anschluß

Ein *ELSA LANCOM* wird an die S_0 -Schnittstelle(n) eines ISDN-Anschlusses in Punkt-zu-Mehrpunkt-Konfiguration (Mehrgeräteanschluß) oder in Punkt-zu-Punkt-Konfiguration (Anlagenanschluß) angeschlossen. Der Router erkennt Ihren Anschlußtyp und das verwendete D-Kanal-Protokoll automatisch. Wählverbindungen mit DSS1 oder 1TR6 können ebenso verwendet werden wie Festverbindungen.

Kanalbündelung und Kompression

Auf der ISDN-Leitung unterstützt das Gerät statische und dynamische Kanalbündelung über MLPPP und BACP. Beim *ELSA LANCOM Business 4100* können bis zu acht Kanäle für die Bündelung verwendet werden. Mit der Stac-Datenkompression (hi/fn) kann eine Steigerung der Datenübertragungsrate um bis zu 400% erreicht werden.

Mehrkanalverwaltung

Beim *ELSA LANCOM Business 4100* stehen Ihnen vier ISDN-Anschlüsse, also insgesamt acht B-Kanäle zur Verfügung. Für jede Verbindung können Sie die Reihenfolge festlegen,

in der die Kanäle verwendet werden sollen. So können Sie z.B. bestimmte Kanäle für RAS-Zugänge freihalten oder nur bestimmte Kanäle für den Internet-Zugang freigeben.

Statusanzeigen

Ein Display und LED-Anzeigen an der Front- und Rückseite Ihres ISDN-Routers ermöglichen die Überprüfung von ISDN- und Ethernet-Anschlüssen sowie der aktuellen Leitungsverbindungen und erleichtern somit die Diagnose bei möglichen Systemstörungen.

ELSA LANmonitor

Den Zustand des Routers können Sie nicht nur an den LEDs ablesen. Für Benutzer von Windows-Betriebssystemen gibt es eine zusätzliche Möglichkeit. Mit dem *LANmonitor* haben Sie die Statusinformationen der *ELSA LANCOM* immer auf dem Bildschirm. Für jedes Gerät im lokalen Netz zeigt der *LANmonitor* die wichtigsten Informationen an, z.B.:

- Verbindungszustand für jeden B-Kanal
- Name der verbundenen Gegenstelle
- Welches Modul aus dem Gerät ist verbunden (Router, *LANCAPI*)
- Verbindungsdauer und Übertragungsraten
- Auszüge aus der Statistik des Geräts (z.B. Informationen aus der PPP-Verhandlung)

Darüber hinaus erlaubt der *LANmonitor* die Protokollierung und Speicherung der Meldungen für spätere Zwecke auf dem PC.

Statistiken

Mit den umfangreichen Statistiken haben Sie den Router im Griff. Hier finden Sie z.B. alle Informationen über die aufgebauten Verbindungen und optimieren so die Konfiguration Ihres ISDN-Routers.

Gebührenschtutz

Bei freigeschalteter „Gebühreninformation während der Verbindung“ im ISDN-Netz (nach AOCD) können die verfügbaren Gebühreneinheiten für einen bestimmten Zeitraum festgelegt werden. So haben Sie immer Kontrolle über Ihre Telefonrechnung.

Falls an Ihrem ISDN-Anschluß keine Gebühreninformationen übermittelt werden, können Sie ersatzweise auch die aktive Verbindungszeit für einen definierten Zeitraum einschränken. Nach Ablauf dieser Zeit läßt der Router dann keinen eigenen Verbindungsaufbau mehr zu.

Least-Cost-Routing

Auch bei einer großen Auswahl von Anbietern für Telekommunikationsdienste wählen Sie mit dem Least-Cost-Router immer die preiswerten Leitungen aus. Sie definieren dabei einmal, welche Provider für Ihre Bedürfnisse die günstigsten Tarife haben, und der Router wählt bei jeder Verbindung (egal ob über den Router oder die *LANCAP1*) automatisch den Anbieter mit dem günstigsten Tarif.

Automatische Zeitkontrolle

Zur Erzeugung von aussagekräftigen Statistiken und zur Auswahl der richtigen Verbindungswege über den Least-Cost-Router benötigt das Gerät stets die genaue Uhrzeit. Diese Zeit kann es selbständig aus dem ISDN-Netz ablesen. Dabei wird die interne Zeit des Routers entweder bei jedem Verbindungsaufbau oder bei jedem Einschalten des Geräts mit der ISDN-Zeit verglichen. Ein manuelles Setzen der Zeit ist natürlich auch möglich.

Konfiguration mit *ELSA LANconfig*

Die Einstellung und Anpassung der Router an Ihre spezielle Aufgabe erfolgt schnell und komfortabel über das mitgelieferte Konfigurationstool *ELSA LANconfig* für Windows-Betriebssysteme. Benutzer anderer Betriebssysteme verwenden Telnet oder ein beliebiges Terminalprogramm. Der Zugriff auf das Gerät ist dabei möglich aus dem WAN, aus dem LAN oder direkt über die eigene Konfigurationsschnittstelle. Bei Konfigurationen aus dem LAN oder WAN wird neben TFTP auch SNMP unterstützt.

Die integrierten Installations-Assistenten helfen Ihnen, die Geräte in wenigen Schritten in Betrieb zu nehmen.

Zugriffsschutz

Zum Schutz vor unberechtigtem Zugriff auf das Firmen-Netz bietet der Router neben dem Paßwortschutz und der Rufnummernerkennung (CLIP) auch eine Rückruf-Funktion, die nur den Verbindungsaufbau zu vorher festgelegten Telefonanschlüssen zuläßt. Firewall-Filter und IP-Masquerading runden das Sicherheitskonzept ab. Zusätzlich verhindert die Login-Sperre „Brute-Force-Angriffe“ und sperrt den Zugang zum Router nach einer einstellbaren Anzahl von Login-Versuchen mit falschem Paßwort.

Kompatibilität durch PPP

Zur Kommunikation mit Produkten anderer Hersteller unterstützt der Router u.a. PPP, ein sehr weit verbreitetes Protokoll zum Austausch von Netzwerkdaten über Punkt-zu-Punkt-Verbindungen.

Fernkonfiguration über PPP

Ein besonderes Highlight der Konfiguration für Router von ELSA, an deren Standort sich niemand um die Einstellung kümmern kann oder soll, ist die Fernkonfiguration über das Windows-DFÜ-Netzwerk. Dabei wird das neue Gerät einfach mit Spannung versorgt und mit dem ISDN-Anschluß verbunden, und schon können Sie den Router einfach über eine PPP-Verbindung anwählen und bequem von Ihrem Standort aus konfigurieren. Bei der ersten Konfiguration wird dieser Zugang durch ein Paßwort geschützt und bleibt unbeberechtigten Anrufern verschlossen.

Software-Update

Damit Sie immer auf dem neuesten Stand der Technik in Sachen Software bleiben, haben die Router einen Flash-ROM-Speicher. Eine neue Firmware kann so komfortabel eingespielt werden, ohne daß man das Gerät öffnen muß. Die aktuelle Version steht immer in unseren Online-Medien für Sie bereit und kann über das LAN, das WAN oder über die Konfigurationsschnittstelle eingespielt werden.

FirmSafe

Beim Einspielen der neuen Firmware gehen Sie kein Risiko ein: Die FirmSafe-Funktion erlaubt die Verwaltung von zwei Firmware-Dateien in einem Gerät. Sollte also die neue Firmware nach dem Upload nicht wie gewünscht arbeiten, können Sie einfach auf die vorherige Version zurückschalten.

Tritt beim Upload ein Fehler auf (z.B. verursacht durch einen Übertragungsfehler), wird automatisch auf die betriebsbereite vorherige Version zurückgeschaltet.

ELSA LANCAPi und ELSA CAPI Faxmodem

Der Einsatz der *LANCAPi* bringt vor allem wirtschaftliche Vorteile. Die *LANCAPi* ist eine spezielle Form der CAPI-2.0-Schnittstelle, über die unterschiedliche Kommunikationsprogramme (z.B. *ELSA-RVS-COM* oder *ELSA-ZOC*) über das Netzwerk auf den Router zugreifen können.

Alle Workstations, die im LAN (Local Area Network) integriert sind, erhalten über die *LANCAPi* uneingeschränkten Zugriff auf Bürokommunikations-Funktionen wie Fax und EuroFileTransfer. Ohne zusätzliche Hardware an den Arbeitsstationen, werden alle Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsstationen installiert.

Beim Versenden von Faxen wird am Arbeitsplatz ein ISDN-Faxgerät simuliert. Mit der *LANCAPi* leitet der PC das Fax über das Netzwerk an den Router weiter, welcher die Verbindung zum Empfänger über ISDN herstellt.

Mit dem *ELSA CAPI Faxmodem* steht Ihnen außerdem unter Windows ein Faxtreiber (Fax Class 1) zur Verfügung, der als Schnittstelle zwischen *ELSA LANCAPI* und Anwendung den Betrieb von Standard-Faxprogrammen mit einem *ELSA LANCOM Business* ermöglicht.

DHCP

ELSA LANCOM Business verfügt über die Funktionen eines DHCP-Servers. Damit können Sie einen bestimmten Bereich von IP-Adressen zur Verfügung stellen, die der DHCP-Server dann selbständig den einzelnen Geräten im lokalen Netz zuweist.

Im Automatik-Modus kann *ELSA LANCOM Business* auch alle Adressen im Netz selbst festlegen und den Geräten im Netz zuweisen.

NetBIOS-Proxy

Router von ELSA sind speziell auf die Kopplung von Microsoft Peer-to-Peer-Netzwerken vorbereitet. Durch integriertes Routing von IP-NetBIOS-Paketen wird die Kopplung zweier Windows-Netze zum Kinderspiel. Damit nicht jedes NetBIOS-Paket zum Verbindungsaufbau führt, werden diejenigen Gegenstellen in einer Liste eingetragen, mit denen NetBIOS-Informationen ausgetauscht werden sollen.

Als NetBIOS-Proxy beantwortet der Router dann die Anfragen nach bekannten Rechnern lokal und vermeidet so den unnötigen Verbindungsaufbau.

DNS-Server

ELSA LANCOM Business verfügt über die Funktionen eines DNS-Servers. Damit können Sie Verknüpfungen zwischen IP-Adressen und Namen von Rechnern oder Netzen herstellen, um so bei Anfragen nach bekannten Rechnernamen direkt die richtige Route zuzuordnen zu können.

Der DNS-Server kann dabei auch auf die Namens- und IP-Informationen aus dem DHCP-Server und aus dem NetBIOS-Modul zurückgreifen.

Als weitere Funktion kann der DNS-Server auch als wirksamer Filter für die Benutzer im eigenen LAN verwendet werden. Für einzelne Rechner oder ganze Netze kann der Zugriff auf bestimmte Domains gesperrt werden.

Einwahl über GSM

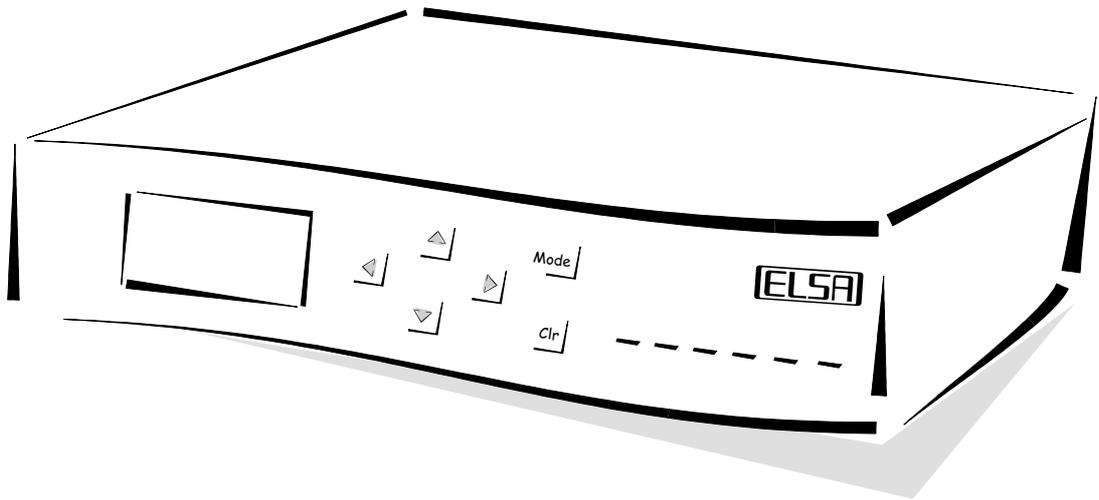
ELSA LANCOM Business erlaubt auch die Einwahl über Mobiltelefone nach dem GSM-Standard. Der Router erkennt dabei den Anruf über das V.110-Protokoll und stellt automatisch den verwendeten Layer auf dieses Übertragungsverfahren ein. RAS-Zugänge über GSM und über ISDN können so den gleichen Layer verwenden.

Vorhang auf für *ELSA LANCOM Business*

In diesem Abschnitt stellen wir Ihnen die Hardware des Geräts vor. Sie erfahren etwas über die Bedeutung der Anzeigeelemente sowie die Anschlußmöglichkeiten.

Wie sieht das Gerät aus?

Zunächst wollen wir Sie mit dem Router vertraut machen. An der Vorderseite finden Sie die Anzeige- und Bedienungselemente: ein Display, einige Tasten und Leuchtdioden (LEDs).



Das Display zeigt die verschiedenen Betriebszustände und Meldungen des Gerätes an. Es werden Betriebszustände und Meldungen in drei verschiedenen Darstellungsarten angezeigt. Mit den Tasten wählen Sie die Darstellungsart aus, bestätigen Meldungen und scrollen ggf. durch die mehrzeilige Anzeige. Die genaue Funktion der einzelnen Tasten in den verschiedenen Betriebszuständen der *ELSA LANCOM* ist im Kapitel 'Konfigurationsmöglichkeiten' beschrieben.

Power/Msg

Diese LED wird beim Einschalten der Versorgungsspannung einmal kurz eingeschaltet. Nach dem Selbsttest wird dann entweder ein evtl. festgestellter Fehler als Blinkcode ausgegeben, oder aber das Gerät geht in Betrieb, und die LED leuchtet konstant.

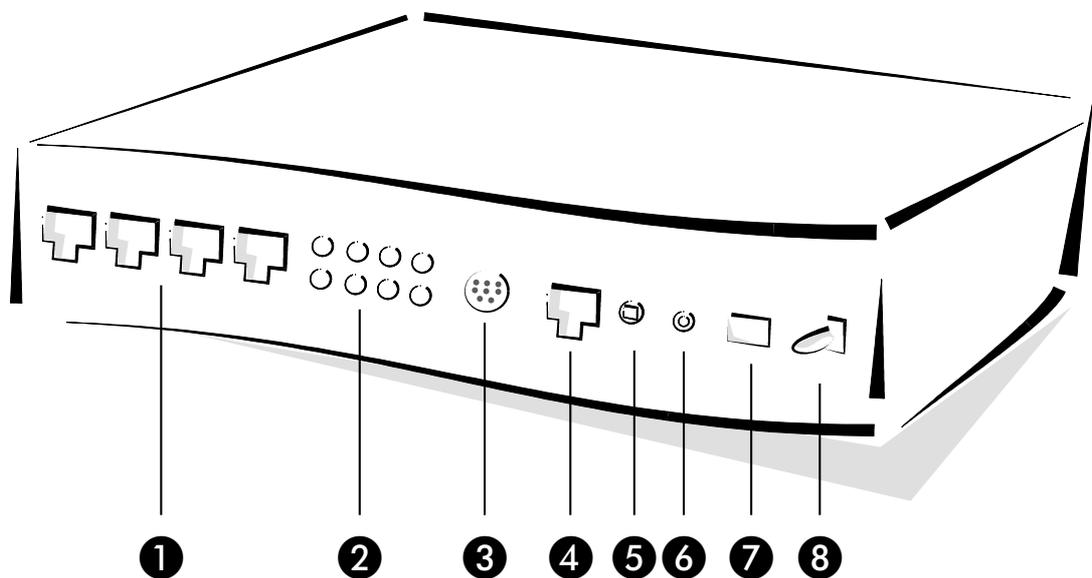
aus		Gerät abgeschaltet
rot	1 x kurz	Bootvorgang (Test und Laden) begonnen
rot	blinkend	Anzeige eines Bootfehlers (im Blinkcode kodiert)
rot		Gerät betriebsbereit
rot	unterbr.	Fehlermeldung oder eine Gebührensperre verhindert abgehende Rufe

LAN-Tx, -Rx,
LAN-Coll, -Link
LAN-FDpx, -Fast

Diese LEDs zeigen die entsprechenden Zustände des Netzwerk-Controllers an:

LAN-Rx/Tx	gelb	Datenpaket vom Gerät an das LAN oder vom LAN an das Gerät gesendet
LAN-Coll	rot	Sendekollision
LAN-Link	grün	Der Anschluß zum LAN ist hergestellt und bereit
LAN-FDpx	grün	Der Router sendet und empfängt Daten gleichzeitig
LAN-Fast	grün	ELSA LANCOM befindet sich im 100-Mbit-Betrieb

Jetzt drehen Sie das Ganze mal um und sehen sich die Rückseite an. Wieder von links finden Sie:



- 1 vier ISDN-S₀-Anschlüsse (ELSA LANCOM Business 4100)
- 2 Status-LEDs für die vier S₀-Anschlüsse:

S ₀ -Status	aus	Bus nicht aktiviert
	blinkt schnell	Bus mit D-Kanal aktiviert, keine TEI
		D-Kanal erkannt, Bus nicht aktiviert
grün	Bus mit D-Kanal aktiviert, TEI zugewiesen	
S ₀ -Line	aus	Kein Anruf, keine Verbindung
	blinkt langsam (1x pro Sek., insgesamt 2 bis 3x)	Ankommender Ruf, der Router ist jedoch nicht zuständig oder der Router baut selbst eine Verbindung auf
	blinkt schnell (3x pro Sek.)	Ruf liegt an, der Router ist zuständig, hat aber (noch) nicht angenommen
	gelb	Verbindung wird/ist hergestellt

- 3 V.24-Konfigurationsschnittstelle
- 4 10/100Base-TX für 10-Mbit- oder 100-Mbit-Netze
- 5 Node/Hub-Umschalter
- 6 Reset-Taster, führt einen Hardware-Reset durch oder setzt das Gerät in den Auslieferungszustand zurück (nach ca. 5 Sek. Drücken).
- 7 Anschluß für das Netzteil
- 8 Ein/Aus-Schalter

Node oder Hub?

Beachten Sie beim Anschluß an das Netzwerk die Stellung des Node/Hub-Umschalters:

- Im Auslieferungszustand steht der Umschalter auf 'Node'. In dieser Stellung verhält sich das Gerät wie ein Knoten in einem Netzwerk. Es kann dann nur an einen Hub angeschlossen werden, nicht direkt an die Netzwerkkarte eines Rechners.
- Stellen Sie den Umschalter auf 'Hub' um, wenn Sie das Gerät nicht an einen Hub anschließen wollen, sondern direkt an einen Arbeitsplatzrechner. Die Leitungen zum Senden und Empfangen der Daten werden in dieser Stellung gekreuzt.



Sie können die korrekte Stellung des Node/Hub-Umschalters mit Hilfe der Link-Status-LED (Link) überprüfen.

CE-Konformität

Dieses Gerät wurde getestet und erfüllt unter praxisgerechten Bedingungen die Schutzanforderungen nach den Richtlinien des Rates der Europäischen Gemeinschaft zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit (89/336/EWG) entsprechend der Normen EN55022 Klasse B sowie EN50082-1.



Bei nicht bestimmungsgemäßen Gebrauch oder bei Betrieb des Gerätes in der Nähe von sehr starken Sendern kann es zu einem zulässigen zeitweiligen Funktionsausfall des Gerätes kommen.

Diese Anforderungen gewährleisten angemessenen Schutz gegen Empfangsstörungen im Wohnbereich. Das Gerät erzeugt und verwendet Signale im Frequenzbereich von Rundfunk und Fernsehen und kann diese abstrahlen. Wenn das Gerät nicht gemäß den Anweisungen installiert und betrieben wird, kann es Störungen im Empfang verursachen. Es kann jedoch nicht in jedem Fall garantiert werden, daß bei ordnungsgemäßer Installation keine Empfangsstörungen auftreten. Wenn das Gerät Störungen im Rundfunk- oder Fernsehempfang verursacht, was durch vorübergehendes Ausschalten des Gerätes

überprüft werden kann, versuchen Sie die Störung durch eine der folgenden Maßnahmen zu beheben:

- Verändern Sie die Ausrichtung oder den Standort der Empfangsantenne.
- Erhöhen Sie den Abstand zwischen dem Gerät und Ihrem Rundfunk- oder Fernsehempfänger.
- Schließen Sie das Gerät an einen anderen Hausstromkreis an als den Rundfunk- oder Fernsehempfänger.
- Wenden Sie sich an Ihren Händler oder einen ausgebildeten Rundfunk- und Fernsehtechniker.

Konfigurationsmöglichkeiten

ELSA LANCOM Business werden immer mit einer aktuellen Software ausgeliefert, in der schon einige Einstellungen für Sie vorbereitet sind.

Trotzdem ist noch eine Ergänzung der Angaben und eine Anpassung an Ihre spezielle Aufgabe für den Router nötig. Diese Einstellungen werden während der Konfiguration vorgenommen.

In diesem Kapitel zeigen wir Ihnen, mit welchen Programmen und über welche Wege Sie auf das Gerät zugreifen können, um die Einstellungen vorzunehmen.

Und wenn das Entwickler-Team eine neue Firmware mit neuen Features für Sie fertiggestellt hat, finden Sie hier Hinweise zum Laden der neuen Software.

Viele Wege führen zum *ELSA LANCOM*

Prinzipiell gibt es verschiedene Möglichkeiten, auf Router von *ELSA* zuzugreifen:

- Über die Konfigurations-Schnittstelle (Config-Schnittstelle) an der Rückseite der Router (auch Outband genannt)
- Über das angeschlossene Netzwerk, LAN oder WAN (Inband)
- Über eine PPP-Verbindung über das DFÜ-Netzwerk o.ä. (Fernkonfiguration)

Was unterscheidet nun diese Möglichkeiten?

Zum einen die Erreichbarkeit der Geräte: Die Konfiguration über Outband ist immer verfügbar. Die Inband-Konfiguration ist jedoch z.B. nicht mehr möglich, wenn das übertragende Netzwerk gestört ist. Auch die Fernkonfiguration ist abhängig vom Übertragungsmedium, z.B. der ISDN-Verbindung.

Zum anderen die Anforderungen an weitere Soft- oder Hardware. Die Inband-Konfiguration benötigt einen der ohnehin vorhandenen Rechner im LAN oder WAN und eine geeignete Software. Die Outband-Konfiguration braucht neben der Software auch einen der Rechner (mit serieller Schnittstelle) und das entsprechende Konfigurationskabel. Die Fernkonfiguration benötigt einen Rechner mit PPP-Client, ISDN-Karte oder Terminaladapter. Am einfachsten ist die Fernkonfiguration bei Verwendung von DFÜ-Netzwerk und *ELSA LANconfig*.

Der direkte Weg: Outband

Mit der Outband-Konfiguration greifen Sie direkt über die Konfigurations-Schnittstelle auf den Router zu.



Die Outband-Konfiguration benötigen Sie im Grunde nur, wenn Sie Ihr Gerät nicht über TCP/IP erreichen können.

Voraussetzungen für die Outband-Konfiguration

Was brauchen Sie dazu?

- Einen Rechner mit Windows 95, Windows 98 oder Windows NT 4.0 und das Konfigurationsprogramm *ELSA LANconfig*.
oder
Einen Rechner mit beliebigem Betriebssystem und ein Terminalprogramm (z.B. *Telix* oder *Hyperterminal*).
- Das mitgelieferte Konfigurationskabel und ggf. den 9/25poligen Adapter zur Verbindung des Rechners mit dem Router (COM-Port des PC an Konfigurations-Schnittstelle des Routers).

Outband-Konfiguration mit *ELSA LANconfig*

Starten Sie *ELSA LANconfig* z.B. aus der Windows-Startleiste mit **Start ▶ Programme ▶ ELSAan ▶ ELSA LANconfig**. *ELSA LANconfig* sucht nun automatisch im lokalen Netz (nicht jedoch an der seriellen Schnittstelle) nach *ELSA LANCOM*-Geräten. Ein neues Gerät an der seriellen Schnittstelle finden Sie mit **Gerät ▶ Suchen ▶ An allen Schnittstellen suchen**. *ELSA LANconfig* zeigt neue Router in der Liste mit der Gerätebezeichnung an.

Für ein neues, noch nicht konfiguriertes Gerät an der Konfigurationsschnittstelle können Sie mit **Extras ▶ Setup Assistent** verschiedene Konfigurationshilfen aufrufen. Wählen Sie einen der angebotenen Assistenten aus, und beantworten Sie einfach seine Fragen. Anschließend ist Ihr *ELSA LANCOM* für die ausgewählte Aufgabe eingestellt.

In der Liste der gefundenen Geräte können Sie mit einem Doppelklick auf die Gerätebezeichnung die aktuelle Konfiguration zur Bearbeitung öffnen.

Outband-Konfiguration mit Terminalprogramm

Wenn das Terminalprogramm gestartet ist, drücken Sie nur einige Male die Return-Taste, um automatisch die Bitrate zu erkennen (bis zu 230 Kbit/s, 38.4 Kbit/s als Standard).

Nach der Eingabe des Paßworts stehen Ihnen alle Befehle aus dem Abschnitt 'Befehle für die Konfiguration' zur Verfügung.

Der komfortable Weg: Inband

Mit der Inband-Konfiguration haben Sie von jedem Rechner aus dem WAN oder LAN aus Zugriff auf den Router. Allerdings nur, wenn er dies zuläßt, denn der Zugang aus dem WAN oder LAN kann über die IP-Zugangsliste eingeschränkt oder ganz gesperrt werden. Für die Inband-Konfiguration verwenden Sie entweder Telnet (gehört zum Lieferumfang der meisten Betriebssysteme) oder das Konfigurationsprogramm *ELSA LANconfig* für Windows. *ELSA LANconfig* ist im Lieferumfang Ihres Routers enthalten. Aktuelle Versionen stehen immer in unseren Online-Medien für Sie bereit.

Voraussetzungen für die Inband-Konfiguration

Die Konfiguration mit Telnet oder *ELSA LANconfig* läuft über TCP/IP bzw. TFTP ab. Dazu muß also auf dem verwendeten Rechner das TCP/IP installiert sein, und Ihr Router benötigt eine IP-Adresse, mit der Sie ihn ansprechen können. Ein noch nicht konfiguriertes Gerät hört auf die IP-Adresse XXX.XXX.XXX.254. Die vielen X stehen dabei für die Netzwerkadresse in Ihrem LAN. Haben die Rechner in Ihrem Netz also z.B. Adressen wie 192.110.130.1, dann können Sie Ihren Router mit der Adresse 192.110.130.254 erreichen.



Haben Sie bereits einen Rechner mit der Adresse XXX.XXX.XXX.254 in Ihrem Netz stehen, dann geben Sie dem Gerät über die Outband-Konfiguration eine neue Adresse, bevor Sie ihn im LAN installieren.

Alternativ: Adreßverwaltung mit dem DHCP-Server

Wenn die Konfiguration der korrekten IP-Adressen „von Hand“ keine absolute Notwendigkeit für Sie ist, erledigt der DHCP-Server diese Arbeit auch gerne selbständig für Sie. Bei der Verwendung des DHCP-Servers können Sie alle IP-Adressen im Netz, inkl. der für den Router selbst, automatisch einstellen lassen (siehe auch Kapitel 'Automatische Adreßzuweisung mit DHCP').

Starten der Inband-Konfiguration über *ELSA LANconfig*

Nach der Installation (mit Doppelklick auf die 'autorun.exe') rufen Sie das Konfigurations-Tool *ELSA LANconfig* z.B. aus der Windows-Startleiste auf mit **Start ▶ Programme ▶ ELSAlan ▶ ELSA LANconfig**. *ELSA LANconfig* sucht nun automatisch im lokalen Netz nach *ELSA LANCOM*-Geräten. Wird dabei ein noch nicht konfiguriertes Gerät im lokalen Netz gefunden, startet *ELSA LANconfig* selbständig den Setup-Assistenten.

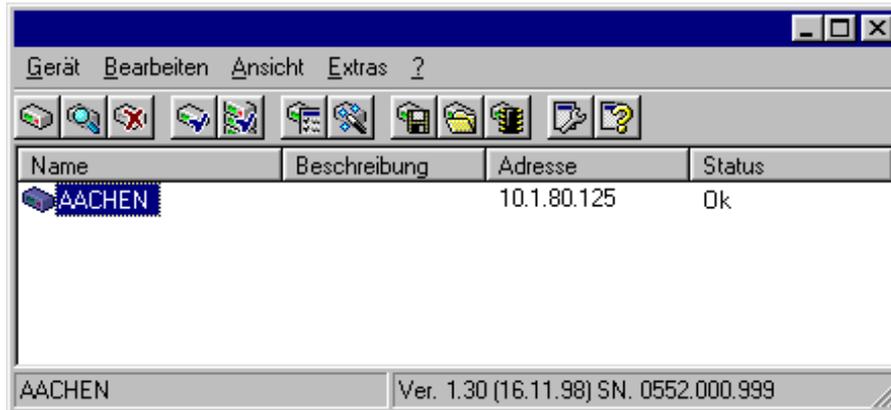
Wählen Sie einen der angebotenen Assistenten aus, und beantworten Sie einfach seine Fragen. Anschließend ist der Router für die ausgewählte Aufgabe eingestellt.



Um die Suche eines neuen Routers manuell einzuleiten, klicken Sie nur auf die Schaltfläche **Suchen** oder rufen den Befehl über **Gerät ▶ Suchen** auf. *ELSA LANconfig* erkun-

digt sich dann, wo es suchen soll. Bei der Inband-Lösung reicht hier die Auswahl des lokalen Netzes, und los geht's.

Sobald *ELSA LANconfig* mit der Suche fertig ist, zeigt es in der Liste alle gefundenen Geräte mit Namen, evtl. einer Beschreibung, der IP-Adresse und dem Status an.



Ein Doppelklick auf den Eintrag für das markierte Gerät, der Klick auf die Schaltfläche **Konfigurieren** oder den Menüeintrag **Bearbeiten ► Konfiguration bearbeiten** liest die aktuellen Einstellungen aus dem Gerät aus und zeigt die allgemeinen Geräteinformationen.

Die weitere Bedienung des Programms erklärt sich im Prinzip selbst bzw. über die Online-Hilfe. Mit einem Klick auf das Fragezeichen oben rechts in jedem Fenster bzw. mit einem rechten Mausklick auf einen unklaren Begriff können Sie jederzeit die kontextsensitive Hilfe aufrufen.

Starten der Inband-Konfiguration über Telnet

Über Telnet starten Sie die Inband-Konfiguration z.B. mit dem Kommando:

```
telnet 10.1.80.125
```

Telnet baut dann eine Verbindung zum Gerät mit der eingegebenen IP-Adresse auf.

Nach der Eingabe des Paßworts stehen Ihnen alle Befehle aus dem Abschnitt 'Befehle für die Konfiguration' zur Verfügung.

Der Fernzugang: Konfiguration über DFÜ-Netzwerk

Besonders einfach wird die Einstellung von Routern an entfernten Standorten mit der Fernkonfiguration über das DFÜ-Netzwerk. Das Gerät ist nach dem Einschalten und der Verbindung mit dem ISDN-Anschluß ohne eine einzige Einstellung sofort vom Administrator zu erreichen. Damit sparen Sie beim Anschluß von anderen Netzwerken an Ihr eigenes LAN viel Zeit und Geld für die Reise zum anderen Netzwerk oder für die Einweisung der Mitarbeiter vor Ort in die Konfiguration der Router.

Außerdem können Sie eine spezielle Rufnummer für die Fernkonfiguration reservieren. Damit kann ein Service-Techniker immer auf den Router zugreifen, auch wenn das Gerät durch fehlerhafte Einstellungen eigentlich nicht mehr ansprechbar ist.

Das brauchen Sie für die Fernkonfiguration

- einen Rechner mit PPP-Client, z.B. Windows DFÜ-Netzwerk
- ein Programm für die Inband-Konfiguration, z.B. *ELSA LANconfig* oder Telnet
- eine ISDN-Karte, einen Terminaladapter oder einen *ELSA LANCOM* mit *ELSA LAN-CAPI*

So bereiten Sie die Fernkonfiguration vor

- ① Versorgen Sie den Router mit der nötigen Spannung.
- ② Verbinden Sie das Gerät mit einem ISDN-Anschluß.

Die erste Fernverbindung mit DFÜ-Netzwerk (*ELSA LANconfig*)

- ① Wählen Sie im *ELSA LANconfig* **Gerät ► Neu**, aktivieren Sie die 'DFÜ-Verbindung' als Anschlußtyp und geben Sie die Rufnummer des ISDN-Anschlusses ein, an dem der *ELSA LANCOM* angeschlossen ist. Stellen Sie dazu ggf. die Zeit ein, nach der eine Verbindung ohne Datentransfer automatisch getrennt werden soll.
- ② *ELSA LANconfig* legt nun automatisch einen neuen Eintrag im DFÜ-Netzwerk an. Wählen Sie ein PPP-fähiges Gerät (z.B. den NDIS-WAN-Treiber aus dem Lieferumfang der *LANCAPI*) für die Verbindung aus, und bestätigen Sie mit **OK**.
- ③ Anschließend zeigt *ELSA LANconfig* in der Geräteliste ein neues Gerät mit dem Namen 'Unbekannt' und der Rufnummer über DFÜ als Adresse an.

Mit dem Eintrag in der Geräteliste wird auch die Verbindung im DFÜ-Netzwerk gelöscht.

- ④ Sie können das Gerät über die Fernverbindung nun genauso einstellen wie alle anderen Geräte. Zum Auslesen der Konfiguration baut *ELSA LANconfig* eine Verbindung über das DFÜ-Netzwerk auf.

Die erste Fernverbindung mit PPP-Client und Telnet

- ① Stellen Sie mit Ihrem PPP-Client eine Verbindung zum *ELSA LANCOM* her, verwenden Sie dabei folgende Angaben:
 - Benutzername 'ADMIN'
 - Paßwort wie beim *ELSA LANCOM* eingestellt, im Auslieferungszustand kein Paßwort
 - eine IP-Adresse für die Verbindung, nur wenn erforderlich



- ② Starten Sie eine Telnet-Verbindung zum *ELSA LANCOM*. Verwenden Sie dazu die folgende IP-Adresse:
 - '172.17.17.18', wenn Sie keine IP-Adresse für den PPP-Client festgelegt haben. Diese Adresse verwendet der *ELSA LANCOM* automatisch, falls nichts anderes vereinbart ist. Der anrufende PC reagiert dann auf die IP '172.17.17.17'.
 - Erhöhen Sie die IP-Adresse des PCs um eins, wenn Sie eine Adresse festgelegt haben. Beispiel: Sie haben für den PPP-Client die IP '10.0.200.123' festgelegt, dann hört der *ELSA LANCOM* auf die '10.0.200.124'. Ausnahme: Bei einer '254' am Ende der IP reagiert der Router auf die 'x.x.x.1'.
- ③ Sie können den *ELSA LANCOM* über die Fernverbindung nun genauso einstellen wie alle anderen Geräte.

Fernkonfiguration einschränken

Die PPP-Verbindung von einer beliebigen Gegenstelle zum Router gelingt natürlich nur dann, wenn das Gerät jeden Ruf mit den entsprechenden Einstellungen für den PPP-Betrieb annimmt. Im Auslieferungszustand geht das auch, da das Standard-Protokoll (Default-Layer) auf PPP eingestellt ist.

Aber vielleicht möchten Sie ja nach der ersten Konfiguration den Default-Layer z.B. für LAN-LAN-Verbindungen auf ein anderes Protokoll einstellen. Dann nimmt das Gerät die Rufe über die DFÜ-Verbindung nicht mehr mit den PPP-Einstellungen an. Abhilfe schafft hier die Vereinbarung einer speziellen Rufnummer für den Konfigurationszugriff. Empfängt das Gerät einen Ruf auf dieser Nummer, wird immer die Einstellung für PPP verwendet, unabhängig von der weiteren Konfiguration des Routers. Dabei wird nur ein spezieller Benutzername während der PPP-Verhandlung akzeptiert, der beim Verbindungsaufbau über *ELSA LANconfig* automatisch eingetragen wird.

- ① Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Security'.
- ② Wählen Sie im Feld 'Konfigurationszugriff' aus, ob die Einstellung aus entfernten Netzen vollständig, nur zum Lesen oder nicht erlaubt ist.

Geben Sie bei einer Telnet- oder Terminalverbindung alternativ den folgenden Befehl ein:

```
set /setup/config-modul/wan-config [ein][read][aus]
```



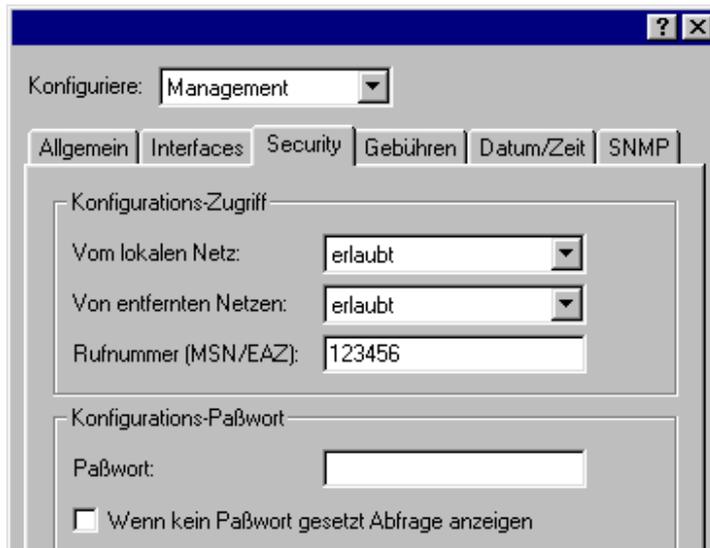
Wenn Sie den Zugriff auf den Router über das WAN ganz sperren wollen, stellen Sie den Konfigurations-Zugriff von entfernten Netzen auf 'nicht erlaubt'.

- ③ Geben Sie als Rufnummer im Bereich 'Konfigurationszugriff' eine MSN oder EAZ Ihres ISDN-Anschlusses ein, die nicht für den Router, die *LANCAPI* oder die a/b-Ports verwendet wird.

Geben Sie alternativ den folgenden Befehl ein:

```
set /setup/config-modul/Fernconfig-(EAZ-MSN) 123456
```

- ④ Schützen Sie die Einstellungen des Geräts ggf. zusätzlich durch die Vergabe eines Paßworts.



The screenshot shows a configuration window titled 'Management'. It has several tabs: 'Allgemein', 'Interfaces', 'Security', 'Gebühren', 'Datum/Zeit', and 'SNMP'. The 'Security' tab is active. Under the heading 'Konfigurations-Zugriff', there are three fields: 'Vom lokalen Netz:' with a dropdown menu set to 'erlaubt', 'Von entfernten Netzen:' with a dropdown menu set to 'erlaubt', and 'Rufnummer (MSN/EAZ):' with a text box containing '123456'. Below this is the 'Konfigurations-Paßwort' section, which includes a 'Paßwort:' text box and a checkbox labeled 'Wenn kein Paßwort gesetzt Abfrage anzeigen'.

Geben Sie alternativ den folgenden Befehl ein:

```
passwd
```

Damit werden Sie zur Eingabe eines neuen Paßworts mit Bestätigung aufgefordert.

Befehle für die Konfiguration

Bei der Verwendung von Telnet (Inband) oder einem Terminalprogramm (Outband) zur Router-Konfiguration geben Sie Befehle und Pfadangaben so ein, wie Sie es von DOS oder UNIX her kennen.

Zur Trennung der Einträge für einen Pfad geben Sie einen Schrägstrich oder einen umgekehrten Schrägstrich ein. Befehle und Tabelleneinträge müssen nicht vollständig ausgeschrieben werden, eine eindeutige Abkürzung reicht aus.

Bei der Konfiguration der Router werden Einträge der Gruppen MENÜ, WERT, TABELLE, TABINFO, AKTION und INFO angezeigt und evtl. geändert. Die folgenden Befehle können Sie dazu verwenden:

Dieser Befehl hat folgende Bedeutung z.B.:
? oder help	ruft Hilfetexte auf.	-
dir, list, ll, ls <MENÜ>, <WERT> oder <TABELLE>	zeigt den Inhalt von MENÜ, WERT oder TABELLE an.	dir/status/wan-statistik zeigt die aktuelle WAN-Statistik.
cd <MENÜ> oder <TABELLE>	wechselt in das angegebene MENÜ oder die TABELLE.	cd setup/tcp-ip-modul (kurz cd se/tc) wechselt in das TCP/IP-Modul.
set <WERT>	So setzen Sie den WERT neu. Bei Tabellenzeilen geben Sie alle Einträge getrennt durch Leerzeichen ein. Ein * läßt den Eintrag unverändert.	set ip-adresse 192.110.120.140 setzt eine neue IP-Adresse. set /setup/name AACHEN gibt dem Gerät den Namen 'AACHEN'
set <WERT> ?	zeigt Ihnen, welche Werte Sie hier eingeben können.	
del <WERT>	löscht eine Zeile aus einer Tabelle.	del /se/wan/nam/AACHEN löscht den Eintrag zur Gegenstelle AACHEN
do <AKTION> (Parameter)	führt die AKTION aus, evtl. mit den angegebenen Parametern.	do /firmware/firmware-upload startet das Einspielen einer neuen Firmware.
passwd	erlaubt die Eingabe eines neuen Paßwortes. Hierzu muß, falls vorhanden, zuerst das alte Paßwort eingegeben werden. Danach muß das neue Paßwort zweimal hintereinander eingegeben und jeweils mit  bestätigt werden.	
repeat <sek> <AKTION>	wiederholt die AKTION im Abstand der angegebenen Sekunden. Jede beliebige Taste beendet die Wiederholung.	repeat 3 dir/status/wan-statistik zeigt alle 3 Sekunden die aktuelle WAN-Statistik.
time	setzt Systemzeit und -datum.	time 24.12.1998 18:00:00
language <Sprache>	setzt die Sprache der aktuellen Konfigurationssitzung.	Unterstützte Sprachen sind z.Zt. Englisch (language english) Deutsch (language deutsch)

Dieser Befehl hat folgende Bedeutung z.B.:
exit, quit, x	Konfiguration wird beendet.	

Textuelle Eingaben mit Leerzeichen werden nur in Anführungszeichen akzeptiert, z.B. `set/se/snmp/admin "Der Administrator"`.

Textuelle Einträge (Einzel- und Tabellenwerte) werden wie folgt gelöscht:

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

Neue Firmware mit FirmSafe

Die Software der Router von ELSA wird ständig weiterentwickelt. Damit Sie auch in den Genuß von neuen Features und Funktionen kommen, haben wir die Geräte mit einem Flash-ROM-Speicher ausgerüstet, der das nachträgliche Ändern der Betriebs-Software zum Kinderspiel macht. Kein EPROM tauschen, kein Gehäuse öffnen: Einfach die neue Version einspielen und fertig!

So funktioniert FirmSafe

FirmSafe macht das Einspielen der neuen Software zur sicheren Sache: Die gerade verwendete Firmware wird dabei nicht einfach überschrieben, sondern es wird eine zweite Firmware zusätzlich im Gerät gespeichert.

Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firmware überschrieben. Sie können selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll:

- 'Unmittelbar': Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:
 - Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.
 - Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert der Router automatisch wieder die bisherige Firmware und startet damit das Gerät neu.
- 'Login': Um den Problemen eines fehlerhaften Uploads zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.
 - Im Unterschied zur ersten Variante wartet der Router anschließend fünf Minuten lang auf einen erfolgreichen Login auf das Gerät über Outband oder Inband (per Telnet). Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.

- Wenn das Gerät nicht mehr ansprechbar ist und ein Login somit unmöglich ist, aktiviert der Router automatisch wieder die bisherige Firmware und startet damit das Gerät neu.
- 'Manuell': Bei der dritten Möglichkeit können Sie vorher selbst eine Zeit bestimmen, in der Sie die neue Firmware testen wollen. Der Router startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, daß die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird.

So spielen Sie eine neue Software ein

Beim Firmware-Upload (so heißt das Einspielen der Software) gibt es verschiedene Wege zum Ziel:

- Konfigurations-Tool *ELSA LANconfig* (empfohlen)
- Terminal-Programme
- TFTP



Beim Firmware-Upload bleiben alle Einstellungen erhalten! Trotzdem sollten Sie sicherheitshalber die Konfiguration vorher speichern (bei *ELSA LANconfig* z.B. mit **Bearbeiten** ► **Konfiguration sichern**).

Enthält die neu eingespielte Version Parameter, die in der aktuellen Firmware des Gerätes nicht vorhanden sind, ergänzt der Router die fehlenden Werte mit den Default-Einstellungen.

ELSA LANconfig



Beim Konfigurations-Tool *ELSA LANconfig* markieren Sie das gewünschte Gerät in der Auswahlliste und klicken auf **Bearbeiten** ► **Firmware-Verwaltung** ► **Neue Firmware hochladen** oder direkt auf die Schaltfläche **Firmware-Upload**. Dann wählen Sie das Verzeichnis, in dem sich die neue Version befindet, und markieren die entsprechende Datei.

ELSA LANconfig informiert Sie dann in der Beschreibung über Versions-Nr. und Datum der Firmware und bietet den Upload an. Mit **Öffnen** ersetzen Sie die vorhandene Firmware durch die ausgewählte Version.

Wählen Sie außerdem aus, ob die Firmware sofort nach dem Laden dauerhaft aktiviert werden soll, oder stellen Sie eine Testzeit ein, in der Sie die Firmware selbst freischalten. Um anschließend die Firmware während der eingestellten Testzeit zu aktivieren, klicken Sie auf **Bearbeiten** ► **Firmware-Verwaltung** ► **Firmware im Test freischalten**.

Terminal-Programm (z.B. *Telix* oder *Hyperterminal* von *Windows*)

Stellen Sie bei Terminalprogrammen im Menü 'Firmware' mit dem Befehl 'set Modus-Firmsafe' zunächst ein, in welchem Modus Sie die neue Firmware laden wollen (unmit-

telbar, login oder manuell). Stellen Sie ggf. zusätzlich mit 'set Timeout-Firmsafe' die Zeit für den Firmwaretest ein.

Mit dem Befehl 'Firmware-Upload' wird der Router anschließend in Empfangsbereitschaft versetzt. Starten Sie anschließend den Upload-Vorgang von Ihrem Terminalprogramm aus:

- Bei *Tel/x* klicken Sie auf die Schaltfläche **Upload**, stellen 'XModem' für die Übertragung ein und wählen die gewünschte Datei zum Upload aus.
- Bei Hyperterminal klicken Sie auf **Übertragung ► Datei senden**, wählen die Datei aus, stellen 'XModem' als Protokoll ein und starten mit **OK**.

TFTP

Über TFTP kann eine neue Firmware mit dem Befehl **writeflash** eingespielt werden. Um eine neue Firmware, die z.B. in der Datei 'LC_1000U.130' vorliegt, in einen Router mit der IP-Adresse 194.162.200.17 zu übertragen, geben Sie z.B. unter Windows NT folgenden Befehl ein:

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



*Durch diesen Befehl wird die entsprechende Datei mit dem Kommando **writeflash** an den Router gesendet. Dabei muß für TFTP die binäre Dateiübertragung eingestellt werden. Auf vielen Systemen ist jedoch das ASCII-Format voreingestellt. In diesem Beispiel für Windows NT erreichen Sie das durch den Parameter '-i'.*

Nach einem erfolgreichen Firmware-Upload bootet das Gerät und aktiviert so direkt die neue Firmware. Tritt während des Uploads ein Fehler auf (Schreibfehler im Flash-ROM, TFTP-Übertragungsfehler o.ä.) so wird die TFTP-Verbindung abgebrochen, um dem Anwender einen Hinweis auf ein Problem zu liefern. Das Gerät bootet in diesem Fall nicht, sondern arbeitet bis zum nächsten Aus/Einschalten mit der bisherigen Firmware weiter. Der Anwender erhält so die Möglichkeit, z.B. die aktuelle Konfiguration des Gerätes zu retten.

Wird das Gerät während eines TFTP-Uploads ausgeschaltet, so kann es nur noch lokal, d.h. über die Outband-Schnittstelle, konfiguriert werden. Bei erneutem Einschalten erwartet das Gerät einen Firmware-Upload über die serielle Schnittstelle.



Achten Sie bitte deshalb darauf, einen Firmware-Upload nur über eine sichere (stabile) Verbindung durchzuführen.

Mit TFTP können auch andere Konfigurations-Befehle ausgeführt werden. Die Syntax ist am einfachsten den folgenden Beispielen zu entnehmen:

- `tftp 10.0.0.1 get readconfig file1` : Liest die Konfiguration aus dem Gerät mit der Adresse 10.0.0.1 und speichert diese unter file1 im aktuellen Verzeichnis ab
- `tftp 10.0.0.1 put file1 writeconfig` : schreibt die Konfiguration aus file1 in das Gerät mit der Adresse 10.0.0.1

- tftp 10.0.0.1 get dir/status/verb file2 : Speichert die aktuellen Verbindungsinformationen in file2

Konfiguration über SNMP

Allgemeines

Das Simple Network Management Protocol (SNMP V.1 nach RFC 1157) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netz von einer zentralen Instanz aus. Diese Instanz wird im üblichen Sprachgebrauch „Manager“ genannt, während die Geräte „Agents“ genannt werden. Die erlaubte Struktur des SNMP-Informationsaustauschs ist relativ simpel. Eine Manager-Applikation hat im Netz Zugriff auf alle SNMP-fähigen Geräte und Dienste (die Agents). Die Zugriffsberechtigungen werden über „Communities“ geregelt.

Wie die folgende Tabelle zeigt, erlaubt SNMP V.1 nur einen sehr begrenzten Befehlssatz:

Befehl	Ziel/Quelle	Funktion
GetRequest	Manager – Agent	ruft eine Information vom Agent ab
GetNextRequest	Manager – Agent	ruft die in der MIB folgende Information vom Agent ab
SetRequest	Manager – Agent	ändert eine Einstellung beim Agent
GetResponse	Agent – Manager	liefert den abgefragten Wert an den Manager zurück
Trap	Agent – Manager	meldet einen Fehler oder einen besonderen Zustand

Mit Hilfe dieser Befehle können SNMP-fähige Geräte in einem Netz zentral überwacht und konfiguriert werden. Die SNMP-Fähigkeiten der Agents werden in sogenannten MIBs = Management Information Bases festgelegt.

In der Firmware der Router von ELSA ist ein Agent für SNMP V.1 (nach RFC 1157) implementiert. Unterstützt wird ein Teil der MIB-2 und eine private MIB, die als separate Datei dem Produkt beiliegt. Um einen Router vollständig über SNMP verwalten zu können, muß diese MIB von einem SNMP-Manager (z.B. HP-OpenView) geladen und übersetzt werden. Danach stehen alle Menüs und Parameter der Konfiguration in einem eigenen Ast des SNMP-Management-Baums zur Verfügung:

```
iso/org/dod/internet/private/enterprises/elsa/isdn-devices/isdn-router/...
oder 1.3.6.1.4.1.2356.400.1...
```

Zugriff auf Tabellen und Parameter über SNMP

Alle Tabellen und Parameter können über die SNMP-Schnittstelle gelesen und ggf. auch geändert werden. Dabei wird in der MIB festgelegt, welche Variablen den Status 'read-only' oder 'read-write' haben. In handelsüblichen SNMP-Managern sind die beiden Zustände 'read-only' und 'read-write' in der Regel farblich gekennzeichnet.

Zugriffsschutz unter SNMP v.1

Der Zugriff auf SNMP-Objekte erfolgt über sogenannte Communities. Eine Community ist im Grunde ein Paßwort, mit dem der Zugriff auf bestimmte Informationsklassen gesteuert werden kann. Im Router darf über die Community 'public' auf alle Parameter und Tabellen lesend zugegriffen werden. Mit dieser Community können allerdings keine Schreibzugriffe getätigt werden.

Falls über SNMP Daten geschrieben werden sollen, so ist als Community das Paßwort des Geräts zu verwenden. Wenn für einen Router kein Paßwort eingegeben wurde, ist prinzipiell **kein** Schreibzugriff über SNMP erlaubt.

Beim Zugriff auf einen Router über SNMP werden die Einstellungen unter 'Setup/Config-Modul' wie folgt ausgewertet:

Eintrag	Wert	Bedeutung
Paßw.Zwang	Ein	Der Zugang über die Community 'public' ist gesperrt.
Paßw.Zwang	Aus	Der Zugang über die Community 'public' ist nur mit Leserechten ausgestattet. Wird als Community das Paßwort angegeben, dürfen alle Aktionen ausgeführt werden.
LAN/WAN-Config	Aus	Jeder Zugang über das LAN/WAN ist gesperrt.
LAN/WAN-Config	Ein	Der Zugang über die Community 'public' ist nur mit Leserechten ausgestattet. Wird als Community das Paßwort angegeben, dürfen alle Aktionen ausgeführt werden.
LAN/WAN-Config	Lese	Sowohl Zugang über die Community 'public' als auch über das Paßwort ist Read-Only.

Bei einem fehlgeschlagenen Zugangsversuch wird ein Trap 'Authentication Failed' ausgelöst und an den/die Manager in der SNMP-Trap-Tabelle geschickt, wenn der Trap-Mechanismus eingeschaltet wurde.

Der Community-Mechanismus im SNMP V.1 ist allerdings nur ein sehr eingeschränkter Zugriffsschutz, da sowohl die Daten, die MIB-IDs als auch die Community innerhalb der Requests und Responses unverschlüsselt im UDP-Datenblock verschickt werden.

Tabellen-Zeilen löschen mit SNMP

SNMP selbst stellt keinerlei spezielle Mechanismen für Löschvorgänge zur Verfügung. Daher muß man sich eines Tricks bedienen, um Einträge in Tabellen zu löschen oder neue Zeilen in Tabellen anzulegen.

Soll eine Zeile gelöscht werden, so muß der Wert des Indexeintrages dieser Zeile, d.h. der Wert in der ersten Spalte, auf seinen derzeitigen Wert geändert werden.

- Beispiel: In der folgenden IP-Routing-Tabelle soll die 3. Zeile gelöscht werden.

IP-Adresse	IP-Netz-Maske	Router-Name	Distanz
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.240.0.0	0.0.0.0	0
10.0.0.0	255.0.0.0	ROBERT	0
224.0.0.0	224.0.0.0	0.0.0.0	0

Via Manager ändert man den Eintrag '10.0.0.0' (also das erste Element der dritten Zeile) auf seinen derzeitigen Wert, also auf '10.0.0.0' und schickt den Set-Befehl ab. Der SNMP-SetRequest enthält dann den Auftrag, das erste Element der dritten Zeile auf '10.0.0.0' zu ändern. Die SNMP-Software erkennt diese redundante Zuweisung auf den Index und interpretiert sie als Löschkommando.

Tabellen-Zeilen hinzufügen mit SNMP

Soll eine Zeile in einer Tabelle hinzugefügt werden, so muß ein beliebiger schon vorhandener Indexeintrag einer Zeile auf den neuen Indexwert der neuen Zeile 'geändert' werden. Die Zeile, die dazu als Quelle der Änderung herangezogen wird, bleibt selbst unverändert.

Fehlermeldungen per SNMP-Trap

Über den Mechanismus der SNMP-Traps können Fehler- oder Warnmeldungen an eine Management-Instanz gesendet werden. Der im Router enthaltene SNMP-Agent erlaubt das Versenden von Traps an bis zu 20 SNMP-Manager. Die IP-Adressen dieser Manager werden im Konfigurations-Menü unter `/setup/SNMP-Modul/IP-Trap-Tabelle` konfiguriert. Das Versenden kann generell mit dem Schalter `/setup/snmp-Modul/Send-Traps` ein- und ausgeschaltet werden.

SNMP und *ELSA LANmonitor*

Die drei Einträge `/setup/SNMP-Modul/...Register-monitor`, `.../Delete-Monitor` und `.../Monitor-table` sind nur für die automatische Anmeldung von *LANmonitor* zuständig und haben für den Benutzer keine weitere Bedeutung. Sie werden nur zu Kontrollzwecken im Menü angezeigt.

Die Management-Information-Base (MIB)

Um SNMP-Management-Systemen Zugriff auf die Konfiguration im *ELSA LANCOM* zu geben, muß eine textuelle Darstellung der Konfigurationsstruktur (die sogenannte private MIB) mit dem Gerät ausgeliefert werden. Die Syntax dieser MIB orientiert sich an der ASN.1 (Abstract Syntax Notation One, ISO 8824). In der Regel ist im Programmpaket der

SNMP-Management-Software ein sogenannter MIB-Compiler enthalten. Dieser Compiler übersetzt diese MIB-Datei in eine vom Manager benutzbare Form.

Die aktuelle ELSA-MIB ist sowohl als Beilage zum Produkt auf der CD zu finden, als auch auf den ELSA-Online-Medien.

Was ist los auf der Leitung?

Nach der Grundkonfiguration der Geräte erhält man weitere wichtige Hinweise über die noch zu ändernden Parameter vor allem durch die Beobachtung des Datenverkehrs auf den verschiedenen Schnittstellen der Router.

Neben den Statistiken des Geräts, die Sie zum Beispiel in einer Telnet- oder Terminalsituation auslesen können, stehen Ihnen dazu noch weitere Möglichkeiten zur Verfügung.

Trace-Ausgaben

Zur Kontrolle der internen Abläufe im Router während oder nach der Konfiguration bieten sich die Trace-Ausgaben an. Durch einen solchen Trace werden z.B. die einzelnen Schritte bei der Verhandlung des PPPs angezeigt. Erfahrene Anwender können durch die Interpretation dieser Ausgaben evtl. Fehler beim Verbindungsaufbau aufspüren. Besonders positiv: Die aufzuspürenden Fehler können sowohl in der Konfiguration eigener *ELSA LANCOM* als auch bei der Gegenseite zu finden sein.



Die Trace-Ausgaben sind leicht zeitverzögert zum tatsächlichen Ereignis, jedoch immer in der richtigen Reihenfolge. Das stört im Regelfall die Interpretation der Anzeigen nicht, sollte aber bei genaueren Analysen berücksichtigt werden.

So starten Sie einen Trace

Der Trace-Aufruf folgt dieser Syntax:

```
trace [Schlüssel] [Parameter]
```

Der Befehl Trace, der Schlüssel, die Parameter und die Kombinationsbefehle werden jeweils durch Leerzeichen voneinander getrennt. Und was steckt hinter Schlüssel und Parameter?

Dieser Schlüssel ruft in Verbindung mit Trace die folgende Reaktion hervor:
?	zeigt einen Hilfetext an
+	schaltet eine Trace-Ausgabe ein
-	schaltet eine Trace-Ausgabe aus
#	schaltet zwischen verschiedenen Trace-Ausgaben um (Toggle)
kein Schlüssel	zeigt den aktuellen Zustand des Traces an

Dieser Parameter ruft beim Trace die folgende Anzeige hervor:
Status	Status-Meldungen der Verbindungen
Error	Fehler-Meldungen der Verbindungen
ELSA	Verhandlung des ELSA-Protokolls
PPP	Verhandlung des PPP-Protokolls

Dieser Parameter ruft beim Trace die folgende Anzeige hervor:
IPX-Router	IPX-Routing
RIP	IPX Routing Information Protocol
SAP	IPX Service Advertising Protocol
IPX-Watchdog	IPX-Watchdog-Spoofing
SPX-Watchdog	SPX-Watchdog-Spoofing
NetBIOS	IPX NetBIOS-Verwaltung
IP-Router	IP-Routing
IP-RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
SCRPT	Script-Verhandlung
IP-Masquerading	Vorgänge im Masquerading-Modul
DHCP	Dynamic Host Configuration Protocol
D-Kanal	Trace des D-Kanals des angeschlossenen ISDN-Busses

Dieser Kombinations-Befehl ruft beim Trace die folgende Anzeige hervor:
All	alle Trace-Ausgaben
Display	Status- und Error-Ausgaben
Protocol	ELSA- und PPP-Ausgaben
TCP-IP	IP-Rt.-, IP-RIP-, ICMP- und ARP-Ausgaben
IPX-SPX	IPX-Tr.-, RIP-, SAP-, IPX-Wd.-, SPX-Wd.-, und NetBIOS-Ausgaben
Time	zeigt vor der eigentlichen Trace-Ausgabe auch die Systemzeit an
Source	zeigt vor der eigentlichen Trace-Ausgabe auch das Protokoll an, das die Ausgabe veranlaßt hat

Die angehängten Parameter werden dabei von links nach rechts abgearbeitet. Dadurch kann ein zunächst aufgerufener Parameter anschließend auch wieder eingeschränkt werden.

Beispiele:

Dieser Schlüssel ruft in Verbindung mit Trace die folgende Reaktion hervor:
trace	zeigt alle Protokolle an, die während der Konfiguration Ausgaben erzeugen können, und den Zustand der jeweiligen Ausgaben (ON oder OFF).
trace + all	schaltet alle Trace-Ausgaben ein.
trace + protocol display	schaltet die Ausgabe aller Verbindungsprotokolle und der Status- und Fehlermeldungen ein.
trace + all - icmp	schaltet alle Trace-Ausgaben mit Ausnahme des ICMP-Protokolls ein.
trace ppp	zeigt den Zustand des PPPs an.
trace # ipx-rt display	schaltet die Trace-Ausgaben des IPX-Routers und der Display-Ausgaben um.
trace - time	schaltet die Ausgabe der Systemzeit vor der eigentlichen Trace-Ausgabe ab.



Hinweise zur Interpretation der Trace-Ausgaben finden Sie im Referenz-Teil des Handbuchs.

ELSA LANmonitor

Mit *ELSA LANmonitor* steht Ihnen ein kleines Überwachungstool zur Verfügung, mit dem Sie unter Windows-Betriebssystemen die wichtigsten Informationen über den Status Ihres Routers immer auf dem Bildschirm haben. Viele der internen Meldungen des Gerätes werden dabei in Klartext umgewandelt, zeigen Ihnen den aktuellen Zustand des Gerätes und helfen Ihnen so bei der Fehlersuche.

ELSA LANmonitor installieren

ELSA LANmonitor wird in der Regel automatisch mit der Konfigurationssoftware *ELSA LANconfig* installiert, und zwar auf dem Rechner, von dem aus Sie Ihren Router einstellen möchten.

Falls *ELSA LANmonitor* noch nicht auf Ihrem Rechner installiert ist, legen Sie die *ELSA LANCOM*-CD ein. Wenn das Setup-Programm beim Einlegen der CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' auf der *ELSA LANCOM*-CD und folgen den weiteren Hinweisen der Installationsroutine.

Aktivieren Sie bei der Installation die Option für 'ELSA LANmonitor'.



Sie können mit ELSA LANmonitor nur solche Geräte überwachen, die Sie Inband über das lokale Netzwerk erreichen. Dazu muß auf diesem Rechner das Netzwerkprotokoll TCP/IP installiert sein. Über die serielle Schnittstelle angeschlossene Router können Sie mit diesem Programm nicht ansprechen.

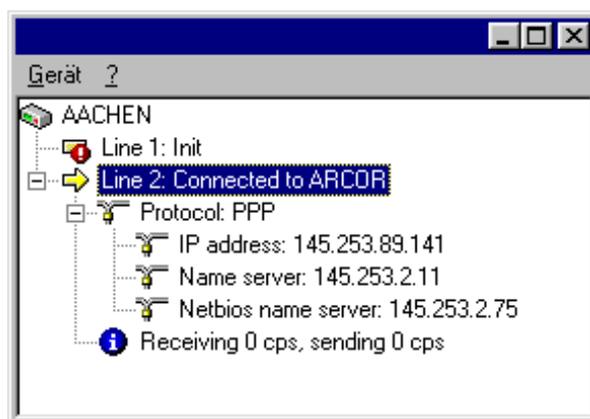
Internetverbindung kontrollieren mit *ELSA LANmonitor*

Als Beispiel für die Funktionen von *ELSA LANmonitor* zeigen wir Ihnen zuerst einmal, welche Informationen *ELSA LANmonitor* über den Verbindungsaufbau zu Ihrem Internet-Provider bereitstellt.

- ① Richten Sie den Router für die Verbindung zu Ihrem Provider ein, z.B. mit dem Setup-Assistenten von *ELSA LANconfig*. Wir haben für dieses Beispiel den Call-by-Call-Zugang von Arcor ausgewählt.
- ② Starten Sie *ELSA LANmonitor* mit **Start ▶ Programm ▶ ELSAlan ▶ ELSA LANmonitor**. Legen Sie ein neues Gerät an mit **Gerät ▶ Neu** und geben im folgenden Fenster die IP-Adresse für den Router an, den Sie überwachen wollen. Falls die Konfiguration des Gerätes mit einem Paßwort gesichert ist, geben Sie dieses gleich mit ein.

Alternativ können Sie im *ELSA LANconfig* das Gerät auswählen und mit **Extras ▶ Gerät überwachen** die Überwachung für ein Gerät starten.

- ③ *ELSA LANmonitor* legt automatisch einen neuen Eintrag in der Geräteliste an und zeigt zunächst den Zustand der B-Kanäle. Starten Sie Ihren Internet-Browser, und geben Sie eine beliebige Web-Seite ein. Sie können im *ELSA LANmonitor* nun sehen, wie auf einem Kanal eine Verbindung aufgebaut wird und welche Gegenstelle dabei gerufen wird. Sobald die Verbindung hergestellt ist, zeigt der B-Kanal durch das Pluszeichen vor dem Eintrag an, daß zu diesem Kanal weitere Informationen vorliegen. Durch Klicken auf das Pluszeichen öffnen Sie eine baumartige Struktur, in der Sie verschiedene Informationen ablesen können.



In diesem Beispiel können Sie aus den Protokoll-Informationen zum PPP ablesen, welche IP-Adresse der Provider Ihrem Router für die Dauer der Verbindung zugewiesen hat und welche Adressen für DNS- und NBNS-Server übermittelt wurden.

Unter den allgemeinen Informationen können Sie beobachten, mit welchen Übertragungsraten aktuell Daten mit dem Internet ausgetauscht werden.

- ④ Durch einen Klick mit der rechten Maustaste auf den aktiven Kanal können Sie die Verbindung manuell trennen.
- ⑤ Wenn Sie zusätzlich zu den Informationen in der Geräteliste von *ELSA LANmonitor* ein reduziertes Infofenster in Form eines LC-Displays wünschen, klicken Sie mit der rechten Maustaste auf den Namen des Gerätes und wählen **Kanalanzeige**.



Mit einem rechten Mausklick in das Anzeigefeld der Kanalanzeige richten Sie dieses virtuelle Display so ein, daß es immer im Vordergrund auf dem Bildschirm liegt.

- ⑥ Wenn Sie ein Protokoll der *LANmonitor*-Ausgaben in Form einer Datei wünschen, wählen Sie in Menü 'Ansicht' die 'Optionen' und wechseln zur Registerkarte 'Protokoll'. Aktivieren Sie die Protokollierung und stellen Sie ein, ob *LANmonitor* täglich, monatlich oder fortlaufend eine Protokolldatei erstellt.

Funktionen und Betriebsarten

Dieses Kapitel stellt Ihnen die Funktionen und Betriebsarten Ihres Gerätes vor. Dabei finden Sie u.a. Informationen zu den folgenden Punkten:

- Sicherheit für die Konfiguration
- Sicherheit für das LAN
- Gebührenmanagement
- ISDN-Verbindungen
- Festverbindungen und Backup-Verfahren
- GSM-Einwahl
- PPP-Unterstützung
- IPX-Routing
- IP-Routing
- DHCP-Server
- DNS-Server
- NetBIOS-Proxy
- IP-Pooling
- *ELSA LANCAPI*
- Zeitkontrolle
- Least-Cost-Router

Neben der Beschreibung der einzelnen Punkte geben wir Ihnen hier auch Hinweise, die Sie bei der Konfiguration unterstützen.

Ausführliche Konfigurationsbeispiele finden Sie im Workshop.

Eine detaillierte Beschreibung aller Parameter und Menüs finden Sie in der elektronischen Dokumentation.

Sicherheit für Ihre Konfiguration

Mit der Konfiguration des Gerätes legen Sie eine Reihe von wichtigen Parametern für den Datenaustausch fest: die Sicherheit des eigenen Netzes, die Kontrolle der Kosten und die Berechtigung einzelner Netzteilnehmer gehören z.B. dazu.

Die von Ihnen einmal eingestellten Parameter sollen natürlich nicht durch Unbefugte verändert werden. Daher bietet ein *ELSA LANCOM Business* die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

Paßwortschutz

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Paßworts. Solange Sie kein Paßwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern.

Das Feld zur Eingabe des Paßworts finden Sie im *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Bei einer Terminal- oder Telnetsitzung schalten Sie die Paßwortabfrage im Menü `/Setup/Config-Modul/Passw.Zwang` ein. Das Paßwort selbst wird in diesem Fall mit dem Befehl `passwd` gesetzt.

Die Login-Sperre

Die Konfiguration im *ELSA LANCOM Business* ist durch eine Login-Sperre gegen „Brute-Force-Angriffe“ geschützt. Es können sowohl die maximal zulässige Anzahl von fehlerhaften Login-Versuchen als auch die Dauer der Sperrung eingegeben werden.

Diese Parameter gelten global für alle Konfigurationsmöglichkeiten (Outband, Telnet, TFTP/*ELSA LANconfig* und SNMP). Tritt auf einem Zugang die Sperre in Kraft, so sind auch alle anderen Zugänge automatisch gesperrt.

Zur Konfiguration der Login-Sperre stehen im *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security' bzw. im Menü `/Setup/Config-Modul` die folgenden Einträge zur Verfügung:

- 'Sperre aktivieren nach' (Login-Fehler)
- 'Dauer der Sperre' (Sperr-Minuten)

Zugangskontrolle über TCP/IP

Mit einer speziellen Filterliste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfiguration-Sitzungen über Telnet oder TFTP (*ELSA LANconfig*) bezeichnet.

Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit Telnet oder TFTP ein Zugriff auf den Router gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen.

Die Zugangsliste finden Sie im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein' bzw. im Menü `/Setup/TCP-IP-Modul/Zugangsliste`.

Sicherheit für Ihr LAN

Sie mögen es sicher nicht, wenn jeder Außenstehende einfach die Daten auf Ihrem Firmen-Server einsehen oder verändern kann. Ein *ELSA LANCOM Business* bietet verschiedene Möglichkeiten, den Zugriff von außen einzuschränken:

- Zugangsschutz mit Name, Paßwort und Rufnummer
- Rückruf an festgelegte Rufnummern
- Filterung von Datenpaketen
- IP-Masquerading (auch NAT oder PAT genannt)

Die Kontrolle

Welcher „Identifizier“ zur Erkennung des Anrufers verwendet werden soll, wird im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Rufannahme' bzw. im Menü / *Setup/WAN-Modul/Schutz* eingestellt. Zur Auswahl stehen die folgenden Möglichkeiten:

- keiner: Anrufe aller Gegenstellen werden angenommen.
- Name: Es werden nur Anrufe von solchen Gegenstellen angenommen, die in der Namenliste eingetragen sind.
- Nummer: Es werden nur Anrufe von solchen Gegenstellen angenommen, die in der Nummernliste eingetragen sind.
- Name oder Nummer: Es werden nur Anrufe von solchen Gegenstellen angenommen, die in der Nummernliste **oder** in der Namenliste eingetragen sind.

Die Identifizierung setzt natürlich voraus, daß die entsprechende Information vom Anrufer auch übermittelt wird.

Überprüfung des Namens

Bei Verbindungen über PPP kann auch der Name der Gegenstelle übertragen werden.

Dazu muß allerdings zunächst eine Verbindung aufgebaut werden, weil der Name nicht über den D-Kanal ausgetauscht werden kann.

Die Reaktion der Router ist klar: Wenn ein Schutz über den Namen vereinbart ist, werden nur Anrufe mit bekannten Namen angenommen, die anderen abgelehnt.

Beim PPP-Protokoll wird überprüft, ob der Name der Gegenstelle in der PPP-Liste als Benutzername vorhanden ist. Fehlt der Benutzername, wird der Gerätenamen als Name der Gegenstelle angenommen und geprüft. Die PPP-Liste finden Sie im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Protokolle' bzw. im Menü / *Setup/WAN-Modul/PPP-Liste*.

Kein Paßwort? Doch, diese besondere Möglichkeit gibt es beim PPP: Hier kann zusätzlich ein speziell für dieses Protokoll gültiger Schutz nach PAP (Password Authentication Protocol) oder CHAP (Challenge Handshake Authentication Protocol) verlangt werden. Dabei handelt es sich um den Schutz, den das eigene Gerät von der Gegenstelle verlangt.



Die Sicherungsverfahren PAP oder CHAP wenden Sie natürlich nicht an, wenn Sie selber mit dem ELSA LANCOM z.B. einen Internet-Service-Provider anwählen. Sie werden den ISP wahrscheinlich nicht dazu bewegen können, eine Anfrage an ihn nach einem Paßwort zu beantworten ...

Und woher kommen Name und Paßwort des Anrufers?

- Bei PPP werden Name und Paßwort beim Verbindungsaufbau mit der Gegenstelle eingegeben, z.B. im entsprechenden Fenster einer Verbindung im DFÜ-Netzwerk. Wenn der Router selbst eine Verbindung aufbaut, werden Gerätenamen, Paßwort und Benutzername aus der PPP-Liste verwendet.

Überprüfung der Nummer

Beim Anruf über eine ISDN-Leitung wird in den meisten Fällen über den D-Kanal die Rufnummer des Anrufers übertragen, schon bevor eine Verbindung zustande kommt (CLI – Calling Line Identifier).

Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen. Ist ein Schutz im ELSA LANCOM über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekanntem Rufnummern abgelehnt.

Der Schutz mit Hilfe der Rufnummer kann mit allen B-Kanal-Protokollen (Layern) verwendet werden.

Der Rückruf

Eine besondere Variante des Zugriffsschutzes wird mit der Rückruffunktion erreicht: Dazu wird in der Namenliste für den gewünschten Anrufer die Option 'Rückruf' aktiviert und ggf. die Rufnummer angegeben.

Mit den Einstellungen in Namen- und Nummernliste und der Auswahl des Protokolls (PPP) können Sie das Rückrufverhalten Ihrer Router steuern:

- Der Router kann den Rückruf ablehnen.
- Es kann eine voreingestellte Rufnummer zurückrufen.
- Die Rufnummer für den Rückruf kann vom Anrufer frei eingegeben werden.

Und ganz nebenbei steuern Sie über die Einstellungen die Verteilung der Kosten für die Verbindung. Ist in der Namenliste ein Rückruf 'Nach Name' vereinbart, übernimmt der rückrufende Router alle Gebühren bis auf eine, die für die Namensübermittlung benötigt wird. Ebenfalls eine Einheit fällt für den Router an, wenn der Anrufer nicht über CLI iden-

tifiziert wird. Ist dagegen eine Identifizierung über die Rufnummer des Anrufers erlaubt und möglich, kommt der Anrufer sogar ganz ohne Kosten weg.

Wenn der Router selbst zurückrufen soll, dann kann für viele Gegenstellen auch das Fast-Call-Back-Verfahren (zum Patent angemeldet) verwendet werden. Dies beschleunigt die Rückrufprozedur um ein beträchtliches.

Das Versteck – IP-Masquerading (NAT, PAT)

Eine der häufigsten Aufgaben für Router ist heute die Anbindung vieler Arbeitsplätze in einem LAN an das Netz der Netze, das Internet. Jeder soll nach Möglichkeit direkt von seinem Arbeitsplatz aus auf das WWW zugreifen und sich brandaktuelle Informationen für seine Arbeit holen können.

Aber da gibt es Einwände der Netzwerkbetreuer, die sich um die Sicherheit der Daten im firmeneigenen Netz sorgen: Jeder Arbeitsplatzrechner im WWW? Da kann doch dann auch jeder von außen dran! – Kann er nicht!

IP-Masquerading heißt das Versteck für alle Rechner im Internet. Dabei wird nur das Routermodul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt dabei Internet und Intranet wie eine Wand. IP-Masquerading wird daher auch als „Firewall-Technik“ bezeichnet.

Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routingtabelle finden Sie im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' bzw. im Menü /Setup/IP-Router/IP-Routing-Tab.

Weitere Informationen finden Sie im Abschnitt 'IP-Routing: IP-Masquerading'.

Gebührenmanagement

Die Eigenschaft des Routers, Verbindungen selbständig zu allen gewünschten Gegenstellen aufzubauen und sie mit dem Ende der Übertragung wieder zu beenden, ermöglicht dem Benutzer sehr komfortablen Zugriff auf Internet oder entfernte Rechner und Netze. Bei der Datenübertragung über ISDN-Wählleitungen können jedoch durch Fehlkonfiguration des Routers (z.B. bei der Filterkonfiguration) oder durch übermäßigen Gebrauch des Angebots (z.B. andauerndes Surfen im Internet) recht hohe Telefonkosten entstehen.

Gebührenabhängige Verbindungsbegrenzung

Um diese Kosten zu begrenzen, bietet die Software die Möglichkeit, die verfügbaren Gebühren für eine bestimmte Periode einzuschränken. Im Default-Zustand dürfen z.B.

maximal 830 Gebühreneinheiten pro Woche verbraucht werden. Ist diese Grenze erreicht, erlaubt der Router keinen weiteren aktiven Verbindungsaufbau.



*Die Gebührenüberwachung des Routers können Sie am besten bei freigeschalteter „Gebühreninformation **während** der Verbindung“ im ISDN-Netz (nach AOCD) nutzen. Beantragen Sie ggf. die Freischaltung dieses Merkmals bei Ihrer Telefongesellschaft. Eine Gebührenüberwachung mit dem Merkmal „Gebühreninformation **nach** der Verbindung“ ist im Prinzip auch möglich, jedoch werden dabei ggf. Dauerverbindungen nicht erkannt!*



Wenn Sie das Least-Cost-Routing für die Router-Module eingeschaltet haben, werden ggf. auch Verbindungen über Provider aufgebaut, die keine Gebühreninformationen übertragen!

Zeitabhängige Verbindungsbegrenzung

Dieser Mechanismus greift jedoch nicht mehr, wenn am ISDN-Anschluß keine Gebühreninformationen übertragen werden. Das ist z.B. dann der Fall, wenn die Übermittlung der Gebühreninformationen entweder nicht beantragt wurde oder die Telefongesellschaft diese Informationen grundsätzlich nicht übermittelt.

Um die Telefonkosten trotzdem begrenzen zu können, kann die maximale Verbindungsdauer auch mit Hilfe der Zeit gesteuert werden. Dazu wird ähnlich dem Gebührenbudget ein Zeitbudget für eine Periode vereinbart. Im Default-Zustand dürfen z.B. für maximal 210 Minuten pro Woche aktiv Verbindungen aufgebaut werden.



Wird eine der beiden Grenzen erreicht, werden automatisch alle offenen Router-Verbindungen beendet, die der Router selbst aufgebaut hat. Erst nach dem Ablauf der aktuellen Periode werden die Budgets wieder freigegeben und aktive Verbindungen ermöglicht. Der Administrator kann die Budgets natürlich auch vorzeitig wieder freigegeben!

Mit einem Budget von 0 Einheiten bzw. 0 Minuten kann die Gebühren- bzw. Zeitüberwachung der Routerfunktionen ausgeschaltet werden.



Nur die Router-Funktionen sind durch den Gebühren- oder Zeitschutz abgesichert! Verbindungen über LANCAP1 werden davon nicht erfaßt.

Einstellungen im Gebührenmodul

Sie finden die Interface-Einstellungen im *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Gebühren' oder bei Telnet- oder Terminalsitzungen unter /Setup/Gebuehren-Modul.

Im Gebührenmodul können Sie die Onlinezeit und registrierte Gebühren einstellen, überwachen und für den Aufbauschutz nutzen.

- Tage/Periode
Dauer einer Überwachungsperiode in Tagen angegeben
- Budget-Einheiten, Minuten-Budget
Maximale Einheiten bzw. Online-Minuten in einer Überwachungsperiode
- Rest-Budget, Rest-Minuten
Verfügbare Einheiten bzw. Online-Minuten in der gegenwärtigen Periode
- Router-Einheiten, Router-Minuten
Einheiten bzw. Online-Minuten über alle Perioden
- Gesamteinheiten
Alle im Gerät anfallenden Gebühren
- Tabelle-Budget, Zeit-Tabelle
Tabellen mit Gebühren bzw. Zeiten für die jeweiligen Module



Die Informationen über die Gebühren und Verbindungszeiten werden über einen Bootvorgang hinaus gesichert (z.B. beim Einspielen einer neuen Firmware) und gehen erst verloren, wenn das Gerät ausgeschaltet wird. Alle hier erwähnten Zeitangaben werden in Minuten gemacht.

ISDN-Verbindungen

Die Datenkommunikation zwischen zwei ISDN-Endgeräten läuft über ISDN-Verbindungen ab. Bei diesen Verbindungen kann es sich prinzipiell um Wählverbindungen oder Festverbindungen handeln.

Die Routermodule ermitteln zunächst nur, zu welcher Gegenstelle ein Datenpaket übertragen werden soll. Damit die entsprechende Verbindung ausgewählt und ggf. aufgebaut werden kann, müssen verschiedene Parameter für alle notwendigen ISDN-Verbindungen vereinbart werden. Diese Parameter sind in unterschiedlichen Listen abgelegt, deren Zusammenspiel die richtigen Verbindungen erlaubt.

Die folgenden Abschnitte stellen Ihnen die Listen und die darin enthaltenen Parameter kurz vor, zeigen den Zusammenhang zu anderen Listen und Parametern und wie sie in der Software konfiguriert werden.

Namenliste

Sie finden die Namenliste im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Gegenstellen' oder bei Telnet- oder Terminalsitzungen unter / Setup/WAN-Modul/Namenliste.

Um die verfügbaren Gegenstellen zu definieren, werden sie in der Namenliste mit einem geeigneten Namen und zusätzlichen Parametern angelegt:

- Name
Mit diesem Namen wird die Gegenstelle in den Routermodulen identifiziert.
- Rufnummer
Diese Rufnummer soll angerufen werden, wenn der Router selbst aktiv eine Verbindung zur Gegenstelle aufbauen soll.
Wenn die Gegenstelle unter verschiedenen Rufnummern erreicht werden kann, tragen Sie die weiteren Rufnummern in der Round-Robin-Liste ein.
Wird diese Gegenstelle über eine Festverbindung erreicht, kann hier die Rufnummer für eine Backup-Leitung über Wählverbindung angegeben werden.
- Haltezeiten
Diese Zeiten geben an, wie lange die B-Kanäle aktiv bleiben, nachdem
 - bei statisch aufgebauten Kanälen für die Haltezeit B1 keine Daten mehr übertragen wurden.
 - bei dynamisch aufgebauten Kanälen für die Haltezeit B2 der Datendurchsatz unter einem fest definierten Schwellwert liegt.
- Layername
Der Layer steht für eine Sammlung von Protokollen, die für diese Verbindung verwendet werden sollen. Der Layer muß auf beiden Seiten der Verbindung gleich eingestellt sein.
- Rückruf
Wenn der Router einen Anruf von dieser Gegenstelle erhält, können Sie hier optional einstellen, daß der Anruf nicht angenommen wird. Stattdessen wird die Gegenstelle zurückgerufen mit den folgenden Optionen:
 - normaler Rückruf
 - Rückruf nach dem schnellen ELSA-Verfahren
 - Rückruf nach Überprüfung des Namens
 - selbst den Rückruf der Gegenstelle nach dem schnellen ELSA-Verfahren erwarten

Interface-Einstellungen

Sie finden die Interface-Einstellungen im *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Interfaces' oder bei Telnet- oder Terminalsitzungen unter `/Setup/WAN-Modul/Interface-Liste`.

In den Interface-Einstellungen legen Sie für jedes Interface (also jeden S₀-Anschluß) die allgemeinen Parameter fest. Diese Parameter gelten für alle Betriebsarten der Geräte. Es sind im einzelnen:

- Das D-Kanal-Protokoll, das an diesem S₀-Anschluß verwendet wird.

Automatische Erkennung, DSS1 (Euro-ISDN), DSS1 Punkt-zu-Punkt, 1TR6, Festverbindung Gruppe 0

- Festverbindungsoption
B-Kanal, der ggf. für die Festverbindung verwendet werden soll.
- Anwahlpräfix
Nummer, die bei abgehenden Rufen der Rufnummer vorangestellt wird, z.B. die Amtskennziffer beim Betrieb an TK-Anlagen.

Router-Interface-Einstellungen

Sie finden die Router-Interface-Einstellungen im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Allgemein' oder bei Telnet- oder Terminal-sitzungen unter `/Setup/WAN-Modul/Router-Interface-Liste`.

In den Router-Interface-Einstellungen legen Sie für jedes Interface (also jeden S₀-Anschluß) die Parameter fest, die in der Betriebsart als Router verwendet werden. Diese Parameter gelten nicht für die anderen Betriebsarten der Geräte. Es sind im einzelnen:

- Rufnummern (MSN/EAZ)
Auf diese Rufnummern reagiert der Router bei eingehenden Anrufen. Mehrere Rufnummern werden durch Semikolon getrennt. Ohne Eingabe der Rufnummer reagiert der Router auf alle anliegenden Rufnummern.

Die erste der eingetragenen Rufnummern wird bei aktivem Verbindungsaufbau an die Gegenstelle übertragen. Ohne Eingabe der Rufnummer wird die Haupt-MSN des Anschlusses übertragen.
- Option für Y-Verbindung
Schalten Sie diese Option ein, wenn die beiden B-Kanäle des Anschlusses parallel Verbindungen zu unterschiedlichen Gegenstellen aufbauen können sollen.
- Unterdrückung der eigenen Rufnummer
Schalten Sie diese Option ein, wenn die eigene Rufnummer bei aktivem Verbindungsaufbau des Routers nicht bei der Gegenstelle angezeigt werden soll.

Diese Funktion muß vom Netzbetreiber unterstützt werden.



LANCAPi-Interface-Einstellungen

Sie finden die *LANCAPi*-Interface-Einstellungen im *ELSA LANconfig* im Konfigurationsbereich 'LANCAPi' auf der Registerkarte 'Allgemein' oder bei Telnet- oder Terminal-sitzungen unter `/Setup/LANCAPi-Modul/Interface-Liste`.

In den Router-Interface-Einstellungen legen Sie für jedes Interface (also jeden S₀-Anschluß) die Parameter fest, die für die *LANCAPI* verwendet werden. Diese Parameter gelten nicht für die anderen Betriebsarten der Geräte. Es sind im einzelnen:

- Rufnummern (MSN/EAZ)
Auf diese Rufnummern reagiert die *LANCAPI* bei eingehenden Anrufen. Mehrere Rufnummern werden durch Semikolon getrennt. Ohne Eingabe der Rufnummer reagiert der Router auf alle anliegenden Rufnummern.
- Zugriff auf die *LANCAPI*
Hier können Sie die Funktion der *LANCAPI* für das Interface ganz ausschalten, nur für ausgehende Rufe zulassen oder für ein- und ausgehende Rufe.
- Übertragung der eigenen Rufnummer
Normalerweise wird beim aktiven Verbindungsaufbau über die *LANCAPI* die Rufnummer übermittelt, die in der CAPI-Applikation eingestellt wurde. Falls diese Rufnummer fehlt oder nicht gültig ist, überträgt die *LANCAPI* keine Rufnummer. Mit dieser Option können Sie festlegen, daß bei fehlender Rufnummer der CAPI-Applikation stattdessen die erste im Feld 'Rufnummer' eingetragene Nummer übertragen wird.

Layer-Liste

Sie finden die Liste der Kommunikationslayer im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Allgemein' oder bei Telnet- oder Terminal-sitzungen unter `/Setup/WAN-Modul/Layer-Liste`.

In einem Layer definieren Sie eine bestimmte Kombination von Protokoll-Einstellungen, die für die Übertragung zu anderen Geräten verwendet werden sollen. Es sind im einzelnen:

- Layername
Unter diesem Namen werden die Protokoll-Einstellungen gespeichert. In der Namenliste wählen Sie die Einstellungen mit dem Layernamen für die entsprechende Verbindung aus.
- Encapsulation
Stellen Sie hier ein, ob den Datenpaketen ein Ethernet-Header hinzugefügt werden soll. Normalerweise reicht die Einstellung 'Transparent', nur bei HDLC-Verbindungen zu Fremdgeräten kann diese Einstellung notwendig sein.
- Layer-3
Layer-3-Protokoll für die Verbindung. Wird bei ankommenden Rufen teilweise automatisch erkannt.
Bei Verwendung von PPP ist ein zusätzlicher Eintrag in der PPP-Liste erforderlich.

Bei Verwendung von Scripts ist ein zusätzlicher Eintrag in der Script-Liste erforderlich.

- Layer-2
Layer-2-Protokoll für die Verbindung.
- Optionen
Aktiviert optional die Kompression der Daten und die Kanalbündelung. Diese Option wird nur wirksam, wenn Sie von den Protokollen auf Layer 2 und Layer 3 unterstützt werden.
- Layer-1
Layer-1-Protokoll für die Verbindung. Wird bei ankommenden Rufen teilweise automatisch erkannt.

Round-Robin-Liste

Sie finden die Round-Robin-Liste im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Gegenstellen' oder bei Telnet- oder Terminalsitzungen unter `/Setup/WAN-Modul/RoundRobin-Liste`.

Wenn eine Gegenstelle unter mehreren Rufnummern zu erreichen ist, tragen Sie zunächst die erste Rufnummer in der Namenliste und alle weiteren in der Round-Robin-Liste ein.

- Gegenstelle
Name der Gegenstelle, wie sie vorher in der Namenliste definiert wurde.
- Round-Robin
Weitere Rufnummern für diese Gegenstelle. Mehrere Nummern werden durch Bindestriche getrennt.
- Anfangen mit:
Geben Sie an, ob ein neuer Verbindungsaufbau mit der zuletzt erfolgreichen Nummer gestartet werden soll oder immer mit der ersten Nummer der Liste.

Kanal-Liste

Sie finden die Kanal-Liste im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Gegenstellen' oder bei Telnet- oder Terminalsitzungen unter `/Setup/WAN-Modul/Kanal-Liste`.

In der Kanal-Liste legen Sie fest, wie viele B-Kanäle für die Verbindung minimal und maximal verwendet werden sollen, welche Kanäle in welcher Reihenfolge aufgebaut werden und wie viele Kanäle bei einer Festverbindung ggf. als Backup-Leitung über Wählverbindungen verwendet werden sollen.

- Gegenstelle

Name der Gegenstelle, wie sie vorher in der Namenliste definiert wurde.

■ Mindestens

Minimale Anzahl von Kanälen, die für die Verbindung aufgebaut werden sollen.

Wird mehr als ein Kanal angegeben, entsteht für diese Verbindung eine statische Kanalbündelung. Der verwendete Layer muß in den Layer-2-Optionen auf Bündelung eingestellt sein.

■ Höchstens

Maximale Anzahl von Kanälen, die für die Verbindung aufgebaut werden sollen.

Werden mehr maximale als minimale Kanäle angegeben, entsteht für diese Verbindung eine dynamische Kanalbündelung. Der verwendete Layer muß in den Layer-2-Optionen auf Bündelung eingestellt sein.

■ Reihenfolge

Die Reihenfolge, in der die Kanäle aufgebaut werden sollen, wird in der Syntax [Interface]-[Kanal];[Interface]-[Kanal] usw. angegeben.

■ Backup

Anzahl der Kanäle, die bei einer Festverbindung über Wählleitungen aufgebaut werden sollen, wenn die Festverbindung gestört ist.

PPP-Liste

Sie finden die PPP-Liste im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Protokolle' oder bei Telnet- oder Terminalsitzungen unter / Setup/WAN-Modul/PPP-Liste.

In der PPP-Liste legen Sie zusätzlich Parameter für eine Verbindung fest, die PPP im Kommunikationslayer auf Layer 3 verwenden.

■ Gegenstelle

Name der Gegenstelle, wie sie vorher in der Namenliste definiert wurde.

■ Username

Benutzername, der zur Anmeldung bei der Gegenstelle verwendet wird.

■ Paßwort

Paßwort, das zur Anmeldung bei der Gegenstelle verwendet wird.

■ IP, NetBIOS, IPX

Protokolle, die über diese Verbindung übertragen werden dürfen.

■ Prüfung

Authentifizierungsverfahren, das der Router von der Gegenstelle verlangen soll.

■ Zeit, Wdh., Conf., Fail., Term.

Parameter zum Verhalten der Verbindung, die hier nicht näher beschrieben werden.

Script

Sie finden die Script-Liste im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Protokolle' oder bei Telnet- oder Terminalsitzungen unter / Setup/WAN-Modul/Script-Liste.

Wenn für die Anwahl der Gegenstelle die Abarbeitung eines Scripts erforderlich ist, können Sie hier das Script eintragen und der Gegenstelle zuordnen.

Das in der Layerliste für diese Verbindung ausgewählte Layer-3-Protokoll muß die Scriptverarbeitung unterstützen.

- Gegenstelle
Name der Gegenstelle, wie sie vorher in der Namenliste definiert wurde.
- Script
Tragen Sie hier das Script ein, wie im Referenzteil der Dokumentation beschrieben.

Rufannahme

Sie finden die Einstellungen für die Rufannahme im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Rufannahme' oder bei Telnet- oder Terminalsitzungen unter / Setup/WAN-Modul/Schutz.

Mit den Einstellungen für die Rufannahme legen Sie fest, unter welchen Umständen das Gerät ankommende Rufe annimmt. Diese Einstellungen gelten nur für die Routerfunktionen des Geräts.

- Alle
Alle Rufe werden angenommen.
- Name
Alle Rufe werden zunächst angenommen. In der Protokollverhandlung wird der Name ermittelt und geprüft, ob dieser Name in der Namenliste vorhanden ist. Nur dann bleibt die Verbindung bestehen, ansonsten wird sie wieder abgebaut.
- Nummer
Der Anruf wird nur angenommen, wenn die Gegenstelle in der Nummernliste eingetragen ist und die Rufnummer der Gegenstelle übermittelt wird.
- Name oder Nummer
Der Anruf wird angenommen, wenn eine der beiden Überprüfungen erfolgreich ist.

Nummernliste

Sie finden die Nummernliste im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Rufannahme' oder bei Telnet- oder Terminalsitzungen unter `/Setup/WAN-Modul/Nummernliste`.

Die Nummernliste wird für den passiven Verbindungsaufbau zum Schutz bei der Rufannahme und für den Start eines Rückrufs verwendet.

- Rufnummer
Rufnummer, die von der anrufenden Gegenstelle übermittelt wird (ggf. inkl. Landes- und Orts-Kennzahlen).
- Gegenstelle
Name der Gegenstelle, wie sie in der Namenliste definiert wurde. Ist in der Namenliste ein Rückruf definiert, wird diese Gegenstelle zurückgerufen.

Festverbindungen und Backup

Wird permanent über die ISDN-Verbindung gearbeitet, oder ist in kurzen Abständen ein wiederholter Zugriff notwendig, kann die Nutzung einer ISDN-Festverbindung wirtschaftlich sein. Da der D-Kanal bei Festverbindungen für die Datenübertragung nicht benötigt wird, die Bereitstellung des Steuerkanals jedoch entsprechend in Rechnung gestellt wird, bieten Festverbindungen ohne D-Kanal das beste Preis-Leistungs-Verhältnis.

Ist ein Kanal auf Dauer ausreichend, wäre die D64S zu wählen. Reicht der Durchsatz nicht aus, sollte die Einrichtung einer D64S2 in Betracht gezogen werden. Für Verbindungen zu zwei verschiedenen Gegenstellen verwenden Sie zweimal D64S. Diese Kombination wird im weiteren auch D64SY bezeichnet:

Festverbindung	Ausführung
D64S	Ein B-Kanal, kein D-Kanal zu einer Gegenstelle
D64S2	Zwei B-Kanäle, kein D-Kanal zu einer Gegenstelle
D64SY	Zwei B-Kanäle, kein D-Kanal zu zwei verschiedenen Gegenstelle

Alle drei Varianten werden im Router als Gruppe-0-Festverbindung in der Interface-Tabelle eingestellt. Unterschieden werden die Varianten durch das „YV-Flag“ in der Interface-Tabelle, durch den Eintrag 'Layer-2-Optionen' in der Layerliste und durch die Einträge in der Kanalliste.

So stellen Sie die Festverbindung ein

Die folgenden Einstellungen sind erforderlich, um den Router auf den Betrieb an den verschiedenen Festverbindungen vorzubereiten.

Einstellungen in der Interface-Tabelle

- In der Interface-Tabelle wird als Protokoll **Grp0** eingegeben.
- Das **YV.-Flag** muß für Verbindungen zu einer Gegenstelle den Wert **Aus** besitzen, bei Verbindungen zu zwei verschiedenen Gegenstellen den Wert **Ein**.
- Im verwendeten Layer kann bei Verbindungen mit einem B-Kanal als Layer-2-Option **compr.** eingetragen werden.
Bei Verbindungen mit zwei B-Kanälen zu einer Gegenstelle wird **buendeln** und ggf. zusätzlich **compr.** eingetragen.
Bei Verbindungen mit zwei B-Kanälen zu verschiedenen Gegenstellen kann **compr.** eingetragen werden.

Einstellungen in der Kanalliste

In der Kanalliste legen Sie fest, welche Kanäle für die Festverbindung verwendet werden sollen. Die Angabe der Kanäle und der Reihenfolge muß auf beiden Seiten der Verbindung gleich eingestellt werden. Außerdem tragen Sie hier (auch auf beiden Seiten der Verbindung gleich) ein, wie viele Kanäle evtl. für Backup eingesetzt werden sollen.

Geraetenname	Min	Max	Reihenfolge	Backup
FVG0	2	2	1-1;1-2	0

Einstellungen in der Namen-Liste

Bei Verwendung einer Gruppe-0-Festverbindung gehen die Geräte nach dem Einschalten automatisch an die Leitung und bauen mit dem Default-Layer eine Verbindung auf.

Soll ein anderer Layer, der Dial-Backup-Mechanismus oder eine dynamische Bündelung über Wählleitungen verwendet werden, so muß die Gegenstelle in der Namenliste auftauchen.

Geraetenname	Rufnummer	B1-HZ	B2-HZ	Layername	Rueckruf
FVG0	1234	20	0	PPPHDLC	Aus

Die Rufnummer wird für den Aufbau von weiteren Kanälen über Wählverbindungen verwendet, die dynamisch zur Festverbindung gebündelt werden sollen. Evtl. benötigte weitere Rufnummern können in der Round-Robin-Liste eingetragen werden.

Wenn die Festverbindung durch Störungen nicht verfügbar ist und auch die evtl. dynamisch gebündelten Wählverbindungen durch den zwischenzeitlichen Rückgang des Datendurchsatzes abgebaut wurden, werden die eingetragenen Rufnummern zum Aufbau der Backupverbindungen verwendet.

Einstellungen in der Layer-Liste

Eine Gruppe 0 Festverbindung wird zunächst immer zur Default-Gegenstelle, d.h. mit dem bei der Default-Gegenstelle eingetragenen Layer aufgebaut. Ist keine Default-Gegenstelle oder bei dieser kein Layer-Eintrag vorhanden, so erfolgt der Aufbau mit dem in der Layer-Liste als DEFAULT eingetragenen Layer. Falls dort auch kein DEFAULT-Eintrag vorhanden ist, so erfolgt der Aufbau mit folgenden Layer-Einstellungen.

Layername	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	Trans	PPP	Trans	keine	HDLC64K

Beispiel: D64S2, dynamische Bündelung (ein Kanal), kein Backup

In der Nameliste weisen Sie der Festverbindung den Layer 'MLHDLC' zu und geben die Rufnummer für die dynamische Wählleitung an:

Geraetenname	Rufnummer	B1-HZ	B2-HZ	Layername	Rueckruf
FVG0	123456	20	20	MLHDLC	Aus

In der Kanalliste tragen Sie die benötigte Anzahl der Kanäle ein und legen fest, welche Kanäle verwendet werden sollen. Es wird kein Backup-Kanal angegeben.

Geraetenname	Min	Max	Reihenfolge	Backup
FVG0	2	3	1-1;1-2;2-1	0

Beispiel: D64S2, dynamische Bündelung (ein Kanal), Backup (ein Kanal)

Der Eintrag in der Nameliste bleibt gleich. In der Kanalliste legen Sie einen Backup-Kanal an.

Geraetenname	Min	Max	Reihenfolge	Backup
FVG0	2	3	1-1;1-2;2-1	1

Beispiel: D64S2, keine Bündelung, Backup (zwei Kanäle)

Der Eintrag in der Nameliste bleibt gleich. In der Kanalliste legen Sie einen Backup-Kanal an.

Geraetenname	Min	Max	Reihenfolge	Backup
FVG0	2	3	1-1;1-2	2

Einwahl über GSM

ELSA LANCOM Business eignet sich mit einer größeren Anzahl an verfügbaren B-Kanälen ideal als Einwahlknoten (Remote-Access-Server) für kleinere und mittlere Unternehmen. Um auch den Außendienstmitarbeitern unterwegs die Möglichkeit zum Zugriff auf das Firmennetz zu geben, unterstützt der Router auch das Protokoll V.110 und ermöglicht so die Einwahl von Notebooks über Mobiltelefone nach dem GSM-Standard.

Der Zugang über GSM wird wie ein normaler Remote-Access-Zugang eingerichtet, z.B. über den komfortablen Assistenten in *ELSA LANconfig*. Anschließend muß nur der verwendete Layer auf das entsprechende Protokoll angepaßt werden.

Layername	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	Trans	APPP	Trans	keine oder comp.	V.110 9600



Die Nutzung von Datendiensten über ein GSM-Mobiltelefon ist nicht bei allen Providern in Standardvertrag enthalten und muß ggf. gebührenpflichtig freigeschaltet werden. Manche Provider unterscheiden dabei auch die Freischaltung für abgehende und ankommende Datenanrufe!

Point-to-Point Protocol

Router von ELSA unterstützen auch das Point-to-Point Protocol (PPP). PPP ist ein Sammelbegriff für eine ganze Reihe von WAN-Protokollen, die das Zusammenspiel von Routern verschiedener Hersteller erleichtern, denn dieses Protokoll wird von fast allen Herstellern unterstützt.

Und gerade weil das PPP nicht einer bestimmten Betriebsart der Router zugeordnet werden kann und natürlich auch wegen der großen und in Zukunft noch weiter steigenden Bedeutung dieser Protokoll-Familie, möchten wir Ihnen die Funktionen der Geräte im Zusammenhang mit dem PPP hier in einem eigenen Abschnitt vorstellen.

Das Protokoll

Was ist PPP?

Das Point-to-Point Protocol (PPP) wurde speziell für Netzwerkverbindungen über serielle Kanäle entwickelt und hat sich als Standard für Verbindungen zwischen Routern behauptet. Es realisiert folgende Funktionen:

- Paßwortschutz nach PAP oder CHAP
- Rückruf-Funktionen

- Aushandlung der über die aufgebaute Verbindung zu benutzenden Netzwerkprotokolle (z.B. IP oder IPX). Dazu gehören auch für diese Protokolle notwendigen Parameter wie z.B. IP/IPX-Adressen. Diese Verhandlung läuft über die Protokolle IPCP und IPXCP (IP Control Protocol und IPX Control Protocol) ab.
- Überprüfung der Verbindung mit dem LCP (Link Control Protocol)
- Bündelung von mehreren Kanälen (Multilink PPP)

Für Router-Verbindungen ist PPP der Standard für die Kommunikation zwischen Geräten bzw. der WAN-Verbindungs-Software unterschiedlicher Hersteller. Um eine erfolgreiche Datenübertragung nach Möglichkeit sicherzustellen, erfolgt die Verhandlung der Verbindungsparameter und eine Einigung auf einen gemeinsamen Nenner über standardisierte Steuerungsprotokolle (LCP, IPCP, IPXCP, CCP), die im PPP enthalten sind.

Wozu wird PPP verwendet?

Das Point-to-Point Protocol wird bei folgenden Anwendungen sinnvoll eingesetzt:

- aus Kompatibilitätsgründen z.B. bei Kommunikation mit Fremdroutern
- Remote-Access von entfernten Arbeitsplatzrechnern mit ISDN-Adaptern
- Internet-Access (mit der Übermittlung von Adressen)

Das im *ELSA LANCOM* implementierte PPP kann synchron oder asynchron sowohl über eine transparente HDLC-Verbindung als auch über eine X.75-Verbindung verwendet werden.

Die Phasen einer PPP-Verhandlung

Der Verbindungsaufbau über PPP startet immer mit einer Verhandlung der Parameter, die für die Verbindung verwendet werden sollen. Diese Verhandlung läuft in vier Phasen ab, deren Kenntnis für die Konfiguration und Fehlersuche wichtig sind.

- Establish-Phase
Nach einem Verbindungsaufbau über den Datenkommunikationsteil startet die Aushandlung der Verbindungsparameter über das LCP.
Es wird festgestellt, ob die Gegenstelle auch bereit ist, PPP zu benutzen, die Paketgrößen und das Authentifizierungsprotokoll (PAP, CHAP oder keines) werden festgelegt. Danach wechselt das LCP in den Opened-Zustand.
- Authenticate-Phase
Falls notwendig, werden danach die Paßworte ausgetauscht. Bei Authentifizierung nach PAP wird das Paßwort nur einmalig übertragen. Bei Benutzung von CHAP wird ein verschlüsseltes Paßwort periodisch in einstellbaren Abständen gesendet.
Evtl. wird in dieser Phase auch ein Rückruf über CBCP (Callback Control Protocol) ausgehandelt.
- Network-Phase

Im *ELSA LANCOM* sind die Protokolle IPCP und IPXCP implementiert.

Nach erfolgreicher Übertragung des Paßwortes können die Netzwerk-Layer IPCP und/oder IPXCP aufgebaut werden.

Ist die Verhandlung der Parameter für mindestens eines der Netzwerk-Layer erfolgreich verlaufen, können von den Router-Modulen IP- und/oder IPX-Pakete auf der geöffneten (logischen) Leitung übertragen werden.

■ Terminate-Phase

In der letzten Phase wird die Leitung geschlossen, wenn die logischen Verbindungen für alle Protokolle abgebaut sind.

Die PPP-Verhandlung im *ELSA LANCOM*

Der Verlauf einer PPP-Verhandlung wird in der PPP-Statistik der Geräte protokolliert und kann im Fehlerfall mit Hilfe der dort detailliert gezählten Protokoll-Pakete überprüft werden.

Eine weitere Analyse-Möglichkeit bieten die PPP-Trace-Ausgaben. Mit dem Befehl

```
trace + ppp
```

kann die Ausgabe der ausgetauschten PPP-Protokoll-Frames innerhalb einer Terminal-Sitzung gestartet werden. Wird diese Terminal-Sitzung in einem Log-File protokolliert, kann nach Abbruch der Verbindung eine detaillierte Analyse erfolgen.

Die PPP-Liste

In der PPP-Liste können Sie für jede Gegenstelle, die mit Ihrem Netz Kontakt aufnimmt, eine eigene Definition der PPP-Verhandlung festlegen. Die PPP-Liste finden Sie im *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Protokolle' bzw. im Menü /Setup/WAN-Modul/PPP-Liste.

Die PPP-Liste kann 64 Einträge aufnehmen, die folgende Werte enthalten:

In dieser Spalte der PPP-Liste tragen Sie folgende Werte ein:
Gerätename	Name der Gegenstelle, mit dem sie sich bei Ihrem Router anmeldet
Sicherung	Verfahren zur Sicherung der PPP-Verbindung ('PAP', 'CHAP' oder 'keine'). Ihr eigener Router verlangt von der Gegenstelle die Einhaltung dieses Verfahrens! Nicht etwa umgekehrt. Daher bietet sich die Sicherung nach 'PAP' oder 'CHAP' nicht an bei Verbindungen zu Internet-Service-Providern, die uns vielleicht kein Paßwort übermitteln wollen. Für solche Verbindungen wählen Sie 'keine' Sicherung.
Paßwort	Paßwort, das von Ihrem Router an die Gegenstelle übertragen wird (falls gefordert). * in der Liste zeigen an, daß ein Eintrag vorhanden ist.

In dieser Spalte der PPP-Liste tragen Sie folgende Werte ein:
Zeit	Zeit zwischen zwei Überprüfungen der Verbindung mit LCP. Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z.B. 2 für 20 Sek.). Gleichzeitig die Zeit zwischen zwei Überprüfungen der Verbindung nach CHAP. Diese Zeit geben Sie in Minuten ein. Für Gegenstellen mit Windows 95, Windows 98 oder Windows NT muß die Zeit auf '0' gesetzt werden!
Wdh	Anzahl der Wiederholungen für den Überprüfungsversuch. Mit mehreren Wiederholungen schalten Sie den Einfluß kurzfristiger Leitungsstörungen aus. Erst wenn alle Versuche erfolglos bleiben, wird die Verbindung abgebaut. Der zeitliche Abstand zwischen zwei Wiederholungen beträgt 1/10 der Zeit zwischen zwei Überprüfungen. Gleichzeitig die Anzahl der „Configure Requests“, die der Router maximal aussendet, bevor es von einer Leitungsstörung ausgeht und selber die Verbindung abbaut.
Conf, Fail, Term	Mit diesen Parametern wird die Arbeitsweise des PPPs beeinflusst. Die Parameter sind in der RFC 1661 definiert und werden hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in dieser RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im allgemeinen sind die Default-Einstellungen ausreichend. Diese Parameter können nur über SNMP oder TFTP (mit dem Konfigurationsprogramm <i>ELSA LANconfig</i>) verändert werden!
Username	Name, mit dem sich Ihr Router bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Gerätenamen Ihres Routers verwendet.
Rechte	Netzwerkprotokolle, die über diese Verbindung geroutet werden sollen: IP, IPX, NTB (NetBIOS). NetBIOS erfordert immer eines der beiden anderen Protokolle.

Alles o.k.? Leitungsüberprüfung mit LCP

Beim Verbindungsaufbau über PPP handeln die beteiligten Geräte ein gemeinsames Verhalten während der Datenübertragung aus. Sie entscheiden z.B. zunächst, ob mit den Einstellungen der Sicherungsverfahren, Namen und Paßwörter überhaupt eine Verbindung zustande kommen darf.

Wenn die Verbindung einmal steht, kann mit Hilfe des LCPs die Zuverlässigkeit der Leitung ständig überprüft werden. Innerhalb des Protokolls geschieht dies mit dem LCP-Echo-Request und dem zugehörigen LCP-Echo-Reply. Der LCP-Echo-Request ist eine Anfrage in Form eines Datenpakets, das neben den reinen Nutzdaten zur Gegenstelle übertragen wird. Wenn auf diese Anfrage eine gültige Antwort (LCP-Echo-Reply) zurückgeschickt wird, ist die Verbindung zuverlässig und stabil. Zur dauerhaften Überprüfung der Verbindung wird dieser Request in bestimmten Abständen wiederholt.

Was passiert nun, wenn der Reply ausbleibt? Zuerst werden einige Wiederholungen der Anfrage gestartet, um kurzfristige Störungen der Leitung auszuschließen. Wenn alle

diese Wiederholungen unbeantwortet bleiben, wird die Leitung abgebaut und ein Ersatzweg gesucht. Der kann z.B. in Form einer Backup-Leitung gefunden werden.



Beim Remote-Access von einzelnen Arbeitsplatzrechnern mit Windows 95, Windows 98 oder Windows NT empfehlen wir, die regelmäßigen LCP-Anfragen auszuschalten, weil diese Betriebssysteme die LCP-Echo-Requests nicht beantworten.

Das Verhalten der LCP-Anfragen stellen Sie in der PPP-Liste für jede Verbindung einzeln ein. Mit dem Eintrag in die Felder 'Zeit' und 'Wdh.' legen Sie fest, in welchen Abständen die LCP-Anfrage gestellt werden soll und wie viele Wiederholungen beim Ausbleiben der Antwort gestartet werden, bis die Leitung als gestört bezeichnet werden darf. Mit einer Zeit von '0' und '0' Wiederholungen stellen Sie die LCP-Requests ganz ab.

Zuweisung von IP-Adressen über PPP

Zur Verbindung von Rechnern, die TCP/IP als Netzwerkprotokoll einsetzen, benötigen alle Beteiligten eine gültige und eindeutige IP-Adresse. Wenn nun eine Gegenstelle keine eigene IP-Adresse hat (z.B. der einzelne Arbeitsplatzrechner eines Teleworkers), dann kann der *ELSA LANCOM* ihm für die Dauer der Verbindung eine IP-Adresse zuweisen und so die Kommunikation ermöglichen.

Diese Art der Adreßzuweisung wird während der PPP-Verhandlung durchgeführt und nur für Verbindungen über das WAN eingesetzt. Die Zuweisung von Adressen mittels DHCP wird dagegen innerhalb eines lokalen Netzwerks verwendet.



Die Zuweisung einer IP-Adresse wird nur dann möglich, wenn der ELSA LANCOM die Gegenstelle beim Eintreffen des Anrufs über die Rufnummer oder den Namen identifizieren kann, d.h. die Authentifizierung erfolgreich war.

■ Beispiel: Remote-Access

Die Zuweisung der Adresse wird durch einen speziellen Eintrag in der IP-Routing-Tabelle ermöglicht. Neben dem Eintrag der IP-Adresse, die der Gegenstelle aus dem Feld 'Router-Name' zugewiesen werden soll, wird als Netzmaske die 255.255.255.255 angegeben. Der Routername ist in diesem Fall der Name, mit dem sich die Gegenstelle beim *ELSA LANCOM* anmelden muß.

Neben der IP-Adresse werden der Gegenstelle bei dieser Konfiguration auch die Adressen der DNS- und NBNS-Server (Domain Name Server und NetBIOS Name Server) inkl. der Backup-Server aus den Einträgen im TCP/IP-Modul übermittelt.

Damit das Ganze funktioniert, muß die Gegenstelle natürlich auch so eingestellt sein, daß sie die IP-Adresse und die Namensserver (DNS und NBNS) vom *ELSA LANCOM* bezieht. Das geschieht z.B. im DFÜ-Netzwerk von Windows durch die Einträge in den 'TCP-Einstellungen' unter 'IP-Adresse' bzw. 'DNS-Konfiguration'. Hier werden die Optionen 'Vom Server zugewiesene IP-Adresse' und 'Vom Server zugewiesene Namensserveradressen' aktiviert.

■ Beispiel: Internet-Access

Wird über den *ELSA LANCOM* der Zugang zum Internet für ein lokales Netz realisiert, kann die Zuweisung von IP-Adressen den umgekehrten Weg nehmen. Hierbei sind Konfigurationen möglich, in denen der *ELSA LANCOM* selbst keine im Internet gültige IP-Adresse hat und sich für die Dauer der Verbindung eine vom Internet-Provider zuweisen läßt. Neben der IP-Adresse erhält der *ELSA LANCOM* während der PPP-Verhandlung auch Informationen über DNS-Server beim Provider.

Im lokalen Netz ist der *ELSA LANCOM* nur mit seiner intern gültigen Intranet-Adresse bekannt. Alle Arbeitsplatzrechner im lokalen Netz können dann auf den gleichen Internet-Account zugreifen und auch z.B. den DNS-Server erreichen.

Die zugewiesenen Adressen schauen sich Windows-User im *LANmonitor* an. Neben dem Namen der verbundenen Gegenstelle finden Sie hier die aktuelle IP-Adresse sowie die Adressen von DNS- und NBNS-Servern. Auch Optionen wie die Kanalbündelung oder die Dauer der Verbindung werden angezeigt.



Der ELSA LANmonitor wird i.d.R. automatisch bei der Installation von ELSA LANconfig installiert. Eine Beschreibung des ELSA LANmonitor finden Sie im Kapitel 'Konfigurationsmöglichkeiten' im Abschnitt 'Was ist los auf der Leitung'.

Rückruf-Funktionen

ELSA LANCOM unterstützen neben dem Rückruf über den D-Kanal und dem Rückruf über das ELSA-Protokoll auch Rückruf über das von Microsoft spezifizierte CBCP sowie Rückruf über PPP nach RFC 1570 (PPP LCP Extensions). Zusätzlich besteht die Möglichkeit eines besonders schnellen Rückrufs über ein von ELSA entwickeltes Verfahren.

PCs mit Windows 95, Windows 98 oder Windows NT können nur über das CBCP zurückgerufen werden. Damit im *ELSA LANCOM* zusätzlich noch eine Rufnummernüberprüfung möglich ist, stehen in der Namenliste für den Rückruf-Eintrag folgende Werte zur Verfügung:

Mit diesem Eintrag stellen Sie den Rückruf so ein:
Aus	Es wird nicht zurückgerufen.
Auto (nicht Windows 95, Windows 98 oder Windows NT, s.u.)	Wenn die Gegenstelle in der Nummernliste gefunden wird, so wird diese zurückgerufen. Hierzu wird der Ruf zunächst abgelehnt und, sobald der Kanal wieder frei ist, zurückgerufen (Dauer ca. 8 Sekunden). Wird die Gegenstelle nicht in der Nummernliste gefunden, so wird sie zunächst als DEFAULT-Gegenstelle angenommen, und der Rückruf wird während der Protokollverhandlung ausgehandelt. Dabei fällt eine Gebühr von einer Einheit an.

Mit diesem Eintrag stellen Sie den Rückruf so ein:
Name	Bevor ein Rückruf erfolgt, wird immer eine Protokollverhandlung durchgeführt, auch wenn die Gegenstelle in der Nummernliste gefunden wurde (z.B. für Rechner mit Windows, die sich auf dem Gerät einwählen). Dabei fällt eine Gebühr von einer Einheit an.
ELSA	Wenn die Gegenstelle in der Nummernliste gefunden wird, wird der schnelle Rückruf durchgeführt, d.h., der <i>ELSA LANCOM</i> sendet ein spezielles Signal zur Gegenstelle und ruft sofort zurück, wenn der Kanal wieder frei ist. Nach ca. 2 Sekunden steht die Verbindung. Nimmt die Gegenstelle den Ruf nicht unmittelbar nach dem Signal zurück, so erfolgt zwei Sekunden später ein Rückfall auf das normale Rückrufverfahren (Dauer wieder ca. 8 Sekunden). Dieses Verfahren steht nur an DSS1-Anschlüssen zur Verfügung.
Looser	Benutzen Sie die Option 'Looser', wenn von der Gegenstelle ein Rückruf erwartet wird. Diese Einstellung erfüllt zwei Aufgaben gleichzeitig. Zum einen sorgt sie dafür, daß ein eigener Verbindungsaufbau zurückgenommen wird, wenn ein Ruf von der gerade angerufenen Gegenstelle hereinkommt, zum anderen wird mit dieser Einstellung die Funktion aktiviert, auf das schnelle Rückruf-Verfahren reagieren zu können. D.h., um den schnellen Rückruf nutzen zu können, muß sich der Anrufer im 'Looser'-Modus befinden, während beim Angerufenen der Rückruf auf 'ELSA' eingestellt sein muß.



Die Einstellung 'Name' bietet die höchste Sicherheit, wenn sowohl ein Eintrag in der Nummernliste als auch in der PPP-Liste konfiguriert ist. Die Einstellung 'ELSA' ermöglicht die schnellste Rückrufmethode zwischen zwei ELSA-Routern.

Bei Windows-Gegenstellen **muß** die Einstellung 'Name' gewählt werden.

Rückruf nach Microsoft CBCP

Das Microsoft CBCP erlaubt verschiedene Arten, die Rückrufnummer zu bestimmen:

- Der Angerufene ruft nicht zurück.
- Der Angerufene erlaubt es dem Anrufer, die Rückrufnummer selbst anzugeben.
- Der Angerufene kennt die Rückrufnummer und ruft auch **nur** diese zurück.

Über das CBCP ist es möglich, von einem Windows-95-, Windows-98- oder Windows-NT-PC eine Verbindung zum *ELSA LANCOM* aufzunehmen und sich von diesem zurückru-

fen zu lassen. Die drei möglichen Einstellungen werden über den Rückruf-Eintrag sowie den Rufnummern-Eintrag in der Namenliste ausgewählt.

Namenliste - Neuer Eintrag

Name:

Rufnummer:

Haltezeit: Sekunden

Haltezeit für Bündelung: Sekunden

Layername:

Automatischer Rückruf:

- Keinen Rückruf durchführen
- Die Gegenstelle zurückrufen
- Die Gegenstelle zurückrufen (schnelles Verfahren)
- Die Gegenstelle nach Überprüfung des Namens zurückrufen
- Den Rückruf der Gegenstelle erwarten

Keinen Rückruf durchführen

Für diese Einstellung muß der Rückruf-Eintrag bei der Konfiguration über Terminalprogramm oder Telnet den Wert 'Aus' haben.

Rückrufnummer selbst wählen

Die Gegenstelle wird nach Überprüfung des Namens zurückgerufen. Für diese Einstellung muß der Rückruf-Eintrag den Wert 'Name' haben, in der Namenliste darf **keine** Rufnummer angegeben sein.

Nach der Authentifizierung erscheint bei Windows 95 die folgende Dialogbox, in der der Anwender seine Rufnummer angeben kann:

Rückruf

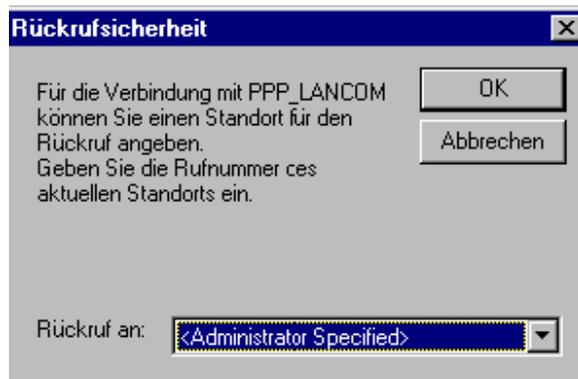
Für die Verbindung mit PPP_LANCOM können Sie eine Rückrufnummer angeben. Geben Sie die Nummer ein, unter der Sie PPP_LANCOM erreichen kann.

Nummer:

Rückrufnummer vom *ELSA LANCOM* bestimmt

Die Gegenstelle wird nach Überprüfung des Namens zurückgerufen. Für diese Einstellung muß der Rückruf-Eintrag der entsprechenden Gegenstelle den Wert 'Name' haben, und in der Namenliste muß **eine** Rufnummer angegeben sein.

Nach der Authentifizierung erscheint bei Windows 95 die folgende Meldung, die der Anwender nur bestätigen kann:



Der Rückruf an eine Windows-95-, Windows-98- oder Windows-NT-Workstation erfolgt ca. 15 Sekunden, nachdem die Verbindung abgebaut wurde. Diese Zeit kann nicht verkürzt werden, da sie vom Windows vorgegeben ist.

Schneller Rückruf nach *ELSA*

Sollen zwei *ELSA LANCOM* miteinander kommunizieren, wobei der eine zurückgerufen wird, bietet sich der schnelle Rückruf über das *ELSA*-spezifische Verfahren an.

- Der Anrufer, der gerne zurückgerufen werden möchte, stellt in der Namenliste 'Den Rückruf der Gegenstelle erwarten' ein ('Looser' bei Konfiguration über Terminalprogramm oder Telnet).
- Der Rückrufer wählt 'Die Gegenstelle zurückrufen (schnelles Verfahren)' in der Namenliste und stellt die Rufnummer ein ('*ELSA*').

Rückruf nach RFC 1570 (PPP LCP Extensions)

Nach RFC 1570 existieren fünf Möglichkeiten, einen Rückruf anzufordern. Alle Versionen werden vom *ELSA LANCOM* akzeptiert. Es wird jedoch bei allen Varianten gleich verfahren:

Der *ELSA LANCOM* baut nach der Authentifizierung der Gegenstelle die Verbindung ab und ruft diese dann drei Sekunden später zurück.

Kanalbündelung mit MLPPP

Wenn Sie eine ISDN-Verbindung zu einer PPP-fähigen Gegenstelle aufbauen, können Sie Ihren Daten Beine machen: Sie können die Daten komprimieren und/oder mehrere B-Kanäle zur Übertragung verwenden (Kanalbündelung).

Die Verbindung mit Kanalbündelung unterscheidet sich von „normalen“ Verbindungen dadurch, daß nicht nur ein, sondern mehrere B-Kanäle parallel für die Übertragung der Daten verwendet werden.

Für die Kanalbündelung wird dabei MLPPP (Multilink-PPP) verwendet. Dieses Verfahren steht natürlich nur zur Verfügung, wenn PPP als B-Kanal-Protokoll verwendet wird. MLPPP bietet sich z.B. an für den Internet-Access über Provider, die bei Ihren Einwahlknoten ebenfalls MLPPP-fähige Gegenstellen betreiben.

■ Statische Kanalbündelung

Wenn eine Verbindung mit statischer Kanalbündelung aufgebaut wird, versucht der Router sofort, die in der Kanalliste als 'Minimal' eingetragenen B-Kanäle aufzubauen. Dabei werden entweder die in der Kanalliste angegebenen Kanäle verwendet oder beliebige freie Kanäle.

■ Dynamische Kanalbündelung

Bei einer Verbindung mit dynamischer Kanalbündelung baut der Router zunächst nur die in der Kanalliste als 'Minimal' eingetragenen B-Kanäle auf und beginnt mit der Datenübertragung. Wenn er dann während der Verbindung feststellt, daß der Durchsatz eine Weile über einem bestimmten Schwellwert liegt, versucht er weitere Kanäle dazuzunehmen, bis die in der Kanalliste als 'Maximal' eingetragene Anzahl erreicht ist. Auch dabei werden entweder die in der Kanalliste angegebenen Kanäle verwendet oder beliebige freie Kanäle.

Wenn die dynamischen Kanäle aufgebaut sind und der Datendurchsatz wieder unter den Grenzwert zurückgeht, wartet der Router noch die eingestellte B2-Haltezeit ab und schließt die Kanäle dann automatisch wieder. Dabei werden die begonnenen Gebühreneinheiten ausgenutzt, sofern die Gebühreninformationen während der Verbindung übermittelt werden. Der Router benutzt die dynamischen Kanäle also nur, wenn und solange er sie auch wirklich braucht!

So stellen Sie die Kanalbündelung ein:

Die Konfiguration der Kanalbündelung für eine Verbindung setzt sich aus drei Einstellungen zusammen:

- ① Erstellen Sie in der Namenliste einen Eintrag für die Verbindung, die die Kanalbündelung verwenden soll. Wählen Sie dabei einen Layer aus, der in den Layer-2-Optionen die Bündelung eingestellt hat.
 - **compr.** nach dem LZS-Datenkompressionsverfahren (Stac) reduziert das Datenvolumen, wenn die Daten nicht schon vorher komprimiert waren. Dieses Verfah-

ren wird auch von Routern anderer Hersteller und von ISDN-Adaptern unter Windows-Betriebssystemen unterstützt.

- **Buendeln** verwendet mehrere B-Kanäle für eine Verbindung. Die Art der Kanalbündelung wird über die Konfiguration der Layer-2-Optionen in der Layerliste, der Haltezeiten in der Namenliste, des Eintrags für die Y-Verbindung in der Interface-Tabelle und des Eintrags in der Kanaltabelle eingestellt.
 - **bnd+compr** nutzt beides (Komprimierung und Kanalbündelung) und stellt damit die maximal mögliche Übertragungsleistung zur Verfügung.
- ② Stellen Sie ebenfalls in der Namenliste die Haltezeiten für diese Verbindung ein. Beachten Sie folgende Regeln:
- Die B1-Haltezeit sollte je nach Anwendungsfall so groß gewählt werden, daß die Verbindung nicht durch das kurzzeitige Ausbleiben von Paketen zu früh abgebaut wird. Erfahrungsgemäß sind Werte zwischen 60 und 180 Sekunden für den Beginn eine gute Basis, die man im Betrieb dann weiter anpassen kann.
 - Die B2-Haltezeit entscheidet darüber, nach welcher Zeit die dynamischen Kanäle wieder abgebaut werden, wenn der Datendurchsatz unter dem Schwellwert liegt.
- ③ Legen Sie in der Kanalliste fest, wie viele Kanäle für die Verbindung verwendet werden sollen. Außerdem können Sie hier bestimmen, welche Kanäle in Anspruch genommen werden dürfen und so z.B. bestimmte Kanäle für die Einwahl über RAS freihalten.

Der Eintrag in der Kanalliste entscheidet darüber, ob es sich um eine statische oder dynamische Kanalbündelung handelt (siehe oben). Mit mehr als einem minimalen Kanal wird die Bündelung statisch, mit mehr maximalen als minimalen Kanälen schaffen Sie die Möglichkeit der dynamischen Kanalbündelung.

- ④ Legen Sie in der Interface-Liste mit dem Eintrag für die Y-Verbindung fest, was geschehen soll, wenn während einer laufenden Verbindung mit Kanalbündelung der Wunsch nach einer weiteren Verbindung zu einer anderen Gegenstelle angemeldet wird, jedoch keine B-Kanäle mehr frei sind.
- Y-Verbindung **Ein**: Der Router unterbricht die Bündelverbindung auf diesem Interface, um die Verbindung zur anderen Gegenstelle aufzubauen. Wenn der Kanal wieder frei wird, holt sich die Bündelverbindung diesen Kanal automatisch wieder zurück (bei statischer Bündelung immer, bei dynamischer nur bei Bedarf).
 - Y-Verbindung **Aus**: Der Router hält die bestehende Bündelverbindung auf diesem Interface, die andere Verbindung muß es auf einem anderen Interface versuchen oder warten, falls keins der Interfaces mit aktiver Kanalbündelung den Abbau eines Kanals zuläßt.

IPX-Routing

Der IPX-Router überträgt Daten aus Netzwerken, die IPX/SPX als Netzwerkprotokoll verwenden (z.B. Novell-Netze). Mit dem Eintrag in der IPX-Routing-Tabelle wird ein entferntes Netz für die Rechner im lokalen Netz bekanntgemacht. In der Routing-Tabelle können bis zu 16 verschiedene Netze eingetragen werden.

IPX-Adressierung

Eine vollständige Adresse in einem IPX-Netzwerk besteht aus drei Teilen: einer Netzwerknummer, der MAC-Adresse der Netzwerkkarte und der Socket-Nummer:

- Die Netzwerknummer kann frei gewählt werden. Sie muß allerdings über alle erreichbaren IPX-Netze hinweg eindeutig sein, um eine richtige Zuordnung zu gewährleisten.
- Die MAC-Adresse ist fest in jede Netzwerkkomponente eingebrennt. Nur in Sonderfällen wird netzintern auch eine andere Adresse verwendet.
- Um nicht nur einen Rechner, sondern auch einen ganz besonderen Dienst auf diesem Rechner anzusprechen, verwendet ein IPX-Netz die Socket-Nummern. Damit werden die verschiedenen Dienste eindeutig identifiziert.

Informationen über das LAN

Wenn an einem Standort mehrere getrennte LANs benötigt werden, so müssen diese nicht unbedingt auch eigene Verkabelungen haben. Verschiedene logische Netze können sich ein Kabel teilen. Damit die Daten der verschiedenen Netzwerke sich nicht stören und ein Netz für die anderen unsichtbar bleibt, verwenden sie unterschiedliche Formate für die Ethernet-Pakete. Diese Formate werden durch das Binding bestimmt, das zu einer eindeutigen Netzwerknummer auf diesem Kabel gehört.

Damit der Router nun auch weiß, zu welchem Netz es gehört, müssen Sie ihm die Netzwerknummer und das zugehörige Binding angeben. Lassen wir die Netzwerkadresse auf der Standard-Einstellung '00000000', ermittelt der Router die Adresse und das Binding selbst. Dazu sucht er sich auf dem angeschlossenen Kabel das Netz aus, auf dem er die meisten SAP-Replies erhält.

IPX-Routing-Tabelle

In der IPX-Routing-Tabelle legen Sie fest, welche Gegenstellen (also welche anderen Router oder Rechner) für das lokale Netzwerk erreichbar sind, und geben ihm einige Parameter für die Verbindung an. Die Tabelle mit maximal 16 Einträgen hat folgenden Aufbau:

Gegenstelle	Netzwerk	Binding	Propagate	Backoff
FILIALE01	00000245	802.3	Route	Ein
FILIALE02	00000320	SNAP	Filt.	Ein
ZENTRALE	00000420	802.2	Filt.	Aus

- Gegenstelle:

Der Name der Gegenstelle, wie er als Geräte-Name in dem entsprechenden Router auf der Gegenseite eingetragen ist.

- Netzwerk:

Adresse des WANs. Das ist nicht die Adresse des Ziel-Netzwerks, sondern eine dritte Adresse, die das Netz zwischen den beiden zu verbindenden Netzen darstellt. Hier gilt also:

LAN-Adresse 1 \neq WAN-Adresse 1 = WAN-Adresse 2 \neq LAN-Adresse 2 \neq LAN-Adr. 1

- Binding:

Hier wird eingestellt, welches Ethernet-Binding auf dem WAN verwendet werden soll. Dieser Eintrag ist nur wirksam, wenn der Layer für diese Verbindung Ethernet-Encapsulation unterstützt. Fehlt der Eintrag, wird 802.3 angenommen.

- Propagate:

Filter für IPX-Pakete vom Typ 20 (NetBIOS Propagated Frames). Das Network Basic Input/Output System wurde ursprünglich für IBM entwickelt, und wird mittlerweile in abgewandelter Form auch von Microsoft verwendet. Dieses Protokoll stellt in Layer 3 und 4 des OSI-Modells Dienste wie Namensauflösung, Datensicherung und korrekte Paketreihenfolge zur Verfügung (gesichertes Protokoll). NetBIOS-Pakete besitzen einen speziellen Pakettyp und Socket (Propagated Pakets). NetBIOS wird in erster Linie für den Datenaustausch zwischen Stationen in einem lokalen Netz (LAN) verwendet.

Diese IPX-Pakete können mit der Einstellung 'Filter' von der Übertragung ausgeschlossen oder geroutet werden. Bei der Einstellung 'Route' werden die Pakete übertragen, wenn eine Verbindung zur entsprechenden Gegenstelle besteht oder noch ein freier Kanal für den Aufbau einer weiteren Verbindung verfügbar ist. Sind alle Leitungen mit anderen Gegenstellen beschäftigt, werden die Propagated Frames verworfen.

- Backoff:

Der IPX-Router benutzt einen speziellen Algorithmus (Exponential Backoff), um bei Fehlkonfigurationen die anfallenden Verbindungskosten so gering wie möglich zu halten.

Wenn im Netz der Gegenstelle kein Server vorhanden ist (z.B. bei Remote-Access von einer Workstation), dann sollte die Backoff-Funktion ausgeschaltet sein (siehe auch 'Exponential-Backoff').

Die Default-Einstellung ist 'Ein'.

Was passiert bei der Datenübertragung im IPX-Netz?

Wenn sich ein Gerät in einem IPX-Netz anmeldet, sendet es zunächst eine Anfrage nach dem Service Advertising Protocol (SAP) aus und erkundigt sich nach dem nächsten erreichbaren Server (Get Nearest Server Request) im Netz mit der Nr. '00000000'. Befindet sich in diesem Netz ein Router oder Server, antwortet dieser auf diese Anfrage und teilt dabei die korrekte Netzwerknummer mit.

Die Server versenden außerdem regelmäßig Informationen darüber, welche Dienste sie anbieten und welche anderen Netzwerke sie erreichen können. Dazu verwenden sie spezielle Datenpakete nach dem Service Advertising Protocol bzw. Routing Information Protocol (RIP).

Wenn der IPX-Router fertig konfiguriert ist und eingeschaltet wird, baut er zunächst einmal zu allen über die Routing-Tabellen erreichbaren Gegenstellen Verbindungen auf und tauscht dann mit diesen Netzen SAP- und RIP-Informationen aus. Der Router speichert diese Daten in seinen internen SAP- und RIP-Tabellen.

RIP- und SAP-Tabellen

Die RIP- und SAP-Informationen erscheinen in den entsprechenden Tabellen alphabetisch sortiert. RIPs sind dabei nur nach dem Netzwerk geordnet, SAPs zuerst nach dem Service-Typ, dann nach dem Servernamen.

Mit jedem neuen RIP- bzw. SAP-Paket werden die RIP- und SAP-Tabellen angepaßt. Damit dabei nur solche Dienste angeboten werden (SAP), die auch erreichbar sind (RIP), nimmt der Router nur diese SAP-Informationen in die eigene Tabelle auf, für die es auch den entsprechenden RIP-Eintrag gibt. Neben den Informationen über erreichbare Routen und Dienste verraten die Einträge der Tabellen z.B. auch, wie viele Router auf dem Weg dorthin zu passieren sind (Hops) oder welche Zeit ein Datenpaket ins Zielnetz braucht (Tics = ca. 1/18 Sekunde). Werden über die RIP-Informationen z.B. mehrere Routen in ein Zielnetz angeboten, wählt der Router anhand der Tabellen den Weg mit den wenigsten Tics und dem kleinsten Hopcount aus und speichert nur diese Route.

RIP-Tabellen können 64, SAP-Tabellen 128 Einträge aufnehmen. Wenn jedes neue Paket die Tabellen aktualisiert, müssen natürlich irgendwann auch die alten Einträge verschwinden. Dazu bekommen die Einträge ein künstliche Alterung. Für alle Einträge in den

RIP/SAP-Tabellen, die durch lokalen Datenaustausch gelernt wurden, wird das Alter alle 60 Sekunden um eins erhöht. Ein neues RIP- bzw. SAP-Paket für einen Eintrag setzt das Alter auf Null zurück. Nach einem einstellbaren Alter von 1 bis 60 wird die Route oder der Service als unerreichbar (Down) bezeichnet. Ist das Doppelte dieser Zeit abgelaufen, wird der Eintrag entfernt. Außerdem werden bei einem Verbindungsaufbau alle RIP- und SAP-Informationen, die diese Gegenstelle betreffen, aus den Tabellen gelöscht und durch neue Informationen ersetzt.

So viele Router hier ...

Ist in einem Netz der Aufbau zu mehr Gegenstellen gleichzeitig erwünscht, als B-Kanäle zur Verfügung stehen, dann wird es Zeit für einen zweiten (dritten ...) Router. Damit das Zusammenspiel der Brüder reibungslos funktioniert und das Netz wirklich immer einen Ansprechpartner findet, werden in allen Routern die gleichen Einträge in der Routing-Tabelle vorgenommen. Durch die RIP-Pakete werden jedem Router dann auch die gleichen Routing-Informationen übermittelt, allerdings mit höherem Tic- und Hopcount (`Setup/IPX-Modul/LAN-Einstellung/RIP-SAP-Skal.` einschalten). Dadurch werden diese Routen quasi als Reserve markiert, wenn auf dem angesprochenen Gerät alle Kanäle besetzt sind.

Redundante Routen

Empfängt ein Router mit einem RIP-Paket Informationen über Routen mit gleichem Tic- und Hopcount wie die eigenen Routen (redundante Routen), muß er dem Absender diese Routen natürlich nicht selbst wieder bekanntgeben. Er sendet diese Routen also nur an die Router, die die Route nicht propagiert haben. Dieses Verfahren nennt man Split Horizon.

Sollte es trotzdem einmal nötig sein, redundante Routen im lokalen Netz bekanntzugeben, kann die Funktion 'Loop-Propagieren' verwendet werden (`Setup/IPX-Modul/LAN-Einstellung/Loop-Propagieren`). Die so gelernten Routen werden in der RIP-Tabelle dann als 'LOOP' gekennzeichnet. Da die Verbreitung von redundanten Routen nach den Novell-Spezifikationen zwar nicht verboten ist, aber trotzdem möglichst unterlassen werden sollte, ist die Default-Einstellung 'Aus'.

Exponential-Backoff

Um die für den Betrieb notwendigen Routing-Informationen (RIP- und SAP-Informationen) der IPX-Gegenstellen zu erhalten, versucht der IPX-Router des Gerätes nach dem Einschalten entsprechende Verbindungen aufzubauen. Falls dies nicht möglich ist, etwa durch eine Fehlkonfiguration des IPX-Routers, vermeidet der Exponential-Backoff-Algorithmus, daß laufend Verbindungsaufbau gestartet wird und spart damit Gebühren.

Gelingt der erste Verbindungsversuch zu einer Gegenstelle nicht, versucht der Router nach einer ständig wachsenden Wartezeit erneut die Gegenstelle zu erreichen. Die Wartezeit wird dabei folgendermaßen bestimmt:

- Die erste Anwahl erfolgt nach $10 + x$ Sekunden. x ist dabei ein Zahl zwischen 0 und 10.
- Der zweite Versuch wird um $10 + x$ Sekunden nach dem Scheitern des ersten Versuchs gestartet. x steht jetzt für eine Zahl zwischen 0 und 20 Sekunden.
- Der obere Wert für x wird nun bei jedem neuen Versuch verdoppelt. Nach dem 16. erfolglosen Versuch gibt der Router schließlich auf. Durch das ständige Anwachsen der Wartezeit ist nach 16 Versuchen maximal ein Tag vergangen.

Bleiben alle Versuche zur Anwahl der Gegenstelle erfolglos, wird die Route gesperrt. Nur eine Änderung des Eintrags in der Routing-Tabelle kann dann zu erneuten Verbindungsversuchen führen.



Die Zeit bis zur nächsten Anwahl und die Zahl der Aufbauversuche können der Netzwerkstatistik entnommen werden (Status/IPX-Statistik/Router-Statistik/Netzwerke).

Filter für die IPX-Pakete

Mit den Einträgen in der Routing-Tabelle legen Sie fest, welche anderen Netze erreichbar sind. Diese Netze sind damit allerdings auch erreichbar für solche Datenpakete, die im Netz der Gegenstelle eigentlich nicht benötigt werden. Diese Pakete führen auch zum Aufbau unerwünschter Verbindungen und kosten Geld.

Also müssen geeignete Filter her. Damit können Sie z.B. Datenpakete, die nur zur internen Kommunikation der Netze verwendet werden, von der Übertragung über das WAN ausschließen oder sie zumindest einschränken:

- Propagated Frames
Diese speziellen Datenpakete verwenden Protokolle, die eigentlich nicht geroutet werden können. Um trotzdem am gemeinsamen Routing teilnehmen zu können, werden diese Daten in normale IPX-Pakete gekapselt und als Broadcast verschickt.
Manchmal sind diese Pakete beim Routing nicht erwünscht. Daher können Sie für diesen Paket-Typ explizit einstellen, ob er geroutet oder gefiltert werden soll.
- Socket-Filter
Jedes Datenpaket in einem IPX-Netz enthält neben Ziel- und Quelladressen auch Ziel- und Quell-Sockets. Sockets bezeichnen die Prozesse, für die die Daten in dem Paket bestimmt sind.
Für die Sockets aus dem lokalen sowie aus den entfernten Netzen gibt es jeweils eine entsprechende Filtertabelle, die die Filter beinhaltet, mit denen einzelne Ziel-Sockets oder ganze Gruppen von der Übertragung ausgeschlossen werden können. Einige Sockets, die bekanntermaßen häufig für unerwünschte Verbindungen sorgen, sind als Voreinstellung schon in der Socket-Filtertabelle eingetragen.
- RIP- und SAP-Informationen

Über die RIPs teilt ein Router nach dem Split-Horizon-Prinzip den anderen Routern alle ihm bekannten Routen (Wege in andere Netze) mit. Das sind sowohl die Einträge aus der eigenen Routing-Tabelle und auch alle Routen, die der Router von anderen Routern gelernt hat. Er lernt dabei sowohl von Routern aus lokalen als auch aus entfernten Netzen. Alle verfügbaren Routing-Informationen trägt er in seiner internen RIP-Tabelle ein.

In den SAP-Informationen bieten die Server ihre Dienste an. Die verschiedenen Dienste werden innerhalb der SAP-Infos durch Nummern dargestellt. Jeder Dienst (z.B. File-Server oder Print-Server) hat eine eindeutige Nummer. Der Router nimmt die Informationen über die verfügbaren Dienste in die interne SAP-Tabelle auf und trägt ein, welcher Service in welchem Netz an welcher MAC-Adresse verfügbar ist. Dabei lernt er auch, ob der angebotene Dienst lokal oder in einem entfernten Netz liegt, und kann den Dienst so ohne Verbindungsaufbau propagieren.



Im IPX-Modul (setup/IPX-Modul/RIP-Einstellung bzw. SAP-Einstellung) der Router können Sie die RIP- und SAP-Tabellen mit den aktuellen Werten einsehen.

RIP- und SAP-Informationen sind natürlich sehr wichtig für die Kommunikation der Geräte in einem Netz, daher gibt es verschiedene Möglichkeiten, die Übertragung dieser Pakete einzustellen:

- Mit einer LAN- und einer WAN-Filtertabelle kann der Router angewiesen werden, Informationen über Routen zu bestimmten Netzen bzw. über bestimmte verfügbare Dienste nicht in die interne RIP- oder SAP-Tabelle zu übernehmen. Die betroffenen Routen werden also nicht verwendet und auch nicht weiter bekanntgegeben, die Dienste werden nicht im eigenen Netz angeboten.
- RIP- und SAP-Pakete werden ohne Filter, also immer übertragen. Diese belegen jedoch auf jeden Fall einen Teil der Verbindungsleitung.
- Die RIP- und SAP-Pakete werden nur dann versendet, wenn sich Änderungen in der Information ergeben haben.
- RIPs und SAPs können in regelmäßigen, einstellbaren Zeiten übertragen werden. Normalerweise werden die Informationen im Abstand von einer Minute verschickt. Mit der Zeiteinstellung kann dieser Abstand auf bis zu 60 Minuten ausgedehnt werden.
- Die gebührenschonendste Behandlung der RIP- und SAP-Pakete überträgt die Informationen einmalig nur dann, wenn eine Verbindung aufgebaut ist.

■ IPX- und SPX-Watchdogs:

Mit diesen Datenpaketen erkundigen sich die Server z.B. bei den Arbeitsplatzrechnern, ob sie noch aktiv sind oder ob sie ggf. abgemeldet werden können. Damit diese „Hallo, bist du noch wach?“-Pakete für Rechner in einem entfernten Netz nicht ständig zum Verbindungsaufbau führen, können Sie die Beantwortung dieser Anfragen folgendermaßen einstellen:

- IPX-Watchdogs bleiben völlig unbeantwortet. Nach der beim Server eingestellten Zeit werden die Rechner abgemeldet.
- IPX- und SPX-Watchdogs können lokal beantwortet werden. Dieses Verfahren nennt man Spoofing. Der Router antwortet dann anstelle der angesprochenen Rechner, die dann natürlich nie abgemeldet werden. Die Einstellung einer Zeit beim Server, nach der die entsprechenden Geräte auf jeden Fall abgemeldet werden, ist also sinnvoll.
- IPX- und SPX-Watchdogs können natürlich auch ganz normal geroutet werden, führen dann aber recht häufig zum Aufbau einer Verbindung.



Weitere Hinweise zu IPX, zum IPX-Router und zu den zugehörigen Parametern finden Sie im Kapitel 'Setup/IPX-Modul' Referenz-Handbuch.

IP-Routing

Ein IP-Router arbeitet zwischen Netzen, die TCP/IP als Netzwerk-Protokoll verwenden. Dabei werden nur Daten übertragen, deren Zieladressen in der Routing-Tabelle eingetragen sind. In diesem Kapitel erfahren Sie, wie die IP-Routing-Tabelle in einem Router von ELSA aufgebaut ist und mit welchen weiteren Funktionen das IP-Routing unterstützt wird.

Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem Router, an welche Gegenstelle (also welchen anderen Router oder Rechner) er die Daten für bestimmte IP-Adressen oder IP-Adreß-Bereiche schicken soll. So ein Eintrag heißt auch „Route“, weil der Weg der Datenpakete damit beschrieben wird. Da Sie diese Einträge selbst vornehmen und sie solange unverändert bleiben, bis Sie selbst sie wieder ändern oder löschen, heißt dieses Verfahren auch „statisches Routing“. Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing“. Dabei tauschen die Router selbständig untereinander Informationen über die Routen aus und erneuern diese fortlaufend. Die statische Routing-Tabelle kann bis zu 64 Einträge aufnehmen, die dynamische Tabelle 128. Bei aktiviertem IP-RIP beachtet der IP-Router beide Tabellen.

Außerdem sagen Sie dem Router in der IP-Routing-Tabelle, wie weit der Weg über diese Route ist, damit im Zusammenspiel mit IP-RIP bei mehreren Routen zum gleichen Ziel der günstigste ausgewählt werden kann. Die Grundeinstellung für Distanz zu einem anderen Router ist 2, d.h., der Router ist direkt erreichbar. Alle lokal erreichbaren Geräte, also weitere Router im eigenen LAN oder Arbeitsplatzrechner, die über Proxy-ARP angeschlossen sind, werden mit der Distanz 0 eingetragen. Mit dem gezielten Eintrag einer höheren Distanz (bis 14) wird die „Qualität“ dieser Route herabgesetzt. Solche „schlechteren“ Routen sollen nur dann verwendet werden, wenn keine andere Route zu der entsprechenden Gegenstelle gefunden werden kann.

Die Routingtabelle finden Sie im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' bzw. im Menü /Setup/IP-Router/IP-Routing-Tab. So sieht eine IP-Routing-Tabelle also z.B. aus:

IP-Adresse	IP-Netzmaske	Router-Name	Distanz	Maskierung
192.168.120.0	255.255.255.0	AACHEN	2	Ein
192.168.125.0	255.255.255.0	BERLIN	3	Aus
192.168.130.0	255.255.255.0	191.168.140.123	0	Statisch

Was bedeuten die einzelnen Einträge in der Liste?

■ IP-Adresse und IP-Netzmaske

Das ist die Adresse des Zielnetzes, zu dem Datenpakete geschickt werden können, mit der zugehörigen Netzmaske. Mit der Netzmaske und der Ziel-IP-Adresse aus den ankommenden Datenpaketen prüft der Router, ob das Paket in das Zielnetz gehört.

■ Router-Name

An diese Gegenstelle überträgt der Router die zur IP-Adresse und Netzmaske passenden Datenpakete. Ist die Gegenstelle ein Router in einem anderen Netz oder ein einzelner Arbeitsplatzrechner, dann steht hier ein Name. Kann der eigene Router die Gegenstelle nicht selbst erreichen, steht hier die IP-Adresse eines anderen Routers, der den Weg ins Zielnetz kennt.

■ Distanz

Anzahl der zwischen dem eigenen und dem Ziel liegenden Router. Dieser Wert wird bei Weitverkehrsverbindungen oft auch mit den Kosten der Übertragung gleichgesetzt und zur Unterscheidung zwischen preiswerten und teuren Übertragungswegen genutzt. Die eingetragenen Distanzwerte werden wie folgt propagiert:

- Während eine Verbindung zu einem Zielnetz aufgebaut ist, werden alle über diese Verbindung erreichbaren Netze mit einer Distanz von 1 propagiert.
- Alle nicht verbundenen Netze werden mit der Distanz propagiert, die in der Routing-Tabelle eingetragen ist (mindestens jedoch mit einer Distanz von 2), solange noch ein freier Übertragungskanal verfügbar ist.
- Ist kein Kanal mehr frei, so werden die verbleibenden Netze mit einer Distanz 16 (= unreachable) propagiert.
- Eine Ausnahme bilden die Gegenstellen, die über Proxy-ARP angeschlossen sind. Diese „Proxy-Hosts“ werden gar nicht propagiert.

■ Maskierung

Mit der Option 'Maskierung' in der Routing-Tabelle informieren Sie den Router darüber, welche IP-Adresse er bei der Weitergabe der Pakete verwenden soll.

- 'aus': Es wird keine Maskierung durchgeführt.

- 'ein': Mit diesem Eintrag fordern Sie von Ihrem Provider die Zuweisung einer beliebigen, im Internet gültigen IP-Adresse an, die Sie im weiteren für die Verbindung und die Maskierung verwenden wollen.
- 'stat.': Mit diesem Eintrag fordern Sie von Ihrem Provider die Zuweisung einer bestimmten Adresse an, die im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein' bzw. im Menü /Setup/TCP-IP-Modul als IP-Adresse eingetragen ist. Diese Adresse soll im weiteren für die Verbindung und die Maskierung verwendet werden.

Weitere Informationen finden Sie im Abschnitt 'IP-Masquerading'.

- Folgende Einträge haben eine besondere Bedeutung:
 - IP-Adresse 255.255.255.255 mit Netzmaske 0.0.0.0: Das ist die Default-Route. Alle Datenpakete, die nicht durch andere Routing-Einträge geroutet werden können, werden an die hier eingetragene Gegenstelle übertragen.
 - Netzmaske 255.255.255.255: Einträge mit voll ausgefüllter Netzmaske kennzeichnen oft nur einzelne Arbeitsplatzrechner (Remote-Access), keine eigenen Netze. Manchmal kann sich dahinter auch ein Netzwerk verbergen, das über IP-Masquerading nur mit einer IP-Adresse nach außen hin sichtbar ist.
 - Router-Name 0.0.0.0: Ausschluß-Routen. Datenpakete für diese „Null-Routen“ verworfen und nicht weitergeleitet. Damit werden z.B. die im Internet verbotenen Routen (Privat Address Spaces, z.B. 10.0.0.0) von der Übertragung ausgeschlossen.

Beispiele mit Erläuterungen:

IP-Adresse	IP-Netzmaske	Router-Name	Dist.	Und das passiert:
192.168.1.9	255.255.255.255	AUSSENDIENST	2	Die Gegenstelle AUSSENDIENST ist unter der IP-Adresse 192.168.1.9 zu erreichen.
192.168.120.0	255.255.255.0	ROUTER01	2	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.120.x werden an ROUTER01 übertragen.
192.168.125.0	255.255.255.0	ROUTER02	3	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.125.x werden an ROUTER02 übertragen.
192.168.130.0	255.255.255.0	192.168.140.123	0	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.130.x werden an den Router mit der IP-Adresse 192.168.140.123 übertragen.
10.0.0.0	255.0.0.0	0.0.0.0	0	Schließt die Übertragung aller Datenpakete in 10er-Netze aus.
255.255.255.255	0.0.0.0	ZENTRALE	2	Alle Datenpakete, die nicht den zuvorstehenden Einträgen zugeordnet werden können, werden an die Gegenstelle ZENTRALE übertragen.



Wichtig ist dabei auch die Reihenfolge der Einträge: Sie werden von oben nach unten abgearbeitet! Der Router sortiert die Einträge dabei selbständig: Zuerst nach den Netzmasken, davon die größte nach oben. Dann nach den IP-Adressen, davon die kleinsten nach oben. Dadurch landet der 'ZENTRALE'-Eintrag ganz am Ende der Liste. Mit diesem Eintrag ganz oben in der Liste würde der Router alle (!) Datenpakete, die nicht ins eigene Netz gehören, ins Netz der Zentrale senden.

Filter für die TCP/IP-Pakete

Mit den Einträgen in der Routing-Tabelle können Sie schon recht genau festlegen, welche Datenpakete übertragen werden sollen. Zusätzlich können Sie mit dem Eintrag '0.0.0.0' im Feld 'Router-Name' ganze Gruppen von IP-Adressen verwerfen.

Manchmal möchten Sie die Übertragung jedoch noch weiter einschränken. Dazu nutzen Sie die Eigenschaft von TCP/IP, neben den Quell- und Ziel-IP-Adressen mit einem Datenpaket auch Portnummern für Ziel und Quelle zu versenden. Der Ziel-Port in einem Datenpaket steht für den Dienst im TCP/IP-Netz, der angesprochen werden soll. Die Ziel-Ports für verschiedene Dienste im TCP/IP-Netz sind fest definiert (siehe auch 'TCP/IP-Ports' Referenz-Handbuch). Die Quell-Ports hingegen werden in bestimmten Bereichen frei gewählt.

Der Router kann sich die Ziel- und Quell-Ports von solchen Datenpaketen ansehen, die TCP oder UDP als Protokoll verwenden. Aus diesen Ports kann er dann ableiten, für welchen Zweck die Daten gedacht sind. So können z.B. FTP-Zugriffe oder Telnet-Sitzungen erkannt werden. Mit Hilfe der entsprechenden Filter-Tabelle kann dann festgelegt werden, daß bestimmte Daten nicht aus dem LAN an die Gegenstelle übertragen werden sollen. Genauso können natürlich auch Daten für bestimmte Ports aus dem WAN in Richtung des LANs gesperrt werden. Neben der Definition der Portbereiche und der zugehörigen Protokolle kann in den Filter-Tabellen mit dem Filter-Typ auch festgelegt werden, ob die betroffenen Datenpakete nie übertragen werden oder ob sie nur nicht zu einem Verbindungsaufbau führen sollen (also nur bei bestehender Verbindung übertragen werden).

Im IP-Router befinden sich zwei separate Filtertabellen für Pakete, die aus dem LAN kommen und Pakete, die von WAN kommen. Diese Filtertabellen finden Sie im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Filter' bzw. im Menü / Setup / IP-Router / WAN-Filtertab bzw. LAN-Filtertab.

Proxy-ARP

Eine Besonderheit im IP-Router stellt die Möglichkeit des Proxy-ARP dar. „Proxy“ ist ein englischer Begriff und heißt auf deutsch „Stellvertreter“. Dieser Stellvertreter wird dann eingesetzt, wenn die Datenübertragung zu IP-Adressen im gleichen logischen Netz wie der Absender erfolgt, die Zieladresse dennoch über einen Router zu erreichen ist. Das ist z.B. bei der Anbindung von einzelnen Arbeitsplatzrechnern (Teleworkern) über TCP-IP an das Firmen-Netz der Fall. Der Teleworker hat dann eine IP-Adresse, die im gleichen loka-

len Netz liegt wie alle anderen Rechner im LAN. Normalerweise würde ein Datenpaket aus dem LAN für den Teleworker also nur lokal einen Abnehmer suchen, leider aber nicht finden.



Um diese Funktion zu nutzen, muß die Option 'Proxy-ARP' eingeschaltet werden (im LAN-config im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' oder im Menü / setup / IP-Router-Modul bei anderen Konfigurationsmöglichkeiten).

Mit folgendem Eintrag in der Routing-Tabelle wird der Router zum Stellvertreter des Teleworkers:

IP-Adresse	IP-Netzmaske	Router-Name	Distanz	IP-Masquerading
192.168.110.123	255.255.255.255	Teleworker01	0	aus

Da der Router auf einen ARP-Request für den Proxy-Rechner mit seiner eigenen MAC-Adresse antwortet, werden Proxy-Hosts in einem RIP-Paket nicht propagiert. In der Routing-Tabelle wird die Distanz auf '0' gesetzt, um das zu verdeutlichen.

Der Router beantwortet nun die Frage nach der MAC-Adresse zur IP-Adresse 192.168.110.123 mit seiner eigenen MAC-Adresse. Dadurch werden alle Pakete für den Teleworker im LAN nun automatisch zum Router geschickt, der die Daten zum Rechner auf der anderen Seite der Verbindung weiterleitet.

Lokales Routing

Sie kennen das folgende Verhalten der Arbeitsplatzrechner in einem lokalen Netz: Möchte der Rechner ein Datenpaket an eine IP-Adresse senden, die nicht in seinem eigenen Netz liegt, sucht er nach einem Router, der ihm weiterhelfen kann. Dieser Router wird normalerweise dem Betriebssystem durch den Eintrag als Standard-Router oder Gateway bekanntgegeben. Gibt es in einem Netz mehrere Router, so kann oft nur ein Standard-Router eingetragen werden, der alle dem Arbeitsplatzrechner unbekannt IP-Adressen erreichen können soll. Manchmal kann dieser Standard-Router jedoch nicht selbst das Zielnetz erreichen, er kennt aber einen anderen Router, der zu diesem Ziel findet.

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

Standardmäßig schickt der Router dem Rechner eine Antwort mit der Adresse des Routers, der die Route ins Ziel-Netz kennt (diese Antwort nennt man ICMP-Redirect). Der Arbeitsplatzrechner übernimmt daraufhin diese Adresse und schickt das Datenpaket sofort an den anderen Router.

Manche Rechner können mit den ICMP-Redirects leider nichts anfangen. Um die Datenpakete trotzdem zustellen zu können, verwenden Sie das lokale Routing (im ELSA LAN-config im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' oder im Menü / Setup / IP-Router-Modul / Lok.-Routing Ein). Dadurch weisen Sie den

Router an, das Datenpaket selbst zum anderen Router zu senden. Außerdem sendet der Router dann keinen ICMP-Redirect mehr.

Ist im Prinzip ja eine tolle Sache, trotzdem sollte das lokale Routing nur im „Notfall“ verwendet werden, denn diese Funktion führt zu einer Verdoppelung aller Datenpakete zum gewünschten Zielnetz. Die Daten werden erst zum Standard-Router und von diesem erneut zum eigentlich zuständigen Router geschickt.

Dynamisches Routing mit IP-RIP

Neben der statischen Routing-Tabelle verfügen Router von ELSA auch über eine dynamische Routing-Tabelle mit bis zu 128 Einträgen. Diese Tabelle füllt der Anwender im Gegensatz zu der statischen nicht selbst aus, das erledigt der Router selbst. Dazu nutzt er das Routing Information Protocol (RIP). Über dieses Protokoll tauschen alle Router in einem lokalen Netz, die RIP beherrschen, Informationen über die erreichbaren Routen aus.

Welche Informationen werden über IP-RIP propagiert?

Ein Router teilt in den IP-RIP-Informationen den anderen Routern im Netz die Routen mit, die es in seiner eigenen statischen Tabelle findet. Nicht berücksichtigt werden dabei die folgenden Einträge:

- Routen, die mit der Router-Einstellung '0.0.0.0' verworfen werden.
- Routen, die auf andere Router im lokalen Netz lauten.
- Routen, die einzelne Rechner über Proxy-ARP an das LAN anbinden.

Die Einträge in der statischen Routing-Tabelle werden zwar von Hand gesetzt, trotzdem ändern sich diese Informationen je nach Verbindungssituation der Router und damit auch die versendeten RIP-Pakete.

- Solange der Router eine Verbindung zu einer Gegenstelle aufgebaut hat, gibt es alle über diese Route erreichbaren Netze in den RIPs mit der Distanz '1' weiter. Damit werden andere Router im LAN darüber informiert, daß hier bei diesem Router eine bestehende Verbindung zu dieser Gegenstelle genutzt werden kann. So kann zusätzlicher Verbindungsaufbau von Routern mit Wählverbindungen verhindert und ggf. Verbindungskosten reduziert werden.
- Wenn darüber hinaus in diesem Router keine weitere Verbindung zu einer anderen Gegenstelle aufgebaut werden kann, werden alle anderen Routen mit der Distanz '16' im RIP weitergemeldet. Die '16' steht dabei für „Im Moment ist diese Route nicht erreichbar“. Daß ein Router neben der bestehenden Verbindung keine weitere aufbauen kann, liegt an einer der folgenden Ursachen:
 - Auf allen anderen Kanälen ist schon eine andere Verbindung hergestellt (auch über *LANCAPI* oder a/b-Ports).
 - Die bestehende Verbindung benutzt alle B-Kanäle (Kanalbündelung).



Um diese Funktion zu nutzen, muß die Option 'IP-RIP' eingeschaltet werden (im ELSA LANconfig im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' oder im Menü `setup / IP-Router-Modul` bei anderen Konfigurationsmöglichkeiten).

RIP-fähige Router versenden die RIP-Pakete ungefähr alle 30 Sekunden. Der Router ist nur dann auf das Versenden und Empfangen von RIPs eingestellt, wenn er eine eindeutige IP-Adresse hat. In der Grundeinstellung mit der IP-Adresse `XXX.XXX.XXX.254` ist das IP-RIP-Modul ausgeschaltet.

Welche Informationen nimmt der Router aus empfangenen IP-RIP-Paketen?

Wenn der Router IP-RIP-Pakete empfängt, baut er sie in seine dynamische IP-Routing-Tabelle ein, und die sieht etwa so aus:

IP-Adresse	IP-Netzmaske	Zeit	Distanz	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

Was bedeuten die Einträge?

IP-Adresse und Netzmaske bezeichnen das Ziel-Netz, die Distanz wird aus den RIP-Informationen übernommen, die letzte Spalte zeigt an, welcher Router diese Route bekanntgemacht hat. Bleibt die 'Zeit'. Damit zeigt die dynamische Tabelle an, wie alt die entsprechende Route ist. Der Wert in dieser Spalte gilt als Multiplikator für das Intervall, in dem die RIP-Pakete eintreffen, eine '1' steht also für etwa 30 Sekunden, eine '5' für etwa 2,5 Minuten usw. Wenn eine Information über eine Route neu eintrifft, gilt diese Route natürlich als direkt erreichbar und erhält die Zeit '1'. Nach Ablauf der entsprechenden Zeit wird der Wert in dieser Spalte automatisch erhöht. Nach 3,5 Minuten wird die Distanz auf '16' gesetzt (Route nicht erreichbar), nach 5,5 Minuten wird die Route gelöscht.

Wenn der Router nun ein IP-RIP-Paket empfängt, muß er entscheiden, ob er die darin enthaltenen Routen in seine dynamische Tabelle aufnehmen soll oder nicht. Dazu geht er wie folgt vor:

- Die Route ist in der Tabelle noch gar nicht vorhanden, dann wird sie aufgenommen (sofern Platz in der Tabelle ist).
- Die Route ist in der Tabelle vorhanden mit der Zeit von '5' oder '6'. Die neue Route wird dann verwendet, wenn sie die gleiche oder eine bessere Distanz aufweist.
- Die Route ist in der Tabelle vorhanden mit der Zeit von '7' bis '10', hat also die Distanz '16'. Die neue Route wird auf jeden Fall verwendet.
- Die Route ist in der Tabelle vorhanden. Die neue Route kommt von dem gleichen Router, der auch diese Route bekanntgegeben hat, hat aber eine schlechtere Di-

stanz als der bisherige Eintrag. Wenn ein Router so die Verschlechterung seiner eigenen statischen Routing-Tabelle bekanntmacht (z.B. durch den Abbau einer Verbindung steigt die Distanz von '1' auf '2'), dann glaubt der Router ihm das und nimmt den schlechteren Eintrag in seine dynamische Tabelle auf.



RIP-Pakete aus dem WAN werden nicht beachtet und sofort verworfen! RIP-Pakete aus dem LAN werden ausgewertet und nicht im LAN weitergeleitet!

Zusammenspiel: statische und dynamische Tabelle

Aus der statischen und der dynamischen Tabelle rechnet der Router sich dann die eigentliche IP-Routing-Tabelle zusammen, mit der er den Weg für die Datenpakete bestimmt. Dabei nimmt er zu den Routen aus der eigenen statischen Tabelle die Routen aus der dynamischen Tabelle auf, die er selber nicht kennt oder die eine kürzere Distanz aufweisen als die eigene (statische) Route.

Router ohne IP-RIP-Unterstützung

Manchmal sind im lokalen Netz auch Router vorhanden, die das Routing Information Protocol nicht unterstützen. Diese Router können die RIP-Pakete nicht erkennen und betrachten sie als normale Broadcast- oder Multicast-Pakete. Liegt in diesem Router jetzt die Standard-Route auf einem entfernten Router, werden durch die RIPs ständig Verbindungen aufgebaut. Um das zu vermeiden, kann der RIP-Port in den Filtertabellen eingetragen werden.

Skalierung durch IP-RIP

Verwenden Sie mehrere Router in einem lokalen Netz mit IP-RIP, können Sie die Router im lokalen Netz nach außen hin als einen einzigen großen Router darstellen. Dieses Vorgehen nennt man auch „Skalierung“. Durch den regen Informationsaustausch der Router untereinander steht so ein Router mit prinzipiell beliebig vielen Übertragungswegen zur Verfügung.

IP-Masquerading (NAT, PAT)

Ein ständig wachsendes Problem des Internets ist die Begrenzung der verfügbaren und allgemein gültigen IP-Adressen. Darüber hinaus ist die Zuweisung von festen IP-Adressen für das Internet durch das Network Information Center (NIC) eine kostspielige Sache. Was liegt also näher, als sich mit mehreren Rechnern eine IP-Adresse zu teilen?

Die Lösung heißt hier IP-Masquerading. Bei diesem Verfahren tritt nur ein Router des LANs mit einer IP-Adresse im Internet in Erscheinung. Diese IP-Adresse wird dem Router z.B. fest vom NIC oder temporär von einem Internet-Provider zugewiesen. Alle anderen Rechner im Netz „verstecken“ sich dann hinter dieser einen IP-Adresse. Neben dem angenehmen Spareffekt bildet das IP-Masquerading auch einen sehr effektiven Schutz gegen Zugriffe aus dem Internet auf das lokale Netz.

Zwei Adressen für den Router

Bei Masquerading treffen zwei gegensätzliche Forderungen an den Router aufeinander: Zum einen soll er eine im lokalen Netz gültige IP-Adresse haben, damit er aus dem LAN erreichbar ist, zum anderen soll er eine im Internet gültige Adresse haben. Da diese beiden Adressen prinzipiell nicht in einem logischen Netz liegen dürfen, hilft hier nur eins: Zwei IP-Adressen müssen her. Der Router bekommt also nun eine **Internet**-Adresse und eine **Intranet**-Adresse, jeweils natürlich mit passender Netzmaske. Mit der Option 'Maskierung' in der Routing-Tabelle informieren Sie den Router darüber, welche der beiden Adressen er bei der Weitergabe der Pakete verwenden soll. Wird dabei vom Provider eine bestimmte Adresse angefordert, gibt es zwei Möglichkeiten der tatsächlichen Adreßzuweisung:

- Der Provider weist dem Router die gewünschte Adresse zu. Die Netzmaske entscheidet nun, wie viele Rechner hinter dem Router maskiert werden.
 - IP-Adresse mit voll ausgefüllter Netzmaske '255.255.255.255': Dieses ist Ihre eigene, einzige vom NIC registrierte IP-Adresse. Alle anderen Rechner im Netz haben keine im Internet gültigen Adressen und werden hinter der festen Adresse der Router maskiert.
 - IP-Adresse mit nicht voll ausgefüllter Netzmaske, z.B. '255.255.255.248': Sie haben mehrere registrierte IP-Adressen, von denen Sie eine dem Router geben. Die anderen IP-Adressen vergeben Sie fest an Geräte im Intranet, die dann über unmaskierte Verbindungen auf das Internet zugreifen können. Die anderen Geräte können trotzdem über maskierte Verbindungen ins Internet.
- Der Provider weist dem Router eine andere Adresse zu. Dann werden **alle** Rechner im lokalen Netz hinter der zugewiesenen Adresse maskiert.

Wie funktioniert IP-Masquerading?

Das Masquerading nutzt die Eigenschaft der Datenübertragung über TCP/IP aus, daß neben der Quell- und Ziel-Adresse auch Portnummer für Quelle und Ziel verwendet werden. Bekommt der Router nun ein Datenpaket zur Übertragung, merkt er sich die IP-Adresse und den Port des Absenders in einer internen Tabelle. Dann gibt er dem Paket seine eigene IP-Adresse und eine beliebige neue Portnummer. Diesen neuen Port trägt es ebenfalls in der Tabelle ein und leitet das Paket mit den neuen Angaben weiter.

Die Antwort auf dieses Paket geht nun an die IP-Adresse der Router mit der neuen Absender-Portnummer. Mit dem Eintrag in der internen Tabelle kann der Router diese Antwort nun wieder dem ursprünglichen Absender zuordnen.



In den Statistiken des Routers können Sie sich diese Tabellen genau ansehen (siehe auch 'Status' im Referenz-Handbuch).

Einfaches und inverses Masquerading

Diese Maskierung funktioniert in beide Richtungen: Wenn ein Rechner aus dem LAN ein Paket ins Internet schickt, wird das lokale Netz hinter der IP-Adresse des Routers maskiert (einfaches Masquerading).

Schickt umgekehrt ein Rechner aus dem Internet ein Paket z.B. an einen FTP-Server im Intranet, so sieht es für diesen Rechner so aus, als wäre der Router der FTP-Server. Der Router kennt über den Eintrag in der Service-Tabelle die Intranet-Adresse des Servers (im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Masq.' oder im Menü `Setup/IP-Router-Modul/Masquerading/Service-Tabelle`). Das Paket wird an diesen Rechner weitergeleitet. Alle Pakete, die vom FTP-Server im lokalen Netz kommen (Antworten des Servers), werden hinter der IP-Adresse des Routers versteckt.

Der kleine Unterschied:

- Der Zugriff von außen auf einen Dienst (Port) im Intranet muß vorher durch Angabe einer Port-Nummer definiert werden. In einer Service-Tabelle wird dazu der Ziel-Port mit der Intranet-Adresse z.B. des FTP-Servers angegeben.
- Beim Zugriff aus dem Intranet auf das Internet hingegen wird der Eintrag in der Tabelle mit Port- und IP-Adreß-Informationen durch den Router selbst vorgenommen. Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also **gleichzeitig** 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

Nach einer einstellbaren Zeit geht der Router jedoch davon aus, daß der Eintrag nicht mehr benötigt wird, und löscht ihn selbständig wieder aus der Tabelle.

Welche Protokolle können mit IP-Masquerading übertragen werden?

Natürlich nur solche, die auch über Ports kommunizieren. Protokolle, die ohne Port-Nummern arbeiten oder die oberhalb von IP im OSI-Modell Ports verwenden, können nicht ohne spezielle Behandlung maskiert werden.

In der aktuellen Version führt der Router ein Masquerading für folgende Protokolle durch:

- FTP
- TCP
- UDP
- ICMP

DNS-Forwarding

Beim Zugriff auf das Internet werden meistens keine IP-Adressen verwendet, um einen Server zu erreichen, sondern Namen. Wer weiß auch schon, welche Adresse sich hinter 'www.domain.com' verbirgt? Der DNS-Server!

DNS heißt Domain Name Service und bezeichnet die Zuordnung von Domain-Namen (wie domain.com) zu den entsprechenden IP-Adressen. Diese Informationen müssen natürlich ständig gepflegt und immer weltweit verfügbar gehalten werden. Dazu gibt es eben diese DNS-Server, die lange Tabellen mit IP-Adressen und Domain-Namen anbieten.

Wenn nun ein Rechner aus dem Intranet eine Homepage aufrufen möchte, sendet er zunächst einen DNS-Request aus: „Welche IP-Adresse gehört zu www.domain.com?“ Wenn der Router bei den Arbeitsplatzrechnern als DNS-Server eingetragen ist, wird diese Anfrage folgendermaßen behandelt:

- Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist (im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Adressen' oder im Menü /Setup/TCP-IP-Module). Wird er dort fündig, baut er eine Verbindung zu diesem Server auf und holt die gewünschte Information.
- Gibt es keinen eingetragenen DNS-Server im Router, versucht er auf einer evtl. bestehenden PPP-Verbindung (z.B. zum Internet-Provider) einen DNS-Server zu erreichen, und holt die Zuordnung der IP-Adresse zum Namen von dort. Das gelingt natürlich nur dann, wenn während der PPP-Verhandlung die Adresse eines DNS-Servers an den Router übermittelt worden ist.
- Besteht keine Verbindung, wird die Default-Route aufgebaut und dort nach dem DNS-Server gesucht.

Durch dieses Verfahren benötigen Sie keine Kenntnisse über die Adressen eines DNS-Servers. Der Eintrag der Intranet-Adresse Ihres Routers als DNS-Server bei den Arbeitsplatzrechnern reicht aus, um die Namenszuordnung zu ermöglichen. Außerdem wird damit die Adresse des DNS-Servers automatisch aktualisiert. Sollte z.B. der Provider, der diese Adresse mitteilt, seinen DNS-Server umbenennen, oder Sie sollten zu einem anderen Provider wechseln, erhält der Router stets die aktuellen Informationen.

Policy Based Routing

Policy Based Routing bezeichnet ein Verfahren, bei dem bestimmte Datenpakete bevorzugt behandelt werden sollen. Dazu wird ein spezielles Feld innerhalb der IP-Datenpakete ausgewertet, das Type-of-Service(TOS)-Feld. Diese bevorzugte Behandlung einiger Datenpakete soll z.B. die Konfiguration der Router über das WAN erleichtern, wenn gleichzeitig viele Daten übertragen werden sollen.



Weitere Informationen zu Policy Based Routing finden Sie in der 'Beschreibung der Menüpunkte' im Referenz-Handbuch.

Automatische Adreßverwaltung mit DHCP

Für einen reibungslosen Betrieb in einem TCP/IP-Netzwerk benötigen alle Geräte in einem lokalen Netzwerk eindeutige IP-Adressen. Zusätzlich brauchen sie noch die Adressen von DNS- und NBNS-Servern sowie eines Standard-Gateways, über das Datenpa-

kete von lokal nicht erreichbaren Adressen geroutet werden sollen. Bei einem kleinen Netzwerk ist es durchaus noch denkbar, allen Rechnern im Netz „von Hand“ diese Adressen einzutragen. Bei einem großen Netz mit vielen Arbeitsplatzrechnern wird das jedoch leicht zu einer unüberschaubaren Aufgabe.

In solchen Fällen bietet sich die Verwendung des DHCP (Dynamic Host Configuration Protocol) an. Über dieses Protokoll kann ein DHCP-Server in einem TCP/IP-Netz den einzelnen Stationen die benötigten Adressen dynamisch zuweisen.

Der Router als DHCP-Server

Der Router kann als DHCP-Server die Adressen in seinem TCP/IP-Netz verwalten. Dabei teilt er den Arbeitsplatzrechnern die folgenden Parameter mit:

- IP-Adresse
- Netzmaske
- Broadcast-Adresse
- DNS-Server
- NBNS-Server
- Default-Gateway
- Gültigkeitsdauer der zugewiesenen Parameter

Der DHCP-Server entnimmt die IP-Adressen entweder aus einem frei definierten Adreß-Pool oder ermittelt die Adressen selbständig aus der eigenen IP- oder Intranet-Adresse.

Ein völlig unkonfigurierter Router von ELSA kann sogar im DHCP-Automode die IP-Adressen für sich selbst und für die Rechner im Netz selbständig festlegen.

Im einfachsten Fall müssen Sie daher nur den neuen Router im Auslieferungszustand in einem Netz ohne andere DHCP-Server anschließen und einschalten. Der Router regelt im Zusammenspiel mit *ELSA LANconfig* über einen Assistenten dann alle weiteren Adreß-Zuweisungen im lokalen Netz selbst.

DHCP – 'Ein', 'Aus' oder 'Auto'?

Der DHCP-Server in der Routern von ELSA kann drei verschiedene Zustände annehmen:

- 'Ein': Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adreß-Pools) überprüft.
 - Bei einer korrekten Konfiguration bietet der Router sich als DHCP-Server im Netz an.
 - Bei einer fehlerhaften Konfiguration (z.B. ungültige Pool-Grenzen) wird der DHCP-Server wieder abgeschaltet und wechselt in den Zustand 'Aus'.
- 'Aus': Der DHCP-Server ist dauerhaft abgeschaltet.

- 'Auto': Der Server befindet sich im Automodus. In diesem Zustand sucht der Router nach dem Einschalten im lokalen Netz nach anderen DHCP-Servern (erkennbar durch das kurze Aufleuchten der Tx-LED nach dem Einschalten).
 - Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Damit wird u.a. verhindert, daß ein unkonfigurierter Router nach dem Einschalten im Netz Adressen vergibt, die nicht im lokalen Netz liegen.
 - Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein.

Ob der Server letztendlich ein- oder ausgeschaltet ist, kann den DHCP-Statistiken entnommen werden.

Die Default-Einstellung für den Zustand ist 'Auto'.

So werden die Adressen zugewiesen

Zuweisung von IP-Adressen

Damit der DHCP-Server den Rechnern im Netz IP-Adressen zuweisen kann, muß er zunächst einmal wissen, welche Adressen er für diese Zuweisung verwenden darf. Für die Auswahl der möglichen Adressen gibt es drei verschiedene Optionen:

- Die zugewiesene IP-Adresse kann aus dem eingestellten Adreß-Pool genommen werden (Start-Adreß-Pool bis End-Adreß-Pool). Hier können beliebige im lokalen Netz gültige Adressen eingegeben werden.
- Wird stattdessen '0.0.0.0' eingegeben, so ermittelt der DHCP-Server selbständig die jeweiligen Adressen (Start bzw. Ende) aus den Einstellungen für die IP-Adresse oder Intranet-Adresse im 'TCP-Modul'. Dabei wird wie folgt vorgegangen:
 - Ist nur die IP-Adresse oder nur die Intranet-Adresse eingegeben, so wird über die zugehörige Netzmaske der Start bzw. das Ende des Pools bestimmt.
 - Sind beide angegeben, so hat die Intranet-Adresse den Vorrang bei der Bestimmung des Pools.

Aus der verwendeten Adresse (IP- oder Intranet-Adresse) und der zugehörigen Netzmaske ermittelt der DHCP-Server die erste und die letzte mögliche IP-Adresse im lokalen Netz als Start- bzw. End-Adresse des Adreß-Pools.

- Wenn der Router weder eine eigene IP- noch eine Intranet-Adresse hat, befindet sich das Gerät in einem besonderen Betriebszustand. Es verwendet dann selbst die IP-Adresse '10.0.0.254' und den Adreß-Pool '10.x.x.x' für die Zuweisung der IP-Adressen im Netz. In diesem Zustand weist der DHCP-Server den anderen Rechnern im Netz nur die IP-Adresse und deren Gültigkeit zu, nicht jedoch die anderen Informationen.

Wenn nun ein Rechner im Netz gestartet wird, der mit seinen Netzwerk-Einstellungen über DHCP eine IP-Adresse anfordert, wird ihm ein Router mit aktiviertem DHCP-Modul die Zuweisung einer Adresse anbieten. Als IP-Adresse wird dabei eine gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit bereits schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

Der DHCP-Server prüft zusätzlich, ob die ausgesuchte Adresse im lokalen Netz noch frei ist. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.

Zuweisung der Netzmaske

Die Zuweisung der Netzmaske erfolgt analog zur Adreßzuweisung. Wenn im DHCP-Modul eine Netzmaske eingetragen ist, wird diese bei der Zuweisung verwendet. Ansonsten wird die Netzmaske aus dem TCP/IP-Modul verwendet (Reihenfolge wie bei der Adreßzuweisung).

Zuweisung der Broadcast-Adresse

In der Regel wird im lokalen Netz für Broadcast-Pakete eine Adresse verwendet, die sich aus den gültigen IP-Adressen und der Netzmaske ergibt. Nur in Sonderfällen (z.B. bei Verwendung von Sub-Netzen für einen Teil der Arbeitsplatzrechner) kann es nötig sein, eine andere Broadcast-Adresse zu verwenden. In diesem Fall wird die zu verwendende Broadcast-Adresse im DHCP-Modul eingetragen.



Die Änderung der Voreinstellung für die Broadcast-Adresse wird nur für erfahrene Netzwerk-Spezialisten empfohlen. Eine Fehlkonfiguration in diesem Bereich kann zu unerwünschten, kostenpflichtigen Verbindungsaufbauvorgängen führen!

Zuweisung von DNS- und NBNS-Server

Hierzu werden die zugehörigen Einträge aus dem 'TCP-Modul' herangezogen.

Ist bei den entsprechenden Feldern kein Server angegeben, so gibt der Router seine eigene IP-Adresse als DNS-Adresse weiter. Diese wird bestimmt, wie unter 'Zuweisung einer IP-Adresse' beschrieben. Der Router verwendet dann DNS-Forwarding (siehe auch 'DNS-Forwarding'), um DNS- oder NBNS-Anfragen des Hosts aufzulösen.

Zuweisung des Default-Gateways

Der Router weist dem anfragenden Rechner immer seine eigene IP-Adresse als Gateway-Adresse zu.

Falls erforderlich, kann diese Zuweisung durch die Einstellungen am Arbeitsplatzrechner überschrieben werden.

Gültigkeitsdauer einer Zuweisung

Die dem Rechner einmal zugewiesenen Adressen haben nur eine begrenzte Gültigkeit. Nach Ablauf dieser Gültigkeitsdauer darf der Rechner sie nicht mehr verwenden. Damit der Rechner die Adressen (vor allem seine IP-Adresse) danach nicht immer wieder verliert, beantragt er rechtzeitig eine Verlängerung, die ihm in der Regel auch immer gewährt wird. Nur wenn die Gültigkeitsdauer abläuft, während der Rechner abgeschaltet ist, verliert er die Adresse.

Bei jeder Anfrage kann ein Host eine bestimmte Gültigkeitsdauer fordern. Ein DHCP-Server kann dem Host aber auch eine davon abweichende Gültigkeitsdauer zuweisen. Das DHCP-Modul bietet zwei Einstellungen, um die Gültigkeitsdauer zu beeinflussen:

- Maximale Gültigkeit in Minuten

Hier kann die maximale Gültigkeitsdauer eingetragen werden, die der DHCP-Server einem Host zuweist.

Fordert ein Host eine Gültigkeit an, die die maximale Dauer von 6000 Minuten überschreitet, so wird ihm nur diese maximale Gültigkeit zugewiesen!

Der Defaultwert von 6000 Minuten entspricht ca. 4 Tagen.

- Default-Gültigkeit in Minuten

Hier kann die Gültigkeitsdauer eingetragen werden, die zugewiesen wird, wenn der Host überhaupt keine Gültigkeitsdauer anfordert. Der Defaultwert von 500 Minuten entspricht ca. 8 Stunden.

Vorfahrt für den DHCP-Server – Zuweisung anfordern

Standardmäßig sind fast alle Einstellungen in der Netzwerkumgebung von Windows so eingestellt, daß die benötigten Parameter über DHCP angefragt werden. Überprüfen Sie die Einstellungen mit einem Klick auf **Start ► Einstellungen ► Systemsteuerung ► Netzwerk**. Wählen Sie den Eintrag für 'TCP/IP' an Ihrem Netzwerkadapter, und öffnen Sie die **Eigenschaften**.

Auf den verschiedenen Registerkarten können Sie nun nachsehen, ob spezielle Einträge z.B. für die IP-Adresse oder das Standard-Gateway vorhanden sind. Wenn Sie alle Werte vom DHCP-Server zuweisen lassen wollen, löschen Sie nur die entsprechenden Einträge.

Auf der Registerkarte 'WINS-Konfiguration' muß zusätzlich die Option 'DHCP für WINS-Auflösung verwenden' eingeschaltet werden, wenn man Windows-Netze über IP mit Namensauflösung über NBNS-Server verwenden will. Der DHCP-Server muß dann außerdem einen NBNS-Eintrag haben.

Vorfahrt für den Rechner – Zuweisung überschreiben

Sollte ein Rechner andere Parameter verwenden als die ihm zugewiesenen (z.B. ein anderes Standard-Gateway), so muß es direkt am Arbeitsplatzrechner eingestellt wer-

den. Der Rechner ignoriert dann die entsprechenden Parameter in der Zuweisung durch den DHCP-Server.

Unter Windows geschieht das z.B. über die Eigenschaften der Netzwerkumgebung.

Klicken Sie auf **Start ► Einstellungen ► Systemsteuerung ► Netzwerk**. Wählen Sie den Eintrag für 'TCP/IP' an Ihrem Netzwerkadapter und öffnen die **Eigenschaften**.

Auf den verschiedenen Registerkarten können Sie nun die gewünschten Werte eintragen.

Im DHCP-Modul des Routers kann über den Punkt 'Setup/DHCP/Tabelle-DHCP' die Zuweisung von IP-Adressen an die jeweiligen Rechner überprüft (bzw. nachgeschaut) werden. Diese Tabelle zeigt die zugewiesene IP-Adresse, die MAC-Adresse, die Gültigkeitsdauer, den Namen des Rechners (falls vorhanden) sowie den Typ der Adreß-Zuweisung.

Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:

- neu
Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.
- unbek.
Bei der Überprüfung der Eindeutigkeit wurde festgestellt, daß die Adresse bereits an einen anderen Rechner vergeben wurde. Der DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.
- stat.
Ein Rechner hat dem DHCP-Server mitgeteilt, daß er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr verwendet werden.
- dyn.
Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

Konfiguration der Router als DHCP-Server

Bei der Konfiguration der Geräte als DHCP-Server gibt es prinzipiell zwei Ausgangssituationen:

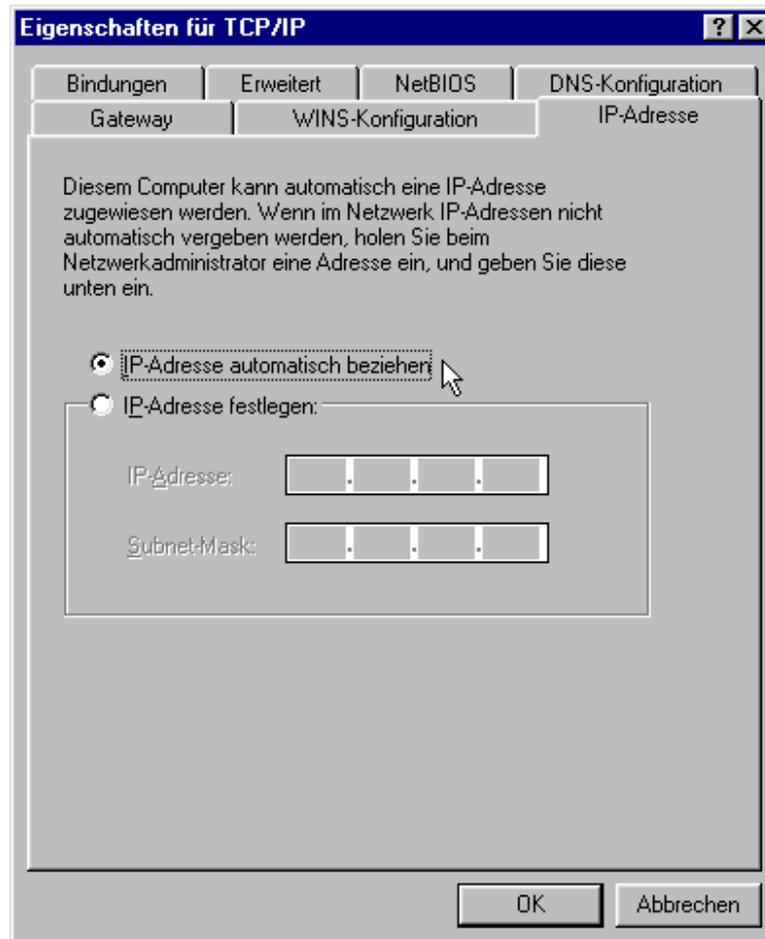
- Sie haben bisher noch kein Netzwerk eingerichtet, oder Ihr vorhandenes lokales Netz verwendet kein TCP/IP. Mit dem DHCP-Server im Router können Sie auf einen Streich allen Rechnern im Netz und dem Router selbst IP-Adressen zuweisen.
- Sie haben auch bisher schon ein Netz mit TCP/IP, aber ohne DHCP-Server betrieben und stellen nun auf DHCP-Betrieb um.

Konfiguration mit *ELSA LANconfig* und den Assistenten

In beiden Situationen hilft Ihnen *ELSA LANconfig* mit einem Assistenten, die notwendigen Einstellungen vorzunehmen:

- ① Verbinden Sie den unkonfigurierten Router über das Netzkabel mit Ihrem lokalen Netz. Wenn Sie das Gerät dabei an einen Hub anschließen, muß der Node/Hub-Umschalter in der 'Node' stehen. Wenn Sie den Router dagegen direkt an die Netzwerkkarte eines Rechners im Netz anschließen, muß sich der Node/Hub-Umschalter in der Position 'Hub' befinden.
- ② Schalten Sie das Gerät ein. Der Router findet dann zunächst keinen anderen DHCP-Server im Netz und aktiviert seine eigenen DHCP-Funktionen.
- ③ Falls noch nicht geschehen, installieren Sie das Protokoll 'TCP/IP' auf allen Rechnern im lokalen Netz.
 - Bei der Installation des Protokolls werden die Rechner meist standardmäßig so eingestellt, daß Sie die IP-Adresse automatisch von einem DHCP-Server beziehen wollen. Nach einem Neustart, der mit dieser Installation verbunden ist, fordern die Rechner automatisch eine IP-Adresse vom DHCP-Server an.
 - Wenn Sie das Protokoll schon installiert haben, aktivieren Sie nun die DHCP-Funktion auf allen Rechnern im lokalen Netz. Öffnen Sie dazu z.B. unter Windows 95 mit **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk** das Fenster zur Konfiguration der Netzwerkeigenschaften. Doppelklicken Sie den Eintrag für das Protokoll 'TCP/IP'.
Aktivieren Sie die Option 'IP-Adresse automatisch beziehen'. Wechseln Sie auf die Registerkarte 'DNS-Konfiguration', und löschen Sie alle vorhandenen DNS-Adressen. Löschen Sie dann auf der Registerkarte 'Gateway' alle evtl. vorhandenen Einträge und schließen alle Fenster mit **OK**. Nach einem Neustart, der mit

dieser Einstellung verbunden ist, fordern die Rechner automatisch eine IP-Adresse aus dem Adreß-Pool des Routers an.



Wie Sie ein Netzwerkprotokoll z.B. unter Windows 95 oder Windows NT installieren, erfahren Sie im Workshop. Hinweise zur Installation von ELSA LANconfig finden Sie im Installation Guide.

- ④ Installieren Sie *ELSA LANconfig* auf einem der Rechner im Netz.
- ⑤ Starten Sie *ELSA LANconfig* aus der Programmgruppe 'ELSAlan'. Beim Start bemerkt *ELSA LANconfig*, daß sich ein unkonfigurierter Router im Netz befindet, und startet den Assistenten für die Grundeinstellungen.
 - Wenn Sie bisher noch keine IP-Adressen in Ihrem Netz verwendet haben, wählen Sie in diesem Assistenten die Option 'Alle Einstellungen automatisch vornehmen', und betätigen Sie im nächsten Fenster die Schaltfläche **Fertigstellen**. Der Assistent weist dem Router nun die IP-Adresse '10.0.0.1' mit der Netzmaske '255.255.255.0' zu und schaltet den DHCP-Server ein. Aus der IP-Adresse ermittelt das Gerät dann den gültigen Adreß-Pool für die DHCP-Zuweisung.
 - Wenn Sie auch vor der Umstellung auf DHCP-Betrieb IP-Adressen in Ihrem Netz verwendet haben, wählen Sie in diesem Assistenten die Option 'Ich möchte die Einstellungen selber vornehmen'. Geben Sie im nächsten Fenster eine freie IP-

Adresse aus dem bisher verwendeten Adreßbereich ein, und schalten Sie den DHCP-Server ein.

Der Assistent weist dem Router nun die eingestellte IP-Adresse mit der zugehörigen Netzmaske zu. Aus der IP-Adresse ermittelt das Gerät dann den gültigen Adreß-Pool für die DHCP-Zuweisung.

- Nach einigen Sekunden werden automatisch alle Rechner im Netz überprüft und erhalten ggf. eine neue IP-Adresse vom DHCP-Server. Zusätzlich werden den Rechnern dann auch die weiteren Parameter wie Broadcast-Adresse, DNS-Server, Default-Gateway etc. mitgeteilt.

Manuelle Konfiguration

Wenn die Konfiguration mit dem Assistenten von *ELSA LANconfig* für Sie nicht in Frage kommt, können Sie die Parameter für den DHCP-Server auch von Hand einstellen: im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'DHCP' oder im Menü /Setup/DHCP-Modul).

DNS

Der Domain-Name-Service (DNS) stellt in TCP/IP-Netzen die Verknüpfung zwischen Rechnernamen bzw. Netzwerknamen (Domains) und IP-Adressen her. Dieser Service ist auf jeden Fall erforderlich für die Kommunikation im Internet, um z.B. einer Anfrage nach 'www.elsa.de' die entsprechende IP-Adresse zurückliefern zu können. Aber auch innerhalb eines lokalen Netzes oder bei der LAN-Kopplung ist es sinnvoll, die IP-Adressen im LAN den Namen der Rechner eindeutig zuzuordnen zu können.

Was macht ein DNS-Server?

Die bei einem DNS-Server nachgefragten Namen bestehen aus mehreren Teilen: ein Teil besteht aus dem eigentlichen Namen des Hosts oder Dienstes, der angesprochen werden soll, ein anderer Teil kennzeichnet die Domain. Innerhalb eines lokalen Netzes ist die Angabe der Domain optional. Diese Namen können also z.B. 'www.domain.com' oder 'ftp.domain.com' heißen.

Ohne DNS-Server im lokalen Netz wird jeder lokal unbekannte Name über die DEFAULT-Route gesucht. Durch die Verwendung eines DNS-Servers können alle Namen, die mit ihrer IP-Adresse bekannt sind, direkt bei der richtigen Gegenstelle gesucht werden. Der DNS-Server kann dabei im Prinzip ein separater Rechner im Netz sein. Folgende Gründe sprechen jedoch dafür, den DNS-Server direkt im *ELSA LANCOM Business* anzusiedeln:

- Ein *ELSA LANCOM Business* kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbständig verteilen. Der DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-Server hätte bei der dynami-

schen Adreßvergabe des DHCP-Servers möglicherweise Schwierigkeiten, die Zuordnung zwischen IP-Adresse und Namen aktuell zu halten.

- Beim Routing von Windows-Netzen über NetBIOS kennt ein *ELSA LANCOM Business* außerdem die Rechnernamen und IP-Adressen in den anderen angeschlossenen NetBIOS-Netzen. Außerdem melden sich auch die Rechner mit fest eingestellter IP-Adresse ggf. in der NetBIOS-Tabelle an und sind damit mit Name und Adresse bekannt.
- Der DNS-Server im *ELSA LANCOM Business* kann gleichzeitig als sehr komfortabler Filtermechanismus eingesetzt werden. Anfragen nach bestimmten Domains, die nicht besucht werden dürfen, können durch die einfache Angabe des Domain-Namens für das ganze LAN, nur für Teilnetze (Subnetze) oder sogar für einzelne Rechner gesperrt werden.

Der DNS-Server bezieht bei Anfragen nach bestimmten Namen alle Informationen in die Suche mit ein, die ihm zur Verfügung stehen:

- Zuerst prüft der DNS-Server, ob der Zugriff auf diesen Namen nicht durch die Filterliste verboten ist. Wenn das der Fall ist, wird der anfragende Rechner mit einer Fehlermeldung darüber informiert, daß er auf diesen Namen nicht zugreifen darf.
- Dann sucht er in der eigenen, statischen DNS-Tabelle nach Einträgen für den entsprechenden Namen.
- Steht in der DNS-Tabelle kein Eintrag für diesen Namen, wird die dynamische DHCP-Tabelle durchsucht. Die Verwendung der DHCP-Informationen kann bei Bedarf ausgeschaltet werden.
- Findet der DNS-Server in den vorausgegangenen Tabellen keine Informationen über den Namen, werden die Listen des NetBIOS-Moduls durchsucht. Auch die Verwendung der NetBIOS-Informationen kann bei Bedarf ausgeschaltet werden.

Sollte der gesuchte Name in allen verfügbaren Informationen nicht gefunden werden, leitet der DNS-Server die Anfrage über den normalen DNS-Forwarding-Mechanismus an einen anderen DNS-Server (z.B. beim Internet-Provider) weiter oder schickt dem anfragenden Rechner eine Fehlermeldung.

So stellen Sie den DNS-Server ein

Die Einstellungen für den DNS-Server finden Sie im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'DNS-Server'. Gehen Sie zur Einstellung des DNS-Servers wie folgt vor:

- ① Schalten Sie den DNS-Server ein.

```
set setup/dns-modul/zustand ein
```

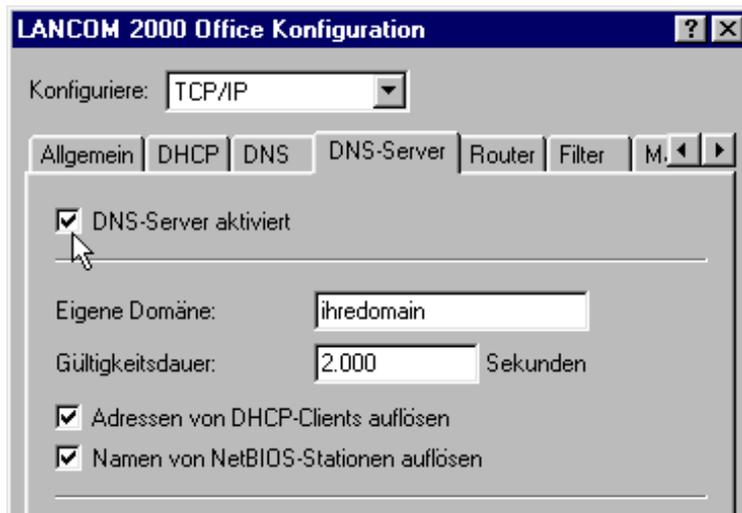
- ② Geben Sie die Domain ein, in der sich der DNS-Server befindet. Mit Hilfe dieser Domain erkennt der DNS-Server bei Anfrage, ob sich der gesuchte Name im eigenen LAN befindet oder nicht. Die Angabe der Domain ist optional.

```
set setup/dns-modul/domain ihredomain.de
```

- ③ Geben Sie an, ob die Informationen aus dem DHCP-Server und dem NetBIOS-Modul verwendet werden sollen.

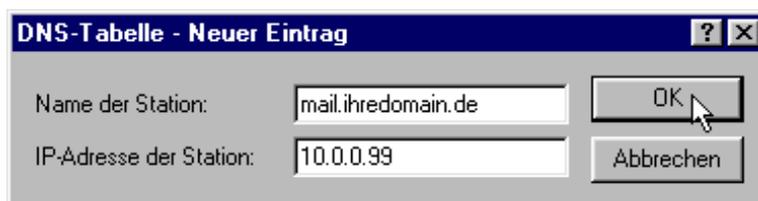
```
set setup/dns-modul/dhcp-verwenden ja
```

```
set setup/dns-modul/NetBIOS-verw. ja
```



- ④ Der DNS-Server dient hauptsächlich dazu, Anfragen nach Namen im Internet von den Anfragen nach Namen bei anderen Gegenstellen zu trennen. Tragen Sie daher alle Rechner in die DNS-Tabelle ein,
- deren Name und IP-Adresse Sie kennen,
 - die nicht im eigenen LAN liegen,
 - die nicht im Internet liegen und
 - die über den Router erreichbar sind.

Wenn Sie z.B. in einem externen Büro arbeiten und über den Router den Mailserver in der Zentrale (Name: mail.ihredomain.de, IP: 10.0.0.99) erreichen wollen, tragen Sie ein:



```
cd setup/dns-modul/dns-tabelle
```

```
set mail.ihredomain.de 10.0.0.99
```

Die Angabe der Domain ist dabei optional, aber zu empfehlen.

Wenn Sie nun das Mailprogramm starten, wird es vermutlich automatisch den Server 'mail.ihredomain.de' suchen. Der DNS-Server gibt daraufhin die IP-Adresse '10.0.0.99' zurück. Das Mailprogramm sucht dann nach dieser IP-Adresse. Mit ent-

sprechenden Einträgen in IP-Routing-Tabelle und Namenliste etc. wird dann automatisch die Verbindung zum Netz in der Zentrale hergestellt, wo der Mailserver schließlich gefunden wird.

- ⑤ Mit der Filterliste können Sie schließlich ganz genau bestimmen, wer auf welche Namen oder Domains nicht zugreifen darf.

```
cd setup/dns-modul/filter-liste
```

```
set 001 www.gesperrte-domain.de 0.0.0.0 0.0.0.0
```

Mit diesem Eintrag (mit dem Index '001') sperren Sie diese Domain für alle Rechner im lokalen Netz. Der Index '001' ist frei gewählt und dient lediglich der Übersichtlichkeit. Bei der Eingabe der Domain sind auch die Wildcards '?' (steht für genau ein Zeichen) und '*' (für beliebig viele Zeichen) erlaubt. Wenn nur ein bestimmter Rechner (z.B. mit IP 10.0.0.123) nicht auf DE-Domains zugreifen können soll, tragen Sie ein:

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



Die Hitliste in der DNS-Statistik zeigt Ihnen die 64 Namen, die am häufigsten nachgefragt werden, und bietet Ihnen damit eine gute Basis für die Einstellung der Filter-Liste.

Durch die geeignete Wahl von IP-Adressen und Netzmasken können bei der Verwendung von Subnetting in Ihrem LAN auch einzelne Abteilungen gefiltert werden. Dabei steht die IP-Adresse '0.0.0.0' jeweils für alle Rechner in einem Netz, die Netzmaske '0.0.0.0' für alle Netze.

NetBIOS-Proxy

Mit der Funktion als NetBIOS-Proxy kann ein *ELSA LANCOM Business* auch NetBIOS-Pakete routen oder als Proxy lokal beantworten. Damit ergibt sich die Möglichkeit, u.a. Windows-Netze über die Routerfunktionen kostengünstig zu verbinden.

Dieser Abschnitt beschreibt die Funktion von NetBIOS-Proxy allgemein und die Konfiguration des Routers und der beteiligten Rechner für die Verbindung von Windows-Netzen.

Kurz und bündig: Was ist NetBIOS?

NetBIOS dient dazu, mehrere Rechner einfach und unkompliziert zu vernetzen. Ein wichtiger Vertreter eines NetBIOS-Netztes ist das Windows-Netz, über das sich mehrere Win-

dows 3.11, 9x und NT Rechner einfach vernetzen lassen, und in dem die Ressourcen der jeweiligen Rechner (Laufwerke oder Drucker) für alle anderen freigegeben werden können.

In einem Windows-Netz werden die Rechner nur über ihre Namen angesprochen. Mehrere Rechner können zu Gruppen und mehrere Gruppen zu Namenräumen (Scopes) zusammengefaßt werden. Damit ein Rechner auf die Ressourcen der anderen zugreifen kann, müssen die verwendeten Namen im ganzen Netz bekannt sein. Damit nun nicht auf jedem Rechner eine Tabelle der bekannten Namen gepflegt werden muß, geben NetBIOS-Rechner ihre Namen selbständig in regelmäßigen Abständen im Netz bekannt.

Die so bekanntgemachten Namen sollen natürlich auch an einer zentralen Stelle im Windows-Netz gesammelt und bereitgestellt werden. Wenn zwei Windows-Netze über Router gekoppelt werden sollen, muß auf beiden Seiten der Verbindung eine solche Namensammelstelle, ein NetBIOS-Nameserver (NBNS) vorhanden sein.

- Dazu kann z.B. ein eigener WINS-Server (Windows Internet Name Service-Server) im Netz installiert sein.
- Da viele Windows-Netze aber eben ohne eigene Server auskommen wollen oder müssen, bietet sich eine zweite Möglichkeit an: Die Informationen über die verwendeten Namen können auch an einer Art „schwarzem Brett“ gesammelt werden, an dem alle Rechner nur ihren Namen und ihre IP-Adresse hinterlassen. Dabei sind die Rechner selbst für die Konsistenz der Namen im Netz verantwortlich.

Ein *ELSA LANCOM Business* verfügt über ein solches schwarzes Brett. Durch diese einfache Realisierung des NBNS ist die Verbindung auch von Windows-Netzen ohne Server möglich. Die Rechner in den verbindungswilligen Netzen geben Ihre Namen nun auch im jeweils anderen Netz bekannt und füllen auch dort das schwarze Brett.

Behandlung von NetBIOS-Paketen

Das äußerst geschwätchige Verhalten der Windows-Rechner kann bei der Verbindung über ISDN-Leitungen hohe Gebühren verursachen, da jedes NetBIOS-Paket mit Namensinformationen automatisch zum Verbindungsaufbau führt (z.B. zum bereits eingerichteten ISP). Durch diese Pakete bleibt die Leitung ständig aufgebaut und es fallen entsprechend hohe Gebühren an, ohne daß wirklich eine Nutzdatenübertragung stattfindet.

Um diesen unnötigen Verbindungsaufbau zu vermeiden, kann ein *ELSA LANCOM Business* die NetBIOS-Pakete entweder routen oder als Proxy selbst beantworten:

- Zum Routen der wirklich benötigten Pakete kann im NetBIOS-Modul festgelegt werden, an welche Gegenstellen die Namensinformationen über NetBIOS übertragen werden sollen. Beim dem Einschalten des NetBIOS-Moduls wird nach einer zufälligen Wartezeit eine Verbindung zu den NetBIOS-Gegenstellen aufgebaut (sofern es sich nicht um einzelne Remote-Access-Rechner handelt). Gelingt der Aufbau nicht, so wird die Spanne der Wartezeit vergrößert. Mit dem anschließenden Austausch der NetBIOS-Informationen wird so erstmalig das schwarze Brett gefüllt.

- In der Funktion als Proxy beantwortet das Gerät Anfragen an die Rechner, die im NetBIOS-Modul (am schwarzen Brett) schon bekannt sind, selbst als Stellvertreter des entsprechenden Rechners. Sowohl bei Nachfragen nach Rechnern im eigenen LAN als auch nach bekannten Rechnern im Netz auf der Gegenseite werden also nach dem ersten Informationsaustausch keine neuen Verbindungen aufgebaut.

Damit die Anfragen nach Rechnern, die weder im eigenen LAN noch bei den festgelegten NetBIOS-Gegenstellen zu finden sind, nicht zum Verbindungsaufbau über die DEFAULT-Route ins Internet führen, fängt der voreingestellte IP-Filter für NetBIOS-Ports diese Pakete ab und verhindert den Verbindungsaufbau.

Welche Voraussetzungen müssen erfüllt sein?

Für die einwandfreie Kommunikation von Windows-Netzen über Router müssen einige Komponenten auf den beteiligten Rechnern installiert sein und verschiedene Einstellungen im Betriebssystem vorgenommen werden.

Installierte Komponenten

Die Installation der benötigten Komponenten wird hier am Beispiel von Windows 95 bzw. Windows 98 beschrieben, läuft aber unter Windows NT 4.0 ähnlich ab. Installieren Sie die folgenden Komponenten auf allen Rechnern in den zu verbindenden Windows-Netzen:

- Netzwerkprotokoll

NetBIOS ist völlig unabhängig vom verwendeten Transportprotokoll. So kann ein NetBIOS-Netzwerk über die Protokolle NetBEUI (NetBIOS Extended User Interface), IPX (Internet Packet eXchange, Novell) oder IP (Internet-Protokoll) übertragen werden.



Im Gegensatz zu IPX und IP ist NetBEUI nicht routbar, also nur in einem Windows-Netz verfügbar. Sollen mehrere Windows-Netze über Router verbunden werden, so muß NetBIOS auf einem routbaren Protokoll, z.B. im ELSA LANCOM Business auf IP aufsetzen!

Das Routing von NetBIOS-Paketen im *ELSA LANCOM Business* basiert aufgrund der besseren Filtermechanismen auf TCP/IP. Dieses Protokoll muß also auf allen Rechnern, die gekoppelt werden sollen, installiert sein.

Um das Netzwerkprotokoll zu installieren, klicken Sie **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ Hinzufügen ▶ Protokoll**. Wählen Sie 'Microsoft' als Hersteller und 'TCP/IP' als Netzwerkprotokoll aus.

- Client

Der Client für Windows-Netzwerke wird benötigt, damit sich die Rechner im Windows-Netz mit Name und Paßwort anmelden können.

Um den Client zu installieren, klicken Sie **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ Hinzufügen ▶ Client**. Wählen Sie 'Microsoft' als Hersteller und dann den 'Client für Windows-Netzwerke' aus.

■ Dienst

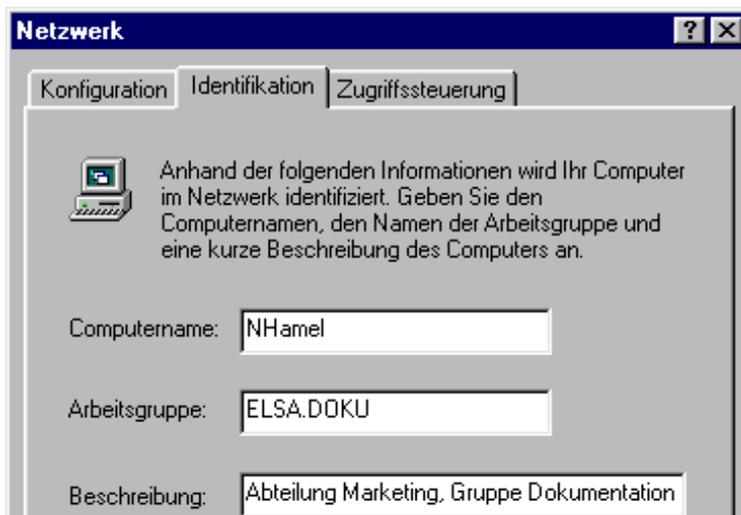
Die Datei- und Druckerfreigabe ermöglicht das Freigeben von Laufwerken oder Druckern für andere Benutzer im Windows-Netz.

Um die Datei- und Druckerfreigabe zu installieren, klicken Sie **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ Hinzufügen ▶ Dienst**. Wählen Sie 'Microsoft' als Hersteller und dann den 'Datei- und Druckerfreigabe für Windows-Netzwerke' aus.

Einstellungen im Windows-Netzwerk

■ Namen und Gruppenbezeichnung

Klicken Sie auf **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk**, und wechseln Sie auf die Registerkarte **Identifikation**.

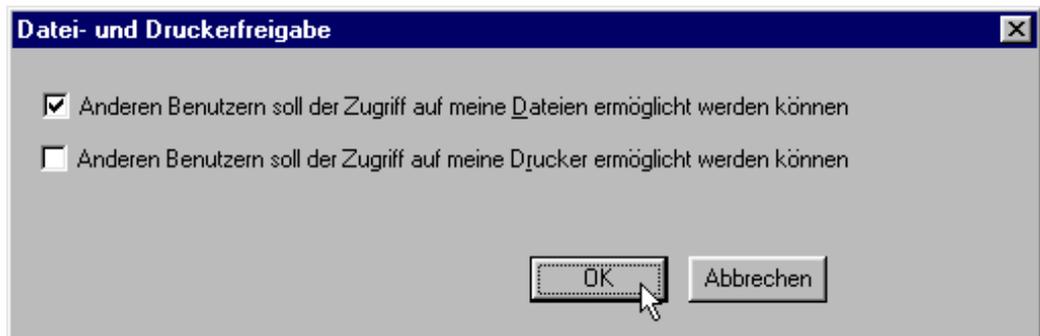


Der Name des Rechners muß eindeutig sein. Das gilt für alle Windows-Netze und alle in diesen Netzen vorhandenen Gruppen, die Sie über NetBIOS verbinden wollen. Auch in verschiedenen Gruppen darf ein Name also nicht mehrfach auftauchen.

■ Datei- und Druckerfreigabe

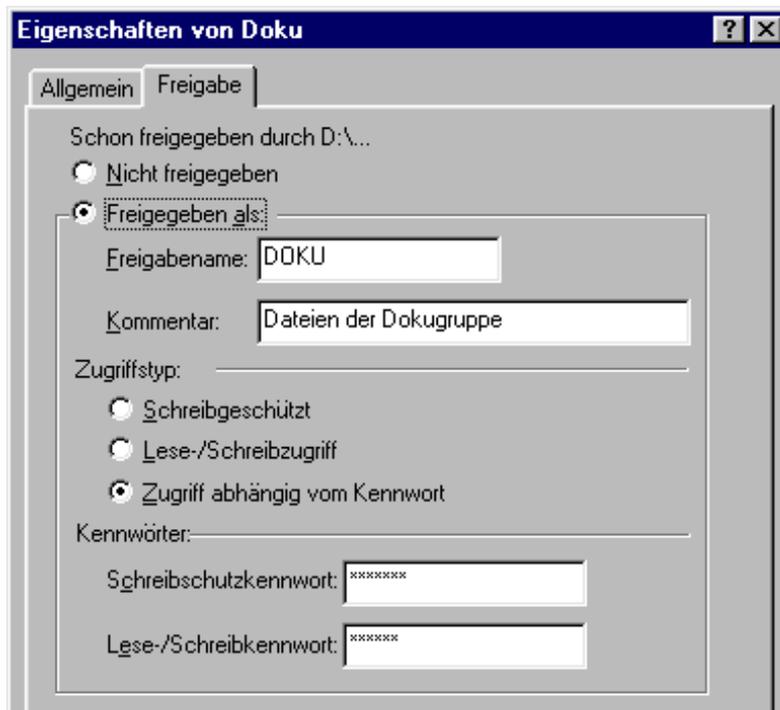
Prüfen Sie nach der Installation, ob die Datei- und Druckerfreigabe aktiviert ist. Klicken Sie dazu **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ Datei- und Druckerfreigabe**. Wählen Sie aus, ob die anderen Benutzer im Win-

dows-Netz den Drucker und/oder die Dateien von diesem Rechner nutzen können.



Alle Benutzer, die auf die freigegebenen Ressourcen zugreifen wollen, müssen sich beim Start von Windows mit Name und Paßwort anmelden.

Klicken Sie dann im Explorer mit der rechten Maustaste die Laufwerke, Ordner oder Drucker, die Sie für die Benutzung durch andere Netzteilnehmer freigeben wollen, und wählen Sie den Punkt **Freigabe** aus dem Kontextmenü.



Geben Sie dem freigegebenen Ordner einen Namen und tragen Sie ggf. einen Kommentar ein. Mit der Auswahl des Zugriffstyps und der Festlegung der Kennwörter stellen Sie ein, wie der Zugriff auf die freigegebenen Ressourcen erfolgen kann.

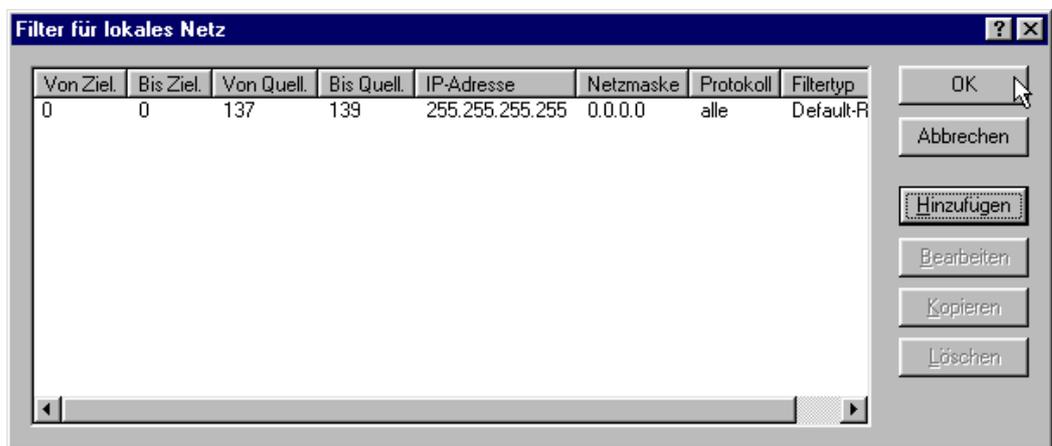


Ob die Einstellungen im Windows-Netzwerk korrekt erfolgt sind, können Sie leicht prüfen: Der eigene Rechner muß in der Netzwerkumgebung mit seinem Namen angezeigt werden.

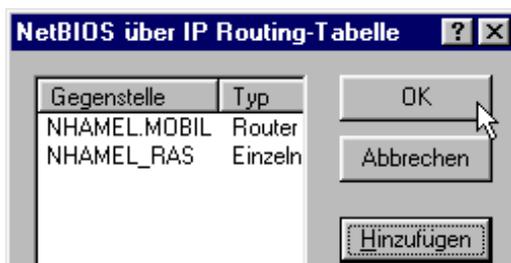
So verbinden Sie zwei Windows-Netze über ISDN

Nachdem alle Vorbereitungen abgeschlossen sind, können Sie nun zwei Windows-Netze verbinden. Die Einstellungen für Arbeitsgruppennetze und Domänen-Netze (Windows NT) sind dabei ähnlich. Die folgenden Schritte sind für beide Seiten der Verbindung auszuführen.

- ① Stellen Sie die beiden Netze für eine LAN-LAN-Kopplung über TCP/IP ein, wie im Workshop beschrieben. Verwenden Sie dazu nach Möglichkeit den komfortablen Assistenten von *ELSA LANconfig*.
- ② Prüfen Sie die Einstellung der IP-Filter. Dieser Filter muß alle NetBIOS-Pakete erfassen, die über die DEFAULT-Route geschickt werden sollen, damit NetBIOS-Pakete nicht zum Verbindungsaufbau über die DEFAULT-Route führen. Im Auslieferungszustand der Geräte ist dieser Filter so voreingestellt:



- ③ Tragen Sie dann die Gegenstelle für das Routing über NetBIOS ein. Wechseln Sie in *ELSA LANconfig* in den Konfigurationsbereich 'NetBIOS', und erstellen Sie einen neuen Eintrag in der Tabelle 'NetBIOS über IP-Routing'.



Bei der Konfiguration über Telnet geben Sie alternativ ein:

```
cd /Setup/NetBIOS-Modul/Gegenstellen-Tab.
set nhamel.mobil router
```

Der Eintrag im Feld 'Typ' gibt an, ob die Gegenstelle nach dem Einschalten des NetBIOS-Moduls direkt angewählt werden soll, um die Namens-Informationen auszutauschen.



Der Parameter 'NT-Domain' kann bei Windows-95- oder Windows-98-Netzen i.d.R. freigelassen werden. Beim Zugriff auf Windows-NT-Maschinen muß die entsprechende Domain/Arbeitsgruppe manuell eingetragen werden.

- ④ Verwendet die NetBIOS-Kopplung eine PPP-Verbindung, müssen Sie in der PPP-Liste die Aktivierung von NetBIOS für den entsprechenden Eintrag prüfen.
- ⑤ Wenn alle Gegenstellen eingetragen sind, aktivieren Sie die NetBIOS-Funktion.

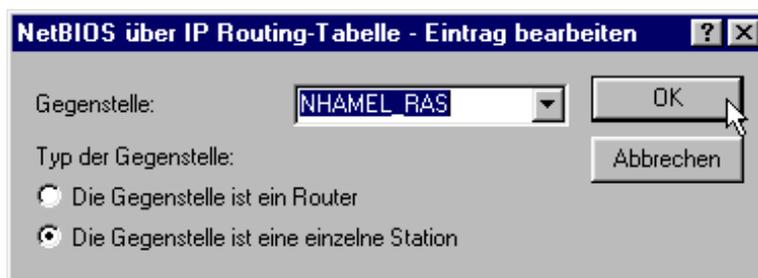
```
cd /Setup/NetBIOS-Modul
set zustand ein
```

Nach dem Einschalten wird (nach einer zufälligen Wartezeit) eine Verbindung zu allen Gegenstellen aufgebaut, die nicht als Einwahl-Knoten gekennzeichnet sind. Bei dieser ersten Verbindung werden dann die notwendigen Informationen über die Rechner in den Netzen ausgetauscht. Erst danach kann auf die Rechner der Gegenseite zugegriffen werden.

So wählt sich ein Remote-Access-Rechner ein

Der Zugriff von einzelnen, entfernten Rechner über Remote-Access auf ein Windows-Netz ist ebenfalls schnell erledigt.

- ① *ELSA LANCOM Business* und Remote-Access-Rechner werden, wie im Workshop beschrieben, auf den Netz-Zugriff vorbereitet. Auch in diesem Fall sind die IP-Filter im *ELSA LANCOM Business* zu prüfen (siehe 'So verbinden Sie zwei Windows-Netze über ISDN').
- ② Wenn die Zuweisung der IP-Adresse für die remote Gegenstelle aus dem IP-Pool realisiert wird, muß für diese Gegenstelle zusätzlich eine Route in der IP-Routing-Tabelle angelegt werden.
- ③ Erstellen Sie auch für die remoten Gegenstellen einen Eintrag in der NetBIOS IP-Routing-Tabelle.



```
cd /Setup/NetBIOS-Modul/Gegenstellen-Tab.
set nhamel.ras workstation
```



Kennzeichnen Sie diesen Eintrag auf jeden Fall als 'einzelne Station', damit diese Gegenstelle nach dem Einschalten des NetBIOS-Moduls nicht automatisch angerufen wird.

- ④ Verwendet die NetBIOS-Kopplung eine PPP-Verbindung, müssen Sie in der PPP-Liste die Aktivierung von NetBIOS für den entsprechenden Eintrag prüfen.

Gesucht - Gefunden: Die Netzwerkumgebung

Wenn alle Beteiligten auf das NetBIOS-Routing vorbereitet sind, kann das Windows-Networking losgehen.

NetBIOS-Routing über LAN-LAN-Kopplung

Nachdem die Netze nach dem Einschalten der NetBIOS-Module gegenseitig die Informationen über die verfügbaren Rechner ausgetauscht haben, ist im *ELSA LANCOM Business* nun eine Liste mit diesen Rechnernamen verfügbar. Über Telnet kann mit

```
dir /Setup/NetBIOS-Modul/host-liste
```

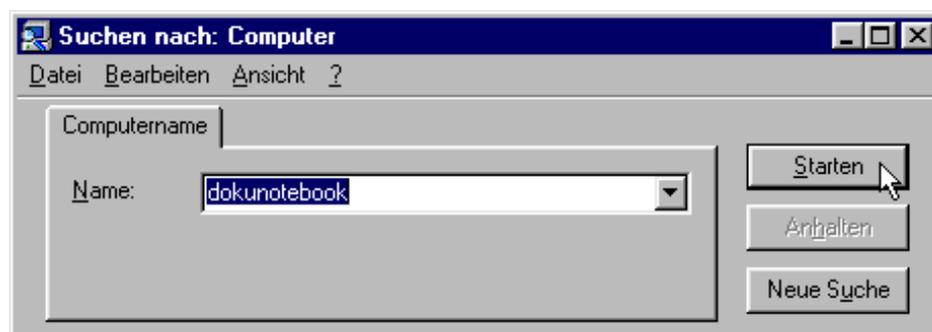
die Liste mit den aktuell erreichbaren Rechnern aufgerufen werden, die z.B. so aussieht:

Name	Typ	IP-Adresse	Gegenstelle	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

Aus dieser Tabelle können Sie nun ablesen, daß z.B. der Rechner mit dem Namen 'DOKUNOTEBOOK' mit der IP-Adresse '10.10.0.53' über die Gegenstelle 'NHAMEL.MOBIL' zu erreichen ist. Die weiteren Parameter werden in der Menü-Beschreibung erläutert.

Um auf die freigegebenen Ressourcen dieses Rechners zugreifen zu können, lassen Sie einfach den Explorer nach dem entsprechenden Rechner suchen mit **Start ▶ Suchen**

▶ **Computer:**



Die Arbeitsgruppen und Rechner des entfernten Netzes können aus technischen Gründen nicht über die Funktion 'gesamtes Netzwerk durchsuchen' in der Windows Netzwerkum-

gebung gefunden werden. Stattdessen kann nach entfernten Computer wie oben beschrieben gesucht werden, bzw. Verknüpfungen und Laufwerksverbindungen eingerichtet werden.

NetBIOS-Routing über RAS-Zugang

Etwas anders sieht das Verfahren beim Zugang zum Windows-Netz über RAS aus. Die beiden grundlegenden Unterschiede zur LAN-LAN-Kopplung:

- Auf der Seite des Einwahl-Knotens ist keine Host-Liste vorhanden, aus der die verfügbaren Rechner im Windows-Netz auf der Gegenseite abgelesen werden könnten. Der RAS-Benutzer muß also die Namen der Rechner kennen, auf die er zugreifen darf und will.
- Die Verbindung wird nicht automatisch aufgebaut. Der RAS-Benutzer muß also erst ein Verbindung über das DFÜ-Netzwerk zum *ELSA LANCOM Business* herstellen.

Wenn die Verbindung dann steht, kann er genau wie bei der LAN-LAN-Kopplung (über **Suchen** ► **Computer**, nicht über die Netzwerkumgebung!) die Computer im anderen Netz suchen und darauf zugreifen.

IP-Pooling für Einwahlzugänge

ELSA LANCOM Business eignet sich mit einer größeren Anzahl von verfügbaren B-Kanälen ideal als Einwahlknoten (Remote-Access-Server) für kleinere und mittlere Unternehmen. Damit nicht für jeden Einwahlzugang eine eigene Route angelegt werden muß, verfügt der Router über einen Pool von IP-Adressen, aus dem der einwählenden Gegenstelle eine für das LAN gültige IP-Adresse für die Dauer der Verbindung zugewiesen wird.

Sie finden die Einstellungen für den IP-Adreß-Pool im *ELSA LANconfig* im Konfigurationsbereich 'TCP-IP' auf der Registerkarte 'Adressen' oder bei Telnet- oder Terminalsitzungen unter `/Setup/IP-Router-Modul`.

Bürokommunikation und *ELSA LANCAPI*

Die *LANCAPI* von ELSA ist eine spezielle Form der weit verbreiteten CAPI-Schnittstelle. CAPI steht für Common ISDN Application Programming Interface und stellt die Verbindung von ISDN-Adapttern zu Kommunikationsprogrammen her. Diese Programme wiederum stellen den Rechnern Funktionen der Bürokommunikation wie z.B. ein Fax oder einen Anrufbeantworter bereit.

Dieses Kapitel stellt Ihnen die *LANCAPI* sowie die mitgelieferten Anwendungsprogramme zur Bürokommunikation kurz vor und gibt Ihnen Hinweise, die bei der Installation der einzelnen Komponenten wichtig sind.

ELSA LANCAPI

Welche Vorteile bietet die LANCAPI?

Der Einsatz der LANCAPI bringt vor allem wirtschaftliche Vorteile. Alle Workstations, die im LAN (Local Area Network) integriert sind, erhalten über die LANCAPI uneingeschränkten Zugriff auf Bürokommunikations-Funktionen wie Fax, Anrufbeantworter, Online-Banking und EuroFileTransfer. Ohne zusätzliche Hardware an jeder einzelnen Arbeitsstation werden alle Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsstationen installiert.

Beim Versenden von Faxen wird z.B. am Arbeitsplatz ein ISDN-Faxgerät simuliert. Mit der LANCAPI leitet der PC das Fax über das Netzwerk an ein ELSA LANCOM Business weiter, welcher die Verbindung zum Empfänger über ISDN herstellt.

Das dynamische Konzept der LANCAPI ermöglicht dabei auch eine leichte Skalierbarkeit der Kommunikationswege. Wenn mehr B-Kanäle benötigt werden, um die Aufgaben zu bewältigen, wird einfach ein weiteres ELSA LANCOM Business im Netz installiert. Alle Geräte im lokalen Netz teilen sich dann die anfallende Arbeit.



Bitte beachten Sie: Alle Anwendungen, die Sie über die LANCAPI betreiben, verwenden direkte ISDN-Verbindungen und laufen nicht über den Router des Geräts ab. Daher werden damit die Firewall- und Gebührenüberwachungsfunktionen außer Kraft gesetzt!

Installation des LANCAPI-Clients

Die LANCAPI besteht aus zwei Komponenten, einem Server (im ELSA LANCOM Business) und einem Client (auf den PCs). Der LANCAPI-Client wird auf den Rechnern im lokalen Netz installiert, die die Funktionen der LANCAPI nutzen möchten.

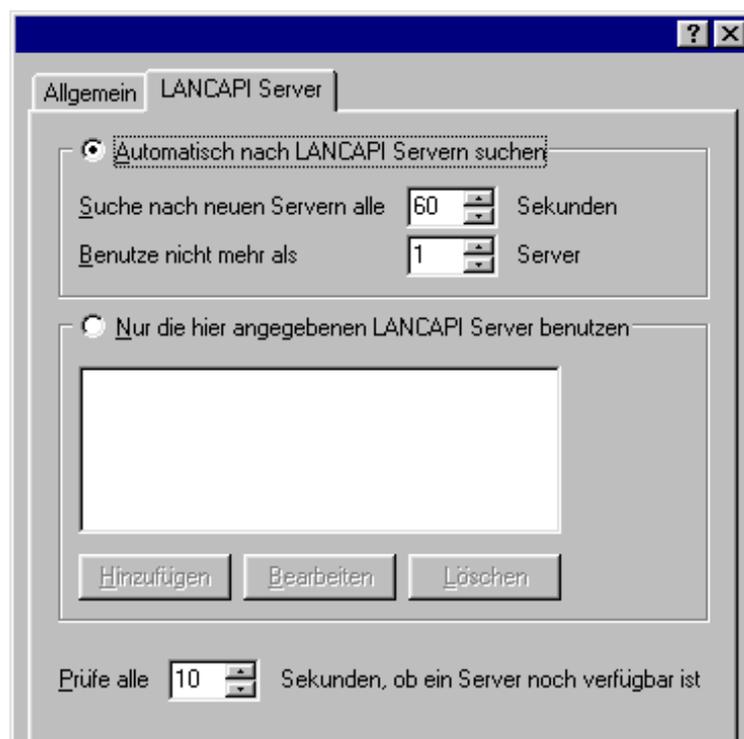
- ① Legen sie die ELSA LANCOM-CD in Ihr CD-ROM-Laufwerk ein. Wenn das Setup-Programm beim Einlegen der CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' auf der ELSA LANCOM-CD.
- ② Wählen Sie den Eintrag 'LANCOM Software installieren'.
- ③ Markieren Sie die Option 'ELSA LANCAPI'. Klicken Sie auf **Weiter**, und folgen Sie den Hinweisen der Installationsroutine.

Nach dem evtl. erforderlichen Neustart des Rechners ist die LANCAPI bereit, alle Aufgaben der Bürokommunikationssoftware entgegenzunehmen. Die ELSA LANCAPI ist nach erfolgreicher Installation als Icon in der Symbolleiste zu sehen. Ein Doppelklick auf dieses Symbol öffnet ein Statusfenster, in dem Sie jederzeit aktuelle Informationen zur ELSA LANCAPI abrufen können.

Einstellen des LANCAPIClient

Bei der Einstellung des Clients für die LANCAPIClient legen Sie fest, welche LANCAPIClient-Server verwendet werden sollen und wie diese überprüft werden. Wenn Sie nur ein ELSA LANCOM Business in Ihrem LAN als LANCAPIClient-Server betreiben, können Sie im Prinzip alle Parameter in den Voreinstellungen belassen.

- ① Starten Sie den LANCAPIClient aus der Programmgruppe 'ELSAIAn'. Auf der Registerkarte 'Allgemein' finden Sie Informationen zum Treiber zum bereitgestellten Dienst.
- ② Wechseln Sie auf das Register 'LANCAPIClient-Server'. Hier können Sie zunächst wählen, ob der PC seinen LANCAPIClient-Server selbst suchen soll oder ob ein bestimmter Server verwendet werden soll.
 - Im ersten Fall legen Sie fest, in welchem zeitlichen Intervall der Client nach einem Server sucht. Dabei sucht er solange, bis er die im nächsten Feld eingestellte Anzahl an Servern gefunden hat. Hat er die geforderte Zahl an Servern gefunden, hört er mit der Suche auf.
 - Wenn der Client nicht automatisch nach Servern suchen soll, geben Sie in der Liste die IP-Adressen der Server an, die der Client verwenden soll. Diese Festlegung ist z.B. dann sinnvoll, wenn Sie mehrere ELSA LANCOM Business in ihrem LAN als LANCAPIClient-Server betreiben und eine Gruppe von PCs einen bestimmten Server verwenden sollen.
 - Für beide Optionen können Sie dazu noch einstellen, in welchem Intervall der Client prüft, ob die gefundenen oder per Liste definierten Server noch aktiv sind.



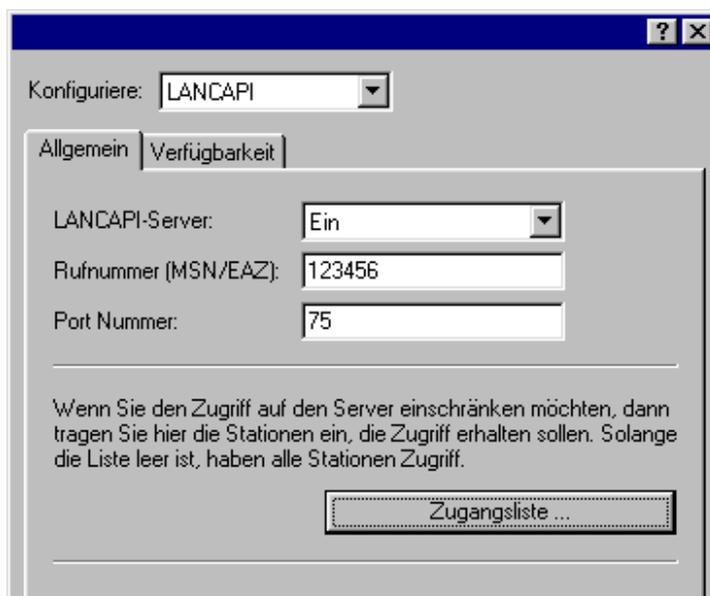
Einstellen des *LANCAPI*-Servers

Bei der Einstellung des *LANCAPI*-Servers werden im Prinzip zwei Fragen behandelt:

- Auf welche Rufnummer aus dem Telefonnetz soll die *LANCAPI* reagieren?
- Welche der Rechner im lokalen Netz sollen über die *LANCAPI* Zugang zum Telefonnetz erhalten?

So stellen Sie die entsprechenden Parameter ein:

- ① Starten Sie *ELSA LANconfig* aus der Programmgruppe 'ELSAAn'. Öffnen Sie die Konfiguration des Routers durch einen Doppelklick auf den Gerätenamen in der Liste, und wählen Sie den Konfigurations-Bereich 'LANCAPI'.

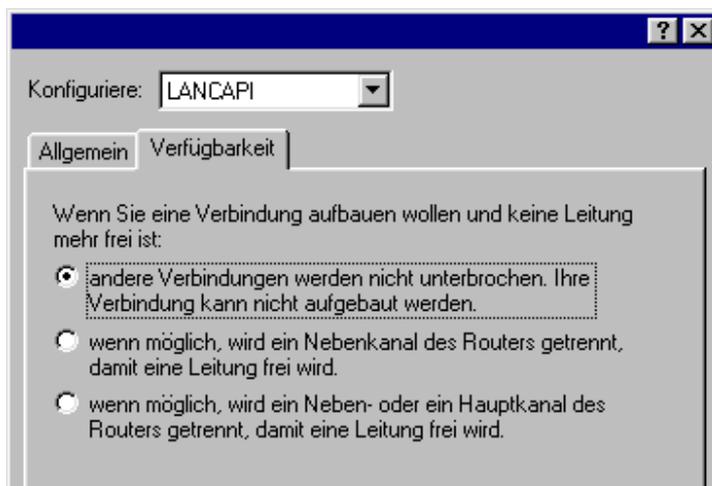


- ② Schalten Sie den *LANCAPI*-Server ein, oder lassen Sie nur abgehende Anrufe zu. In diesem Fall reagiert die *LANCAPI* nicht auf ankommende Rufe und kann z.B. nicht zum Empfangen von Faxmitteilungen eingesetzt werden. Lassen Sie z.B. dann nur abgehende Rufe zu, wenn Sie für die *ELSA LANCAPi* keine eigene Rufnummer frei haben.
- ③ Wenn der *LANCAPI*-Server eingeschaltet ist, geben Sie im Feld 'Rufnummern' die Telefonnummern ein, auf die *LANCAPI* reagieren soll. Mehrere Rufnummern können Sie durch Semikola getrennt eingeben. Wenn Sie hier keine Rufnummer eingeben, werden alle eingehenden Rufe an die *LANCAPI* gemeldet.
- ④ Der von der *LANCAPI* verwendete Port ist auf '75' (any private telephony service) voreingestellt. Verändern Sie diese Einstellung nur dann, wenn dieser Port in Ihrem lokalen Netz schon für andere Dienste verwendet wird.
- ⑤ Falls nicht alle Rechner aus dem lokalen Netz Zugriff auf die Funktionen der *LANCAPI* haben sollen, können Sie in der Zugangsliste die berechtigten Teilnehmer (über die IP-Adressen) genau festlegen.



Wenn Sie mehrere Rufnummern für die LANCAPi eingeben, können Sie den einzelnen Arbeitsplätzen z.B. ein persönliches Fax oder einen persönlichen Anrufbeantworter bereitstellen. Dazu geben Sie bei der Installation der Kommunikationsprogramme wie z.B. ELSA-RVS-COM an verschiedenen Arbeitsplätzen jeweils verschiedene Rufnummern an, auf die das Programm reagieren soll.

Wechseln Sie auf die Registerkarte 'Verfügbarkeit'. Hier legen Sie fest, wie sich ein ELSA LANCOM Business verhält, wenn über die LANCAPi eine Verbindung aufgebaut werden soll (ankommender oder abgehender Ruf), beide B-Kanäle jedoch besetzt sind (Prioritätensteuerung). Mögliche Optionen sind hier:



- Die Verbindung über die LANCAPi kann nicht aufgebaut werden. Ein Faxprogramm, das die LANCAPi nutzt, wird dann wahrscheinlich zu einem späteren Zeitpunkt den Versand erneut versuchen.
- Die Verbindung über die LANCAPi kann aufgebaut werden, wenn ein Hauptkanal frei ist. Ein Hauptkanal ist der erste B-Kanal, der bei einer Routerverbindung aufgebaut wird. Nebkanäle werden zur Kanalbündelung hinzugenommen.
- Die Verbindung über die LANCAPi kann auf jeden Fall aufgebaut werden, eine bestehende Routerverbindung wird ggfs. für die Dauer des Gespräches abgebaut. So ist z.B. die Faxfunktion immer erreichbar.

So verwenden Sie die LANCAPi

Zur Verwendung der LANCAPi gibt es zwei Möglichkeiten:

- Sie setzen eine Software ein, die direkt auf einer CAPI-Schnittstelle (in diesem Fall der LANCAPi) aufsetzt, wie z.B. ELSA-RVS-COM. Eine solche Software sucht bei der Installation nach der CAPI und verwendet diese anschließend automatisch.
- Andere Programme wie LapLink können Verbindungen über verschiedene Wege aufbauen, z.B. über das DFÜ-Netzwerk von Windows. Beim Anlegen einer neuen DFÜ-Verbindung können Sie auswählen, welches der installierten Kommunikationsgeräte Sie verwenden möchten. Wählen Sie für die LANCAPi den Eintrag 'ISDN WAN Line 1'.

ELSA CAPI Faxmodem

Mit dem *ELSA CAPI Faxmodem* steht Ihnen unter Windows ein Faxtreiber (Fax Class 1) zur Verfügung, der als Schnittstelle zwischen *ELSA LANCAPI* und Anwendung den Betrieb von Standard-Faxprogrammen mit einem *ELSA LANCOM Business* ermöglicht.

Installation

Das *ELSA CAPI Faxmodem* wird über das CD-Setup installiert. Installieren Sie das *ELSA CAPI Faxmodem* immer zusammen mit der aktuellen *ELSA LANCAPI*. Nach dem Neustart steht Ihnen im System das *ELSA CAPI Faxmodem* zur Verfügung, z.B. unter Windows 95 oder Windows 98 unter **Start** ► **Systemsteuerung** ► **Modems**.

Faxen über *ELSA CAPI Faxmodem*

Das *ELSA CAPI Faxmodem* wird von den gängigen Faxprogrammen bei der Installation automatisch erkannt und als 'Class 1'-Faxmodem identifiziert. Damit sind Faxübertragungen mit bis zu 14.400 bit/s möglich. Falls Ihr Faxprogramm eine Unterscheidung erlaubt (z.B. WinFax bzw. Talkworks Pro), wählen Sie bei der Einrichtung des Modems die Option 'CLASS 1 (Software Flow Control)' aus.



Das ELSA CAPI Faxmodem ist nur dann für die Übertragung von Faxnachrichten bereit, wenn die ELSA LANCAPI aktiv ist. Das erkennen Sie z.B. an dem kleinen CAPI-Symbol rechts unten in der Ecke des Bildschirms. Beachten Sie bitte auch die Einstellungen der LANCAPI selbst.

Der Least-Cost-Router

Seit der Liberalisierung des Telefonmarktes in Deutschland und in Europa stehen dem Benutzer von Telekommunikationsdiensten eine Reihe von Providern (Netzbetreiber) zur Auswahl, die sich durch z.T. sehr unterschiedliche Tarife unterscheiden. Die Provider unterscheiden sich außerdem danach, ob man fest mit diesem Anbieter verbunden ist und automatisch immer dessen Netz verwendet (Preselection) oder ob man sich bei jedem Anruf frei entscheidet, welchen Provider man nutzen möchte (Call-by-Call). Um eine Verbindung über einen Call-by-Call-Provider aufzubauen, wählt man nach dem Abheben zunächst die passende Vorwahl, um in das entsprechende Leitungsnetz zu kommen. Erst nach dieser Netzkennziffer wählt man die normale Telefonnummer, um seine Gegenstelle zu erreichen.

Für Telefonate zu bestimmten Tageszeiten und in verschiedenen Regionen ist der jeweils günstigste Tarif jedoch leider nicht bei immer demselben Provider, sondern oft bei verschiedenen Anbietern zu finden: morgens Provider 1, nachmittags Provider 2 und für Auslandsgespräche evtl. Provider 3. Um immer besonders günstig zu telefonieren, im Internet zu surfen oder Daten zu anderen Netzen zu übertragen, müßten Sie nun eigentlich vor

jeder Verbindung überlegen, welcher Tarif nun gerade der günstigste ist. Ein *ELSA LANCOM Business* nimmt Ihnen diese Arbeit ab. Least-Cost-Routing (LCR) heißt die Funktion, die hier hilft. Sie definieren dabei einmal, welche Provider für Ihre Bedürfnisse die günstigsten Tarife haben, und das Gerät wählt bei jeder Verbindung (egal ob über Router, *LANCAPI* etc.) automatisch den Anbieter mit dem günstigsten Tarif.

So arbeitet der Least-Cost-Router im *ELSA LANCOM*

Der LCR analysiert die Ziffern, die z.B. vom Router oder der *LANCAPI* gewählt werden.

Nach jeder Ziffer wird im Gerät überprüft, ob in der LCR-Tabelle eine eindeutige Übereinstimmung mit der bisher gewählten Nummer (Vorwahl) zu finden ist. Wird ein passender Eintrag gefunden, der zudem für die aktuelle Uhrzeit und das aktuelle Datum gültig ist, dann wird die Netzkennzahl für die Umleitung der Verbindung noch vor der Vorwahl eingefügt. Erst wenn die Rufnummer auf diese Weise vervollständigt wurde, wird sie nach außen an die Vermittlungsstelle weitergegeben.

Der LCR benötigt also folgende Eingaben:

- Ein Wählpräfix (Vorwahl), das bestimmt, welche Rufe für eine Umleitung in Frage kommen.
- Eine oder mehrere Netzkennzahlen, die den Provider bestimmen, der für dieses Wählpräfix genutzt werden soll.
- Die Wochentage und Feiertage, für die der Eintrag gültig ist.
- Die Tageszeit, zu der dieser Eintrag gültig ist.

Die ersten Versuche

Mit einigen wenigen Einträgen können Sie schon eine Menge an Gebühren sparen. An einem einfachen Beispiel wollen wir die Programmierung des LCRs erläutern.

Sie wissen z.B., daß man insbesondere bei Fern- oder Auslandsverbindungen mit dem Call-by-Call-Verfahren sparen kann. Sie haben sich außerdem bei einigen Call-by-Call-Anbietern (CbC) erkundigt und haben die jeweils günstigsten Tarife herausgesucht. Die ersten Einträge in der LCR-Tabelle sehen dann z.B. folgendermaßen aus:

Wählpräfix	Netzkennzahl des CbC	Wochentage	Tageszeit
089	01097	Sa + So	0:00h bis 23:59h
089	01098	Mo + Di + Mi + Do + Fr	8:00h bis 18:00h
00	01097	So	0:00h bis 23:59h

Diese Einträge bedeuten, daß alle Verbindungen am Wochenende nach München (oder andere Nummern, die mit '089' beginnen), über den Provider mit der Netzkennzahl '01097' geführt werden. Wochentags wird für diese Rufe in der Zeit zwischen 8:00 Uhr und 18:00 Uhr der Provider mit der Netzkennzahl '01098' verwendet. Auslandsgespräche am Sonntag gehen über den Provider mit der Netzkennzahl '01097'.

Für Fortgeschrittene: LCR mit System

- Im ersten Beispiel haben Sie gesehen, daß Sie bereits mit wenigen Einträgen Gebühren sparen können. Wenn Sie das Least-Cost-Routing optimal nutzen möchten, müssen Sie sich zunächst genau über die Tarifstruktur der Call-by-Call-Anbieter informieren, die für Sie in Frage kommen. Anschließend überlegen Sie, wie die Tarife und Tarifzonen am besten auf die LCR-Tabelle im *ELSA LANCOM Business* abgebildet werden können. Dazu gibt es verschiedene Ansätze:
- Eindeutige Sparmöglichkeiten können Sie direkt eintragen:
 - '00' für Auslandsverbindungen
- Mit einer einzigen '0' werden zunächst alle Verbindungen umgeleitet, die mit der Null beginnen. Da es aber i.d.R. angrenzende Ortsnetze gibt, deren Nummer ebenfalls mit '0' beginnt, die aber trotzdem als Ortsgespräch berechnet werden, sollten Sie diese Vorwahlen separat aufführen und die Umleitung wieder aufheben. Denken Sie bei dieser Strategie auch an Sonderrufnummern wie '0800', '0190' etc.
- Eine andere Strategie zielt auf die möglichst vollständige Regelung der Umleitungen ab. Dabei beginnen Sie mit den Vorwahlen des Ortsbereiches und definieren dann die größeren Zonen. Die nahen und damit günstigeren Tarifzonen werden dabei mit längeren Wahlpräfixen festgelegt, die verbleibenden, weiter entfernten Tarifzonen werden mit wenigen Ziffern erfaßt.

Diese Einstellung können Sie bei Bedarf natürlich weiter verfeinern und ausbauen. Hier einige Anregungen, was Sie dabei beachten können:

- Einige Ortsnetze erreichen Sie zwar über eine Vorwahl, trotzdem aber zum normalen Ortstarif. Falls Sie diese Bereiche mit einem allgemeinen Eintrag umgeleitet haben, können Sie die Vorwahlen mit Ortstarif über die Vorwahl Ihrer Telefongesellschaft umleiten (z.B. '01033' für das Netz der Deutschen Telekom). Ein leerer Eintrag für die Netzkennzahl bedeutet ebenfalls „keine Umleitung“.
- Vielleicht geht der größte Teil Ihrer ISDN-Verbindungen in die gleichen Ortsnetze. Wenn die meisten Ihrer Gegenstellen in München liegen, können Sie diese Gegenstellen über einen bestimmten Anbieter erreichen.
- Untersuchen Sie die verschiedenen Tarifzonen. Welche Vorwahlen in welche Zone gehören, können Sie z.B. unter www.billiger-telefonieren.de im Internet nachsehen.

Wenn Sie die Vorwahlen gefunden haben, die Sie umleiten möchten, können Sie an die Zuweisung der Call-by-Call-Provider gehen. Dazu brauchen Sie natürlich die aktuellen Tarife möglichst aller Telefongesellschaften. Auch hier hilft das Internet. Adressen wie z.B. 'www.billiger-telefonieren.de' oder 'www.focus.de' verraten Ihnen tagesaktuell die Preise für alle denkbaren Verbindungen. Mit diesen Informationen können Sie sich nun daran machen, Ihren Least-Cost-Router zu füttern ...

So stellen Sie den Least-Cost-Router ein

Zur Einstellung des Least-Cost-Routers sind im wesentlichen zwei Fragen zu klären:

- Welche Betriebsarten im *ELSA LANCOM Business* sollen die Dienste des Least-Cost-Routers nutzen?
- Welche Rufe sollen wann über welchen Provider geführt werden?

Um diese Fragen zu beantworten, gehen Sie so vor:

- ① Wechseln Sie im *ELSA LANconfig* im Konfigurationsbereich 'Least-Cost-Router' auf die Registerkarte 'Allgemein'.
- ② Aktivieren Sie die Funktion des Least-Cost-Routers. Der Least-Cost-Router läßt sich nur dann aktivieren, wenn die Zeit des Geräts entweder manuell gesetzt wurde oder wenn schon einmal eine gültige Zeit aus dem ISDN-Netz übermittelt wurde (siehe auch 'Die Uhrzeit für die Auswahl' weiter unten). Schalten Sie den LRC je nach Bedarf für die folgenden Betriebsarten ein:
 - Router
 - *LANCAPI*



Wenn Sie das Least-Cost-Routing auch für die Router-Module eingeschaltet haben, werden ggf. auch Verbindungen über Provider aufgebaut, die keine Gebühreninformationen übertragen! Die Gebührenüberwachung geht damit evtl. unbemerkt verloren. Verwenden Sie in diesem Fall alternativ die Zeitbudgets.

- ③ Wechseln Sie auf die Registerkarte 'Zeiten und Feiertage'. Öffnen Sie die **Least-Cost-Tabelle**, fügen Sie einen neuen Eintrag hinzu, und geben Sie die benötigten Daten ein:
 - Welche Vorwahl soll umgeleitet werden?
 - Über welche Provider soll diese Vorwahl umgeleitet werden? Wenn Sie hier mehrere Netzkennzahlen durch Semikola getrennt eintragen, wechselt der LCR automatisch zur nächsten Vorwahl, wenn eine vorherige besetzt ist.
 - An welchen Tagen und zu welchen Uhrzeiten soll die Umleitung aktiv sein? Beachten Sie bitte, daß keine tagesübergreifenden Uhrzeiten (18:00 Uhr bis 6:00 Uhr) möglich sind!
 - Soll der Anruf über die normale Telefongesellschaft geführt werden, wenn alle Call-by-Call-Leitungen besetzt sind? Wenn der 'automatische Rückfall' ausgeschaltet ist, beginnt der LCR ggf. nach der letzten Netzkennzahl wieder mit der ersten ...

- ④ Wenn Sie in der LCR-Tabelle auch Einträge für Feiertage gemacht haben, öffnen Sie anschließend die Liste der **Feiertage**. Tragen Sie jeden Feiertag mit dem vollständigen Datum ein (TT.MM.JJJJ).
- ⑤ Kontrollieren Sie die interne Uhr des Geräts (inkl. Datum), damit der LCR auch zur richtigen Zeit die Umleitungen aktiviert (siehe auch weiter unten, 'Die Uhrzeit für die Auswahl').



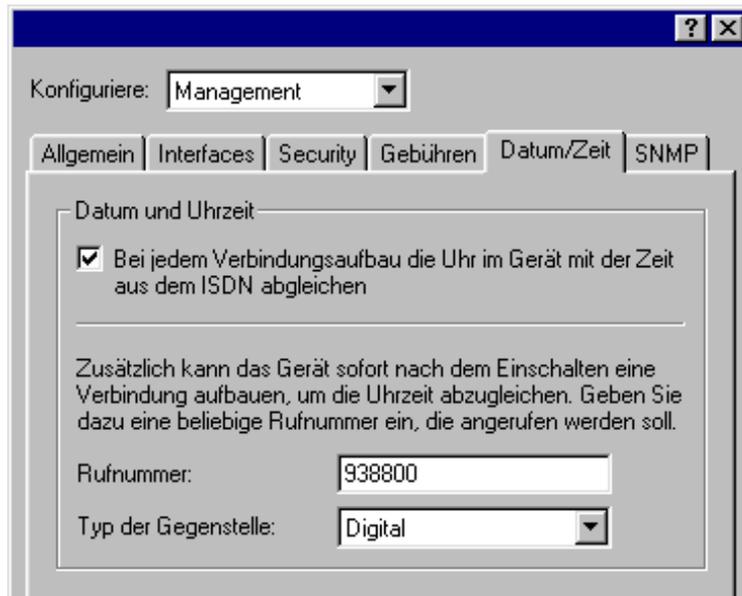
*Bauen Sie Ihre LCR-Tabelle schrittweise auf, und überprüfen Sie jeweils das Ergebnis. Öffnen Sie dazu z.B. den ELSA LANmonitor und starten Sie über die ELSA LANCAPI Verbindungen zu Gegenstellen, die der Tabelle nach umgeleitet werden sollten. Anhand der gewählten Rufnummer können Sie leicht ablesen, ob die Einstellung des LCRs Ihren Wünschen entspricht. Für Routerverbindungen können Sie die gewählte Nummer aus dem Logfile ablesen (LANmonitor: **Ansicht** ► **Optionen** ► **Protokoll** ► **Anzeigen**).*

Die Uhrzeit für die Auswahl

Damit der Least-Cost-Router mit Hilfe der Tabelleneinträge tatsächlich die richtige Verbindung auswählt, muß die interne Uhr im *ELSA LANCOM Business* natürlich immer auf dem aktuellen Stand sein. Aber auch hier hilft sich der Router selbst: Er kann entweder bei jedem Verbindungsaufbau oder bei jedem Einschalten des Geräts die interne Uhrzeit mit der aktuellen Zeit im ISDN-Netz abgleichen.

- ① Wechseln Sie im *ELSA LANconfig* im Konfigurationsbereich 'Management' auf die Registerkarte 'Datum/Zeit'.
- ② Aktivieren Sie ggf. die Option für den automatischen Zeitabgleich bei jedem Verbindungsaufbau. Falls Sie die Zeit lieber manuell eintragen möchten, schalten Sie diese Option aus.
- ③ Beim Ausschalten verliert das Gerät die aktuelle Zeit. Geben Sie die Rufnummer einer beliebigen Gegenstelle ein, wenn das Gerät direkt nach dem Einschalten eine Verbindung aufbauen und so die Zeit mit dem ISDN-Netz abgleichen soll. Wählen

Sie dabei aus, ob es sich um eine digitale Gegenstelle (z.B. Mailboxen oder Internet-Provider) handelt oder um eine analoge Gegenstelle (Telefonansage oder Sprachdienst).



Bitte prüfen Sie die Zeit nach der ersten Übermittlung. Manche TK-Anlagen übermitteln dem Router z.B. ungültige Zeiten, die die Funktion des Least-Cost-Routers beeinträchtigen!

Workshop

In den Beispielen der folgenden Abschnitte wollen wir Ihnen zeigen, wie Sie alles aus Ihrem Router herausholen.

Bei allen Konfigurationen gehen wir von einem Gerät im Auslieferungszustand aus. Wenn Sie also ein Beispiel komplett nachvollziehen wollen, setzen Sie Ihren Router ggf. mit einem System-Reset auf die Ausgangskonfiguration zurück.

Dieser Abschnitt macht Sie vertraut mit den verwendeten Zeichen und Symbolen.

Unser Entwicklungsteam ist ständig damit beschäftigt, neue Features in die Software einzubauen und die Bedienung mit *ELSA LANconfig* noch angenehmer zu gestalten. Daher weichen die Bildschirmfotos im Workshop möglicherweise leicht vom Aussehen Ihrer aktuellen Software ab, was jedoch nichts an der Funktionalität der Menüs ändert.

Die Grundeinstellungen, wie z.B. die Angabe der eigenen Rufnummern, tauchen in allen Beispielen wiederholt auf, um jeden einzelnen Abschnitt zu einer vollständigen Beschreibung zu machen. Daher werden hier auch Einstellungen beschrieben, die für die Grundfunktion vielleicht nicht benötigt werden.



Konfiguration mit *ELSA LANconfig* und den Assistenten

In den Abschnitten mit diesem Zeichen zeigen Ihnen, wie Sie die Konfigurationen unter Windows-Betriebssystemen ganz schnell und komfortabel mit *ELSA LANconfig* und seinen Assistenten vornehmen.



Konfiguration ohne Assistenten

In den Schritt-für-Schritt-Anleitungen finden Sie genaue Hinweise auf die Menüs, in denen die Einstellungen vorgenommen werden, entweder mit *ELSA LANconfig* oder über eine Terminal- oder Telnet-Verbindung.

	Setup/WAN-Modul	
	Interface	S0 DSS1 0 123456 123456

Die gezeigten Werte können Sie direkt in einer Konfigurationssitzung eingeben, z.B.:

```
cd setup/WAN-Modul/Interface
```

```
set S0 DSS1 123456 123456
```

Weitere Hinweise zur Konfiguration mit Telnet oder Terminal-Programmen finden Sie im Kapitel 'Konfigurationsmöglichkeiten'.

Folgende Symbole finden Sie in den Schritt-für-Schritt-Anleitungen wieder:

	Menü	Zeigt ein Untermenü an
	Wert	Zeigt einen Wert an, der verändert kann
	Tabelle	Zeigt eine Tabelle an, deren Einträge verändert werden können.

Welches Gerät verwenden Sie?

Die im Workshop beschriebenen Aufgaben können mit verschiedenen Modellen aus der *ELSA LANCOM*-Familie gelöst werden. Einschränkungen bzgl. bestimmter Modelle werden durch entsprechende Symbole neben dem Text angezeigt.

Alle Beschreibungen gelten für Router mit einem S_0 -Bus (Interface), also mit 2 B-Kanälen. Für Geräte mit mehreren S_0 -Bussen (z.B. *ELSA LANCOM Business 4100*) müssen die Einstellungen ggf. auf die anderen Interfaces und Kanäle übertragen werden.

Zusätze



Dieses Symbol zeigt Ihnen die optionalen Einstellungen an, die zur reinen Funktion der Beispielkonfiguration nicht unbedingt erforderlich sind. Dazu gehören z.B. Filtereinstellungen, die spezielle Datenpakete von der Übertragung ausschließen oder Schutzmechanismen, die den Zugang zum Gerät einschränken.

Internet-Anwendungen

Im ersten Abschnitt über die praktischen Einsätze der Geräte stellen wir Ihnen Anwendungen im Zusammenhang mit dem Internet vor.

Das erste Beispiel zeigt das lokale Netzwerk in einer Firma, das über einen Router an das Internet angeschlossen werden soll. Dabei erhalten alle Arbeitsplatzrechner im LAN über einen Account bei einem Provider Zugang zu den Diensten und Möglichkeiten des Internets. Gleichzeitig soll der Router in dieser Anwendung aber auch als Firewall das lokale Netz vor Zugriffen von außen schützen und die Arbeitsplatzrechner aus dem Internet heraus unerreichbar machen.

Im zweiten Beispiel möchte die Firma nicht nur als passiver Teilnehmer die Angebote im Internet nutzen, sondern auch aktiv ein eigenes Informationsangebot bereitstellen. Dazu wird im lokalen Netz der Firma ein Web-Server installiert, der über eine Festverbindung an den Provider angeschlossen wird. Dieser Server muß dabei natürlich aus dem Internet erreichbar sein, alle anderen Rechner im Netz sollen hinter der Firewall geschützt bleiben.

Internet für alle PCs im LAN

Die Motivation

Viele Firmen wünschen sich einen Anschluß ans Internet für alle Rechner im lokalen Netzwerk. Zwei Gründe sprachen in einigen Fällen allerdings bisher dagegen:

- Eigene Accounts für jeden einzelnen Rechner bei einem Internet-Service-Provider (ISP) oder sogar der Kauf von registrierten, im Internet gültigen IP-Adressen sind in den meisten Fällen viel zu teuer. Dazu kommt noch der Aufwand für die Einrichtung und Wartung der einzelnen Internet-Zugänge.
- Eine weitere Sorge beim Anschluß der einzelnen Rechner ans WWW ist die Unsicherheit, ob damit nicht dem Zugriff auf das Firmen-Netz von außen Tür und Tor geöffnet wird.

Der Router löst beide Probleme mit einer einzigen Funktion: IP-Masquerading. Kurz gesagt passiert dabei folgendes:

Der Router ist das einzige Gerät im LAN, das eine im Internet gültige IP-Adresse hat. Diese kann z.B. dynamisch über PPP bei der Anwahl vom Internet-Provider zugewiesen werden (wie bei T-Online, AOL, CompuServe etc.). Die Rechner im Netz verwenden Adressen aus einem geschützten Bereich (z.B. „10er“-Adressen). Durch das IP-Masquerading wird nun das komplette lokale Netz hinter der einen registrierten IP-Adresse des Routers „versteckt“.

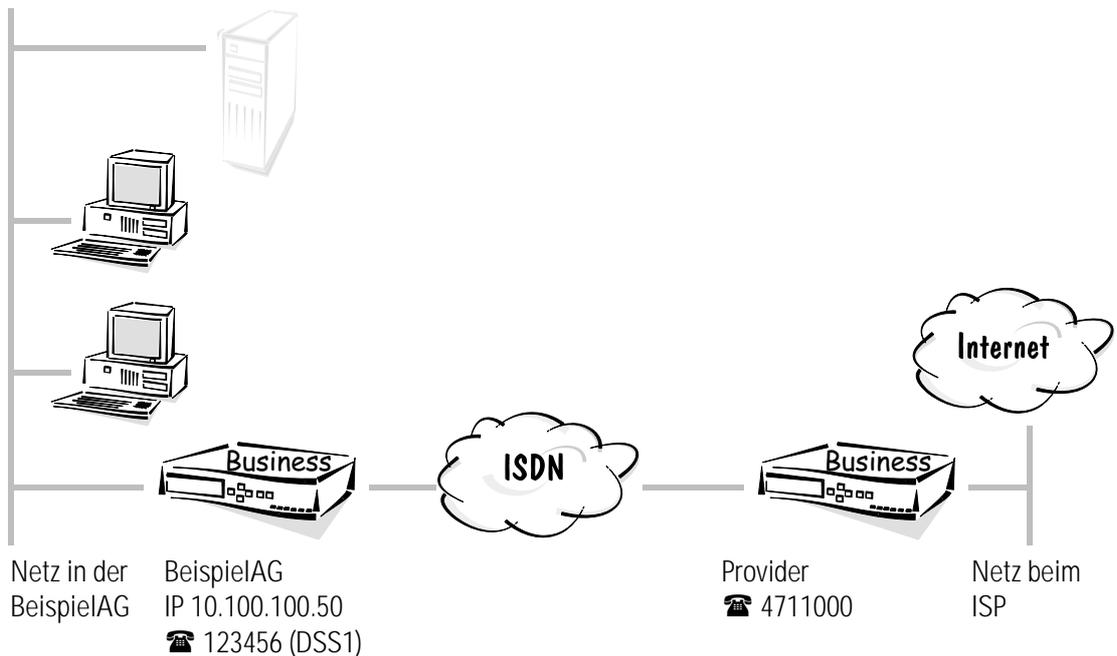
Dieses Verfahren hat gleich mehrere Vorteile:

- IP-Masquerading macht den Internet-Zugang einfach.
Nur ein Gerät muß konfiguriert werden. Und dabei helfen Ihnen noch die Setup-Assistenten von *ELSA LANconfig*.
- IP-Masquerading macht den Internet-Zugang kostengünstig.
Alle Rechner im lokalen Netz können nach außen hin die IP-Adresse des Routers nutzen und so am Internet teilnehmen. Dabei wird für viele Benutzer nur ein Account beim Provider benötigt. Außerdem verwaltet der Router selbständig die ISDN-Leitung und stellt nur dann eine Verbindung zum Provider her, wenn tatsächlich Daten übertragen werden müssen.
- IP-Masquerading macht den Internet-Zugang sicher.
Die Rechner im lokalen Netz werden nach außen hin nicht sichtbar. Im Internet wird nur die IP-Adresse des Routers bekannt. Ein Zugriff von außen auf das lokale Netz ist also nicht möglich, das IP-Masquerading wirkt als effektiver Firewall und trennt so Internet und Intranet. Außerdem ist der Router die einzige Schnittstelle zum Internet, die leichter zu kontrollieren ist als viele einzelne Geräte an den Arbeitsplätzen.

Die Aufgabe im Beispiel

Wir haben auf der einen Seite ein lokales Netzwerk in einer Firma mit einigen Arbeitsplatzrechnern und einen Router an einem Euro-ISDN-Anschluß. Ein Server kann in diesem Netz vorhanden sein, muß aber nicht.

Auf der anderen Seite haben wir ein Netz beim Internet-Service-Provider mit einem ISDN-Router als Einwahlknoten für die Benutzer. Dieser Einwahlknoten möchte mit PPP angesprochen werden und verlangt dabei eine Sicherung nach 'CHAP'. Die Zugangsdaten liegen mit dem Benutzernamen 'WEB_USER' und dem Paßwort 'Surfen' vor.



Die folgende Tabelle zeigt die Zuordnung von allen wichtigen Daten, wie sie im Beispiel verwendet werden. Wir empfehlen das Anlegen einer solchen Tabelle für jede Anwendung. Sie unterstützt Ihre Arbeit bei der Konfiguration, bei der Fehlersuche und bei Support-Anfragen.

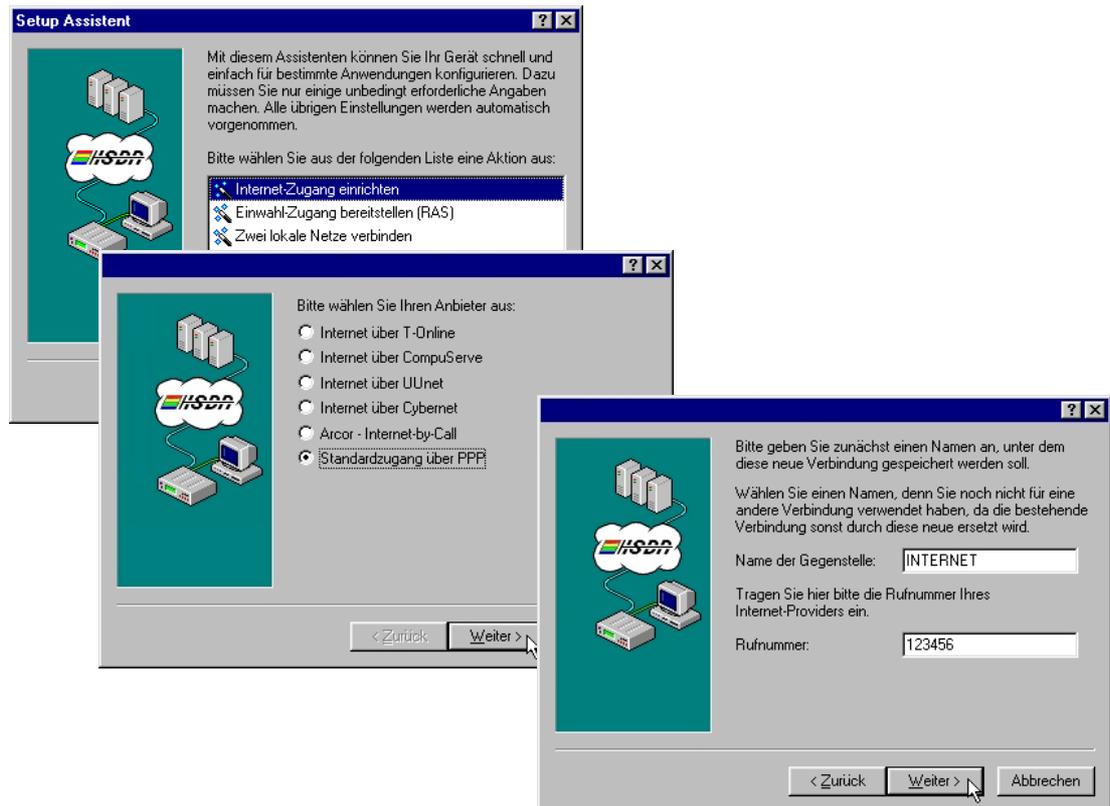
	lokales Netz in der Beispiel AG	lokales Netz beim Provider
IP-Adresse des LAN	10.100.100.0	
IP-Adresse für den Router	10.100.100.50	
IP-Netzmaske	255.255.255.0	
Gerätename	BeispielAG	Provider
Rufnummer	123456	4711000



Internet ganz einfach mit *ELSA LANconfig* und den Assistenten

Für die *ELSA LANCOM*-Konfiguration zum Zugriff auf das Internet stehen im *ELSA LANconfig* verschiedene Assistenten bereit, die alle notwendigen Einstellungen in der *ELSA LANCOM*-Software für Sie vornehmen. Wählen Sie nach dem Start des Assistenten

(automatisch oder mit **Extras ▶ Setup Assistent**) den gewünschten Assistenten aus. In diesem Beispiel haben wir uns nicht für einen der großen Online-Dienste, sondern für einen anderen ISP entschieden, der Einwahlknoten über PPP anbietet. Also wählen Sie den Eintrag 'Internet über PPP'. Der Assistent fragt dann die wenigen benötigten Daten ab und gibt Ihnen anschließend einen Hinweis, was Sie bei den Arbeitsplatzrechnern noch einstellen müssen.



Schritt für Schritt: Welche Einstellungen nehmen Sie im Router vor?

- ① Zuerst tragen Sie die Rufnummer für ankommende und abgehende Rufe in der Router-Interface-Tabelle ein (Konfigurationsbereich 'Kommunikation', Register 'Allgemein'):

```
cd /Setup/WAN-Modul/Router-Interface-Liste
S0-1 123456 EIN oder AUS
```

Beim Eintrag mehrerer Rufnummern wird die erste Nummer für abgehende Rufe verwendet.



Die Einstellung der Option 'Y-Verbindung' richtet sich danach, ob über den zweiten B-Kanal gleichzeitig eine Verbindung zu einer anderen Gegenstelle aufgebaut werden soll.

- ② Ein neuer Eintrag in der Namenliste (Konfigurationsbereich 'Kommunikation', Register 'Gegenstellen') mit Bezeichnung der Gegenstelle und der zugehörigen Rufnummer sowie Auswahl des voreingestellten Layers 'PPPHDL' (ohne Rückruf) erlaubt es dem Router in der Firma, den Router beim ISP anzurufen:

```
cd Setup/WAN-Modul/Namenliste
set Provider 4711000 * * PPPHDLc AUS
```

- ③ In der PPP-Liste werden Benutzername und Paßwort hinterlegt, die bei der Anwahl der Gegenstelle übermittelt werden. Weil nur der ISP von Ihnen Name und Paßwort verlangt, Sie aber nicht von ihm, hat die PPP-Verhandlung von dieser Seite aus 'keine' Sicherung.

```
cd Setup/WAN-Modul/PPP-Liste
set Provider keine Surfen * * WEB_USER IP
```

Das Paßwort 'Surfen' wird bei der Eingabe durch einige * ersetzt! Die anderen * in diesem Eintrag zeigen die Werte an, die unverändert übernommen werden sollen.



Beachten Sie bitte, daß bei Benutzernamen und Paßwort Groß- und Kleinschreibung unterschieden werden.

- ④ Jetzt müssen nur noch die Adressen geklärt werden. Damit der Router im eigenen TCP/IP-Netz gefunden wird, braucht er eine freie IP-Adresse aus dem Intranet. Die bekommt es mit dem Eintrag der Intranet-Adresse mit der zugehörigen Netzmaske (Konfigurationsbereich 'TCP/IP', Register 'Allgemein').

```
cd Setup/TCP-IP-Modul
set Intranet-Adresse 10.100.100.50
set Intranet-Netzmaske 255.255.255.0
set Zustand Ein
```



Die Einträge für die IP-Adresse und die IP-Netzmaske bleiben frei, weil der Router in diesem Beispiel die IP-Adresse dynamisch vom ISP bezieht. Sind hingegen registrierte, im Internet gültige IP-Adressen vorhanden, würde hier eine davon mit der zugehörigen Netzmaske eingetragen (siehe auch 'Intranet mit eigenem Web-Server im Internet').

- ⑤ Mit den bisherigen Einstellungen ist der Router praktisch Bestandteil des Internets geworden, die Rechner im LAN können aber noch nicht surfen. Um das zu erreichen, legen Sie einen Eintrag in der Routing-Tabelle an (Konfigurationsbereich 'TCP/IP', Register 'Router'), durch den alle Pakete für lokal nicht erreichbare Adressen ins Internet geroutet werden (DEFAULT-Route).

```
cd Setup/IP-Router-Modul
set IP-Routing-Tabelle 255.255.255.255 0.0.0.0 Provider 2 EIN
```

Die Route auf die IP-Adresse '255.255.255.255' mit Netzmaske '0.0.0.0' fängt alle Pakete ein, die nicht lokal zugeordnet werden können. 'Provider' ist die Bezeichnung der Gegenstelle, zu der die entsprechenden Daten geschickt werden sollen. Die Gegenstelle kann von Ihrem Router aus direkt erreicht werden, deshalb steht die Distanz auf '2'. Mit der Option 'EIN' für das IP-Masquerading werden alle Rechner

im LAN hinter der Adresse des Routers versteckt und treten nicht im Internet in Erscheinung.

- ⑥ Jetzt schalten Sie nur den IP-Router ein, und dann ist der Router vorbereitet für das WWW.

```
cd Setup/IP-Router-Modul  
set Zustand Ein
```

- ⑦ Was bleibt noch zu tun? Die Rechner im LAN müssen natürlich auch wissen, daß der *ELSA LANCOM* die Vermittlungsstelle für das Internet ist. Dazu wird die Intranet-Adresse des Routers als Default-Gateway und DNS-Server bei den Arbeitsplatzrechnern eingetragen.



Bei Verwendung des Routers als DHCP-Server können Sie diese Einstellungen automatisch zuweisen lassen (siehe 'DHCP-Server').

Das Ergebnis

Wenn einer der Mitarbeiter auf seinem Arbeitsplatzrechner nun einen Browser startet und eine Web-Adresse eingibt (z.B. ELSA), dann wird über den im Betriebssystem eingetragenen DNS-Server (hier also über den Router) versucht, die zugehörige IP-Adresse zu ermitteln. Der Router gibt als Internet-Gateway diese Anfrage an den DNS-Server des ISPs weiter, der letztendlich die IP-Adresse zu diesem Namen ermittelt (z.B. 168.192.156.100) und über den Router an den Arbeitsplatzrechner zurückgibt. Weil diese Adresse im lokalen Netz nicht gefunden wird, schickt der Router anschließend alle Pakete für diese IP-Adresse über die Default-Route ins Internet.

Intranet mit eigenem Web-Server im Internet

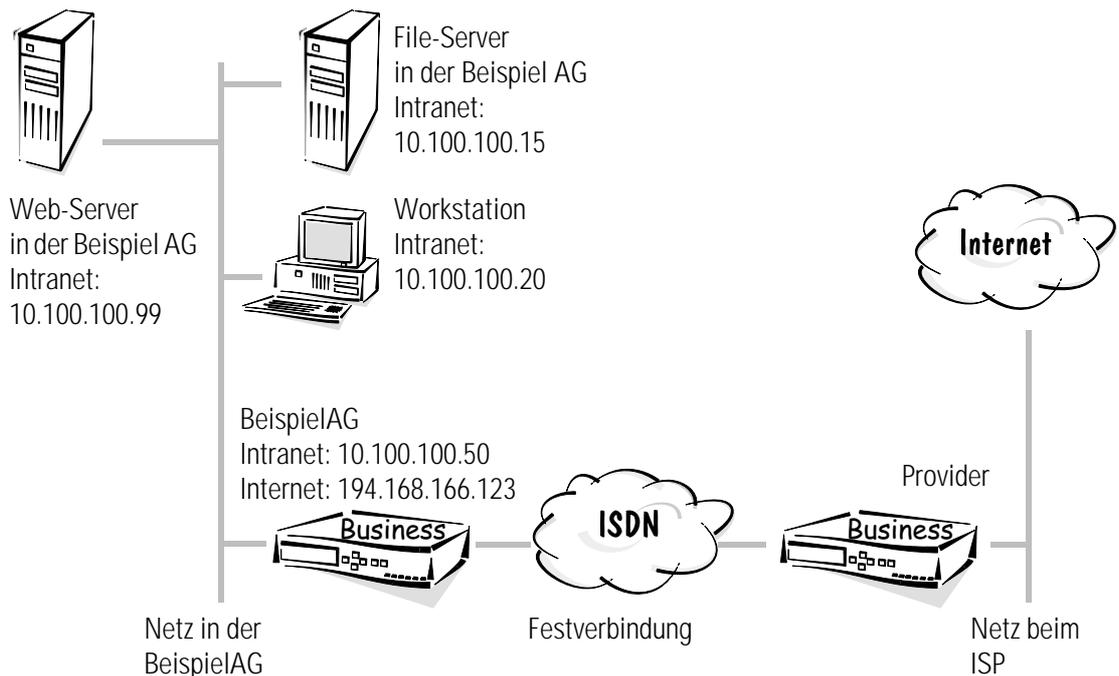
Die Motivation

Im Beispiel 'Internet für alle PCs im LAN' haben Sie gesehen, wie man ein komplettes TCP/IP-Netz über einen Router an das Internet anschließt (mit IP-Masquerading).

Im folgenden Beispiel bekommt das LAN in der Beispiel AG zusätzlich einen eigenen Web-Server, der aus dem Internet erreichbar sein soll. Dazu benötigen Sie neben dem Account beim ISP eine feste IP-Adresse. Diese registrierte IP-Adresse wird dem Router zugewiesen. Der Router nimmt dann eine Umsetzung von der registrierten Adresse zur Intranet-Adresse des Web-Servers vor. Der Web-Server wird somit im Internet unter der registrierten Adresse sichtbar (inverses IP-Masquerading). Alle anderen Rechner im lokalen Netz bleiben wie bisher versteckt.

Die Aufgabe im Beispiel

Wir haben auf der einen Seite ein Netzwerk bei der Beispiel AG mit einigen Arbeitsplatzrechnern und einem Router an einem Euro-ISDN-Anschluß. In diesem Netz ist neben den lokalen Servern auch ein Web-Server vorhanden.



Auf der anderen Seite haben wir das Netz beim Internet-Service-Provider. Zum Anschluß an dieses Netz gibt es prinzipiell zwei verschiedene gängige Möglichkeiten:

- Wenn der Web-Server sehr oft frequentiert wird, möchten Sie vielleicht eine Standleitung (Festverbindung) zum Provider haben (z.B. D64S mit einem B-Kanal ohne D-Kanal). In diesem Fall stellen Sie ein zweiten Router bei Ihrem ISP auf und konfigurieren beide Geräte für die verwendete Festverbindung.
- Wenn eine Festverbindung nicht nötig ist, reicht auch ein Router in Ihrem lokalen Netz aus. Damit dem ISP keine Gebühren für die Verbindung zu Ihrem Web-Server entstehen, richten Sie Ihren Router auf Rückruf für den Provider ein.

Bei der zweiten Möglichkeit werden bei jedem Zugriff auf Ihre Web-Site Verbindungen zum ISP aufgebaut, die Kosten auf Ihrer Telefonrechnung verursachen. Da diese Gebühren nicht zu kontrollieren sind (außer durch die Verwendung von Gebührenbudgets, die hier keinen Sinn machen), bevorzugen wir in diesem Beispiel die erste Variante.

Die folgende Tabelle zeigt die Zuordnung von allen wichtigen Daten, wie sie im Beispiel verwendet werden. Wir empfehlen das Anlegen einer solchen Tabelle für jede Anwen-

derung. Sie unterstützt Ihre Arbeit bei der Konfiguration, bei der Fehlersuche und bei Support-Anfragen.

	lokales Netz in der Beispiel AG	lokales Netz beim Provider
IP-Adresse für den Router	194.168.166.123	
IP-Netzmaske für den Router	255.255.255.255	
Intranet-Adresse des LAN	10.100.100.0	
Intranet-Adresse für den Router	10.100.100.50	
Intranet-Adresse für den Web-Server	10.100.100.99	
Intranet-Netzmaske	255.255.255.0	
Gerätename	BeispielAG	Provider



Festverbindung: Welche Einstellungen nehmen Sie im Router vor?

Die Einstellung in den beiden Geräten ist wieder sehr ähnlich. Wir gehen von der Einstellung des Routers in der Beispiel AG aus und zeigen ggf. die Unterschiede für den Router beim Provider auf.

- ① Zuerst stellen Sie den Router in der Interface-Tabelle auf die Verwendung einer Festverbindung nach D64S ein (Konfigurationsbereich 'Management', Register 'Interfaces'):

```
cd Setup/WAN-Modul/Interface-Liste
set S0-1 GRP0 1
```

Der verwendete B-Kanal muß bei beiden Routern gleich sein!

- ② Schon mit diesen Einstellungen können die beiden Router selbständig eine Verbindung aufbauen, sobald Sie an die Festverbindung angeschlossen und eingeschaltet sind. Dabei verwenden Sie automatisch den Layer 'DEFAULT'.

Damit die Festverbindung einen anderen Layer verwendet, legen Sie in der Layer-Liste einen neuen Layer an und stellen ihn in der Layer-Liste (Konfigurationsbereich 'Kommunikation', Register 'Allgemein') bei beiden Geräten gleich Ihren Wünschen entsprechend ein, z.B. mit dem Protokoll 'PPP' und Komprimierung:

```
cd Setup/WAN-Modul/Layerliste
set FVG0 TRANS PPP TRANS compr. HDLC64K
```

- ③ Ein neuer Eintrag in der Namenliste (Konfigurationsbereich 'Kommunikation', Register 'Gegenstellen') mit Bezeichnung der Gegenstelle und des zu verwendenden Layers erlaubt es dem einen Router, die Festverbindung mit den richtigen Einstellungen aufzubauen. Der Eintrag einer Rufnummer ist nicht erforderlich:

```
cd Setup/WAN-Modul/Namenliste
```

```
set Festverbindung * 0 0 FVG0 Aus
```

Dabei werden die Haltezeiten auf '0' gesetzt, da es sonst wegen unnötiger Verbindungsaufbauversuche zu Verzögerungen kommen kann.

- ④ In der Kanalliste legen Sie fest, welche Kanäle für die Festverbindung verwendet werden sollen. Die Angabe der Kanäle und der Reihenfolge muß auf beiden Seiten der Verbindung gleich eingestellt werden. Außerdem tragen Sie hier (auch auf beiden Seiten der Verbindung gleich) ein, wie viele Kanäle evtl. für Backup eingesetzt werden sollen (Konfigurationsbereich 'Kommunikation', Register 'Gegenstellen'):

```
cd Setup/WAN-Modul/Kanalliste
```

```
set Festverbindung 1 1 1-1 0
```

- ⑤ Damit die Namen aus der Namenliste der Router übermittelt und erkannt werden, benennen Sie das Gerät passend (Konfigurationsbereich 'Kommunikation', Register 'Allgemein'):

```
cd Setup
```

```
set Name BeispielAG
```

- ⑥ Jetzt müssen nur noch die IP-Adressen geklärt werden. Damit der Router bei der Beispiel AG im eigenen TCP/IP-Netz gefunden wird, braucht er eine freie IP-Adresse aus dem Intranet. Die bekommt er mit dem Eintrag der Intranet-Adresse mit der zugehörigen Netzmaske (Konfigurationsbereich 'TCP/IP', Register 'Allgemein'). Außerdem bekommt er wie vereinbart die registrierte IP-Adresse inkl. Netzmaske. Damit diese Einträge auch wirksam werden, schalten Sie das TCP/IP-Modul ein.

```
cd /Setup/TCP-IP-Modul
```

```
set IP-Adresse 194.168.166.123
```

```
set IP-Netzmaske 255.255.255.255
```

```
set Intranet-Adresse 10.100.100.50
```

```
set Intranet-Netzmaske 255.255.255.0
```

```
set Zustand Ein
```

Der andere Router bekommt analog eine feste IP-Adresse und (bei Verwendung von IP-Masquerading) eine Intranet-Adresse aus dem Adreß-Bereich beim ISP.

- ⑦ Mit dem Eintrag der IP-Adresse ist der Router der Beispiel AG praktisch Bestandteil des Internet geworden, die Rechner im LAN können aber noch nicht surfen. Um das Internet für die eigenen Mitarbeiter zu öffnen, legen Sie einen Eintrag in der Routing-Tabelle an (Konfigurationsbereich 'TCP/IP', Register 'Router'), durch den alle Pakete für lokal nicht erreichbare Adressen ins Internet geroutet werden (DEFAULT-Route).

```
cd Setup/IP-Router-Modul
```

```
set IP-Routing-Tabelle 255.255.255.255 0.0.0.0 Fest-
verbindung 2 Ein
```

Die Route auf die IP-Adresse '255.255.255.255' mit Netzmaske '0.0.0.0' fängt alle Pakete ein, die nicht lokal zugeordnet werden können. 'Provider' ist die Bezeichnung der Gegenstelle, zu der die entsprechenden Daten geschickt werden sollen. Die Gegenstelle kann vom Router in der Beispiel AG aus direkt erreicht werden, deshalb steht die Distanz auf '2'. Mit der Option 'EIN' für das IP-Masquerading werden alle Rechner im LAN hinter der Adresse des Routers versteckt und treten nicht im Internet in Erscheinung.

- ⑧ Der Router beim ISP muß ebenfalls einen Eintrag in der Routing-Tabelle erhalten. Diese Route enthält die registrierte IP-Adresse des Routers in der Beispiel AG und den Namen der Gegenstelle. Für diese Route bleibt das 'IP-Masquerading' ausgeschaltet, weil in diese Richtung geroutet und nicht maskiert werden soll.

```
cd /Setup/IP-Router-Modul
set IP-Routing-Tabelle 194.168.166.123 255.255.255.255
BeispielAG 2 Aus
```

Da diese IP-Adresse im eigenen Adreß-Bereich des Providers liegt, muß die Funktion 'Proxy-ARP' eingeschaltet werden:

```
cd /Setup/IP-Router-Modul
set Proxy-ARP Ein
```

- ⑨ Der Web-Server wird im Internet sichtbar durch einen Eintrag in der Service-Tabelle im Gerät der Beispiel AG (Konfigurationsbereich 'TCP/IP', Register 'Masquerading'):

```
cd /Setup/IP-Router-Modul/Masquerading/Service-Tabelle
set 80 10.100.100.99
```

Die Angabe des Wertes '80' zeigt an, daß es sich bei dem nach außen sichtbaren Dienst um HTTP (WWW) handelt, die Adresse '10.100.100.99' wählt den Rechner mit dieser speziellen Intranet-Adresse als Web-Server aus.



Eine Liste mit weitere Diensten finden Sie im Kapitel 'TCP/IP-Ports'.

- ⑩ Jetzt schalten Sie nur den IP-Router ein (Konfigurationsbereich 'TCP/IP', Register 'Router'), und dann ist der Router vorbereitet für das WWW.

```
cd /Setup/IP-Router-Modul
set Zustand Ein
```

- ⑪ Was bleibt noch zu tun? Die Rechner im LAN müssen natürlich auch wissen, daß der Router die Vermittlungsstelle für das Internet ist. Dazu wird die Intranet-Adresse des Routers als Default-Gateway bei den Arbeitsplatzrechnern eingetragen. Zusätzlich wird als DNS-Server die IP-Adresse des entsprechenden Servers beim ISP bekanntgegeben.



Bei Verwendung des Routers als DHCP-Server können Sie diese Einstellungen automatisch zuweisen lassen (siehe 'DHCP-Server').

Der Internet-Service-Provider muß anschließend noch dafür sorgen, daß Ihr Web-Server mit der registrierten IP-Adresse und dem Namen der Domäne in seinem DNS-Server eingetragen wird, z.B. 'www.beispielag.de'.

Das Ergebnis

Ziel der Einstellungen war die Möglichkeit des Datenaustausches mit dem Internet in zwei Richtungen: Anfragen aus dem lokalen Netz ins Internet und umgekehrt Anfragen aus dem Internet an den Web-Server im lokalen Netz. Das haben Sie jetzt erreicht:

■ Internet für die Mitarbeiter:

Wenn einer der Mitarbeiter auf seinem Arbeitsplatzrechner nun einen Browser startet und eine Web-Adresse eingibt (z.B. ELSA), dann wird über den im Betriebssystem eingetragenen DNS-Server versucht, die zugehörige IP-Adresse zu ermitteln. Der Router gibt als Internet-Gateway diese Anfrage an den DNS-Server des ISPs weiter, der letztendlich die IP-Adresse zu diesem Namen ermittelt (z.B. 168.192.156.100) und über den Router an den Arbeitsplatzrechner zurückgibt. Weil diese Adresse im lokalen Netz nicht gefunden wird, schickt er anschließend alle Pakete für diese IP-Adresse über die Default-Route ins Internet.

■ Web-Site der Firma im Internet

Wenn ein Internet-Teilnehmer irgendwo auf der Welt nun seinen Browser startet und Ihre Web-Adresse eingibt (z.B. www.beispielag.de), dann bekommt sein Rechner über den DNS-Server die IP-Adresse des Routers in der Firma zurück (194.168.166.123). Anschließend kann der Rechner des Web-Users mit dieser IP-Adresse direkt mit dem Router kommunizieren. Der Router setzt die Anfragen für den Port 80 (WWW) dann automatisch um auf die Intranet-Adresse des Web-Servers und ermöglicht so den Zugriff auf die Web-Site Ihrer Firma.

Natürlich können auch andere Dienste wie FTP und Gopher im Internet angeboten werden, wenn die Service-Tabelle entsprechend erweitert wird. Ob dabei ein Server oder mehrere für die verschiedenen Dienste eingesetzt werden, kann mit Hilfe der Service-Tabelle beliebig gestaltet werden.

LAN-LAN-Kopplungen

Wenn die Geschäfte der Beispiel AG richtig gut laufen, wird es langsam Zeit für eine Tochtergesellschaft oder eine Niederlassung in den globalen Märkten. Auch die Filiale hat natürlich ihr eigenes lokales Netz und möchte immer auf dem laufenden sein.

Die LAN-LAN-Kopplung verbindet die einzelnen LANs zu einem großen Netzwerk, wenn es sein muß über Kontinente hinweg. Bei Verbindung über Wählleitungen sorgt eine

intelligentes Line-Management im Zusammenspiel mit ausgefeilten Filtermechanismen für geringe Verbindungskosten. Natürlich ist auch der Betrieb über Festverbindungen sogar in Kombination mit Wählleitungen möglich.

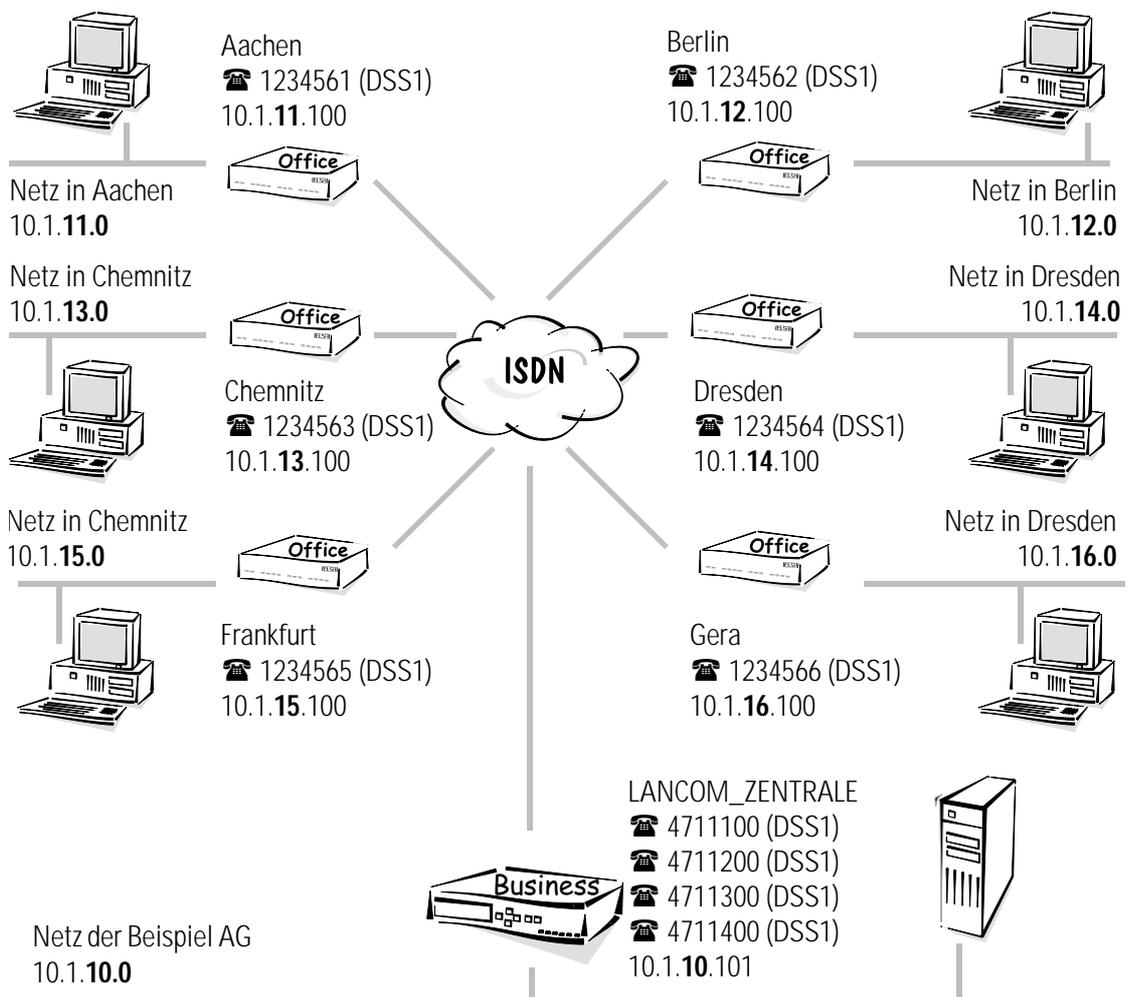
Netze verbinden mit dem IP-Router

Die Motivation

Mit dem IP-Router können Sie Netzwerke verbinden, die auf TCP/IP als Netzwerkprotokoll setzen. Im Gegensatz zum Internet-Access über IP-Masquerading ('Internet für alle PCs im LAN') werden bei der Kopplung von Netzen über den IP-Router **alle** IP-Adressen aus den beteiligten Netzen in den anderen angeschlossenen Netzen sichtbar, nicht nur die der Router.

Die Aufgabe im Beispiel

In dieser Aufgabe hat die Zentrale sechs Filialen. In jeder der Filialen steht ein „kleiner“ Router, die über das ISDN-Wählverbindungen an ein *ELSA LANCOM Business* in der Zentrale angeschlossen werden. .



Die folgende Tabelle zeigt die Zuordnung von Gerätenamen, Adressen und Telefonnummern, wie sie im Beispiel verwendet werden:

Netz	Beispiel AG	Aachen	Berlin	Chemnitz	Dresden	Frankfurt	Gera
IP-Adresse LAN	10.1.10.0	10.1.11.0	10.1.12.0	10.1.13.0	10.1.14.0	10.1.15.0	10.1.16.0
IP-Adressen für die Router	10.1.10.101	10.1.11.100	10.1.12.100	10.1.13.100	10.1.14.100	10.1.15.100	10.1.16.100
IP-Netzmaske	255.255.255.0						
Gerätename	Beispiel_AG	Aachen	Berlin	Chemnitz	Dresden	Frankfurt	Gera
Rufnummern	4711100 4711200 4711300 4711400	1234561	1234562	1234563	1234564	1234565	1234566



IP-Routing ganz einfach mit *ELSA LANconfig* und den Assistenten

Für die Konfiguration zur LAN-Kopplung steht im *ELSA LANconfig* ein Assistent bereit, der alle notwendigen Einstellungen in der Software für Sie vornimmt und die Besonderheiten von TCP/IP-Netzen gleich mit berücksichtigt. Wählen Sie nach dem Start des Assistenten (automatisch oder mit **Extras ▶ Setup Assistent**) den Eintrag 'Zwei lokale Netz miteinander koppeln'. Der Assistent fragt dann kurz die benötigten Daten – darunter auch das verwendete Netzwerkprotokoll – ab und gibt Ihnen anschließend einen Hinweis, was Sie bei den Arbeitsplatzrechnern noch einstellen müssen.

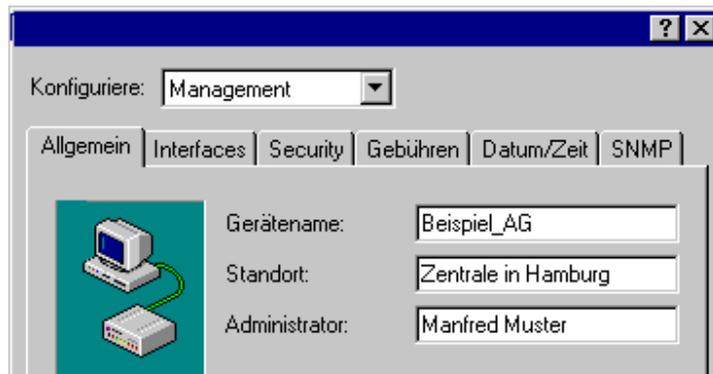
Da Sie in diesem Beispiel mehrere Netze koppeln möchten, führen Sie den Assistenten bei dem Router der Zentrale für jedes anzuschließende Netz einmal aus. In jedem Filial-Router kommt der Assistent ebenfalls einmal zum Einsatz.



Schritt für Schritt: Welche Einstellungen nehmen Sie in den Routern vor?

Die Einstellungen sind im Prinzip für alle Router gleich. In den folgenden Konfigurationsschritten zeigen wir, ausgehend vom Router in der Zentrale, genau auf, was gleich eingestellt wird, und geben Hinweise auf die Abweichungen in den anderen Routern.

- ① Damit die Namen, die Sie in der Namenliste verwenden werden, auch von den Routern übermittelt und erkannt werden, benennen Sie das Gerät passend (Konfigurationsbereich 'Management', Register 'Allgemein').:

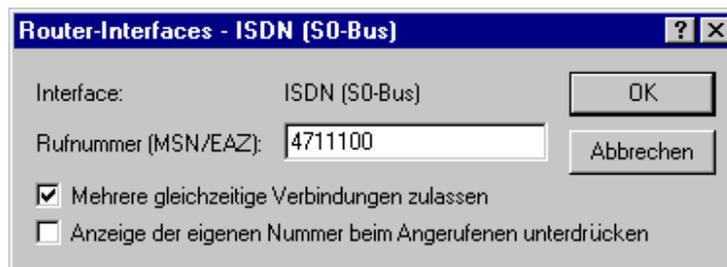


Bei Konfigurationen mit anderen Hilfsmitteln stellen Sie den Namen des Gerätes direkt im Menü 'Setup' ein:

```
set /Setup/Name Beispiel_AG
```

Die Geräte in den Filialen erhalten entsprechend die Namen 'Aachen' bis 'Gera'.

- ② Dann tragen Sie die **eigenen** Rufnummern des Routers in der Zentrale ein (Konfigurationsbereich 'Kommunikation', Register 'Allgemein'):



```
cd /Setup/WAN-Modul/Router-Interface-Liste
set s0-1 4711100 Ein Nein
```

Die anderen Interfaces und Geräte bekommen dementsprechend ihre eigenen Rufnummern.

- ③ Neue Einträge in der Namenliste (Konfigurationsbereich 'Kommunikation', Register 'Gegenstellen') mit Bezeichnung der Gegenstellen und der zugehörigen Rufnummern sowie Auswahl eines bei allen Routern vorhandenen Layers (hier z.B. der voreingestellte DEFAULT-Layer) erlaubt es dem Router in der Zentrale, die Router in den anderen Netzwerken anzurufen. Mit den Standard-Werten für die B1- und B2-Haltezeiten wird jede Verbindung getrennt, wenn für 20 Sekunden keine Daten auf dieser

Leitung fließen. Jedes Netz soll die Telefonkosten selbst tragen, deshalb bleibt der Rückruf-Eintrag auf AUS:

Namenliste - Neuer Eintrag

Name: AACHEN OK

Rufnummer: 1234561 Abbrechen

Haltezeit: 20 Sekunden

Haltezeit für Bündelung: 20 Sekunden

Layername: DEFAULT

Automatischer Rückruf:

- Keinen Rückruf durchführen
- Die Gegenstelle zurückrufen
- Die Gegenstelle zurückrufen (schnelles Verfahren)
- Die Gegenstelle nach Überprüfung des Namens zurückrufen
- Den Rückruf der Gegenstelle erwarten

```
cd /Setup/WAN-Modul/Namen-Liste
```

```
set AACHEN 1234561 * * DEFAULT AUS
```

Die anderen Geräte tragen nur den Router 'Beispiel_AG' ein und dazu die Rufnummer des entsprechenden Interfaces. Der Bindestrich vor der Rufnummer signalisiert, daß in der Round-Robin-Liste noch weitere Rufnummern für dieses Netz vorhanden sind.

Namenliste - Neuer Eintrag

Name: BEISPIEL_AG OK

Rufnummer: -4711100 Abbrechen

Haltezeit: 20 Sekunden

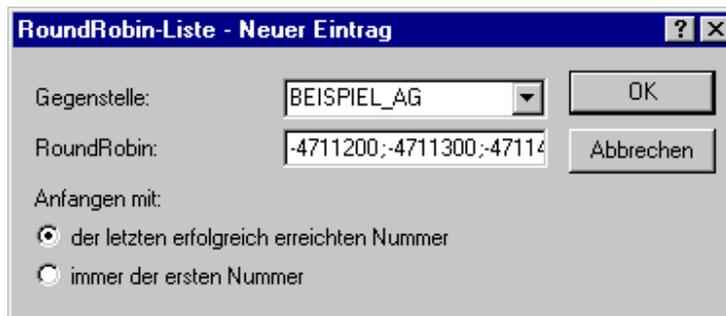
Haltezeit für Bündelung: 20 Sekunden

Layername: DEFAULT

Automatischer Rückruf:

- Keinen Rückruf durchführen

- ④ Mit der Round-Robin-Liste geht's auch gleich weiter. Hier tragen Sie in den Routern der Filialen die Rufnummern der anderen Interfaces des Routers in der Zentrale ein, die Sie vorher nicht in die Namenliste eingetragen haben.



```
cd /Setup/WAN-Modul/RoundRobin-Liste
set Beispiel_AG 4711200 letzter
```

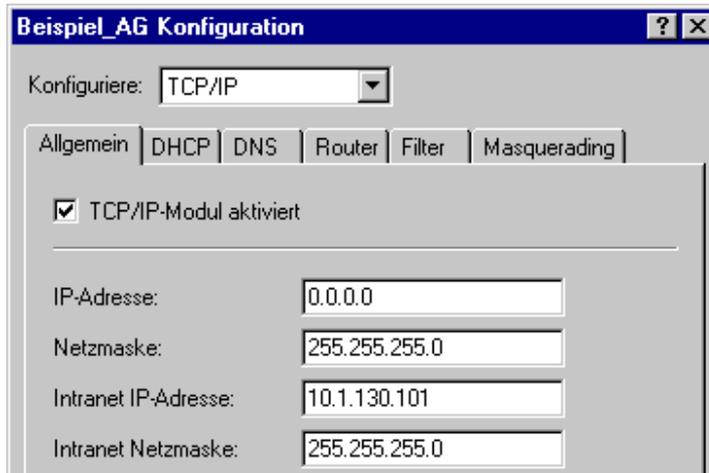
- ⑤ Wenn die Verbindungen zu den Filial-Netzen nur bestimmte B-Kanäle benutzen sollen, um die anderen Kanäle z.B. für Einwahlzugänge über RAS freizuhalten, legen Sie in der Kanal-Liste des Zentral-Routers für jede Gegenstelle einen Eintrag an, der die erlaubten Kanäle definiert.



```
cd /Setup/WAN-Modul/Kanal-Liste
set AACHEN 1 2 2-1;2-2 0
```

- ⑥ Jetzt müssen noch die Adressen geklärt werden. Damit die Geräte in den eigenen TCP/IP-Netzen gefunden werden, brauchen sie jeweils eine freie IP-Adresse aus dem Intranet. Die bekommen sie mit dem Eintrag der Intranet-Adresse mit der zuge-

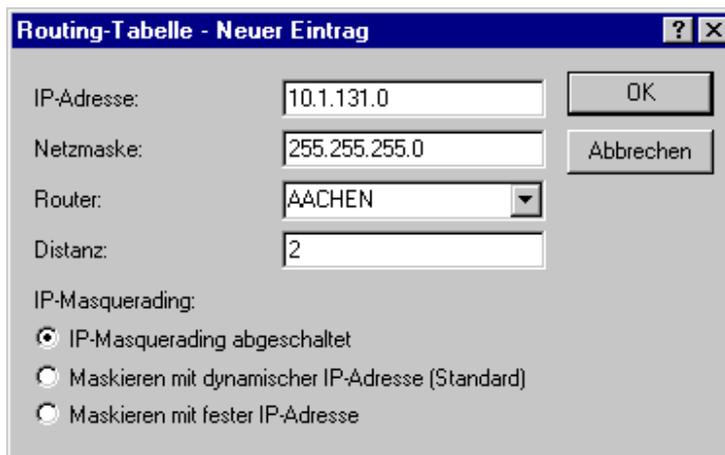
hörigen Netzmaske (Konfigurationsbereich 'TCP/IP', Register 'Allgemein'). Damit diese Einträge auch wirksam werden, schalten Sie das TCP/IP-Modul ein.



```
cd /Setup/TCP-IP-Modul/RoundRobin-Liste
set Intranet-Adresse 10.1.130.101
set Intranet-Netzmaske 255.255.255.0
```

Die Router in den Filialen bekommen die IP-Adressen 10.131.1.100 bis 10.136.1.100, alle mit der Netzmaske 255.255.255.0, wie im Bild und in der Übersicht dargestellt.

- ⑦ Und welche IP-Adressen sollen die Router wohin routen? In der Routing-Tabelle des Routers in der Zentrale geben Sie die IP-Adressen und Netzmasken aller Filialen mit der zugehörigen Gegenstelle an (ohne IP-Masquerading!):



Zum Schluß schalten Sie den IP-Router ein, und dann ist der erste *ELSA LANCOM* vorbereitet für die Verbindung zu den anderen Netzen.

```
cd /Setup/IP-Router-Modul/IP-Routing-Tab.
set 10.1.131.0 255.255.255.0 Aachen 2 Aus
cd /Setup/IP-Router-Modul
set Zustand Ein
```

Die Router in den Filialen bekommen jeweils einen Eintrag für die Zentrale. Damit werden alle Verbindungen der Filialen untereinander über den Router in der Zentrale geroutet.



Alternativ können die Zentralen untereinander auch direkt kommunizieren. Dazu bekommen sie zunächst die gleichen Einträge in der Namenliste wie der Router in der Zentrale. Zusätzlich erhalten sie dieselben Einträge in der Routing-Tabelle wie die Geräte in der Zentrale, wobei der Routing-Eintrag für das eigene Netz durch den Eintrag für das Netz der Zentrale ersetzt wird.

- ⑧ Was bleibt noch zu tun? Die Rechner im LAN müssen natürlich auch wissen, daß der Router die Vermittlungsstelle für die anderen Netzwerke ist. Dazu wird die Intranet-Adresse des Routers als Default-Gateway bei den Arbeitsplatzrechnern und Servern eingetragen.



Bei Verwendung des Routers als DHCP-Server können Sie diese Einstellungen automatisch zuweisen lassen (siehe 'DHCP-Server').

Das Ergebnis

Beim Zugriff von einem Rechner in einer Filiale auf das Netz der Zentrale besteht nun die Möglichkeit, über den Eintrag in der Round-Robin-Liste auf ein anderes Interface auszuweichen, wenn das zuerst angewählte besetzt ist.

Netze verbinden mit dem IPX-Router

Die Motivation

Mit dem IPX-Router können Sie Netzwerke verbinden, die auf IPX/SPX als Netzwerkprotokoll setzen. Sie können z.B. die Zentrale einer Firma mit den Netzen von mehreren Filialen verbinden.

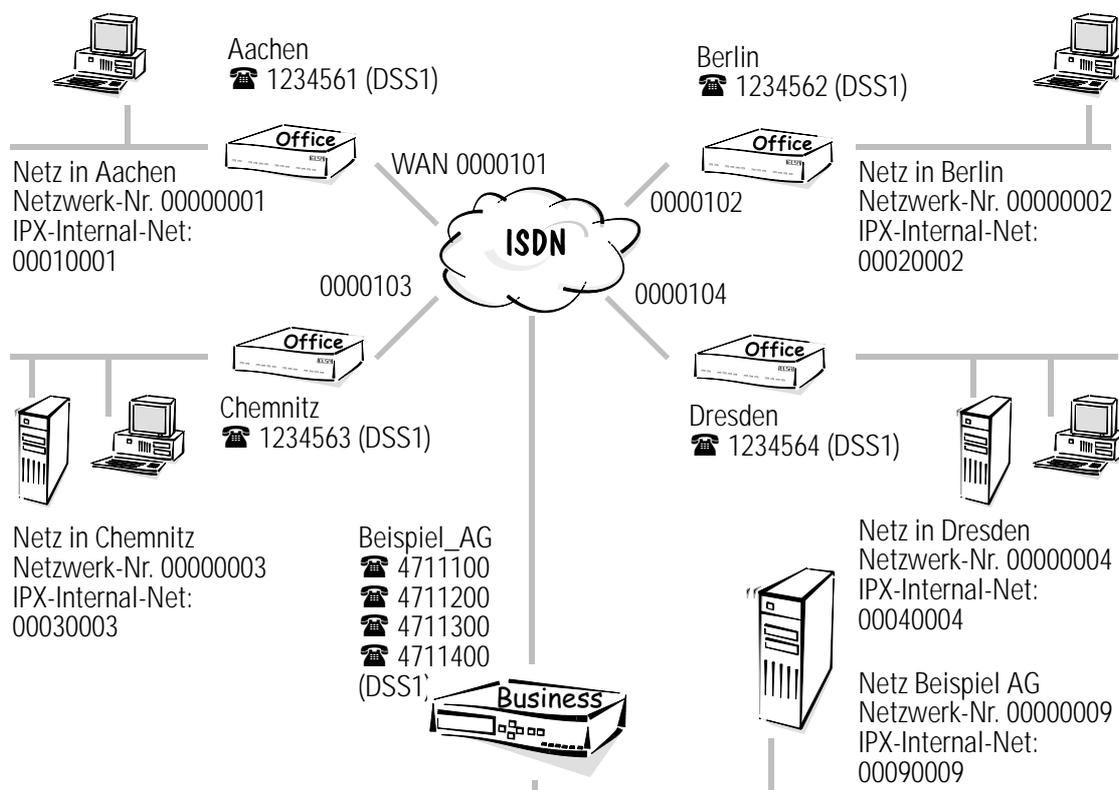
Die Aufgabe im Beispiel

In dieser Aufgabe hat die Zentrale vier Filialen. In jeder der Filialen steht ein „kleiner“ Router, die über das ISDN-Wählverbindungen an ein *ELSA LANCOM Business* in der Zentrale angeschlossen werden.

Die folgende Tabelle zeigt die Zuordnung von Gerätenamen, Adressen und Telefonnummern, wie sie im Beispiel verwendet werden:

Netz	LAN Beispiel AG	LAN Aachen	LAN Berlin	LAN Chemnitz	LAN Dresden
Netzwerk-Adresse	00000009	00000001	00000002	00000003	00000004
IPX-Internal-Net	00090009	00010001	00020002	00030003	00040004
Binding	802.3	SNAP	SNAP	802.3	802.3

Gerätename	Beispiel_AG	Aachen	Berlin	Chemnitz	Dresden
Rufnummer	4711100 4711200 4711300 4711400	1234561	1234562	1234563	1234564
WAN-Netze		0000101	0000102	0000103	0000104



Schritt für Schritt: Welche Einstellungen nehmen Sie in den Routern vor?

In den folgenden Konfigurations-Schritten zeigen wir, ausgehend vom Router in der Zentrale, die Einstellungen genau auf, und geben Hinweise auf die Abweichungen in den anderen Routern.

- ① Damit die Namen, die Sie in der Namenliste verwenden werden, auch von den Routern übermittelt und erkannt werden, benennen Sie das Gerät passend (Konfigurationsbereich 'Management', Register 'Allgemein'):

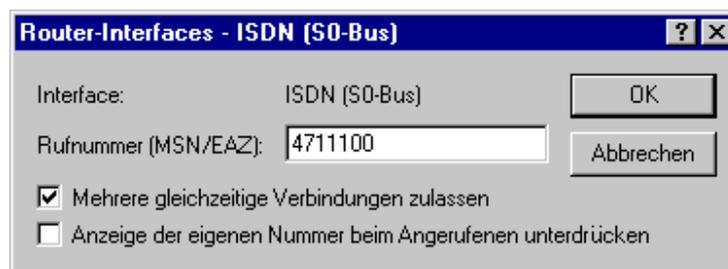


Bei Konfigurationen mit anderen Hilfsmitteln stellen Sie den Namen des Gerätes direkt im Menü 'Setup' ein:

```
cd Setup
set Name Beispiel_AG
```

Die Router in den Filialen erhalten entsprechend die Namen 'Aachen', 'Berlin', 'Chemnitz' und 'Dresden'.

- ② Dann tragen Sie die **eigene** Rufnummer des Routers in der Zentrale ein (Konfigurationsbereich 'Kommunikation', Register 'Allgemein'):



```
cd Setup/WAN-Modul/Router-Interface-Liste
S0-1 4711100
S0-2 4711200
S0-3 4711300
S0-4 4711400
```

Die anderen Geräte bekommen dementsprechend ihre eigenen Rufnummern (1234561, 1234562, 1234563 und 1234564).

- ③ Neue Einträge in der Namenliste (Konfigurationsbereich 'Kommunikation', Register 'Gegenstellen') mit Bezeichnung der Gegenstellen und der zugehörigen Rufnummern sowie Auswahl eines bei allen Routern vorhandenen Layers (hier z.B. der voreingestellte DEFAULT-Layer) erlauben es dem Router in der Zentrale, die Router in den

anderen Filial-Netzen anzurufen. Jedes Netz soll die Telefonkosten selbst tragen, deshalb bleibt der Rückruf-Eintrag auf AUS:

```
cd Setup/WAN-Modul/Namenliste
set Aachen 1234561 * * DEFAULT AUS
set Berlin 1234562 * * DEFAULT AUS
set Chemnitz 1234563 * * DEFAULT AUS
set Dresden 1234564 * * DEFAULT AUS
```

Die Router in den Filialen tragen nur den Router 'Beispiel_AG' ein und dazu die Rufnummer eines der Interfaces beim Router in der Zentrale.

- ④ Jetzt müssen noch die Adressen geklärt werden. Damit der Router das eigene LAN von den anderen LANs und dem WAN unterscheiden kann, tragen Sie die Netzwerk-Adresse und das Binding für das Netz der Beispiel AG ein (Konfigurationsbereich 'IPX', Register 'Allgemein'):

```
Setup/IPX-Modul/LAN-Einstellung
set Netzwerk 00000009
set Binding 802.3
```



Das Netz in der Zentrale hat einen Server. Wenn Sie die Netzwerk-Nummer nicht wissen, können Sie diese mit der Einstellung '00000000' als Netzwerk-Nummer automatisch ermitteln lassen. Auch das Binding können Sie automatisch ermitteln lassen. Da der Router dabei immer das Netz auswählt, in dem die meisten RIP/SAP-Informationen ausgetauscht werden, bietet sich dieses Verfahren z.B. dann an, wenn nur ein logisches Netz auf dem Ethernet-Strang verwendet wird.

Für die Geräte in den Filialen in Chemnitz und Dresden tragen Sie ebenfalls die jeweilige Netzwerk-Adresse mit dem Binding 'Auto' ein.

```
cd /Setup/IPX-Modul/LAN-Einstellung
set Netzwerk 00000003 bzw. 00000004
set Binding Auto
```

Für die Filial-Netze in Aachen und Berlin müssen Sie das Binding, z.B. 'SNAP', und die Netzwerk-Nummer explizit angeben, da in diesen Netzen kein Server steht:

```
cd /Setup/IPX-Modul/LAN-Einstellung
set Netzwerk 00000001 bzw. 00000002
set Binding SNAP
```

- ⑤ Und wohin sollen die Geräte routen? In der Routing-Tabelle (Konfigurationsbereich 'IPX', Register 'Router') geben Sie die Gegenstellen mit einer **eigenen** Netzwerk-Adresse für das WAN (nicht des anderen LANs!) an. Für den Router im Netz der Zentrale sehen die Tabelleneinträge so aus:

```
cd /Setup/IPX-Modul/WAN-Einstellung/Routing-Tabelle
set Aachen 00000101 802.3 Route Aus
set Berlin 00000102 802.3 Route Aus
set Chemnitz 00000103 802.3 Route Ein
set Dresden 00000104 802.3 Route Ein
```

Neben dem Gerätenamen des Routers im Netz der Gegenstelle erhält jeder Eintrag in der Routing-Tabelle eine eigene WAN-Adresse. Netzwerk-Adresse des WANs, auf dem das Binding '802.3' verwendet wird. Weil vom Netz in der Zentrale aus gesehen bei den Gegenstellen in Chemnitz und Dresden ein Server vorhanden ist, wird der 'Exponential Backoff'-Mechanismus aktiviert.



Weitere Hinweise zur Funktion des 'Exponential-Backoff'-Mechanismus finden Sie in 'Exponential Backoff'.

Für das Netz in der Aachener Filiale sieht der Eintrag z.B. so aus:

```
cd /Setup/IPX-Modul/WAN-Einstellung/Routing-Tabelle
set Beispiel_AG 00000101 802.3 Route Ein
```

Die Netzwerk-Adresse des WANs stimmt jeweils mit dem Eintrag für das Filial-Netz im Router der Zentrale überein. Als Binding wird auf dem WAN immer '802.3' verwendet. Weil von den Netzen in den Filialen aus gesehen auf der Gegenseite immer ein Server vorhanden ist, wird der 'Exponential-Backoff'-Mechanismus hier eingeschaltet.

Remote-Access

Die Arbeit vieler Mitarbeiter in modernen Organisationen wird immer unabhängiger von bestimmten Orten – wichtig ist vor allem der ständige Zugriff auf gemeinsame, frei verfügbare Informationen.

Remote-Access heißt hier das Zauberwort. Teleworking für die Kollegen im Home Office oder Kontakt zur Zentrale für Außendienst-Mitarbeiter von unterwegs werden über den

Router im lokalen Netz der Zentrale ermöglicht. Auch beim Remote-Access tut der Router natürlich alles für den Schutz der firmeneigenen Datenbestände: Die Rückruffunktion über eingetragene Namen und Rufnummern gibt nur bestimmten Personen den Sesam-öffne-dich-Schlüssel. Und für die leichtere Abrechnung werden damit die Telefonkosten in der Firma zentral erfaßt.

Remote-Access mit TCP/IP

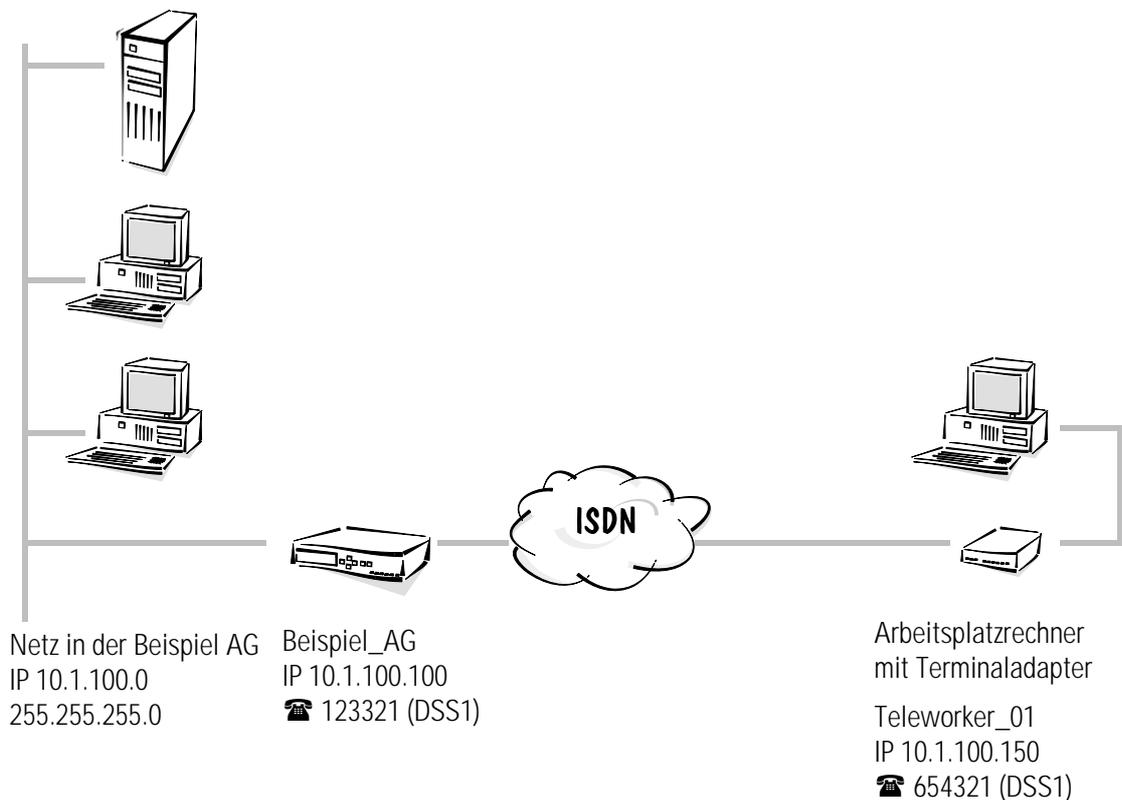
Die Motivation

Eine Firma beschäftigt einige Mitarbeiter, die als Außendienstler oder Teleworker nicht jeden Tag in der Firma sind. Trotzdem sollen sie von ihrem Rechner aus Zugang zum lokalen Netz (Intranet) der Firma haben, um Daten und Informationen (z.B. E-Mails) austauschen zu können. Als Protokoll für die Datenübertragung wird PPP verwendet, weil das alle üblichen Geräte und Betriebssysteme beherrschen. Um den Aufwand bei der Pflege der Einwahlzugänge zu reduzieren, werden die IP-Adressen über IP-Pooling zugewiesen.

Die Aufgabe im Beispiel

Die am Remote-Access beteiligten Mitarbeiter haben zu Hause einen Arbeitsplatzrechner mit einem ISDN-Terminaladapter oder einer ISDN-Karte. Von unterwegs wählen sich einige Außendienstmitarbeiter auch mit einem Notebook über GSM-Mobiltelefone in das Firmennetz ein.

Auf den entfernten Rechnern ist ein PPP-Client installiert, in diesem Beispiel das DFÜ-Netzwerk von Windows mit TCP/IP als Protokoll. Damit die Außendienstler auch über die Datei- und Druckerfreigabe auf die Windows-Netze zugreifen können, soll auch das Routing von NetBIOS-Paketen unterstützt werden. Im LAN der Firma steht ein *ELSA LANCOM Business*, das die Arbeitsplatzrechner bei Bedarf zurückrufen soll.



Remote-Access ganz einfach mit *ELSA LANconfig* und den Assistenten

Für die Konfiguration Einwahlzugänge steht im *ELSA LANconfig* ein Assistent bereit, der alle notwendigen Einstellungen in der Software für Sie vornimmt und die Besonderheiten von TCP/IP-Netzen gleich mit berücksichtigt. Wählen Sie nach dem Start des Assistenten (automatisch oder mit **Extras ▶ Setup Assistent**) den Eintrag 'Einwahlzugang bereitstellen (RAS)'. Der Assistent fragt dann kurz die benötigten Daten ab, darunter auch das verwendete Netzwerkprotokoll.



Schritt für Schritt: Welche Einstellungen nehmen Sie im Router vor?

- ① Zuerst tragen Sie die **eigene** Rufnummer für ankommende und abgehende Rufe in der Router-Interface-Tabelle ein (Konfigurationsbereich 'Kommunikation', Register 'Allgemein'):

```
cd /Setup/WAN-Modul/Router-Interface-Liste
set S0-1 123321 EIN
```

Beim Eintrag mehrerer Rufnummern wird die erste Nummer für abgehende Rufe verwendet.



Die Option 'Y-Verbindung' wird in diesem Fall eingeschaltet, damit auch Verbindungen zu zwei verschiedenen Teleworkern gleichzeitig möglich sind.

- ② Der Remote-Access-Zugang soll auch ohne die Prüfung der eingehenden Rufnummer möglich sein, da die Außendienst-Mitarbeiter manchmal von wechselnden

Standorten Zugriff auf das Firmennetz verlangen. Die Zuordnung eines Layers, der PPP verwendet, ist über die Rufnummernerkennung also nicht zu realisieren. Prüfen Sie die Werte für den 'DEFAULT'-Layer, und stellen Sie diesen Layer ggf. auf die benötigten Werte ein:

```
cd /Setup/WAN-Modul/Layer-Liste
set DEFAULT trans PPP trans keine HDLC64K
```

Damit wird jeder Anrufer, der nicht über die Nummernliste zugeordnet werden kann, sofort mit einer PPP-Verhandlung begrüßt.

Stellt der Router fest, daß die Gegenstelle über GSM anruft, werden automatisch die Protokoll-Einstellungen `Trans APPP Trans keine V.110 9600` verwendet, um den Verbindungsaufbau zu ermöglichen.

- ③ Für den Rückruf zu den GSM-Mobiltelefonen wird später ein Layer benötigt, der auf die Verbindung über das Protokoll V.110 eingestellt ist:

```
cd /Setup/WAN-Modul/Layer-Liste
set RAS_GSM Trans APPP Trans keine oder comp. V.110 9600
```

- ④ Der Eintrag in der Namenliste für jede RAS-Gegenstelle mit Bezeichnung der Gegenstelle, dem Layer ('DEFAULT' oder 'RAS_GSM') und der Rückrufoption 'Name' erlaubt es dem *ELSA LANCOM*, den Rechner des Außendienst-Mitarbeiters zurückzurufen. Dabei wird eine Protokollverhandlung über PPP erzwungen, die Rufnummer für den Rückruf bleibt in der Namenliste frei und kann vom Außendienstmitarbeiter selbst bestimmt werden. Ruft ein Außendienstler abwechselnd über ISDN und GSM an, müssen für diesen Mitarbeiter zwei Einträge in der Namenliste angelegt werden.

```
cd /Setup/WAN-Modul/Namenliste
set Teleworker_01_ISDN * * * DEFAULT Name
set Teleworker_01_GSM * * * RAS_GSM Name
set Teleworker_02 * * * DEFAULT Name
```

- ⑤ In der Kanalliste können Sie festlegen, wie viele Kanäle für einen Einwahlzugang verwendet werden sollen und optional die Kanäle bestimmen, die benutzt werden dürfen. Beim Zugang über ISDN soll die Bündelung von zwei Kanälen erlaubt werden. Bei der GSM-Einwahl steht nur ein Kanal auf einem anderen Interface zur Verfügung:

```
cd /Setup/WAN-Modul/Kanalliste
set Teleworker_01_ISDN 1 2 1-1;1-2 0
set Teleworker_01_GSM 1 1 2-1 0
set Teleworker_02 1 2 1-1;1-2 0
```

- ⑥ Da Sie für den Zugang der entfernten Rechner PPP verwenden, können Sie in der PPP-Liste Benutzernamen (z.B. Mustermann) und Paßwort (z.B. Remote) für die Gegenstelle 'Teleworker_01' vereinbaren. Als Sicherungsverfahren verwenden Sie dabei PAP und erlauben das Routing von IP- und NetBIOS-Paketen über diese Verbindung:

```
cd /Setup/WAN-Modul/PPP-Liste
Teleworker_01_ISDN PAP Remote 0 0 Teleworker_01 IP+NTB
Teleworker_01_GSM PAP Remote 0 0 Teleworker_01 IP+NTB
```

Als Benutzername können Sie hier den beiden Einträgen für ISDN und GSM wieder den gleichen Wert zuweisen. Dann kann sich der entsprechende Mitarbeiter immer mit dem gleichen Namen anmelden. Das Paßwort „Remote“ wird nach der Eingabe durch einen * ersetzt!



Beachten Sie bitte, daß bei Benutzernamen und Paßwort Groß- und Kleinschreibung unterschieden werden.

- ⑦ Für das Routing der NetBIOS-Pakete ist auch ein Eintrag in NetBIOS-Tabelle notwendig. Damit machen Sie dem Router klar, daß mit dieser Gegenstelle NetBIOS-Informationen ausgetauscht werden dürfen und daß es sich dabei um eine einzelne Workstation handelt, die also nicht direkt angefrufen werden soll:

```
cd /Setup/NetBIOS-Modul/Gegenstellen-Tab.
Teleworker_01_ISDN Workstation
Teleworker_01_GSM Workstation
```

- ⑧ Jetzt müssen noch die Adressen geklärt werden. Damit der Router im eigenen TCP/IP-Netz gefunden wird, braucht er eine freie IP-Adresse aus dem Firmen-Netz. Die bekommt es mit dem Eintrag einer Intranet-Adresse und der zugehörigen Netzmaske:

```
cd /Setup/TCP-IP-Modul
set Intranet-Adresse 10.1.100.100
set Intranet-Netzmaske 255.255.255.0
```

- ⑨ Und die IP-Adresse für den anrufenden Rechner? Die werden aus einem Pool von IP-Adressen dynamisch für die Dauer der Verbindung zugewiesen. Dazu werden nur Anfang und Ende des Adreß-Bereichs festgelegt. Der Eintrag in der IP-Routing-Tabelle wird damit unnötig:

```
cd /Setup/IP-Router-Modul
set Start-WAN-Pool 10.1.100.110
set Ende-WAN-Pool 10.1.100.120
```

- ⑩ Damit der Router die Daten für einen entfernten Rechner mit einer Adresse aus dem eigenen logischen Netz überhaupt routen kann, muß das Proxy-ARP eingeschaltet werden.

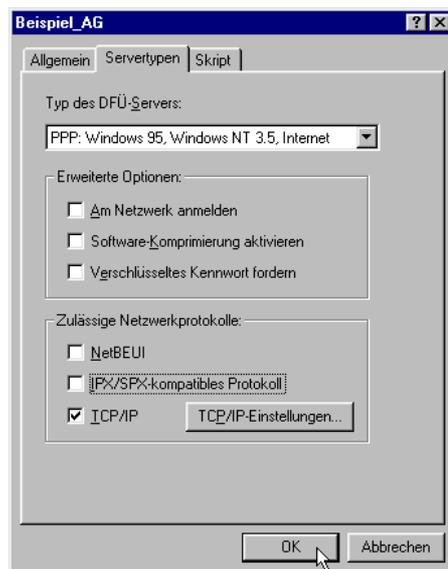
```
cd /Setup/IP-Router-Modul  
set Proxy-ARP Ein
```

- ⑪ Jetzt schalten Sie den IP-Router ein, und dann ist der Router vorbereitet für Einwahl von Außendienstmitarbeitern.

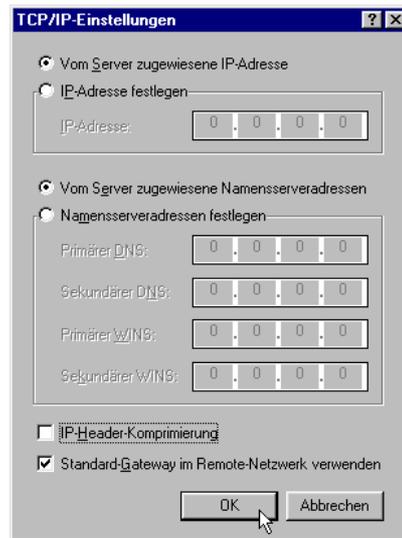
```
cd /Setup/IP-Router-Modul  
set Zustand Ein
```

- ⑫ Was bleibt noch zu tun? Der Arbeitsplatzrechner des Außendienst-Mitarbeiters muß noch so eingerichtet werden, daß auch von seiner Seite aus der Zugriff auf das Firmen-Netz möglich ist. Dazu sind die folgenden Einstellungen nötig, die hier nur kurz aufgeführt werden:

- DFÜ-Netzwerk korrekt eingerichtet
- TCP/IP installiert und auf den DFÜ-Adapter gebunden
- neue Verbindung im DFÜ-Netzwerk mit Rufnummer des Routers
- Terminaladapter oder ISDN-Karte auf PPPHDLC eingestellt
- PPP als DFÜ-Servertyp ausgewählt, 'Software-Komprimierung aktivieren' und 'Verschlüsseltes Kennwort fordern' ausgeschaltet
- TCP/IP als Netzwerkprotokoll ausgewählt

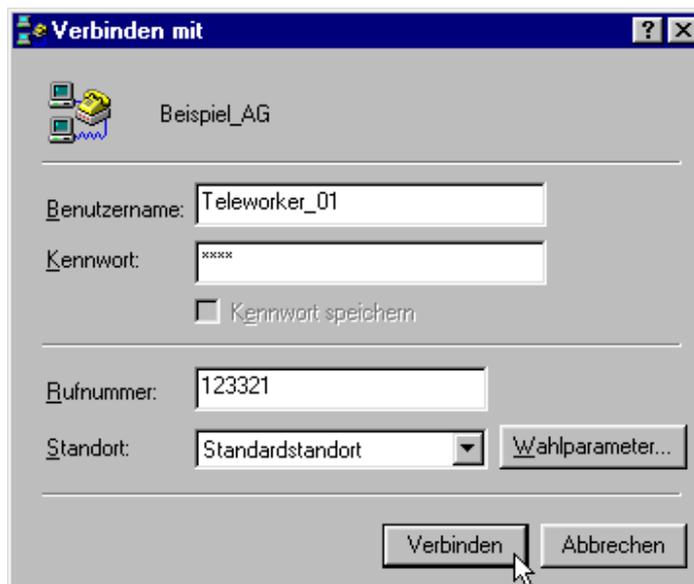


- Zuweisung von IP-Adresse und Namensserveradresse aktiviert, 'IP-Headerkomprimierung' deaktiviert



Was haben Sie nun erreicht?

Der Mitarbeiter am entfernten Arbeitsplatzrechner kann nun die Verbindung zum Firmennetz über das DFÜ-Netzwerk herstellen. Dabei gibt er den in der PPP-Liste vereinbarten Benutzernamen und das zugehörige Paßwort an.



Anschließend kann er auf die freigegebenen Server und Windows-Netze im TCP/IP-Netz zugreifen. Diese Server findet er z.B. mit drei Klicks auf **Start** ► **Suchen** ► **Computer** in der Windows-Startleiste.

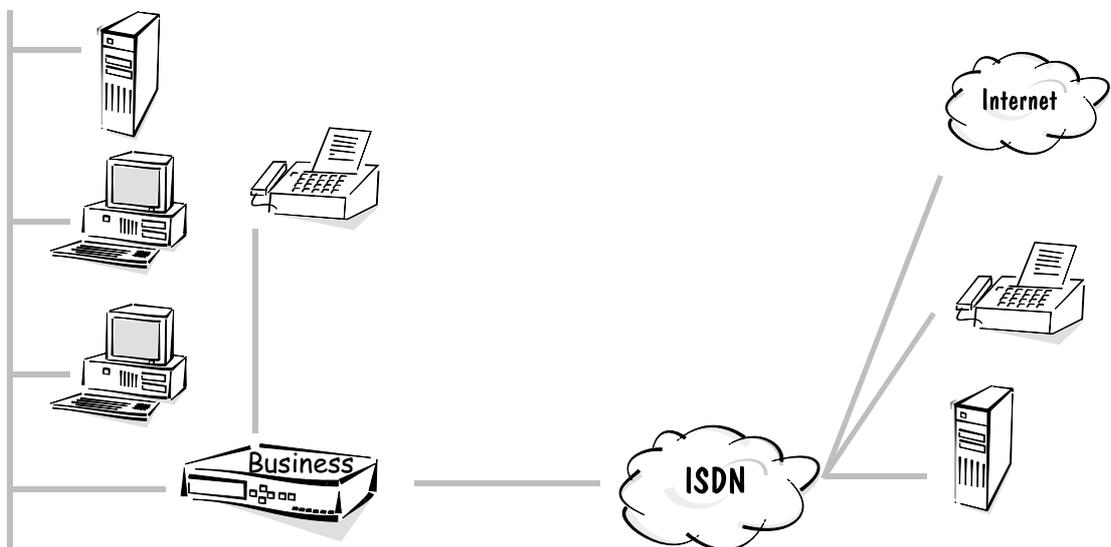
Least-Cost-Router

In diesem Kapitel zeigen wir Ihnen an einem Beispiel, wie Sie durch die Verwendung des Least-Cost-Routers eine Menge an Gebühren sparen können.

Der Least-Cost-Router sucht nach der Einstellung bei jedem Verbindungsaufbau automatisch den Provider mit den günstigsten Konditionen und versucht die Verbindung über dessen Netz herzustellen.

Beispiel:

Als Beispiel betrachten wir hier ein kleines Ingenieurbüro (eine Außenstelle eines größeren Planungsbüro) mit zwei Arbeitsplätzen. An beiden Arbeitsplätzen steht ein Telefon, dazu gibt es ein Faxgerät und einen Anrufbeantworter.



Die beiden Mitarbeiter in diesem Büro nutzen folgende Funktionen im *ELSA LANCOM Business*:

- Den Zugang zum Internet über einen Provider haben Sie mit *ELSA LANconfig* und seinen Assistenten in Windeseile eingerichtet. Dabei wird der IP-Router verwendet.
- Der Datenaustausch mit der Zentrale findet über eine LAN-LAN-Kopplung mit den Funktionen des IPX-Routers statt.
- Zum Versenden von Faxnachrichten direkt aus dem PC heraus verwenden sie *ELSA-RVS-COM* über die *LANCAPI*.

Das Beispielbüro in diesem Kapitel möchte natürlich auch seine Verbindungen beim Faxen, beim Internetzugriff und beim Datenabgleich mit der Zentrale so günstig wie möglich abwickeln. Dazu wird der Least-Cost-Router verwendet, der automatisch bei jeder Anwahl die günstigste Verbindung sucht. Informationen über die verwendeten Tarife erhalten Sie z.B. aus Zeitschriften, Broschüren oder aus dem Internet.

Unser Beispielbüro liegt in Aachen und hat einen Telefonanschluß der Deutschen Telekom. Die nachfolgenden Einträge für den Least-Cost-Router sind aufgrund dieser lokalen Gegebenheiten und anhand von Informationen aus dem Internet über Zonen und Tarife erstellt.



Bitte beachten Sie, daß Sie diese Einträge nicht unbedingt auf andere Situationen übertragen können, sie dienen nur als Beispiel.



Least-Cost-Router einstellen mit *ELSA LANconfig*

Mit den folgenden Schritten machen Sie den *ELSA LANCOM Business* zum Preisfuchs:

- ① Öffnen Sie die Konfiguration des Geräts im *ELSA LANconfig* mit einem Doppelklick auf den Eintrag in der Geräteliste, und wechseln Sie in den Konfigurationsbereich 'Least-Cost-Router'.
- ② Aktivieren Sie auf der Registerkarte 'Allgemein' die Funktion des LCR für alle angebotenen Betriebsarten. Da das Büro keine Gebührenüberwachung benötigt, ist die Verwendung des LCR auch für die Routermodule unkritisch.
- ③ Bearbeiten Sie dann die Feiertagstabelle auf der Registerkarte 'Zeiten und Feiertage'.
 - Geben Sie zunächst die jährlich wiederkehrenden Feiertage mit Tag und Monat, aber ohne Jahr ein. Diese Einträge werden automatisch für jedes Jahr gesetzt.
 - Geben Sie dann die variablen Feiertage mit Tag, Monat und Jahr ein, am besten gleich für die nächsten zwei, drei Jahre.
- ④ Anschließend geht es zum Kern der Sache: Die Einträge in der LCR-Tabelle. Bei einigen Einträgen gibt es mehrere Netzkennzahlen. Diese werden der Reihe nach durchgewählt, wenn die vorherigen Nummern besetzt sind. Damit aber immer innerhalb kurzer Zeit eine Verbindung zustande kommt, wird für alle Einträge der automatische Rückfall auf die eigene Telefongesellschaft (in diesem Fall die Deutsche Telekom) aktiviert.
- ⑤ Zuerst sind die Fernverbindungen dran. Mit diesem Eintrag leiten Sie nun alle Fernverbindungen im Inland um, je nach Tageszeit über einen anderen Provider:

Vorwahl	Call-by-Call-Netzkennzahl	Tage	Uhrzeit	Rückfall
0	01015	Mo–Fr	0:00–1:59	Ja
0	01033	Mo–Fr	2:00–4:59	Ja
0	01015	Mo–Fr	5:00–7:59	Ja
0	01050	Mo–Fr	8:00–8:59	Ja
0	01028	Mo–Fr	9:00–17:59	Ja
0	01015	Mo–Fr	18:00–23:59	Ja

Vorwahl	Call-by-Call-Netzkennzahl	Tage	Uhrzeit	Rückfall
0	01015	Sa, So, Feiertage	0:00–7:59	Ja
0	01050	Sa, So, Feiertage	8:00–8:59	Ja
0	01013:01090	Sa, So, Feiertage	8:00–20:59	Ja
0	01015	Sa, So, Feiertage	21:00–23:59	Ja

- ⑥ Die Fernverbindungen ins Ausland sind relativ selten. Deshalb soll in diesem Beispiel auch nur ein Eintrag für alle Auslandsverbindungen gültig sein:

Vorwahl	Call-by-Call-Netzkennzahl	Tage	Uhrzeit	Rückfall
00	01015:01028	alle Tage	0:00–23:59	Ja

- ⑦ Einige Ortsnetze in der Nähe Ihres Standortes sind sicherlich mit Vorwahl, aber zum Ortstarif zu erreichen. Die sollen nun nicht von der Umleitung für die Ferngespräche erfaßt werden, werden also daher wieder „zurückgeholt“ durch das Freilassen der Netzkennzahl. Das Büro aus dem Beispiel liegt in Aachen. Aus dem Internet haben die Mitarbeiter erfahren, welche Ortsnetze noch zur Nahzone gehören, deshalb kommen nun folgende Einträge dazu:

Vorwahl	Call-by-Call-Netzkennzahl	Tage	Uhrzeit	Rückfall
02408		alle Tage	0:00–23:59	Ja
02464		alle Tage	0:00–23:59	Ja
02404		alle Tage	0:00–23:59	Ja
02401		alle Tage	0:00–23:59	Ja
02403		alle Tage	0:00–23:59	Ja
02454		alle Tage	0:00–23:59	Ja
02451		alle Tage	0:00–23:59	Ja
02406		alle Tage	0:00–23:59	Ja
02407		alle Tage	0:00–23:59	Ja
02429		alle Tage	0:00–23:59	Ja
02465		alle Tage	0:00–23:59	Ja
02423		alle Tage	0:00–23:59	Ja
02471		alle Tage	0:00–23:59	Ja
02456		alle Tage	0:00–23:59	Ja
02473		alle Tage	0:00–23:59	Ja

Vorwahl	Call-by-Call-Netzkennzahl	Tage	Uhrzeit	Rückfall
02409		alle Tage	0:00–23:59	Ja
02402		alle Tage	0:00–23:59	Ja
02405		alle Tage	0:00–23:59	Ja

Wenn Sie den ersten Eintrag erstellt haben, können Sie diesen ganz einfach kopieren und jedesmal nur die Vorwahl ändern.

- ⑧ Auch einige Sonderrufnummern können von der Umleitung befreit werden, z.B. die '0130', '0180', '0190' und '0800':

Vorwahl	Call-by-Call-Netzkennzahl	Tage	Uhrzeit	Rückfall
01		alle Tage	0:00–23:59	Ja
0800		alle Tage	0:00–23:59	Ja

- ⑨ Fertig! Damit haben Sie Ihren Least-Cost-Router schon sehr genau eingestellt. Kontrollieren Sie die Arbeitsweise des LCR zu Beginn im Betrieb mit *ELSA LANmonitor*, und werfen Sie am Monatsende einen Blick auf Ihre Telefonrechnung. Evtl. finden Sie mit Hilfe der Einzelverbindungsübersicht noch einige Vorwahlen, die Sie in die LCR-Tabelle eintragen können.



Least-Cost-Router Schritt für Schritt

Falls Sie das Konfigurations-Tool *ELSA LANconfig* nicht verwenden können, erreichen Sie das gleiche Ziel bei der Einstellung über Telnet (oder Terminalprogramm) mit folgenden Befehlen:

Menü	Parameter	Bemerkung oder Wert
Setup/LCR-Modul	Router-Nutzung	Aktivierung des LCR-Moduls für die einzelnen Betriebsarten.
	LANC-API-Nutzung	
	Beispiel	'set router ein' 'set lancapi ein' 'set ab-port ein'
Setup/LCR-Modul/ Zeittabelle	Index	Durchlaufender Index für die Einträge in der Tabelle.
	Praefix	Vorwahl, die umgeleitet werden soll.
	Tage	Gültigkeit des Eintrags für Wochen- und Feiertage in Darstellung einer 8-bit-Maske: Bit 0 steht für Montag, Bit 7 für Feiertage. Der Eintrag '31' bezeichnet also alle Werkzeuge, '192' die Sonn- und Feiertage.
	Start	Anfangszeit für die Gültigkeit des Eintrags an den definierten Tagen.

Menü	Parameter	Bemerkung oder Wert
	Stop	Endzeit für die Gültigkeit des Eintrags an den definierten Tagen.
	Nummernliste	Netzkennzahl des Call-by-Call-Providers.
	Rueckfall	Automatischer Rückfall auf die eigene Telefongesellschaft, falls alle Call-by-Call-Nummern besetzt sind.
	Beispiel	'set 1 02 31 1:00 11:59 01030:01090:01070 Ein' leitet alle Ferngespräche in die Region '02' zwischen ein und zwölf Uhr um auf den Provider mit der Netzkennzahl '01030'. Falls da besetzt ist, werden die Netzkennzahlen '01090' und '01070' versucht. Sind die auch nicht verfügbar, wird die Verbindung über die normale Telefongesellschaft aufgebaut.

Legen Sie nach diesem Muster alle benötigten Einträge an, und orientieren Sie sich dabei an den Tabellen bei der Einstellung über *ELSA LANconfig*.

Anhang

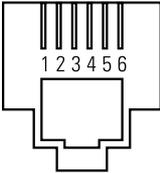
In diesem Anhang finden Sie neben den technischen Daten u.a. die Steckerbelegungen, und die allgemeinen Garantiebedingungen.

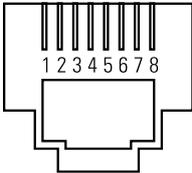
Technische Daten

Funktionsarten:	IP-Router, IPX-Router, CAPI-Server, DHCP-Server; Least-Cost-Router für Router- und CAPI-Verbindungen, gleichzeitiger Betrieb aller Funktionsarten möglich
LAN-Anschluß:	Ethernet IEEE 802.3, 10/100Base-TX (RJ45, Node/Hub, Switch), auto-sense, Full-Duplex-Betrieb
Netzwerk-Protokolle:	IP-Router: IP, TCP, ICMP, ARP, RIP-1, RIP-2, PROXY ARP, DHCP IPX-Router: RIP, SAP, Novell NetBIOS, Novell-Burst-Mode
Filter-Möglichkeiten:	IP-Router: TCP-, UDP-Portfilterung, Quell- und Zielnetzfilter IPX-Router: RIP, SAP, IPX- und SPX-Watchdog, Sockets, Propagated Packets
Spoofing:	IPX-Router: RIP- und SAP-Packets; IPX- und SPX-Watchdogs, Novell NetBIOS, Keep-alive-Packets
ISDN-Schnittstelle:	Anschluß: ISDN-S0-Bus, Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-Konfiguration, I.430 D-Kanal: 1TR6, Euro-ISDN (DSS1), auto-sense, Festverbindungen Gruppe 0 (D64S, D64S2, D64SY) B-Kanal: PPP (asynch./synch.), MLPPP, X.75, HDLC, V.110, CAPI 2.0 über ELSA LANCAPI, Stac-Datenkompression
CAPI-Server:	virtuelle CAPI 2.0 für Windows-Betriebssysteme, NDIS-WAN-Treiber, Fax-Class 1
Leistungssteuerung:	automatischer Rückruf mit oder ohne Verbindungsaufbau; Line-on-Demand (dynamische Kanalbündelung), Short-Hold-Modus, Round-Robin-Auswahl, Fast Call Back, Dial-Backup für Festverbindungen
Gebührenschatz:	Anzahl der max. Gebühreneinheiten in einem vorgegebenen Zeitraum festlegbar
Security- und Firewall-Funktionen:	Auswertung der Rufnummer der Gegenstelle; PAP und CHAP, Authentifizierungsmechanismen im PPP; automatischer Firewall-Rückruf über CLIP, PPP oder ELSA-Protokoll; Filtermöglichkeiten im IP-, IPX- und Bridge-Betrieb; Schutz der Konfiguration über Zugangslisten und Paßwort, Aufzeichnung der letzten Verbindungsinformationen, IP-Masquerading, Verschlüsselung in Vorbereitung.
IP-Masquerading:	(NAT/PAT) IP-Adreß- und Port-Umsetzung über eine IP-Adresse, statische/dynamische Zuweisung der IP-Adresse über PPP, Maskierung von TCP, UDP, ICMP, FTP; DNS-Forwarding; inverses Masquerading für IP-Dienste aus dem Intranet
Management:	via LAN, ISDN (Fernwartung) oder V.24, Managementsoftware ELSA LAN-config und ELSA LANmonitor für Windows, Konfiguration über SNMP v.1, TFTP, Telnet oder Terminal möglich
Betriebssicherheit:	Hardware-Watchdogs, regelmäßige Selbsttests, FirmSafe-Konzept für Remote-Software-Upgrade

Statistiken:	LAN- und WAN-Paketzähler, Fehler-, Verbindungs-, Zeit- und Gebührenzähler
Anzeigen/Bedienung:	LCD-Display und Tastatur, LEDs für LAN- und WAN-Status
Stromversorgung:	12 V AC mit Steckernetzteil für 230 V, 12 VA
Umgebungsbedingungen:	Temperatur: 5..40°C, Luftfeuchtigkeit: 0..80%, nicht kondensierend
Ausführung und Maße:	stabiles Metallgehäuse, Anschlüsse auf der Rückseite; Abmessungen 230 x 38 x 228 mm (B x H x T)
Lieferumfang:	Zubehör: Netzteil, ISDN-Anschlußkabel, Kabel für Outband-Schnittstelle, Twisted-Pair-Kabel (CAT-5), ausführliche Dokumentation und ELSA LAN-COM-CD-ROM Software: ELSA LANconfig, ELSA LANmonitor, ELSA LANCAPI, TFTP-Client, Bürokommunikationssoftware ELSA RVS-COM, Terminalprogramm ELSA-ZOC, Fernwartungssoftware LapLink für Windows, T-Online, CompuServe
Zulassungen:	für Deutschland, Schweiz und alle Länder der EU in Vorbereitung
Service und Garantie:	6 Jahre Garantie, ELSAcare (Vorab-Austausch innerhalb der ersten 100 Tage)
Support:	über Hotline, ELSA LocalWeb und Internet

Steckerbelegungen:

Steckverbindung	RJ11-Pin	Leitung
 a/b-Ports – RJ11	1	frei
	2	frei
	3	a
	4	b
	5	frei
	6	frei

Steckverbindung	RJ45-Pin	Leitung	IAE
 ISDN – RJ45	1	frei	frei
	2	frei	frei
	3	T+	2a
	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	frei	frei
	8	frei	frei

Allgemeine Garantiebedingungen vom 01.06.1998

Diese Garantie gewährt die ELSA AG den Erwerbern von ELSA-Produkten nach ihrer Wahl zusätzlich zu den ihnen zustehenden gesetzlichen Gewährleistungsansprüchen nach Maßgabe der folgenden Bedingungen:

1 Garantieumfang

- a) Die Garantie erstreckt sich auf das gelieferte Gerät mit allen Teilen. Sie wird in der Form geleistet, daß Teile, die nachweislich trotz sachgemäßer Behandlung und Beachtung der Gebrauchsanweisung aufgrund von Fabrikations- und/oder Materialfehlern defekt geworden sind, nach unserer Wahl kostenlos ausgetauscht oder repariert werden. Alternativ hierzu behalten wir uns vor, das defekte Gerät gegen ein Nachfolgeprodukt auszutauschen oder dem Käufer den Original-Kaufpreis gegen Rückgabe des defekten Geräts zu erstatten. Handbücher und evtl. mitgelieferte Software sind von der Garantie ausgeschlossen.
- b) Die Kosten für Material und Arbeitszeit werden von uns getragen, nicht aber die Kosten für den Versand vom Erwerber zur Service-Werkstätte und/oder zu uns.
- c) Ersetzte Teile gehen in unser Eigentum über.
- d) Wir sind berechtigt, über die Instandsetzung und den Austausch hinaus technische Änderungen (z.B. Firmware-Updates) vorzunehmen, um das Gerät dem aktuellen Stand der Technik anzupassen. Hierfür entstehen dem Erwerber keine zusätzlichen Kosten. Ein Rechtsanspruch hierauf besteht nicht.

2 Garantiezeit

Die Garantiezeit beträgt für ELSA-Produkte sechs Jahre. Ausgenommen hiervon sind ELSA-Farbmonitore und ELSA-Videokonferenzsysteme; hierfür beträgt die Garantiezeit drei Jahre. Die Garantiezeit beginnt mit dem Tag der Lieferung des Gerätes durch den ELSA-Fachhändler. Garantieleistungen bewirken weder eine Verlängerung der Garantiefrist, noch setzen sie eine neue Garantiefrist in Lauf. Die Garantiefrist für eingebaute Ersatzteile endet mit der Garantiefrist für das ganze Gerät.

3 Abwicklung

- a) Zeigen sich innerhalb der Garantiezeit Fehler des Gerätes, so sind Garantieansprüche unverzüglich, spätestens jedoch innerhalb von sieben Tagen geltend zu machen.
- b) Transportschäden, die äußerlich erkennbar sind (z.B. Gehäuse beschädigt), sind unverzüglich gegenüber der Transportperson und uns geltend zu machen. Äußerlich nicht erkennbare Schäden sind unverzüglich nach Entdeckung, spätestens jedoch innerhalb von sieben Tagen nach Anlieferung, schriftlich gegenüber der Transportperson und uns zu reklamieren.
- c) Der Transport zu und von der Stelle, welche die Garantieansprüche entgegennimmt und/oder das instandgesetzte Gerät austauscht, geschieht auf eigene Gefahr und Kosten des Erwerbers.
- d) Garantieansprüche werden nur berücksichtigt, wenn mit dem Gerät das Rechnungsoriginal vorgelegt wird.

4 Ausschluß der Garantie

Jegliche Garantieansprüche sind insbesondere ausgeschlossen,

- a) wenn das Gerät durch den Einfluß höherer Gewalt oder durch Umwelteinflüsse (Feuchtigkeit, Stromschlag, Staub u.ä.) beschädigt oder zerstört wurde;

- b) wenn das Gerät unter Bedingungen gelagert oder betrieben wurde, die außerhalb der technischen Spezifikationen liegen;
- c) wenn die Schäden durch unsachgemäße Behandlung – insbesondere durch Nichtbeachtung der Systembeschreibung und der Betriebsanleitung – aufgetreten sind;
- d) wenn das Gerät durch hierfür nicht von uns ermächtigte Personen geöffnet, repariert oder modifiziert wurde;
- e) wenn das Gerät mechanische Beschädigungen irgendwelcher Art aufweist;
- f) wenn Schäden an der Bildröhre eines ELSA-Monitors festgestellt werden, die insbesondere durch mechanische Belastungen (Verschiebung der Bildröhrenmaske durch Schockeinwirkung oder Beschädigungen des Glaskörpers), starke Magnetfelder in unmittelbarer Nähe (bunte Flecken auf dem Bildschirm), permanente Darstellung des gleichen Bildes (Einbrennen des Phosphors) hervorgerufen wurden;
- g) wenn und soweit sich die Luminanz der Hintergrundbeleuchtung bei TFT-Panels im Laufe der Zeit allmählich reduziert;
- h) wenn der Garantieanspruch nicht gemäß Ziffer 3a) oder 3b) gemeldet worden ist.

5 Bedienungsfehler

Stellt sich heraus, daß die gemeldete Fehlfunktion des Gerätes durch fehlerhafte Fremd-Hardware, -Software, Installation oder Bedienung verursacht wurde, behalten wir uns vor, den entstandenen Prüfaufwand dem Erwerber zu berechnen.

6 Ergänzende Regelungen

- a) Die vorstehenden Bestimmungen regeln das Rechtsverhältnis zu uns abschließend.
- b) Durch diese Garantie werden weitergehende Ansprüche, insbesondere solche auf Wandlung oder Minderung, nicht begründet. Schadensersatzansprüche, gleich aus welchem Rechtsgrund, sind ausgeschlossen. Dies gilt nicht, soweit z.B. bei Personenschäden oder Schäden an privat genutzten Sachen nach dem Produkthaftungsgesetz oder in Fällen des Vorsatzes oder der groben Fahrlässigkeit zwingend gehaftet wird.
- c) Ausgeschlossen sind insbesondere Ansprüche auf Ersatz von entgangenem Gewinn, mittelbaren oder Folgeschäden.
- d) Für Datenverlust und/oder die Wiederbeschaffung von Daten haften wir in Fällen von leichter und mittlerer Fahrlässigkeit nicht.
- e) In Fällen, in denen wir die Vernichtung von Daten vorsätzlich oder grob fahrlässig verursacht haben, haften wir für den typischen Wiederherstellungsaufwand, der bei regelmäßiger und gefahrenentsprechender Anfertigung von Sicherheitskopien eingetreten wäre.
- f) Die Garantie bezieht sich lediglich auf den Erstkäufer und ist nicht übertragbar.
- g) Gerichtsstand ist Aachen, falls der Erwerber Vollkaufmann ist. Hat der Erwerber keinen allgemeinen Gerichtsstand in der Bundesrepublik Deutschland oder verlegt er nach Vertragsabschluß seinen Wohnsitz oder gewöhnlichen Aufenthaltsort aus dem Geltungsbereich der Bundesrepublik Deutschland, ist unser Geschäftssitz Gerichtsstand. Dies gilt auch, falls Wohnsitz oder gewöhnlicher Aufenthalt des Käufers im Zeitpunkt der Klageerhebung nicht bekannt ist.
- h) Es findet das Recht der Bundesrepublik Deutschland Anwendung. Das UN-Kaufrecht gilt im Verhältnis zwischen uns und dem Erwerber nicht.

Konformitätserklärung



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

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

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:

This is to confirm that this product meets all essential protection requirements relating to the

Niederspannungs Richtlinie (73/23/EWG)

Low Voltage Directive (73/23/EEC)

ISDN Vorschrift (97/346/EG)

ISDN Directive (97/346/EEC)

EMV Richtlinie (89/336/EWG)

EMC Directive (89/336/EEC).

Zur Beurteilung der Konformität wurden folgende **Normen** herangezogen:

The assessment of this product has been based on the following standards

EN 50082: 1992 Teil 2: EN 61000-4-2, 3, 4, 5, 6

EN 50081: 1992 Teil 1: EN 55022B: 1994

EN 60950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997

TBR 3

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:

On behalf of the manufacturer / importer:

ELSA AG
Sonnenweg 11
D-52070 Aachen

abgegeben durch:
this declaration is submitted by:

Aachen, 8. Februar 1999

Aachen, 8th February 1999

i.V. Peter Wieninger
Bereichsleiter Entwicklung
VP Engineering

Glossar

- **10BaseT** – Twisted Pair; 10-Mbit-Ethernet-Anschlußvariante; Netzwerkanschluß mit Steckertyp RJ45
- **10Base2** – Thin Ethernet; Cheapernet; 10-Mbit-Ethernet-Anschlußvariante; Netzwerkanschluß mit Steckertyp BNC
- **10Base5** – Thick Ethernet; 10 MBit-Ethernet-Anschlußvariante; Netzwerkanschluß mit Steckertyp AUI oder SUB-D 15polig
- **100BaseTX** – Twisted Pair; 100-Mbit-Fast-Ethernet-Anschlußvariante; Netzwerkanschluß mit Steckertyp RJ45
- **1TR6** – nationales ISDN; ehemals verbreitetes D-Kanal-Protokoll im deutschen ISDN; wird von der deutschen Telekom nur noch auf besonderen Antrag hin eingerichtet.
- **ARP** – Adress Resolution Protocol ist ein Protokoll der →TCP/IP-Protokoll-Familie. Durch ARP werden IP-Adressen auf zugehörige MAC-Adressen abgebildet.
- **Asynchrone Übertragung** – Bei der seriellen Datenübertragung wird ein Verfahren zur Herstellung des Gleichlaufs zwischen Sender und Empfänger benötigt, um den Empfänger in die Lage zu versetzen, Anfang und Ende eines übertragenen Zeichens zu erkennen. Zu dieser Strukturierung wird bei der asynchronen Übertragung jedes zu sendende Byte mit einem Startbit und einem oder zwei Stopbits markiert. Dieses Start-Stop-Verfahren gehört besonders im Bereich der Microcomputer zu den am häufigsten verwendeten Übertragungsverfahren, da es technisch, im Gegensatz zur synchronen Übertragung, relativ einfach zu realisieren ist.
- **AUI** – Attachment Unit Interface = Schnittstelle für allgemeine Netzwerkanschlüsse.
- **B-Kanal** – Datenübertragungskanal im ISDN (64Kbit); ein ISDN-Basisanschluß hat 1 D-Kanal und 2 B-Kanäle.
- **Basisanschluß** – ISDN-Teilnehmeranschluß mit zwei →Basiskanälen (je 64.000 bit/s) und einem Signalisierungskanal (16.000 bit/s). Schnittstelle des Basisanschlusses zum Teilnehmer ist die →S₀-Schnittstelle.
- **BNC** – Gängige Anschlußtechnik für Cheapernet (Thin-Ethernet). Dieser Anschluß wird auch T-BASE2 genannt. Zum Anschluß von Geräten mit BNC-Buchsen muß ein T-Verbindungsstecker eingesetzt werden.
- **Bridge** – Eine Bridge (Brücke) ist eine Verbindung zweier Netzwerke mit gleicher Layer-2-Struktur im →OSI-Modell. Eine solche Bridge kann aus zwei Geräten bestehen, die über eine Datenübertragungs-Strecke miteinander verbunden sind. Diese Konstellation wird Remote-Bridge genannt.
- **Broadcast** – Broadcasts sind spezielle Datenpakete, die an alle empfangsbereiten Stationen gerichtet sind. Im Ethernet-Netzwerk sind diese Datenpakete durch die Zieladresse FFh FFh FFh FFh FFh FFh (d.h. an alle) gekennzeichnet.
- **Burst Mode** – Burst Mode ist eine spezielle Art des Datenpakettransportes in Novell-Netzwerken, bei dem mehrere Datenpakete hintereinander ohne Empfangsbestätigung übertragen werden.

- **CEPT** – Conférence Européenne des Postes et des Télécommunications = europäisches Gremium zur Festlegung von Normen für die Telekommunikation.
- **Client** – Client = Arbeitsplatzrechner. Ein Client ist ein Nutzer eines von einem →Server angebotenen Dienstes.
- **CLIP** – Caller Line Identification Parameter = Rufnummer des Anrufers, die im ISDN mit übertragen werden kann.
- **Datenkompression** – Methode zur Reduktion der zu übertragenden Datenmenge; mit Datenkompression kann man den Durchsatz über einen Verbindungsweg erhöhen (bekannte Verfahren: V.42bis, STAC, MPPC)
- **D-Kanal** – Signalisierungskanal im ISDN (Anwahl, Rufnummernübermittlung, Gebühreninformationen, Auf- und Abbau); ein ISDN-Basisanschluß hat 1 D-Kanal und 2 B-Kanäle.
- **Datenpaket** – Ein Datenpaket enthält eine vom Datennetz vorgeschriebene Anzahl von Zeichen (Steuerbefehlen) zur Übermittlung von Daten.
- **DNS** – Domain Name Server. Bezeichnet einen Server, der für jeden Rechner einer →Domäne einen Namensdienst zur Verfügung stellt. Durch Anfrage bei diesem Server kann eine andere Maschine, die nur den symbolischen Namen ihres Ziels kennt, die zugehörige IP-Adresse erfahren.
- **Domäne** – (engl. Domain) Als Domäne wird ein logisch begrenzter Netzwerkverbund bezeichnet, z.B. Firmennetze oder Internet-Provider.
- **DSS1** – Euro-ISDN; heutzutage gängiges D-Kanal-Protokoll im ISDN
- **dynamische Kanalbündelung** – Bandwith-on-Demand; je nach Bedarf wird durch automatische Zunahme des 2. (oder auch mehr) B-Kanals die Bandbreite erhöht.
- **DSS1** – Vom →ETSI erarbeiteter europäischer Standard für das D-Kanal-Protokoll (auch Euro-ISDN). Seit Ende 1993 ist dieser Standard in Deutschland eingeführt und soll den FTZ-Standard 1TR6 ersetzen. Für eine Übergangszeit sind ISDN-Anschlüsse verfügbar, die beide Standards unterstützen.
- **EAZ** – Die EAZ = Endgeräteauswahlziffer dient beim 1TR6-Protokoll der Unterscheidung verschiedener Endgeräte, die am gleichen →Basisanschluß des ISDN angeschlossen sind. Diese Ziffer wird vom Anrufer als letzte Ziffer an die Rufnummer angehängt.
- **Ethernet-Netzwerk** – Ein Ethernet-Netzwerk ist ein →Bussystem mit →CSMA/CD-Zugriff und →Basisbandübertragung. 1979 wurde dieses lokale Netzwerk von den Firmen DEC, Intel und Xerox entwickelt. Als eines der ersten →LANs wurde es zum De-Facto-Standard und vom IEEE (Institute of Electrical and Electronics Engineers) als Standard übernommen (Norm 802.3). Die Übertragung erfolgt auf Koax-, Twisted Pair-, Lichtwellenleiter oder anderen Übertragungsmedien mit 10 Mbit pro Sekunde.
- **ETSI** – European Telecommunications Standards Institute = Europäisches Institut für Telekommunikationsstandards. Von diesem Normungsgremium wurde ein europäischer Standard für das D-Kanal-Protokoll erarbeitet (DSS1).
- **Firewall** – Schutzmechanismen für ein Intranet gegen Zugriffe von außen; das *ELSA LANCOM* unterstützt die Firewall-Mechanismen IP-Masquerading, Portfilterung, Accessliste.
- **Flash-ROM** – Ein Flash-ROM ist ein elektrisch lösch- und wiederbeschreibbarer Fest-

wertspeicher. Flash-ROMs werden häufig in Geräten eingesetzt, deren Firmware durch Updates erweitert werden kann.

- **Gateway** – Netzwerkkomponente, die auf einem Layer des → OSI-Modells Zugang zu anderen Netzwerkkomponenten bietet (z.B. in Windows 95 auf Layer 3).
- **HDLC** – High Level Data Link Control. Format eines Datenpaketes, das über eine CRC-Berechnung gesichert wird.
- **HOPS** – Anzahl der Router, über die eine Netzwerkverbindung aufgebaut wurde.
- **Hub** – Netzwerkkomponente; Verteiler; Kollektor; auch zur Umsetzung von einem Anschluß-Typ auf einen anderen; ein Netzwerk-Eingang – mehrere Netzwerkausgänge zur sternförmigen Verteilung
- **Internet** – Das Internet ist ein Zusammenschluß aller Netzwerke, die über →TCP/IP miteinander verbunden sind.
- **Intranet** – Domäne; Netzwerk, das nur auf z.B. die eigene Firma begrenzt ist und nur ge-regelten Zugriff von außen und nach außen zuläßt.
- **IP** – Internet Protocol ist eine Anfang der siebziger Jahre vom DoD (Department of Defence) entwickelte umfangreiche Protokoll-Familie zur Verbindung heterogener Wide Area Networks.
- **IPX** – Internet Packet eXchange = ein von Novell definiertes Transportprotokoll zur Übertragung von Daten über ein Netzwerk. Auf einem PC wird dieses Protokoll durch den Treiber IPX.COM bzw. die →VLM-Shell realisiert.
- **IP-Adresse** – 1. Teil der Adresse, mit der sich eine Netzwerkkomponente im TCP/IP-Netz identifiziert.
- **IP-Netzmaske** – 2. Teil der Adresse, mit der sich eine Netzwerkkomponente im TCP/IP-Netz identifiziert.
- **IP-Masquerading** – Singel IP-Adresse; Port Adress Translation; Verfahren zur Anbindung eines Intranets (mehrere Workstations) ans Internet über eine einzige IP-Adresse; das *ELSA LANCOM* beherrscht dieses Verfahren.
- **IPX** – Internet Paket eXchange; Transport-Protokoll; Netzwerkprotokoll, wird vornehmlich Novell-Netzen eingesetzt.
- **IPX-Adresse** – besteht aus → Node-ID, IPX-Netzwerk-Adresse und Socket; dient der eindeutigen Bestimmung einer Netzwerkkomponente innerhalb eines IPX-Netzwerkes.
- **IPX-Watchdog** – Pakete, die zur Überwachung einer Workstation vom Server in bestimmten Zeitintervallen verschickt werden. Antwortet eine Workstation nicht, wird diese automatisch abgemeldet.
- **ISDN** – Integrated Services Digital Network = Dienstintegrierendes digitales Telekommunikationsnetz.
- **ISO** – International Standardization Organization. Die ISO ist eine internationale Organisation, die die Entwicklung weltweiter Normen – für alle Sachgebiete – koordiniert und für deren Veröffentlichung sorgt. Ihre Mitglieder sind die nationalen Normungsinstitute wie beispielsweise DIN (Deutschland), ANSI (USA), BSI (Großbritannien) oder AFNOR (Frankreich).
- **ITU-T** – Der Standardisierungssektor Telekommunikation der International Telecommunications Union (ITU) befaßt sich mit der Standardisierung der Daten- und Fernsprechdienste. Die ITU-T-Empfehlungen der V.-Serie behandeln u.a. die Datenübertragung im Telefonnetz. ITU-T ist die Nachfolgeorganisation

des CCITT (Comité Consultatif International Télégraphique et Téléphonique).

- **Kanalbündelung** – Bündelung beider B-Kanäle im ISDN zu einer logischen Verbindung, um die Übertragungsgeschwindigkeit zu verdoppeln
- **LAN** – Local Area Network (Lokales Netzwerk). Laut →ISO ist ein lokales Netzwerk ein innerhalb von Grundstücksgrenzen unter rechtlicher Kontrolle des Benutzers befindliches Netzwerk für die bitserielle Übertragung von Informationen zwischen dessen unabhängigen, miteinander gekoppelten Elementen. Ein lokales Netzwerk ist also ein örtlich stark eingeschränktes Netzwerk, das meistens innerhalb eines Gebäudes oder eines Firmensitzes installiert ist.
- **Layer** – Schicht, Ebene (s. OSI-Modell); Schicht innerhalb einer modular aufgebauten Verbindung zwischen zwei kommunizierenden Systemen
- **Line-on-Demand** – Verbindungsaufbau auf Anforderung. Bei dem *ELSA LANCOM* entscheidet der Inhalt empfangener Datenpakete vom LAN über einen Verbindungsaufbau.
- **MAC** – Media Access Control = Zugriffssteuerung auf das Medium. Von der →ISO definierte Unterebene der Schicht 2 des ISO-Modells. Bei Ethernet-Netzwerken gehören die Quell- und Ziel-Adresse sowie der Protokolltyp zu den MAC-Layer-Daten.
- **MPPC** – Microsoft Point to Point Compression; Verfahren zur Datenkompression (zur Zeit vom *ELSA LANCOM* nicht unterstützt)
- **MPR** – Multi-Protokoll-Router; Router (wie das *ELSA LANCOM Business 4100*), der mehrere Protokolle routen kann
- **MSN** – Multiple Subscriber Number = Mehrfachrufnummer. Beim DSS1-Protokoll können einem ISDN-Anschluß mehrere Rufnummern von der zuständigen Vermittlungsstelle zugewiesen werden. In der Regel sind dies drei Rufnummern, maximal jedoch acht. Über diese Rufnummern können, ähnlich wie beim 1TR6-Protokoll über die EAZ, gezielt Endgeräte an der S₀-Schnittstelle angesprochen werden. Im Gegensatz zur eingestellten EAZ, die an die eigentlichen Rufnummern angehängt wird, kann die MSN aus maximal 16 Ziffern bestehen.
- **Multicast** – Multicasts sind spezielle Datenpakete, die an alle empfangsbereiten Stationen einer Gruppe gerichtet sind.
- **Multilink-PPP** – MLPPP; Verfahren zur Kanalbündelung unter PPP; (*ELSA LANCOM* unterstützt dies zur Zeit nicht)
- **NBNS** – Net Bios Name Server. Bezeichnet einen Server, der für jeden Rechner einer →Domäne einen Namensdienst zur Verfügung stellt. Durch Anfrage bei diesem Server kann eine andere Maschine, die nur den symbolischen Namen ihres Ziels kennt, die zugehörige Adresse erfahren.
- **Netzwerk** – Ein Netzwerk ist ein Mehrbenutzer- und Mehrfunktionssystem einer Gruppe von Computersystemen und Terminals zur gemeinsamen Nutzung von Informationen und Ressourcen, die über Kommunikationsleitungen miteinander verbunden sind.
- **NETX** – NETX = NetWare-Shell. Dieses Programm stellt eine Schnittstelle zwischen Anwendungsprogrammen und dem Netzwerkbetriebssystem von Novell dar.
- **Node** – Node = Knoten. Als Node wird ein an das Netzwerk angeschlossenes Gerät bezeichnet, das Daten empfängt oder sendet. Dieses können einzelne *ELSA LANCOMs*, Rechner, Server oder Drucker sein, die von

mehreren Netzteilnehmern angesprochen werden.

- **Node-ID** – MAC-Adresse
- **Novell** – Hersteller des Netzwerk-Betriebssystems Novell NetWare
- **OSI** – Open System Interconnection = offene Kommunikationssysteme. Von der →ISO (International Standardization Organization) entwickeltes Referenzmodell für Netzwerke zur Festlegung der Schnittstellen-Standards zwischen Computerherstellern für den Bereich der Hard- und Software-Anforderungen.
- **Outband-Konfiguration** – Bei der Outband-Konfiguration, oder auch Out-of-Band-Konfiguration, erfolgt der Datenaustausch mit dem zu konfigurierenden Gerät über eine serielle V.24-Schnittstelle. Die Konfigurationsverbindung bleibt auch bei Störungen eines Netzan schlusses erhalten.
- **Ping** – Befehl über ICMP; ähnlich dem Ping (Echolot) von U-Booten, wird durch diesen Befehl die Entfernung einer Netzwerkkomponente im TCP/IP-Netzwerk bestimmt
- **PPP** – Point to Point Protocol; Protokoll-Familie (LCP, IPCP, IPXCP, CBCP, ECP, CCP usw.); Protokoll zur Aushandlung von Verbindungsparametern bei einer Punkt-zu-Punkt-Verbindung von Netzwerkkomponenten (z.B. Rückruf, Netzwerk-Protokolle, Kompression)
- **Protokoll** – zum Aufbau und zur Sicherung von Verbindungen (Netzwerk, ISDN, analoge Verbindungsarten); Dialog zwischen verbundenen Komponenten
- **Proxy-ARP** – Mit Proxy-ARP wird erreicht, daß Stationen, die normalerweise direkt an ein lokales TCP/IP-Netzwerk angeschlossen werden und deshalb eine lokal passende IP-Adresse besitzen, auch über einen Router (also über eine WAN-Verbindung) erreichbar sind. Der Router gibt sich bei einer ARP-Rundfrage im lokalen Netzwerk als das entfernte Gerät aus, gibt also seine eigene MAC-Adresse preis. Anschließend kann er die Datenpakete empfangen und zur Remote-Seite schicken.
- **RIP** – Routing Information Protocol; dient in Netzwerken (hier Netware-IPX) zur Verbreitung von Informationen für Router.
- **Round-Robin** – Ein Verfahren zur Anwahl einer logischen Gegenstelle (z.B. Konzernzentrale) über verschiedene Rufnummern auf unterschiedlichen Geräten. Dabei wird, falls die Standard-Gegenstelle besetzt ist, automatisch auf weitere freie Gegenstellen ausgewichen.
- **Router** – Ein Router ist ein Gerät zur Verbindung zweier Netzwerke mit gleicher Layer-3-Struktur im →OSI-Modell. Ein solcher Router kann aus zwei Geräten bestehen, die über eine Datenübertragungstrecke miteinander verbunden sind. Diese Konstellation wird auch Remote-Router genannt.
- **RTS** – Request to Send = Sendeteil anschalten
- **S₀-Leistungsanschluß** – Schnittstelle des Basisanschlusses zum Teilnehmer. Bei dieser Schnittstelle handelt es sich um einen Bus, an den bis zu acht ISDN-Endgeräte angeschlossen werden können. Bis zu 12 Steckdosen können an diesem Bus installiert sein.
- **SAP** – Service Advertising Protocol. Wird in NetWare-Netzwerken zur Verbreitung von Diensten verwendet.
- **Server** – Ein Server ist ein Anbieter von Dienstleistungen, die von einem →Client in Anspruch genommen werden. Viele Netzwerk-Betriebssysteme verfügen über eine Client-Server-Architektur, d.h., daß ein speziel-

ler, sehr leistungsfähiger Rechner als Server arbeitet, von dem eine große Anzahl von Clients (Arbeitsplatzrechnern) Daten und Programme beziehen.

- **Short-Hold-Modus** – Nach einer vorher definierbaren Zeit wird eine Verbindung abgebaut, wenn keine Daten mehr übertragen werden müssen. Damit kann erreicht werden, daß die Verbindung eine zeitlang bestehen bleibt, bis keine Daten mehr übertragen werden.
- **SNMP** – Simple Network Management Protocol; genormtes Protokoll zum Management von Netzwerkkomponenten; Vorteil: Kontrolle verschiedener Netzwerkkomponenten über ein und dieselbe Oberfläche (z.B. HP-Openview oder Cabletron-Spectrum); herstellerunabhängig; *ELSA LANCOM* unterstützt SNMP-Version 1
- **Socket** – Kennnummer, die den Dienst bezeichnet unter dem ein Datenpaket gesendet wird
- **Spoofing** – Das Spoofing ist eine Methode, die eingesetzt wird, um unnötig anfallende Verbindungskosten zu vermeiden. Dabei werden Anfragen von der LAN-Seite direkt vom Router beantwortet, ohne daß ein Verbindungsaufbau zur Versendung von Daten an die Gegenseite stattfindet.
- **SPX** – Sequenced Packet eXchange = ein von Novell definiertes Protokoll zur gesicherten Übertragung von Daten im Netzwerk. Auf einem PC wird dieses Protokoll durch den Treiber NETX.COM (o.ä.) realisiert.
- **SPX-Watchdog** – Pakete, die zur Überwachung einer SPX-Verbindung vom Server in bestimmten Zeitintervallen verschickt werden.
- **SPV** – Semipermanente Verbindung = vorbestellte Dauerwählverbindung. Eine semipermanente Verbindung wird zur Zeit für das →1TR6-Protokoll angeboten und kann zwischen zwei beliebigen ISDN-Anschlüssen eingerichtet werden. Die Einrichtung erfolgt dabei für jeden B-Kanal getrennt. Sobald die semipermanente Verbindung aktiv ist, wird nicht mehr im Zeittakt abgerechnet, sondern über einen monatlichen Pauschalbetrag. Dadurch können im Einzelfall Gebühren gespart werden.
- **STAC-Kompression** – Verfahren zur Datenkompression
- **Stand-alone-Lösung** – Das *ELSA LANCOM Business 4100* ist eine solche Stand-alone-Lösung, weil man zur Netzwerkkopplung keinen zusätzlichen Rechner einrichten oder zusätzliche Software auf einem Server installieren muß, wie es bei herkömmlichen Routern der Fall war, d.h., er ist eine eigene Netzwerkkomponente.
- **Standleitung** – Eine Standleitung ist eine feste (stehende) Verbindung zwischen zwei Teilnehmern, die ausschließlich von diesen beiden Teilnehmern genutzt werden kann.
- **Steuerkanal** – ISDN-Signalisierungskanal (auch →D-Kanal), zur Übertragung von Steuerinformationen (z.B. die Meldung eines ankommenden Rufes o.ä.) zwischen ISDN-Anschluß und Vermittlungsstelle mit einer Übertragungskapazität von 16.000 bit/s bei →Basisanschlüssen bzw. 64.000 bit/s bei →Primärmultiplexanschlüssen. Wird auch als D-Kanal bezeichnet.
- **Synchrone Übertragung** – Die synchrone Übertragung ist wie die →asynchrone Übertragung ein Verfahren zur Herstellung des Gleichlaufs zwischen Sender und Empfänger. Bei diesem Datenübertragungsformat wird

der Gleichlauf im Gegensatz zur asynchronen Übertragung nicht durch Start- und Stopbits für ein ganzes Zeichen, sondern durch Taktimpulse für jedes einzelne Bit hergestellt. Dadurch, daß keine Start- und Stopbits zusätzlich übertragen werden, ist die synchrone Übertragung zwar schneller, technisch jedoch wesentlich aufwendiger zu realisieren.

- **TCP/IP** – Transmission Control Protocol/Internet Protocol. Eine Anfang der siebziger Jahre vom DoD (Department of Defence) entwickelte umfangreiche Protokoll-Familie zur gesicherten Verbindung heterogener Wide Area Networks. Die beiden Fundamente dieser Protokoll-Familie sind das IP, welches die Schicht 3 des →OSI-Modells implementiert und dessen Analogon TCP für die vierte Schicht.
- **Telnet** – Telnet ist ein Protokoll aus der →TCP/IP-Protokoll-Familie. Es ermöglicht den Fernzugriff von einer Workstation auf ein anderes im Netzwerk befindliches Computersystem. Das Telnet-Protokoll verwendet zur Datenübertragung das →TCP-Protokoll, da es eine gesicherte bidirektionale Kommunikation benötigt. Einem Telnet-Client wird so ein virtuelles Terminal auf dem Telnet-Host zur Verfügung gestellt.
- **TFTP** – Trivial File Transfer Protocol; einfaches Protokoll zur Übertragung einer Datei (z.B. Firmware-Upload, Konfiguration sichern/wiederherstellen)
- **TICS** – Systemzeiteinheit des *ELSA LANCOMs*
- **Transceiver** – Transceiver = Signalwandler. Ein Transceiver ist ein Gerät, das ein EingangssignalfORMAT auf ein anderes Ausgangsformat umwandelt.
- **UDP** – User Datagram Protocol = Trägt zur Übertragung von Daten von bestimmten Dien-
- sten in IP-Netzwerken bei, sorgt allerdings im Gegensatz zu TCP nicht für eine gesicherte Datenübertragung.
- **UNIX** – UNIX ist ein Betriebssystem für leistungsfähige Microcomputer, Computer und Großrechner, das von AT&T entwickelt wurde.
- **V.24 Schnittstelle** – serielle Schnittstelle; Schnittstelle z.B. zum Anschluß eines Modems; das *ELSA LANCOM* besitzt eine V.24-Schnittstelle, um auch mit einem angeschlossenen Modem eine analoge Einwahl zu bieten.
- **V.42bis** – Empfehlung des →ITU-T zur Komprimierung von Daten innerhalb eines Datenstroms.
- **V.110** – Empfehlung des →ITU-T zur Anpassung serieller asynchroner und synchroner Datenströme an die ISDN-Bitrate von 64 Kbit pro Sekunde zur Übertragung im ISDN-→B-Kanal (wird auch I.463 genannt).
- **VLM** – Virtual Loadable Module = Dieses Programm stellt die Schnittstelle zwischen Anwendungsprogrammen und dem Netzwerkbetriebssystem von Novell dar.
- **WAN** – Wide Area Network = Weitverkehrsdatennetze wie beispielsweise Verbindungen über ISDN-Geräte.
- **Workstation** – Bezeichnung für einen Arbeitsplatzrechner.
- **X.75** – Empfehlung des →ITU-T zur gesicherten Übertragung von Daten nach dem HDLC-Übertragungsformat im ISDN-→B-Kanal
- **XModem** – XModem ist ein →Übertragungsprotokoll mit automatischer Fehlererkennung und Fehlerkorrektur. Die Datenübertragung erfolgt in Blöcken mit einer Größe von 128 Bytes. Wird ein Übertragungsfeh-

ler erkannt, wird der fehlerhafte Block erneut gesendet. XModem gehört zu den weltweit meistverwendeten Protokollen. Es wird von vielen Standard-Terminalprogrammen unterstützt, wurde aber inzwischen in seiner Leistungsfähigkeit von moderneren Protokollen wie ZModem überholt.

- **Y-Verbindung** – Gleichzeitige Verbindung zu zwei unterschiedlichen Gegenstellen über je einen B-Kanal des selben ISDN-S₀-Leistungsanschlusses.

Index

■ Numerics

10/100Base-TX	10
100BASE-T	R-51
100Mbit-Netz	10
1TR6	3, R-41
802.2	R-52
802.3	R-52

■ A

Abbau	R-49
Adapter	14
Administrator	R-71
Adreß-Pool	80, 85, 97, R-73
Adreßverwaltung	78
Adreßzuweisung	15
Aging	R-57, R-59
Amtsholung	R-43
Anlagenanschluß	3
Anrufbeantworter	1, 2
Anschluß	R-50
Anschlüsse	9
Anwahlpräfix	R-43
AOCD	4, 40
APPP	R-45
ARP-Aging-Min	R-63
ARP-Cache	R-63
ARP-Tabelle	R-63
asynchrones PPP	R-45
Aufbau	R-49
Auslandsgespräche	102
Ausschluß-Routen	70
Authentifizierung	58, R-47
automatischer Zeitabgleich	106
Automode	79
Auto-Modus	R-73

■ B

Backoff	R-55
BACP	3
Benutzername	18, 38
Betriebsarten	35

Betriebszustände	8
Binding	R-52
B-Kanal	32
Verbindungszustand	4
B-Kanal-Protokoll	38, R-44
Brute-Force	5, 36
Bürokommunikation	97

■ C

Cache	R-63
Call-by-Call	102, 103, R-80
Calling Line Identification Restriction	R-41
CAPI Faxmodem	102
CAPI-Schnittstelle	97
CBCP	57
CE	10
Challenge Handshake Authentication Protocol	38, R-47
CHAP	38, R-47
CLI	38, R-47
Client für Windows-Netzwerke	91
CLIP	5
CLIR	R-41
Common ISDN Application Programming Interface	97
Communities	25
Compuserve	95
Compuserve-Anwahl	96
Conf.-Haltezeit	R-78

■ D

D64S	48
D64S2	48
D64SY	48
Datei- und Druckerfreigabe	92
Datenkompression	R-46
Datenkompressionsverfahren	
LZS	60
Datenübertragung	60
Datenübertragung im IPX-Netz	64
Default-Layer	18

DFÜ-Netzwerk 13, 16, 38
 DHCP 7, 78, R-72
 DHCP für WINS-Auflösung 82
 DHCP-Automode 79
 DHCP-Server 7, 15, 79, 86, R-72
 Konfiguration 83
 Dienst 86
 Display 4, 8
 Distanz einer Route 69
 D-Kanal 38
 DNS 78, 86, R-62
 DNS-Anfrage R-67
 DNS-Backup R-62
 DNS-Forwarding 77, R-62
 DNS-Forwarding-Mechanismus 87
 DNS-Server 7, 78, 81, 86
 Filterliste 89
 Filtermechnismus 87
 verfügbare Informationen 87
 Domain Name Service 78, 86
 Domains 86
 Domains sperren 89
 DSS1 3, R-41
 Durchsatz 60
 Durchwahlnummern R-44
 Dynamic Host Configuration Protocol 79
 dynamische Bündelung R-43
 dynamische IP-Routing-Tabelle R-69
 Dynamische Kanalbündelung 60
 dynamische Kanalbündelung 3
 dynamische Zuweisung der IP-Adresse . R-64
 dynamischer Short-Hold R-42
 dynamisches Routing 68

E

Einwahlknoten 3
 Einwahlzugang 97
 ELSA CAPI Faxmodem 6
 ELSA-RVS-COM 2
 ELSA-ZOC 2
 E-Mail 2
 Encaps R-45
 End-Adresse 80

Ende-Adreß-Pool R-72
 erreichbare Rechner 96
 Ethernet 3
 10/100Base-T 3
 Fast-Ethernet 3
 Ethernet-Header R-45
 Ethernet-Paketformat R-52
 EuroFileTransfer 6
 Exponential-Backoff R-55

F

Fast Call Back 39
 fast Callback R-43
 Fast-Ethernet 3
 10/100Base-T 3
 Fax 1, 2, 6, 102
 Fax Class 1 7, 102
 Faxmodem 6
 LANCAPi 102
 Faxtreiber 7, 102
 Faxübertragung 102
 Fehlersuche 31
 Feiertage 103
 Ferngespräche 103
 Fernkonfiguration 6, 13
 Fernverbindung 17
 Fernzugang 16
 feste IP-Adresse 115
 Festverbindung 110, 116, R-45
 Festverbindungen 2, 121
 einstellen 48
 Filetransfer 2
 Filter 37
 Filtermechanismen 2, 121
 Firewall 5, 110
 Firewall-Funktion 39, R-67
 Firewallfunktion 98
 FirmSafe 6, 21
 Firmsafe R-83
 Firmware 6, R-83
 Firmware-Upload 22, R-83
 mit LANconfig 22
 mit Terminal-Programm 22

- mit TFTP 23
- Flash-ROM-Speicher 6, 21
- Freigabe 93
- freigegebene Ressourcen 93
- **G**
- Gateway 39, 78, 81
- Gebühr R-43
- Gebühren 39, 90, R-53, R-57
- Gebührenbegrenzung 39
- Gebühreneinheit R-42
- Gebühreneinheiten 40, 60
- Gebühreninformation 4, 40
- Gebühreninformationen 60, R-42
- Gebührenmanagement 39
- Gebührenschatz 4
- Gebührenüberwachungsfunktion 98
- Gegenstellen-Tabelle R-75
- Gerätename R-42
- Gerätenamen R-42
- Geschwindigkeit R-46
- Gruppen 90
- Gruppentabelle R-76
- GSM 7
- Gültigkeitsdauer 79, 82
- **H**
- Haltezeit 60
- Haltezeiten R-42
- HDLC56K R-46
- HDLC64K R-46
- HDLC-Paket R-45
- Heap-Reserve R-51
- hohe Telefonkosten 39
- Home-Office 2, 131
- Host 86
- Host-Tabelle R-76
- Hub 10
- Hyperterminal 14
- **I**
- ICMP R-66, R-71
- ICMP-Routing-Methode R-68
- Identifikation 92, R-38
- Identifizierung des Anrufers 37
- Inband 13, 15
 - mit Telnet 16
 - Voraussetzungen 15
- Inband-Konfiguration 13
- Installation 3
- Interface-Liste R-39
- Interface-Tabelle 49
- interne Uhr 106
- Internet 2, 39
- Internet-Access 55
- Internet-Account 110
- Internet-Adresse 76
- Internet-Anwendungen 110
- Internet-Service-Provider 1
- Internet-Zugang einrichten 111
- Intranet-Adresse 76, R-61
- Intranet-Maske R-61
- inverses IP-Masquerading 115
- inverses Masquerading R-70
- IP Masquerading 39
- IP-Adresse 15, 32, 39, 55, R-60
- IP-Adressen 7
- IP-Adreß-Pool 97
- IP-Broadcast R-69
- IP-Filter 91
- IP-Header R-68
- IP-Masquerading 2, 5, 37, 75, 111, R-64, R-70
 - einfaches Masquerading 77
 - unterstützte Protokolle 77
- IP-Multicast R-69
- IP-Netzmaske R-60
- IP-Pooling 3, 97
- IP-Routing
 - Filter 71
 - FTP 71
 - Telnet 71
- IP-Routing-Tab R-64
- IP-Routing-Tabelle 68
- IPX Watchdogs 67
- IPX-Adressierung 62
- IPX-Router R-52
- IPX-Routing

- Backoff 63
- Binding 62, 63
- Exponential Backoff 65
- Filter 66
- Gegenstelle 63
- Hops 64
- Loop-Propagieren 65
- Netzwerk 63
- Propagate 63
- RIP- und SAP-Tabellen 64
- Tics 64
- IPX-Routing-Tabelle 63
- IPX-Watch R-53
- IP-Zugangsliste 15
- ISDN-Kabel 3
- ISDN-Layer R-44
- ISDN-Wählleitungen 39
- ISDN-Zeit 5, R-6
- K**
- Kanalanzeige 33
- Kanalbündelung 3, 60, R-45, R-46
 - Dynamisch 60
 - dynamische 3
 - Statisch 60
 - statische 3
- keine Gebühreninformationen 40
- Kennwörter 93
- Kompatibilität R-44
- Kompression 3
- Konfiguration 5
 - Befehle 20
 - SNMP 25
 - Verfahren 13
- Konfigurationsmöglichkeiten R-77
- Konfigurationsrufnummer 18
- Konfigurations-Schnittstelle 13
- Konfigurationszugriff 18
- Kontrollausgaben 97
- Kosten begrenzen 39
- L**
- LAN-Anschluß 3
- LANCAPi 1, 2, 6, 17, 97, R-78
- LANCAPi-Client 98
- LANCAPi-Server 100
- LAN-Coll 9
- LAN-Config R-78
- LANconfig 5, 13, 15, 17, 22, 31
 - Assistenten 15
- LAN-Filtertab. R-56, R-58, R-66
- Langner openISDN config
 - Assistenten 15
- LAN-LAN-Kopplung 2
- LAN-LAN-Kopplungen 120
- LAN-Link 9
- LANmonitor 4, 27, 31, 106
- LAN-Rx 9
- LAN-Tx 9
- Layer-Liste 50
- Layer-Name R-45
- Layername R-43
- LCP-Echo-Reply 54
- LCP-Echo-Request 54
- LCR 5, 40, 103, R-80
- LCR-Tabelle 103
- Least-Cost-Router 102, 105
 - automatischer Rückfall 105
 - Betriebsarten 105
 - Gebührenüberwachung 105
- Least-Cost-Routing 5, 40
- LED 8
- LED-Anzeigen 4
- Line-Management 2, 121
- Link-Status-LED 10
- Login 21
- Login-Fehler R-78
- Login-Sperre 36, R-78
- Login-Versuche 36
- Lok.-Routing R-53, R-67
- LOOP-propagieren R-54
- Looser R-43
- LZS-Datenkompression 60
- M**
- MAC-Adresse R-50
- Mailserver 89

Management-Information-Base 27
 Manager 27
 manueller Verbindungsaufbau R-49
 Masquerading R-61, R-64, R-70
 Maximale-Verb. R-78
 Mehrgeräteanschluß 3
 Mehrkanalverwaltung 3
 Meldungen 8
 MIB 25
 MLPPP 3, 60
 Modembetrieb R-45
 Multilink PPP 52
 Multilink-PPP 60

■ N

Name R-38
 Namen 90
 Namen und Gruppenbezeichnung 92
 Namenliste R-42
 Namenräume 90
 Namensinformationen 90
 Namensüberprüfung R-48
 Name-Server R-62
 NAT 37, 39, 75
 NBNS 90, R-62
 NBNS-Backup R-62
 NBNS-Server 78, 81, 82
 NetBIOS 7, 87, R-53
 Gegenstelle 94
 IP-Filter 94
 LAN-LAN-Kopplung 94
 Netzwerkprotokoll 91
 Remote Access 95
 TCP/IP 91
 NetBIOS Name Server R-62
 NetBIOS Propagated Frames R-55
 NetBIOS-Gegenstellen 90
 NetBIOS-Nameserver 90
 NetBIOS-Netze 87
 NetBIOS-Ports 91
 NetBIOS-Proxy 89
 NetWare-Server R-52
 Network Information Center 75

Netzbetreiber 102
 Netzkennziffer 102
 Netzwerk R-52
 Netzwerk-Adresse R-54
 Netzwerkanschlusses R-50
 Netzwerknamen 86
 Netzwerkumgebung 96
 Netzwerk-Verbindung 1
 NIC 75
 Node 10
 Node/Hub-Umschalter 10
 Node-ID R-51
 Novell R-54
 NT-Domaene R-75
 Nummernliste R-47

■ O

Objekte 26
 Online-Banking 1
 Online-Medien 15
 Online-Recherchen 2
 Ortsgespräch 104
 Ortsnetz 104
 Ortstarif 104
 Outband 13
 Voraussetzungen 14
 Outband-Konfiguration 13, 14

■ P

PAP 38, R-47
 Passw.Zwang R-78
 Password Authentication Protocol ... 38, R-47
 Paßwort 19, 32, 37, 38, 53, R-47, R-61
 Paßwortschutz 5, 36
 PAT 37, 39, 75
 Peer-to-Peer-Netzwerke 7
 Periode 39
 Point-to-Point Protocol R-45
 Policy Based Routing 110
 Port 100
 Port-Nr. 77
 Power 8
 PPP 5, 6, 32, 38, 60, R-45, R-46, R-48
 Leitungsüberprüfung mit LCP 54

- Rückruf-Funktionen 56
- Zuweisung von IP-Adressen 55
- PPP LCP Extensions 59
- PPP-Client 13, 17
- PPP-Liste 37
- PPP-Verbindung 13, 18
- PPP-Verhandlung 18, R-61
- Preselection 102
- Prioritätensteuerung 101
- Private Address Spaces R-64
- Propagated Frames 66, R-55
- Provider 102
- Proxy 7
- Proxy-ARP R-64, R-65, R-67
- Pufferspeicher R-50
- Punkt-zu-Mehrpunkt-Konfiguration 3
- Punkt-zu-Punkt-Konfiguration 3
- **Q**
- Quell-Port R-66
- **R**
- R1-Maske R-69
- Rechner-Namen 86
- Rechnernamen 90
- registrierte IP-Adresse R-61
- registrierte IP-Adressen 111
- Remote Access R-67
- Remote Access mit TCP/IP 132
- Remote-Access 2, 55, 90, 132, R-55
- reservierte Adreßbereiche R-64
- RIP 64, R-69
- RIP-SAP-Skal. R-54
- RIP-Tabellen 64
- Round-Robin R-44
- RoundRobin- Liste R-44
- Round-Robin-Liste R-43
- Routen/FRM R-57
- Router-Name 69
- Routing 90
- Routing Information Protocol 64
- Routing-Methode R-68
- Routing-Tabelle R-54
- besondere Einträge 70
- IP-Masquerading 70
- Rückruf 2, 37, 38, R-43, R-48, R-50
- Fast Call Back 39
- Rückruf-Funktion 5
- Rückruffoptionen R-43
- Rufnummer R-42
- Rufnummern R-47
- Rufnummernerkennung 5
- **S**
- S0-Schnittstelle 3
- SAP 64, R-57
- SAP-Nummern 87
- SAP-Services R-58
- SAP-Tabellen 64
- schnelles Rückrufverfahren R-43
- Schnittstellen 9
- Schutz R-48
- Scope-ID R-75
- Scopes 90
- Script-Liste R-48, 96
- Script-Verarbeitung 95
- Scriptverarbeitung R-45, R-48
- semipermanente Festverbindung R-43
- serielle Schnittstelle 13, 23
- Server/FRM R-59
- Server-Informationen R-57
- Server-Liste R-77
- Service Advertising Protocol 64
- Service-Informationen R-58
- Service-Tab. R-70
- Setup
- IP-Router-Modul R-63
- IPX-Modul R-51
- LAN-Modul R-50
- SNMP-Modul R-72
- TCP-IP-Modul R-60
- WAN-Modul R-39
- Setup Assistent 14
- Short-Hold R-42
- Sicherheit 35, 37, 39, 111
- Sicherheitsfunktionen 2
- Sicherung 53

- Sicherungsverfahren 38, R-47
 Single User Access 39
 Skalierung R-53
 SNAP R-52
 SNMP 25, R-71
 Agents 25
 Manager 25
 MIB 25
 Socket-Filter 66, R-53, R-55
 Software einspielen 21
 Software-Update 6
 Sonderrufnummern 104
 Sonstiges R-85
 Sparmöglichkeiten beim Telefonieren 104
 Sperre 36
 Sperr-Minuten R-78
 Split Horizon 65
 Spoofing R-57, R-59
 Sprache R-78
 SPX Watchdogs 67
 SPX-Watch R-53
 Stac 60, R-46
 Stac-Datenkompression 3
 Standard-Faxprogramme 102
 Standard-Route R-65
 Standort R-39, R-71
 Start-Adresse 80
 Start-Adreß-Pool R-72
 statische Bündelung R-43
 statische IP-Adresse R-64
 Statische Kanalbündelung 60
 statische Kanalbündelung 3
 statisches Routing 68
 Statistiken 4
 Status R-3
 Betriebszeit R-6
 Config-Statistik R-30, R-31
 Info-Verbindung R-33
 IP-Router-Statistik R-28
 IPX-Statistik R-18
 LAN-Statistik R-9
 Layer-Verb. R-33
 PPP-Statistik R-10
 Ruf-Info-Tabelle R-34, R-36, R-37
 SO-Bus R-6
 TCP-IP-Statistik R-22
 Verb.-Statistik R-32
 Verbindung R-5
 WAN-Statistik R-6
 Werte-löschen R-37
 Statusanzeigen 4
 Symbole 110
 System-Boot R-85
 System-Reset R-85
 System-Upload R-85
- T**
 Tab.-Masquerade R-71
 Tabelle-RIP R-56, R-69
 Tabelle-SAP R-58
 Tageszeit 103
 Tarife 102
 Tarifstruktur 104
 Tarifzone 104
 Tasten 8
 TCP R-66, R-71
 TCP/IP 15, 68
 TCP/IP-Netze 86
 TCP-Aging-Min R-63
 TCP-Max.-Verb. R-63
 Technische Daten 143
 Telefongesellschaft 104, R-80
 Telework 132
 Teleworker R-67
 Teleworking 2
 Telex 14
 Telnet 5, 17
 Telnet-Server R-61
 Terminalprogramm 5, 14
 TFTP 15
 TFTP-Server R-61
 Timeout 60, R-74
 TOS R-68, 110
 Trace
 Beispiele 31
 Schlüssel und Parameter 29

- starten 29
 - Trace-Ausgaben 29, 97
 - ARP 107
 - Bedienung 98
 - Beispiele 99
 - Error 101
 - ICMP 108
 - IP-RIP 107
 - IP-Rt. 106
 - IPX-NetBIOS 105
 - IPX-Rt. 103
 - IPX-Watchdogs 105
 - PPP 102
 - RIP 103
 - SAP 104
 - SCRPT 109
 - Source 101
 - SPX-Watchdogs 105
 - Time 101
 - Unterstützte Protokolle 99
 - Trap 27
 - Trap-IP R-71
 - Traps-senden R-71
 - Typ R-69
 - Type-of-Service 78, R-68
- **U**
- Überprüfungen der Gegenstelle R-47
 - Überprüfungsversuche R-47
 - Übertragungsraten 4, 32
 - Überwachung 31
 - UDP R-66, R-71
 - Uhrzeit 103, 106
 - Umleitung 103
 - Unterdrückung der abgehenden MSN ... R-41
 - Upload 6, 21
 - Username 54, R-47
- **V**
- V.110-Protokoll 7
 - V.24-Konfigurationsschnittstelle 10
 - Verbindungsaufbau 90
 - Verbindungsbegrenzung 39, 40
 - Verbindungsdauer 4
- verbotene Adreßbereiche R-64
 - Verfügbarkeit 101
 - Versions- Tabelle R-83
 - Vorwahl 102
- **W**
- Wählleitungen 2, 121
 - Wählpräfix 103
 - Wahlsonderzeichen R-42, R-43
 - WAN-Anschluß 3
 - WAN-Config R-78
 - WAN-Filtertab. R-56, R-58, R-67
 - WAN-Update-Zeit R-57, R-59
 - Watchdog R-53
 - Watchdogs 67
 - Web-Serve 115
 - Web-Server 110
 - Web-Server im Internet installieren 115
 - Wildcards 89
 - Windows Internet Name Service-Server ... 90
 - Windows-Networking 96
 - Windows-Netz 82, 89
 - Windows-Netze 7
 - Windows-Netze routen 89
 - WINS-Konfiguration 82
 - WINS-Server 90
 - Wochentage 103
 - WWW 39
- **X**
- X.75-Daten sicherung R-45
 - X.75-gesichert R-45
 - XModem 23
- **Y**
- Y-Verbindung 61
 - Y-Verbindungen R-41
- **Z**
- Zeit R-6, R-47, R-82
 - Zeit im ISDN-Netz 106
 - Zeitabhängige Verbindungsbegrenzung 40
 - Zeitbudget 40
 - Zeitkontrolle 5
 - Ziel-Adresse R-67

Ziel-Netzmaske	R-67
Zielnetzwerk	R-64
Ziel-Port	R-66
Zugangskontrolle	36
Zugangsliste	R-61
Zugangsschutz	37
keiner	37
Name	37
Name oder Nummer	37
Nummer	37
Zugriffschutz	5
Zugriffstyp	93
Zustand	R-51, R-60, R-64

Beschreibung der Menüpunkte

Der Menübaum der *ELSA LANCOM*-Konfiguration ist in sogenannte Status-Informationen, Setup-Parameter, Firmware-Informationen und Sonstiges aufgeteilt.

Zur leichteren Orientierung zeigen wir Ihnen zunächst eine Übersicht über die Menüstruktur.

In der vollständigen Liste aller Menüpunkte finden Sie anschließend die genaue Beschreibung aller Anzeigen, Menüs und Aktionen mit den zugehörigen Parametern, Standardwerten und Eingabemöglichkeiten.



Die im Referenz-Teil beschriebenen Eigenschaften gelten z.T. nur für bestimmte Modelle der *ELSA LANCOM*-Familie. Die Einschränkungen bzgl. bestimmter Modelle werden durch die nebenstehenden Symbole angezeigt.

Sie erreichen die Menüs bei Konfigurationen über Telnet oder Terminal-Programme sowie über SNMP (siehe auch 'Konfigurationsmöglichkeiten').

Bei der Konfiguration mit *ELSA LANconfig* steht Ihnen ein integriertes Hilfesystem mit Kurzbeschreibungen zu den einzelnen Parametern zur Verfügung.



Alle kanalbezogenen Statistiken und Menüs sind in dieser Beschreibung nur mit zwei Kanälen aufgeführt, obwohl die Geräte möglicherweise mehr als zwei Kanäle bereitstellen. Ebenso sind interfacebezogene Angaben nur für ein Interface aufgeführt. Die entsprechenden Informationen gelten für die weiteren Kanäle und Interfaces sinngemäß.

Symbole

	Menü	zeigt ein weiteres Untermenü an.
	Info	zeigt einen Wert an, der nicht verändert werden kann.
	Wert	zeigt einen Wert an, der verändert werden kann.
	Tabelle	zeigt eine Tabelle an, deren Einträge verändert werden können.
	Info-Tabelle	zeigt eine Tabelle an, deren Einträge nicht verändert werden können.
	Aktion	führt eine Aktion aus.

Menü-Übersicht

 Setup	 Status
 Name	 Verbindung
 WAN-Modul	 Aktuelle-Zeit
 Gebühren-Modul	 Betriebszeit
 LAN-Modul	 WAN-Statistik
 IPX-Modul	 LAN-Statistik
 TCP-IP-Modul	 PPP-Statistik
 IP-Router-Modul	 IPX-Statistik
 SNMP-Modul	 TCP-IP-Statistik
 DHCP-Modul	 IP-Router-Statistik
 NetBIOS-Modul	 Config-Statistik
 Config-Modul	 Queue-Statistik
 LANCAP-Modul	 Verbindungs-Statistik
 LCR-Modul	 Info-Verbindung
 DNS-Modul	 Layer-Verbindung
 Zeit-Modul	 Ruf-Info-Tabelle
 Firmware	 Gegenstellen-Statistik
 Versions-Tabelle	 S ₀ -Bus
 Tabelle-Firmsafe	 Kanalstatistik
 Modus-Firmsafe	 Zeit-Statistik
 Timeout-Firmsafe	 LCR-Statistik
 Firmware-Upload	 Werte löschen
 Test-Firmware	 Sonstiges
	 Manuelle Wahl
	 System-Reset
	 System-Boot
	 System-Upload

Status

Das Menü 'Status' enthält Informationen zum aktuellen Status und über interne Abläufe im LAN und im WAN, die sich auf die Datenübertragungs-Strecke (z.B. Anwahl bzw. Verbindung) oder Statistiken (z.B. Anzahl empfangener bzw. gesendeter Datenblöcke) beziehen können. Die statistischen Anzeigen bieten eine leistungsfähige Hilfestellung bei der Überprüfung der korrekten Arbeitsweise und bei der Optimierung der Parametereinstellung. Darüber hinaus liefern sie bei einem Fehlverhalten wertvolle Informationen zur Fehleranalyse.

Die meisten Statusanzeigen werden laufend aktualisiert und können mit einer im jeweiligen Menü enthaltenen **Werte löschen**-Aktion auf 0 gesetzt werden.

Das Menü besitzt den folgenden Aufbau:

Status		Fortlaufende Statusanzeigen
Verbindung		Zustand der WAN-Strecke
Aktuelle-Zeit		Aktuelle Zeit im Gerät
Betriebszeit		Betriebszeit des Gerätes seit dem letzten Einschalten
S ₀ -Bus		Zustand der S ₀ -Schnittstelle
WAN-Statistik		Anzeige der WAN-Statistiken
LAN-Statistik		Statistiken des Netzwerk-Bereichs
PPP-Statistik		Statistiken des Point-to-Point-Protokolls
IPX-Statistik		Statistiken aus dem IPX- und IPX-Router-Bereich
TCP-IP-Statistik		Statistiken aus dem TCP/IP-Bereich
IP-Router-Statistik		Statistiken aus dem IP-Router
Config-Statistik		Statistiken der Remote-Konfiguration
Queue-Statistik		Statistiken über die Pakete in den Queues der einzelnen Module
Verbindungs-Statistik		Verbindungs-Informationen für jedes Interface
Info-Verbindung		Informationen zur letzten Verbindung für jedes Interface
Layer-Verbindung		Informationen über das verwendete B-Kanal-Protokoll für jedes Interface
Ruf-Info-Tabelle		Informationen über die letzten 100 angekommenen Rufe
Gegenstellen-Statistik		Statistik über die letzten 100 Verbindungen
Kanal-Statistik		Informationen über den Zustand der einzelnen Kanäle.

Status	Fortlaufende Statusanzeigen	
Zeit-Statistik		Informationen aus dem Zeit-Modul
LCR-Statistik		Informationen aus dem Least Cost Router
Werte löschen		Alle Werte außer Tabellen der untergeordnet. Statistik löschen

Display und Tastatur

Über das Display werden Statusinformationen des Gerätes sowie Fehlermeldungen angezeigt. Dabei sind folgende Anzeigemodi vorhanden:

- B-Kanal Übersicht (ein Zeichen je Kanal)
- B-Kanal Statusanzeige (eine Zeile je Kanal)
- Gerätestatus / Gerätefehlermeldungen

Insgesamt stehen sechs Tasten zur Verfügung (Cursortasten + "Mode" + "Clr"), sowie ein zweizeiliges Display mit je 40 Zeichen, von denen jeweils 16 Zeichen aktuell dargestellt werden. Die Textinformationen werden je nach Geräteeinstellung in Englisch oder Deutsch angezeigt.

B-Kanal-Übersicht

In der B-Kanal-Übersicht werden die Kanäle in Form einer Tabelle dargestellt. Die einzelnen Felder der Tabelle haben folgende Bedeutung:

P: x (Zustand von Port 1, erster B-Kanal)	P: x	P: x	P: x
1: x (Zustand von Port 1, zweiter B-Kanal)	2: x	3: x	4: x

Für den Kanalzustand (in der vorhergehenden Tabelle durch x dargestellt) werden folgende Symbole verwendet:

.	Kanal in Ruhezustand (deaktiviert)
-	Kanal in Ruhezustand (aktiviert)
E (blinkend)	Auf dem Kanal ist ein Fehler aufgetreten
A (blinkend)	Abgehender Ruf
A	Verbunden (abgehend)
P (blinkend)	Anliegender Ruf
P	Verbunden (ankommend)
N (blinkend)	Verhandlung

Die Cursortasten haben in diesem Modus keine Funktion.

B-Kanal-Statusanzeige

In der B-Kanal-Statusanzeige wird ein Auszug aus einer Tabelle gezeigt, in der je B-Kanal ein Eintrag vorhanden ist. Bei Veränderungen des Zustandes eines Kanals springt die Tabelle jeweils zu dem aktuellen Eintrag, wenn mindestens 5 Sekunden lang keine Cursor-taste gedrückt wurde. In den Textzeilen ist jeweils der Status des Kanals im Klartext angezeigt, z.B.:

CH11: Verbindung LC_PPP

CH12: Gegenstelle LC_PPP antwortet nicht

Fehlermeldungen bleiben 60 Sekunden erhalten. Angezeigt werden auch Informationen zur Aktivierung und Deaktivierung von S₀-Anschlüssen.

Mit den Auf- und Ab-Cursor-tasten kann zwischen den einzelnen Zeilen geblättert werden, mit den Links- und Rechts-Tasten kann innerhalb der Zeilen geschoben werden. Obwohl nur 16 Zeichen Displaybreite bereitstehen, wird das Display als 40 Zeichen Breite angenommen (der sichtbare Ausschnitt kann verschoben werden). 5 Sekunden nach der letzten Seitwärtsbewegung wird wieder an den Anfang gesprungen.

Gerätestatus und Gerätefehlermeldungen

In diesem Anzeigemodus werden kanalunabhängige Gerätestatusmeldungen und vor allem Fehlermeldungen (bei gleichzeitigem Blinken der Power/Msg-Led) angezeigt. Beim Auftreten eines neuen Fehlers wird automatisch in diesen Modus geschaltet.

Mit den Auf- und Ab-Cursor-tasten kann zwischen allen vorhandenen Meldungen geblättert werden, als letzte Meldung (die immer vorhanden ist) erscheint die Modellnummer (z.B. "Model 4100") sowie die Firmwareversion. Diese Anzeige erscheint auch direkt nach dem Einschalten, bevor dann in den letzte aktuellen Anzeigemodus gewechselt wird. Auch hier können die Fehlertexte wieder bis zu 40 Zeichen lang sein.

Mit der Mode-Taste wird manuell zwischen den o.g. Anzeigemodi umgeschaltet.

Die Clr-Taste löscht angezeigte Fehler im Anzeigemodus für Gerätsstatus und Gerätefehlermeldungen.

Status/Verbindung

Der Menüpunkt **Status/Verbindung** gibt die Statusmeldungen der einzelnen Kanäle wieder.

/Verbindung		Fortlaufende Statusanzeigen
Verbindung		CH01: Bereit; CH02: Bereit

Status/Aktuelle-Zeit

Hier wird die aktuelle Zeit des Gerätes angezeigt, die z.B. für die Least-Cost-Router-Berechnungen oder einige Statistiken verwendet wird. Diese Zeit kann entweder aus dem ISDN-Netz abgelesen werden (ISDN-Zeit, siehe auch Setup/Zeit-Modul) oder manuell gesetzt werden (mit dem Befehl 'time').

Status/Betriebszeit

Hier wird die Betriebszeit des Routers seit dem letzten Einschalten in Tagen, Stunden, Minuten und Sekunden angezeigt.

Status/S₀-Bus

Unter diesem Menüpunkt wird der aktuelle Zustand der S₀-Schnittstelle angezeigt. Die Statistik hat den folgenden Aufbau:

/S ₀ -Bus		Fortlaufende Statusanzeigen
D-Info		Übersicht über den Zustand eines D-Kanals.
D2-Statistik		Aufschlüsselung der Layer-2-Informationen des D-Kanals für die einzelnen B-Kanäle.

D-Info

Diese Tabelle zeigt allgemeine D-Kanal-Informationen:

Kanal	Kennzeichnung des B-Kanals.
Protokoll	D-Kanal-Protokoll. Entweder das in der Interface-Tabelle fest eingestellte Protokoll oder das bei der Einstellung 'Auto' am ISDN-Anschluß detektierte Protokoll.
Layer-2	Aktivierung der Schicht 2 des D-Kanals ('Ja' oder 'Nein')
TEI	TEI zugewiesen ('Ja' oder 'Nein')
S ₀ -Aktivierung	Zustandsanzeige der Aktivierung ('Ja' oder 'Nein')

D2-Statistik

Diese Tabelle zeigt Layer-2-Informationen zu den einzelnen B-Kanälen:

Kanal	Kennzeichnung des B-Kanals.
TEI	Von der Vermittlungsstelle zugewiesener T erminal E quipment I dentifizier.
L2-Aktivierung	Aktivierung der Schicht 2 des D-Kanals ('Ja' oder 'Nein').
Verbindungen	Anzahl der Verbindungen, die über die angezeigte TEI abgewickelt wurden.

Status/WAN-Statistik

Unter diesem Menüpunkt werden verschiedene statistische Parameter des WAN-Anschlusses angezeigt. Viele Werte über das übertragene Datenvolumen liefern nützlich.

che Informationen über die Auslastung des WAN-Anschlusses, aufgetretene Fehler und im aktuellen Betriebszustand vorhandene interne Ressourcen der Geräte.

Die WAN-Statistik wird interfacebezogen geführt, d.h., für jedes Interface existiert eine eigene Statistik, in welcher übertragene Daten und Fehler registriert werden. Das Menü **Status/WAN-Statistik** besitzt folgenden Aufbau:

/WAN-Statistik		Fortlaufende Statusanzeigen
Byte-Transport-Statistik		Statistik für übertragene Bytes
Paket-Transport-Statistik		Statistik für übertragene Daten-Pakete
Fehler-Statistik		Statistik über aufgetretene Übertragungsfehler
WAN-Tx-Verworfen		Anzahl durch Fehler/Ressourcenmangel verworfener Pakete
WAN-Heap-Pakete		Anzahl belegter Puffer
WAN-Queue-Pakete		Anzahl verfügbarer Puffer
WAN-Queue-Fehler		Anzahl durch Puffermangel verworfener Datenpakete
Durchsatz-Statistik		Statistik für die auf jedem Kanal übertragenen Bytes
Werte löschen		WAN-Statistik löschen

Byte-Transport-Statistik

Der Menüpunkt **Status/WAN-Statistik/Byte-Transport-Statistik** enthält für jedes verfügbare Interface eine Statistik über die auf diesem Interface übertragenen Bytes. Die dort aufgeführte Tabelle hat folgendes Aussehen:

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
CRx-Bytes	Anzahl der empfangenen Bytes (komprimiert)
Rx-Bytes	Anzahl der empfangenen Bytes (unkomprimiert)
Tx-Bytes	Anzahl der gesendeten Bytes (unkomprimiert)
CTx-Bytes	Anzahl der gesendeten Bytes (komprimiert)

Paket-Transport-Statistik

Der Menüpunkt **Status/WAN-Statistik/Paket-Transport-Statistik** enthält für jedes verfügbare Interface eine Statistik über die auf diesem Interface übertragenen Datenpakete. Die dort aufgeführte Tabelle hat folgendes Aussehen:

Ifc	Rx	Tx-gesamt	Tx-normal	Tx-gesichert	Tx-urgent
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
Rx	Anzahl der empfangenen Pakete
Tx-gesamt	Anzahl der gesendeten Pakete (Daten- und Protokoll-Pakete)
Tx-normal	Anzahl der gesendeten normalen Daten-Pakete
Tx-gesichert	Anzahl der gesichert übertragenen Daten-Pakete
Tx-urgent	Anzahl der bevorzugt übertragenen Daten-Pakete (Urgent-Queue)

Fehler-Statistik

Der Menüpunkt **Status/WAN-Statistik/Fehler-Stat.** enthält für jedes verfügbare Interface eine Statistik über die auf diesem Interface aufgetretenen Übertragungsfehler. Die dort aufgeführte Tabelle hat folgendes Aussehen:

Ifc	Rx-L3-F.	Rx-L2-F.	Rx-L1-F.	Tx-Fehler	Stack-F.
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
Rx-L3-F.	Anzahl Layer-3-Fehler bei empfangenen Daten (d.h., der Protokoll-Header der Layer-3 ist nicht korrekt)
Rx-L2-F.	Anzahl Layer-2-Fehler bei empfangenen Daten (d.h., analog zu den Layer-3-Fehlern, z.B. defekter PPP-Header)
Rx-L1-F.	Anzahl Layer-1-Fehler bei empfangenen Daten (analog zu Layer-3-Fehlern)
Tx-Fehler	Anzahl Übertragungsfehler beim Senden
Stack-F.	Anzahl Stack-Fehler bei empfangenen Daten. Stack-Fehler entstehen durch empfangene Frames, die keinem internen Verarbeitungsprozeß (z.B. IP Router) zugeordnet werden können.

*Durchsatz-
Statistik*

Der Menüpunkt **Status/WAN-Statistik/Durchsatz-Statistik** enthält für die beiden Kanäle eine Statistik über die auf diesem Interface übertragenen Bytes. Die dort aufgeführte Tabelle hat folgendes Aussehen:

lfc	Rx aktuell	Tx aktuell	Rx gemittelt	Tx gemittelt
Ch01	0	0	0	0
Ch02	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	bezeichnet den zugehörigen Kanal.
Rx/s aktuell	Durchsatz auf dem Kanal in der letzten Sekunde in Empfangsrichtung
Tx/s aktuell	Durchsatz auf dem Kanal in der letzten Sekunde in Senderichtung
Rx/s gemittelt	mittlerer Durchsatz auf dem Kanal in Empfangsrichtung
Tx/s gemittelt	mittlerer Durchsatz auf dem Kanal in Senderichtung

Status/LAN-Statistik

Analog zum vorherigen Menüpunkt werden hier die für den LAN-Anschluß relevanten Statistiken angezeigt. Das Menü **Status/LAN-Statistik** besitzt folgenden Aufbau:

/LAN-Statistik	Fortlaufende Statusanzeigen	
LAN-Rx-Pakete		Anzahl empfangener Datenpakete
LAN-Tx-Pakete		Anzahl gesendeter Datenpakete
LAN-Rx-Fehler		Anzahl fehlerhaft empfangener Datenpakete
LAN-Tx-Fehler		Anzahl fehlerhaft gesendeter Datenpakete
LAN-Stack-Fehler		Anzahl Pakete ohne passendes Empfangsmodul (Bridge/Router)
LAN-NIC-Fehler		Anzahl vom NIC verworfener Datenpakete
LAN-Heap-Pakete		Anzahl verfügbarer Puffer
LAN-Queue-Pakete		Anzahl belegter Puffer
LAN-Queue-Fehler		Anzahl durch Puffermangel verworfener Pakete
LAN-Kollisionen		Anzahl Kollisionen während des Sendevorgangs
Verbindung-aufgebaut		Anzeige der korrekten Verbindung auf dem Ethernet (Datenübertragung möglich). Entspricht der 'Link'-LED am Gerät.
Verhandlung-abgeschlossen		Die Aushandlung der Übertragungsart zwischen Router und Gegenstelle ist abgeschlossen. Hat nur eine Bedeutung, wenn Setup/LAN-/Anschluss auf 'Auto' steht.

/LAN-Statistik	Fortlaufende Statusanzeigen	
Anschluß		Dieser Punkt zeigt an, welche Übertragungsart momentan auf dem Ethernet-Anschluß gefahren wird: 10B-TX: 10MBit, halbduplex FD10B-TX: 10MBit, voll duplex 100B-TX: 100MBit, halbduplex FD100B-TX: 100 MBit, voll duplex Wenn unter Setup/LAN- als Anschluß 'Auto' eingestellt ist, ist dies die Übertragungsart, die beide Seiten untereinander ausgehandelt haben, entspricht also den 'Fast' und 'FDpx'-LEDs am Gerät. Ist dagegen eine feste Übertragungsart eingestellt, ist dieser Wert gleich dem in Setup/LAN-/Anschluss.
LAN-Rx-Bytes		Anzahl vom LAN empfangener Zeichen
LAN-Tx-Bytes		Anzahl zum LAN gesendeter Zeichen
LAN-Rx-Broadcasts		Anzahl vom LAN empfangener Broadcast-Pakete
LAN-Rx-Multicasts		Anzahl vom LAN empfangener Multicast-Pakete
LAN-Rx-Unicasts		Anzahl vom LAN empfangener direkt adressierter Pakete
WAN-Rx-Broadcasts		Anzahl vom WAN empfangener Broadcasts
WAN-Rx-Multicasts		Anzahl vom WAN empfangener Multicasts
WAN-Rx-Unicasts		Anzahl vom WAN empfangener Unicasts
Werte löschen		LAN-Statistik löschen

Status/PPP-Statistik

Innerhalb der PPP-Statistik werden die Zustände einzelner Sub-Protokolle des PPPs für jedes Interface separat verwaltet. Die Statistiken der übertragenen Frames einzelner Sub-Protokolle werden dagegen nur innerhalb einer gemeinsamen Statistik mitgeführt. Das Menü **Status/PPP-Statistik** besitzt daher folgenden Aufbau:

/PPP-Statistik	Fortlaufende Statusanzeigen	
Zustände		Statistik über Zustand der PPP-Protokollverhandlung für jedes Interface
LCP-Statistik		Anzeige der PPP/LCP-Statistiken
PAP-Statistik		Anzeige der PPP/PAP-Statistik
CHAP-Statistik		Anzeige der PPP/CHAP-Statistik
IPXCP-Statistik		Anzeige der PPP/IPXCP-Statistik
IPCP-Statistik		Anzeige der PPP/IPCP-Statistik
CBCP-Statistik		Anzeige der PPP/CBCP-Statistik
CCP-Statistik		Anzeige der PPP/CCP-Statistik
ML-Statistik		Anzeige der PPP/ML-Statistik

/PPP-Statistik		Fortlaufende Statusanzeigen
BACP-Statistik		Anzeige der PPP/BACP-Statistik
Rx-Optionen		Anzeige der empfangenen LCP-, IPCP- und IPXCP-Informationen
Tx-Optionen		Anzeige der gesendeten LCP-, IPCP- und IPXCP-Informationen
Werte löschen		Löschen der PPP-Statistiken

Die PPP-Statistik gibt insbesondere bei Connect-Problemen mit Fremdprodukten genauen Aufschluß über den Verlauf einer PPP-Verhandlung. Sie enthält entscheidende Hinweise für eine Fehlerdiagnose.

Zustände

Der Menüpunkt **Status/PPP-Statistik/Zustände** enthält für jedes verfügbare Interface eine Liste der aktuellen Zustände der PPP-Protokollverhandlung. Die dort aufgeführte Tabelle hat folgendes Aussehen:

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	bezeichnet den zugehörigen Kanal.
Phase	enthält die Phase, in der sich das PPP befindet. Mögliche Werte sind AUTHENTICAT , NETWORK und TERMINATE .
LCP	Zustand des Subprotokolls 'Link-Control-Protokoll'. Mögliche Werte sind: Initial , Startng , Stoppng , Stopped , Closing , Closed , ReqSent , AckRcvd , AckSent und Opened .
IPCP	analog zu 'LCP' wird hier der Zustand des Subprotokolls 'IP-Control-Protocol' angezeigt.
IPXCP	analog zu 'LCP' wird hier der Zustand des Subprotokolls 'IPX-Control-Protocol' angezeigt.
CCP	analog zu 'LCP' wird hier der Zustand des Subprotokolls 'Compression-Control-Protocol' angezeigt.

Unter **Status/PPP-Statistik/Zustände** wird die jeweilige Phase des PPPs aktuell angezeigt. Diese Zustände sind, wie oben angegeben, Ruhezustand (Dead), Bereitschaftszustand (Establish), Überprüfung der Zugangsparameter (Authenticate) und Netzwerkphase (Network). In den Unterstatistiken werden die ausgetauschten Frames nach Art und Menge gesondert aufgeschlüsselt.

Status/PPP-Statistik/LCP-Statistik

Das **LCP** (Link Control Protocol) verhandelt die grundlegenden Eigenschaften der PPP-Verbindungen. Die während der PPP-Verhandlung ausgetauschten LCP-Frames werden

nach Art und Anzahl statistisch erfaßt und angezeigt. Sollte das LCP bei einer Verbindung nicht in den OPEN-Zustand wechseln, geben diese Statistikwerte Hinweise auf Fehler, die in der Anfangsphase der PPP-Verhandlung aufgetreten sind. Die Parameter in dieser Statistik bedeuten im einzelnen:

Rx-Fehler	Anzahl fehlerhaft empfangener PPP-Pakete
Rx-Verworfen	Anzahl verworfener PPP-Pakete
Rx-Config-Request	Anzahl empfangener Configure-Request-Pakete für LCP
Rx-Config-Ack.	Anzahl empfangener Configure-Acknowledge-Pakete für LCP
Rx-Config-Nack.	Anzahl empfangener Configure-Negative Acknowledge-Pakete
Rx-Config-Reject	Anzahl empfangener Configure-Reject-Pakete für LCP
Rx-Term-Request	Anzahl empfangener Terminate-Request-Pakete für LCP
Rx-Term-Ack	Anzahl empfangener Terminate-Acknowledge-Pakete für LCP
Rx-Code-Reject	Anzahl empfangener Code-Reject-Pakete für PPP
Rx-Protocol-Reject	Anzahl empfangener Protocol-Reject-Pakete für PPP
Rx-Echo-Request	Anzahl empfangener Echo-Request-Pakete für LCP
Rx-Echo-Reply	Anzahl empfangener Echo-Response-Pakete für LCP
Rx-Discard-Request	Anzahl empfangener Discard-Request-Pakete für LCP
Tx-Config-Request	Anzahl gesendeter Configure-Request-Pakete für LCP
Tx-Config-Ack.	Anzahl gesendeter Configure-Acknowledge-Pakete für LCP
Tx-Config-Nack.	Anzahl gesendeter Configure-Negative-Acknowledge-Pakete
Tx-Config-Reject	Anzahl gesendeter Configure-Reject-Pakete für LCP
Tx-Term-Request	Anzahl gesendeter Terminate-Request-Pakete für LCP
Tx-Term-Ack.	Anzahl gesendeter Terminate-Acknowledge-Pakete für LCP
Tx-Code-Reject	Anzahl gesendeter Code-Reject-Pakete für PPP
Tx-Protocol-Reject	Anzahl gesendeter Protocol-Reject-Pakete für PPP
Tx-Echo-Request	Anzahl gesendeter Echo-Request-Pakete für LCP
Tx-Echo-Reply	Anzahl gesendeter Echo-Response-Pakete für LCP
Tx-Discard-Request	Anzahl gesendeter Discard-Request-Pakete für LCP
Werte löschen	LCP-Statistik löschen

Status/PPP-Statistik/PAP-Statistik

Das **PAP** (Password Authentication Protocol) ist eines von zwei üblichen Verfahren zur Überprüfung von Gegenstellen im PPP. Es überprüft beim Verbindungsaufbau einmalig das Paßwort der Gegenstelle und läßt die Verbindung nur nach erfolgreichem Paß-

wortaustausch zu (siehe auch Kapitel 'Point-to-Point Protocol'). Die Parameter in dieser Statistik bedeuten im einzelnen:

Rx-Verworfen	Anzahl verworfener PAP-Pakete
Rx-Request	Anzahl empfangener PAP-Request-Pakete
Rx-Success	Anzahl empfangener PAP-Success-Pakete
Rx-Failure	Anzahl empfangener PAP-Failure-Pakete
Tx-Retry	Anzahl gesendeter Wiederholungen von PAP-Request-Paketen
Tx-Request	Anzahl gesendeter PAP-Request-Pakete
Tx-Success	Anzahl gesendeter PAP-Success-Pakete
Tx-Failure	Anzahl gesendeter PAP-Failure-Pakete
Werte löschen	PAP-Statistik löschen

Status/PPP-Statistik/CHAP-Statistik

Das **CHAP** (Challenge Authentication Protocol) ist die zweite Möglichkeit, Gegenstellen unter PPP zu überprüfen. Dabei findet eine Paßwortüberprüfung beim Verbindungsaufbau und erneut in einstellbaren Abständen während der Verbindung statt (siehe auch Kapitel 'Point-to-Point Protocol'). Die Parameter in dieser Statistik bedeuten im einzelnen:

Rx-Verworfen	Anzahl verworfener CHAP-Pakete
Rx-Challenge	Anzahl empfangener CHAP-Challenge-Pakete
Rx-Response	Anzahl empfangener CHAP-Response-Pakete
Rx-Success	Anzahl empfangener CHAP-Success-Pakete
Rx-Failure	Anzahl empfangener CHAP-Failure-Pakete
Tx-Retry	Anzahl gesendeter Wiederholungen v. CHAP-Challenge-Paketen
Tx-Challenge	Anzahl gesendeter CHAP-Challenge-Pakete
Tx-Response	Anzahl gesendeter CHAP-Response-Pakete
Tx-Success	Anzahl gesendeter CHAP-Success-Pakete
Tx-Failure	Anzahl gesendeter CHAP-Failure-Pakete
Werte löschen	CHAP-Statistik löschen

Status/PPP-Statistik/IPXCP-Statistik

Das **IPXCP** (Internet Exchange Protocol Control Protocol) zeigt bei Verwendung von IPX den Zustand des Protokolls und die zur Verhandlung ausgetauschten Pakete. Die Parameter in dieser Statistik bedeuten im einzelnen:

Rx-Rejected	Anzahl verworfener IPXCP-Pakete
Rx-Config-Request	Anzahl empfangener Configure-Request-Pakete für IPXCP
Rx-Config-Ack.	Anzahl empfangener Configure-Acknowledge-Pakete für IPXCP

Rx-Config-Nack.	Anzahl empfangener Configure-Negative Acknowledge-Pakete
Rx-Config-Reject	Anzahl empfangener Configure-Reject-Pakete für IPXCP
Rx-Term-Request	Anzahl empfangener Terminate-Request-Pakete für IPXCP
Rx-Term-Ack.	Anzahl empfangener Terminate-Acknowledge-Pakete für IPXCP
Rx-Code-Reject	Anzahl empfangener Code-Reject-Pakete für IPXCP
Tx-Config-Request	Anzahl gesendeter Configure-Request-Pakete für IPXCP
Tx-Config-Ack.	Anzahl gesendeter Configure-Acknowledge-Pakete für IPXCP
Tx-Config-Nack.	Anzahl gesendeter Configure-Negative-Acknowledge-Pakete
Tx-Config-Reject	Anzahl gesendeter Configure-Reject-Pakete für IPXCP
Tx-Term-Request	Anzahl gesendeter Terminate-Request-Pakete für IPXCP
Tx-Term-Ack.	Anzahl gesendeter Terminate-Acknowledge-Pakete für IPXCP
Tx-Code-Reject	Anzahl gesendeter Code-Reject-Pakete für IPXCP
Werte löschen	IPXCP-Statistik löschen

Status/PPP-Statistik/IPCP-Statistik

Das **IPCP** (Internet Protocol Control Protocol) zeigt bei Verwendung von IP den Zustand des Protokolls und die zur Verhandlung ausgetauschten Pakete.

Rx-Rejected	Anzahl verworfener IPCP-Pakete
Rx-Config-Request	Anzahl empfangener Configure-Request-Pakete für IPCP
Rx-Config-Ack.	Anzahl empfangener Configure-Acknowledge-Pakete für IPCP
Rx-Config-Nack.	Anzahl empfangener Configure-Negative-Acknowledge-Pakete
Rx-Config-Reject	Anzahl empfangener Configure-Reject-Pakete für IPCP
Rx-Term-Request	Anzahl empfangener Terminate-Request-Pakete für IPCP
Rx-Term-Ack.	Anzahl empfangener Terminate-Acknowledge-Pakete für IPCP
Rx-Code-Reject	Anzahl empfangener Code-Reject-Pakete für IPCP
Tx-Config-Request	Anzahl gesendeter Configure-Request-Pakete für IPCP
Tx-Config-Ack.	Anzahl gesendeter Configure-Acknowledge-Pakete für IPCP
Tx-Config-Nack.	Anzahl gesendeter Configure-Negative-Acknowledge-Pakete
Tx-Config-Reject	Anzahl gesendeter Configure-Reject-Pakete für IPCP
Tx-Term-Request	Anzahl gesendeter Terminate-Request-Pakete für IPCP
Tx-Term-Ack.	Anzahl gesendeter Terminate-Acknowledge-Pakete für IPCP
Tx-Code-Reject	Anzahl gesendeter Code-Reject-Pakete für IPCP
Werte löschen	IPCP-Statistik löschen

Status/PPP-Statistik/CBCP-Statistik

Das **CBCP** (Callback Control Protocol) zeigt bei Verwendung von IP den Zustand des Protokolls und die zur Verhandlung ausgetauschten Pakete.

Rx-Request	Anzahl empfangener CBCP-Request-Pakete
Rx-verworfen	Anzahl verworfener CBCP-Pakete
Rx-Ack	Anzahl empfangener CBCP-Acknowledge-Pakete
Tx-Request	Anzahl gesendeter CBCP-Request-Pakete
Tx-Response	Anzahl gesendeter CBCP-Response-Pakete
Tx-Ack	Anzahl gesendeter CBCP-Acknowledge-Pakete
Request-verworfen	Anzahl verworfener CBCP-Request-Pakete
Response-verworfen	Anzahl verworfener CBCP-Response-Pakete
Ack.-verworfen	Anzahl verworfener CBCP-Acknowledge-Pakete
Werte löschen	IPCP-Statistik löschen

Status/PPP-Statistik/CCP-Statistik

In der Statistik zum Compression Control Protocol (CCP) finden Sie die während der PPP-Verhandlung ausgetauschten Pakete zur Datenkompression.

Rx-verworfen	Anzahl aller verworfenen CCP-Pakete
Rx-Config-Request	Anzahl der empfangenen CCP-Anfragen
Rx-Config-Ack.	Anzahl der akzeptierten CCP-Anfragen
Rx-Config-Nak.	Anzahl der CCP-Anfragen, die aufgrund nicht akzeptierter Parameter der Anfrage zurückgewiesen wurden.
Rx-Config-Reject	Anzahl der CCP-Anfragen, die aufgrund anderer Gründe zurückgewiesen wurden.
Rx-Termination-Request	Anzahl der CCP-Anfragen nach einem Abau der Kompression.
Rx-Termination-Ack.	Anzahl der bestätigten CCP-Anfragen nach einem Abau der Kompression.
Rx-Code-Reject	Anzahl der zurückgewiesenen CCP-Anfragen, weil die Gegenstelle keine Kompression einsetzen will oder kann.
Rx-Reset-Request	Anzahl der CCP-Anfragen nach einer Synchronisation der Kompression (z.B. nach Übertragungsfehlern)
Rx-Reset-Ack	Anzahl der bestätigten CCP-Anfragen nach einer Synchronisation der Kompression
Tx-Config-Request	Anzahl der gesendeten CCP-Anfragen
Tx-Config-Ack.	Anzahl der von der Gegenstelle akzeptierten CCP-Anfragen
Tx-Config-Nak.	Anzahl der CCP-Anfragen, die von der Gegenstelle aufgrund nicht akzeptierter Parameter der Anfrage zurückgewiesen wurden.
Tx-Config-Reject	Anzahl der CCP-Anfragen, die von der Gegenstelle aufgrund anderer Gründe zurückgewiesen wurden.

Tx-Termination-Request	Anzahl der gesendeten CCP-Anfragen nach einem Abau der Kompression.
Tx-Termination-Ack.	Anzahl der gesendeten CCP-Bestätigungen für den Abau der Kompression.
Tx-Code-Reject	Anzahl der zurückgewiesenen CCP-Anfragen, weil der <i>ELSA LANCOM</i> keine Kompression einsetzen will (durch Einstellung in der Layer-Liste).
Tx-Reset-Request	Anzahl der gesendeten CCP-Anfragen nach einer Synchronisation der Kompression (z.B. nach Übertragungsfehlern)
Tx-Reset-Ack	Anzahl der gesendeten CCP-Bestätigungen für eine Synchronisation der Kompression
Werte-löschen	CCP-Statistik löschen

Status/PPP-Statistik/ML-Statistik

Die Statistik zum MLPPP gibt hauptsächlich Auskunft darüber, wie bei einer gebündelten PPP-Verbindung die Gegenstelle die einzelnen Pakete behandelt.

Buendel-Verb	Anzahl der Verbindungen, die MLPPP verwendet haben
Rx-Seq-Verlust	Anzahl der Pakete, bei denen ein Fehler in der Reihenfolge der Sequenznummern aufgetreten ist.
Rx-Seq-Wiederholung	Anzahl der Pakete, die der reihenfolge der Sequenznummern nach verspätet eingetroffen sind.
Rx-Mrru-Ueberlauf	Anzahl der Pakete, bei denen nach dem Zusammenbauen eine Verletzung der in der PPP-Verhandlung ausgehandelten MRRU (maximal received reassembled unit) festgestellt wurde.
Rx-Header-Fehler	Anzahl der Pakete mit fehlerhaftem Header.
Rx-verworfen	Anzahl aller verworfenen MLPPP-Pakete.
Rx-Frag-Start	Anzahl der Pakete mit gesetztem Start-Flag (erster Teil eines fragmentierten Pakets).
Rx-Frag-Mid	Anzahl der Pakete mit gesetztem Mid-Flag (mittlerer Teil eines fragmentierten Pakets).
Rx-Frag-Ende	Anzahl der Pakete mit gesetztem End-Flag (letzter Teil eines fragmentierten Pakets).
Rx-unfragmentiert	Anzahl der Pakete mit gesetztem Start- und End-Flag (unfragmentierte Pakete).
Werte-löschen	ML-Statistik löschen

Status/PPP-Statistik/Rx- und Tx-Optionen

In den Optionen der PPP-Statistik wird aufgezeichnet, welche Informationen bei der Verhandlung über LCP, IPCP oder IPXCP ausgetauscht werden.

Rx-Optionen Hier kann nachgeschaut werden, was die Gegenstelle angefordert (LCP) bzw. was dem Router zugewiesen (IPCP und IPXCP) wurde.

Tx-Optionen Hier kann nachgeschaut werden, was der Router von der Gegenstelle angefordert (LCP) bzw. was er dieser zugewiesen (IPCP und IPXCP) hat.

Die beiden Untermenüs besitzen jeweils den gleichen Aufbau:

/Rx- und Tx-Optionen		Anzeige
LCP		Informationen über Paketgrößen, Steuerzeichen, Sicherungsverfahren und Rückruf
IPXCP		Informationen über Adressen und Routingverfahren im IPX-Netzwerk
IPCP		Informationen über Adressen im IP-Netzwerk

In der Tabelle LCP sind für jeden Kanal gesondert aufgeführt:

MRU	M aximum R eceive U nit, kennzeichnet die maximale Paketgröße, die die Gegenstelle empfangen kann
ACCM	A synchron C ontrol C haracter M ap, kennzeichnet die Zeichen im asynchronen Datenstrom, die als Steuerzeichen interpretiert werden
Authent.	verwendetes Authentifizierungsverfahren (PAP/CHAP)
Callback	Art der Rückruf-Verhandlung

In der Tabelle IPXCP sind wieder für jeden Kanal gesondert die ausgehandelten IPX-Optionen aufgeführt:

Netzwerk	Netzwerknummer des WAN-Netzes
Node-Id	in den Rx-Optionen steht die dem <i>ELSA LANCOM</i> zugewiesene Node-ID (i.a. 000000000000 oder die MAC-Adresse des Routers) in den Tx-Optionen kann die Node-ID der Gegenstelle abgelesen ermittelt werden (auch wieder 000000000000 oder die MAC-Adresse der Gegenstelle).
Routing	hier wird das verwendete Routing-Protokoll angegeben (RIP/SAP oder keins), wiederum bei Rx das, welches uns die Gegenstelle zugewiesen hat und bei Tx dasjenige, daß der <i>ELSA LANCOM</i> der Gegenstelle zuweist.

Zu guter Letzt stehen unter IPCP die ausgehandelten IP-Optionen wieder nach Kanal getrennt:

IP-Adresse	auch hier gilt wieder, daß in den Rx-Optionen, die Adressen stehen, die von der Gegenstelle zugewiesen wurden, und unter den Tx-Optionen die stehen, die der <i>ELSA LANCOM</i> der Gegenstelle zuweist (damit ist z.B. ganz einfach die IP-Adresse des Einwahlknotens beim Internet-Provider in den Tx-Optionen abzulesen).
DNS-Server	
NBNS-Server	

Status/IPX-Statistik

Hier werden die Statistiken aus dem IPX-Bereich gesammelt, gegliedert nach Typen-, Socket- und Router-Informationen. In der IPX-Statistik finden Sie die folgenden Parameter:

/IPX-Statistik	Statistiken aus dem IPX- und IPX-Router-Bereich	
MAC-Statistik		Statistiken aus dem Media Access Control von IPX-Paketen
Watchdog-Statistik		Statistiken für Watchdog-Pakete
Propagate-Statistik		Statistiken für IPX-Propagated-Pakete (IPX-Typ 20)
RIP-Statistik		Statistiken für NetWare-RIP
SAP-Statistik		Statistiken für NetWare-SAP
IPX-Router-Statistik		Statistiken des Remote-IPX-Routers
Werte löschen		IPX-Statistiken löschen

In den Unterstatistiken finden Sie dann die weiteren Parameter zu den einzelnen Menüs.

Status/IPX-Statistik/MAC-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

IPX-LAN-Rx	Anzahl vom LAN empfangener IPX-Pakete
IPX-LAN-Rx-Broadcasts	Anzahl vom LAN empfangener Broadcast-IPX-Pakete
IPX-LAN-Rx-Multicasts	Anzahl vom LAN empfangener Multicast-IPX-Pakete
IPX-LAN-Rx-Unicasts	Anzahl vom LAN empfangener direkt adressierter IPX-Pakete
IPX-LAN-Tx	Anzahl zum LAN gesendeter IPX-Pakete
IPX-WAN-Rx	Anzahl vom WAN empfangener IPX-Pakete
IPX-WAN-Rx-Broadcasts	Anzahl vom WAN empfangener Broadcasts
IPX-WAN-Rx-Multicasts	Anzahl vom WAN empfangener Multicasts
IPX-WAN-Rx-Unicasts	Anzahl vom WAN empfangener direkt adressierter IPX-Pakete
IPX-WAN-Tx	Anzahl zum WAN gesendeter IPX-Pakete
Werte löschen	MAC-Statistik löschen

Status/IPX-Statistik/Watchdog-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

IPX-Watchdog-LAN-Rx	Anzahl vom LAN empfangener IPX-Watchdog-Pakete
IPX-Watchdog-LAN-Tx	Anzahl zum LAN gesendeter IPX-Watchdog-Pakete
IPX-Watchdog-WAN-Rx	Anzahl vom WAN empfangener IPX-Watchdog-Pakete

IPX-Watchdog-WAN-Tx	Anzahl zum WAN gesendeter IPX-Watchdog-Pakete
SPX-Watchdog-LAN-Rx	Anzahl vom LAN empfangener SPX-Watchdog-Pakete
SPX-Watchdog-LAN-Tx	Anzahl zum LAN gesendeter SPX-Watchdog-Pakete
SPX-Watchdog-WAN-Rx	Anzahl vom WAN empfangener SPX-Watchdog-Pakete
SPX-Watchdog-WAN-Tx	Anzahl zum WAN gesendeter SPX-Watchdog-Pakete
Werte löschen	Watchdog Statistik löschen

Status/IPX-Statistik/Propagate-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

Propagate-LAN-Rx	Anzahl vom LAN empfangener IPX-Propagated-Pakete
Propagate-LAN-Filter	Anzahl vom LAN empfangener/gefilterter IPX-Propagated-Pakete
Propagate-LAN-Tx	Anzahl zum LAN gesendeter IPX-Propagated-Pakete
Propagate-LAN-Socket-Fehler	Anzahl vom LAN über Socket-Filter gefilterter IPX-Propagated-Pakete
Propagate-LAN-Hop-Fehler	Anzahl vom LAN über Hop-Count gefilterter IPX-Propagated-Pakete
Propagate-LAN-Backroute-Fehler	Anzahl vom LAN zurückzuroutende IPX-Propagated-Pakete
Propagate-LAN-Contention	Anzahl vom LAN zu routende Pakete während einer falschen Verbindung
Propagate-WAN-Rx	Anzahl vom WAN empfangener IPX-Propagated-Pakete
Propagate-WAN-Filter	Anzahl vom WAN empfangener/gefilterter IPX-Propagated-Pakete
Propagate-WAN-Tx	Anzahl zum WAN gesendeter IPX-Watchdog-Pakete
Propagate-WAN-Socket-Fehler	Anzahl vom WAN über Socket-Filter gefilterter IPX-Propagated-Pakete
Werte löschen	IPX-Propagated-Paket-Statistik löschen

Status/IPX-Statistik/RIP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

RIP-LAN-Rx	Anzahl vom LAN empfangener RIP-Pakete
RIP-LAN-Fehler	Anzahl vom LAN empfangener RIP-Pakete mit fehlerhaftem Inhalt
RIP-LAN-Tx	Anzahl zum LAN gesendeter RIP-Pakete
RIP-WAN-Rx	Anzahl vom WAN empfangener RIP-Pakete
RIP-WAN-Fehler	Anzahl vom WAN empfangener RIP-Pakete mit fehlerhaftem Inhalt
RIP-WAN-Tx	Anzahl zum WAN gesendeter RIP-Pakete
Werte löschen	RIP-Statistik löschen
Tabelle-RIP	Anzeige der RIP-Tabelle

Tabelle-RIP In der **RIP-Tabelle** finden Sie 256 Einträge mit RIP-Informationen. Sie hat den folgenden Aufbau:

Netzwerk	Hops	Tics	Node-ID	Zeit	Flags
Adresse des Netzwerks	Anzahl der zu passierenden Router auf dem Weg zum anderen Netz	Benötigte Zeit für diese Route in tics	MAC-Adresse des Servers	Anzahl der Aktualisierungen der Tabelle, bis der Eintrag entfernt wird	lokal, remote, loop oder down

Status/IPX-Statistik/SAP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

SAP-LAN-Rx	Anzahl vom LAN empfangener SAP-Pakete
SAP-LAN-Fehler	Anzahl vom LAN empfangener SAP-Pakete mit fehlerhaftem Inhalt
SAP-LAN-Tx	Anzahl zum LAN gesendeter SAP-Pakete
SAP-WAN-Rx	Anzahl vom WAN empfangener SAP-Pakete
SAP-WAN-Fehler	Anzahl vom WAN empfangener SAP-Pakete mit fehlerhaftem Inhalt
SAP-WAN-Tx	Anzahl zum WAN gesendeter SAP-Pakete
Werte löschen	SAP-Statistik löschen
Tabelle-SAP	Anzahl vom LAN empfangener SAP-Pakete

Tabelle-SAP In der **SAP-Tabelle** finden Sie 512 Einträge mit SAP-Informationen. Sie hat den folgenden Aufbau:

Typ	Server-Name	Netzwerk	Node-ID	Socket	Hops	Zeit	Flags
SAP-Nr. des Dienstes	Rechnername des Servers	Adresse des Netzwerks	MAC-Adresse des Servers	Socket für den Dienst	Anzahl der Router bis zum Ziel-Netz	Anzahl der Aktualisierungen der Tabelle, bis der Eintrag entfernt wird	lokal, remote, loop oder down

Status/IPX-Statistik/IPX-Router-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

IPXr-LAN-Rx	Anzahl vom LAN zu routender IPX-Pakete
IPXr-LAN-Tx	Anzahl zum LAN gerouteter IPX-Pakete
IPXr-LAN-Hop-Fehler.	Anzahl vom LAN zu routender über Hop-Count gefilterter IPX-Pak.
IPXr-LAN-Socket-Fehler	Anzahl vom LAN zu routender über Socket-Filter gefilterter IPX-Pakete
IPXr-LAN-Netzwerk-Fehler	Anzahl vom LAN zu routende Pakete zu falschen Netzwerken
IPXr-LAN-Backroute-Fehler	Anzahl vom LAN zurückzuroutende IPX-Pakete
IPXr-LAN-Contention	Anzahl vom LAN zu routender Pakete während einer falschen Verbindung

IPXr-LAN-Down-Fehler	Anzahl vom LAN zu routender IPX-Pakete zu abgemeldeten Netzen
IPXr-WAN-Rx	Anzahl vom WAN zu routender IPX-Pakete
IPXr-WAN-Tx	Anzahl zum WAN gerouteter IPX-Pakete
IPXr-WAN-Hop-Fehler.	Anzahl vom WAN zu routender über Hop-Count gefilterter IPX-Pakete
IPXr-WAN-Socket-Fehler	Anzahl vom WAN zu routender über Socket-Filter gefilterter IPX-Pak.
IPXr-WAN-Netzwerk-Fehler	Anzahl vom WAN zu routender Pakete zu falschen Netzwerken
IPXr-WAN-Backroute-Fehler	Anzahl vom WAN zurückzuroutender IPX-Pakete
IPXr-WAN-Down-Fehler	Anzahl vom WAN zu routender IPX-Pakete zu abgemeldeten Netzen
IPXr-Int-Rx	Anzahl der Pakete von internen Modulen an den IPX-Router
Netzwerke	Tabelle der Netzwerke in der IPX-Routing-Tabelle mit Node-IDs
Werte löschen	IPX-Router-Statistik löschen
Aufbau-Tabelle	Tabelle der letzten 20 Pakete, die eine Verbindung erforderten

Aufbau-Tabelle Die **Aufbau-Tabelle** ist ein weiterer Unterpunkt der Router-Statistik. Darin finden Sie die letzten 20 Einträge mit Informationen über die Systemzeit, die IPX-Ziel-Adresse, die IPX-Quell-Adresse der Datenpakete, die zu einem Verbindungsaufbau geführt haben.

Eine IPX-Aufbau-Tabelle kann wie folgt aussehen:

Systemzeit	Ziel-Adresse	Quell-Adresse
1T; 16:45:01	00000081 ffffffff 0453	00000001 00a05702000a 0453
1T; 10:45:10	00000081 ffffffff 0452	00000001 00a05702000a 0452

Als 'Systemzeit' wird entweder die Betriebszeit des Geräts angezeigt oder die Echtzeit des ISDN-Netzes (falls diese vom ISDN-Anschluß zur Verfügung gestellt wird). Die Ziel-Adresse 'fffffff' deutet z.B. auf ein Broadcast-Paket hin. Die Ziel- und Quell-Adressen besteht jeweils aus der Netzwerknummer, MAC-Adresse und der Socketnummer (alles hexadezimale Werte).

Netzwerke Auch die **Netzwerk-Statistik** ist der IPX-Router-Statistik untergliedert. Diese Tabelle zeigt erweiterte Informationen zu einer statischen Route (Gegenstelle). Sie hat den folgenden Aufbau:

Gegenstelle	Netzwerk	Binding	Propagate	Backoff	Zeit	Node-ID
logische Gegenstelle	Netzwerk-Adresse	Binding	Route /Filter	Aufbau-Zähler	Restzeit bis zum nächsten Aufbau	Node-ID der Gegenstelle

Die Einträge habe die folgende Bedeutung:

Gegenstelle	Logischer Name der Gegenstelle, wie in der Routing-Tabelle eingetragen. Zusätzlich ist noch ein Eintrag für die LAN-Anbindung vorhanden. Dieser steht an erster Stelle der Tabelle und hat den Namen „LAN“.
Netzwerk	Adresse des Netzwerks in dem sich die Gegenstelle befindet. Für WAN-Gegenstellen entspricht dieser dem Eintrag in der Routing-Tabelle. Falls in der IPX-Routing-Tabelle (/SETUP/IPX-MODUL/LAN-EINSTELLUNG/NETZWERK) die Autodetect-Funktion eingestellt ist, kann an dieser Stelle abgelesen werden, welches Netzwerk erkannt wurde.
Binding	Ethernet-Binding, auf das die Gegenstelle gebunden ist. Für WAN-Gegenstellen entspricht dieses dem Eintrag in der Routing-Tabelle. Falls in der IPX-Routing-Tabelle (/SETUP/IPX-MODUL/LAN-EINSTELLUNG/NETZWERK) die Autodetect-Funktion eingestellt ist, kann an dieser Stelle abgelesen werden, welches Binding erkannt wurde.
Propagate	Filterflag für IPX Typ 20 (propagated) Frames. Für WAN-Gegenstellen entspricht dieses dem Eintrag in der Routing-Tabelle. Für das LAN ist hier immer Route eingetragen.
Backoff	Aufbau-Zähler für den Exponential-Backoff-Algorithmus. Wenn der Aufbau-Zähler den Wert 16 hat, so wird kein erneuter Versuch mehr durchgeführt, die Route ist damit inaktiv (auch für das LAN möglich).
Zeit	Restzeit bis zum nächsten Aufbauversuch des Exponential-Backoff-Algorithmus in Sekunden. War ein Aufbau erfolgreich, so wird die Restzeit auf Null gesetzt. Damit ist die Route aktiv.
Node-ID	Node-ID des zuständigen Routers im WAN-Netz. Für den LAN-Eintrag ist hier die Node-ID des Routers eingetragen.

Status/TCP-IP-Statistik

Hier werden die Statistiken aus dem TCP/IP-Bereich dargestellt, gegliedert nach verschiedenen Typen von Subprotokollen des TCP/IP. In der TCP-IP-Statistik finden Sie die folgenden Parameter:

/TCP-IP-Statistik		Statistiken aus dem TCP/IP-Bereich
ARP-Statistik		Statistiken aus dem ARP-Bereich
IP-Statistik		Statistiken aus dem IP-Bereich
ICMP-Statistik		Statistiken für ICMP-Pakete
TCP-Statistik		Statistiken für TCP-Pakete von TCP-Sitzungen zum Router
TFTP-Statistik		Statistiken für TFTP-Operationen
DCHP-Statistik		Statistiken aus dem DCHP-Server
NetBIOS-Statistik		Statistiken aus dem NetBIOS-Modul
DNS-Statistik		Statistiken aus dem DNS-Server
Werte löschen		TCP/IP-Statistiken löschen

In den Unterstatistiken finden Sie dann die weiteren Parameter zu den einzelnen Menüs.

Status/TCP-IP-Statistik/ARP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

ARP-LAN-Rx	Anzahl vom LAN empfangener ARP-Anfragen und -Antworten
ARP-LAN-Tx	Anzahl zum LAN gesendeter ARP-Anfragen und -Antworten
ARP-LAN-Fehler	Anzahl vom LAN fehlerhaft empfangener ARP-Anfragen
ARP-WAN-Rx	Anzahl vom WAN empfangener ARP-Anfragen und -Antworten
ARP-WAN-Tx	Anzahl zum WAN gesendeter ARP-Anfragen und -Antworten
ARP-WAN-Fehler	Anzahl vom WAN fehlerhaft empfangener ARP-Anfragen
Werte löschen	ARP-Statistiken löschen
Tabelle-ARP	Anzeige der ARP-Tabelle

Tabelle-ARP

In der **ARP-Tabelle** finden Sie 128 Einträge mit ARP-Informationen. Sie hat den folgenden Aufbau:

IP-Adresse	Node-ID	Letzter Zugriff	Anschluß
IP-Adresse, die schon einmal über ARP-Request gefunden wurde	zugehörige MAC-Adresse	Zeit seit dem letzten Zugriff in tics	lokal oder remote

Status/TCP-IP-Statistik/IP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

IP-LAN-Rx	Anzahl vom LAN empfangener IP-Pakete
IP-LAN-Tx	Anzahl zum LAN gesendeter IP-Pakete
IP-LAN-Checksummen-Fehler	Anzahl vom LAN fehlerhaft empfangener IP-Pakete
IP-LAN-Service-Fehler	Anzahl vom LAN empfangener IP-Pakete für falschen Dienst
IP-WAN-Rx	Anzahl vom WAN empfangener IP-Pakete
IP-WAN-Tx	Anzahl zum WAN gesendeter IP-Pakete
IP-WAN-Checksummen-Fehler	Anzahl vom WAN fehlerhaft empfangener IP-Pakete
IP-WAN-Service-Fehler	Anzahl vom WAN empfangener IP-Pakete für falschen Dienst
IP-WAN-Rx-verworfen	Anzahl vom WAN durch Time-Out-Management verworfener Pakete
Werte löschen	IP-Statistiken löschen

Status/TCP-IP-Statistik/ICMP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

ICMP-LAN-Rx	Anzahl vom LAN empfangener ICMP-Pakete
ICMP-LAN-Tx	Anzahl zum LAN gesendeter ICMP-Pakete
ICMP-LAN-Checksummen-Fehler	Anzahl vom LAN fehlerhaft empfangener ICMP-Pakete
ICMP-LAN-Service-Fehler	Anzahl vom LAN empfangener, nicht unterstützter ICMP-Pakete
ICMP-WAN-Rx	Anzahl vom WAN empfangener ICMP-Pakete
ICMP-WAN-Tx	Anzahl zum WAN gesendeter ICMP-Pakete
ICMP-WAN-Checksummen-Fehler	Anzahl vom WAN fehlerhaft empfangener ICMP-Pakete
ICMP-WAN-Service-Fehler	Anzahl vom WAN empfangener, nicht unterstützter ICMP-Pakete
Werte löschen	ICMP-Statistiken löschen

Status/TCP-IP-Statistik/TCP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

TCP-LAN-Rx	Anzahl vom LAN empfangener TCP-Pakete
TCP-LAN-Tx	Anzahl zum LAN gesendeter TCP-Pakete
TCP-LAN-Tx-Wdh.	Anzahl zum LAN wiederholt gesendeter TCP-Pakete
TCP-LAN-Checksummen-Fehler	Anzahl vom LAN fehlerhaft empfangener TCP-Pakete
TCP-LAN-Service-Fehler	Anzahl vom LAN empfangener TCP-Pakete für falschen Port
TCP-LAN-Verbindungen	Anzahl der aktuellen TCP-Verbindungen vom LAN
TCP-WAN-Rx	Anzahl vom WAN empfangener TCP-Pakete
TCP-WAN-Tx	Anzahl zum WAN gesendeter TCP-Pakete
TCP-WAN-Tx-Wiederholungen	Anzahl zum WAN wiederholt gesendeter TCP-Pakete
TCP-WAN-Checksummen-Fehler	Anzahl vom WAN fehlerhaft empfangener TCP-Pakete
TCP-WAN-Service-Fehler	Anzahl vom WAN empfangener TCP-Pakete für falschen Port
TCP-WAN-Verbindungen	Anzahl aktueller TCP-Verbindungen vom WAN
Werte löschen	TCP-Statistiken löschen

Status/TCP-IP-Statistik/TFTP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

TFTP-LAN-Rx	Anzahl vom LAN empfangener TFTP-Pakete
TFTP-LAN-Rx-Read-Request	Anzahl vom LAN empfangener TFTP-Read-Requests
TFTP-LAN-Rx-Write-Request	Anzahl vom LAN empfangener TFTP-Write-Requests
TFTP-LAN-Rx-Data	Anzahl vom LAN empfangener TFTP-Daten-Pakete
TFTP-LAN-Rx-Ack.	Anzahl vom LAN empfangener TFTP-Acknowledges

TFTP-LAN-Rx-Option-Ack.	Anzahl vom LAN empfangener TFTP-Option-Acknowledges
TFTP-LAN-Rx-Fehler	Anzahl vom LAN empfangener TFTP-Error-Pakete
TFTP-LAN-Rx-unb.	Anzahl vom LAN empfangener, unbekannter TFTP-Pakete
TFTP-LAN-Tx	Anzahl auf das LAN gesendeter TFTP-Pakete
TFTP-LAN-Tx-Data	Anzahl auf das LAN gesendeter TFTP-Daten-Pakete
TFTP-LAN-Tx-Ack.	Anzahl auf das LAN gesendeter TFTP-Acknowledges
TFTP-LAN-Tx-Option-Ack.	Anzahl auf das LAN gesendeter TFTP-Option-Ack
TFTP-LAN-Tx-Fehler	Anzahl auf das LAN gesendeter TFTP-Error-Pakete
TFTP-LAN-Tx-Wiederholungen	Anzahl wiederholt aufs LAN gesendeter TFTP-Pakete
TFTP-LAN-Verbindungen	Anzahl zum LAN aufgebauter TFTP-Verbindungen
TFTP-WAN-Rx	Anzahl vom WAN empfangener TFTP-Pakete
TFTP-WAN-Rx-Read-Request	Anzahl vom WAN empfangener TFTP-Read-Requests
TFTP-WAN-Rx-Write-Request	Anzahl vom WAN empfangener TFTP-Write-Requests
TFTP-WAN-Rx-Data	Anzahl vom WAN empfangener TFTP-Daten-Pakete
TFTP-WAN-Rx-Ack.	Anzahl vom WAN empfangener TFTP-Acknowledges
TFTP-WAN-Rx-Option-Ack.	Anzahl vom WAN empfangener TFTP-Option-Acknowledges
TFTP-WAN-Rx-Fehler	Anzahl vom WAN empfangener TFTP-Error-Pakete
TFTP-WAN-Rx-unb.	Anzahl vom WAN empfangener, unbekannter TFTP-Pakete
TFTP-WAN-Tx	Anzahl auf das WAN gesendeter TFTP-Pakete
TFTP-WAN-Tx-Data	Anzahl auf das WAN gesendeter TFTP-Daten-Pakete
TFTP-WAN-Tx-Ack.	Anzahl auf das WAN gesendeter TFTP-Acknowledges
TFTP-WAN-Tx-Option-Ack.	Anzahl auf das WAN gesendeter TFTP-Option-Ack
TFTP-WAN-Tx-Fehler	Anzahl auf das WAN gesendeter TFTP-Error-Pakete
TFTP-WAN-Tx-Wiederholungen	Anzahl wiederholt aufs WAN gesendeter TFTP-Pakete
TFTP-WAN-Verbindungen	Anzahl zum WAN aufgebauter TFTP-Verbindungen
Werte löschen	TFTP-Statistik löschen

Status/TCP-IP-Statistik/DHCP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

DHCP-LAN-Rx	Anzahl aus dem LAN empfangener DHCP-Pakete
DHCP-LAN-Tx	Anzahl in das LAN gesendeter DHCP-Pakete
DHCP-WAN-Rx	Anzahl aus dem WAN empfangener DHCP-Pakete
DHCP-Verworfen	Anzahl verworfener DHCP-Pakete
DHCP-Rx-Discover	Anzahl empfangener Discover-Messages
DHCP-Rx-Request	Anzahl empfangener Request-Messsges
DHCP-Rx-Dcline	Anzahl empfangener Decline-Messages
DHCP-Rx-Inform	Anzahl empfangener Inform-Messages

DHCP-Rx-Release	Anzahl empfangener Release-Messages
DHCP-Tx-Offer	Anzahl gesendeter Offer-Messages
DHCP-Tx-Ack.	Anzahl bestätigter DHCP-Pakete
DHCP-Tx-Nak	Anzahl nicht bestätigter DHCP-Pakete
DCHP-Server-Fehler	Anzahl empfangener DHCP-Pakete, die nicht für diesen Server bestimmt waren
DHCP-Zugewiesen	Anzahl aktuell zugewiesener Adressen
DHCP-MAC-Konflikte	Anzahl abgelehnter Zuweisungen aufgrund belegter IP-Adressen
Tabelle-DHCP	Tabelle mit den Zuweisungen von IP-Adressen zu MAC-Adressen
Werte löschen	DHCP-Statistik löschen

Tabelle-DHCP In der **DHCP-Tabelle** finden Sie Einträge mit DHCP-Informationen. Sie enthält 16 (oder vielfache von 16) Einträge. Die Tabelle paßt sich dynamisch an die Erfordernisse an und wächst oder schrumpft entsprechend. Sie hat den folgenden Aufbau:

IP-Adresse	Node-ID	Timeout	Rechner-name	Typ
IP-Adresse, die über DHCP zugewiesen wurde	zugehörige MAC-Adresse	Gültigkeitsdauer der Zuweisung in Minuten	Name des Rechners	Art der Zuweisung

Status/TCP-IP-Statistik/NetBIOS

Über das Menü /Status/TCP-IP-Statistik/NetBIOS-Statistik können zusätzliche Informationen über das NetBIOS-Modul erhalten werden. Dieses Menü hat den folgenden Aufbau:

LAN-Rx, WAN-Rx		Anzahl der NetBIOS-Pakete, die vom LAN bzw. WAN empfangen wurden
LAN-Tx, WAN-Tx		Anzahl der NetBIOS-Pakete, die auf das LAN bzw. WAN gesendet wurden
Registrierungen		Anzahl der erfolgten Namenregistrierungen
Konflikte		Anzahl der festgestellten Namenskonflikte. Da das NetBIOS-Modul nur eine Art schwarzes Brett ist, an dem jeder Rechner seinen Namen anheftet, überprüft es auch nicht die Konsistenz der Daten. Daher wird der Zähler nur erhöht, wenn ein Host selbst einen Konflikt festgestellt hat und dieses über einen Broadcast im Netz bekannt macht
Freigaben		Anzahl der erfolgten Namensfreigaben
Erneuerungen		Anzahl der erfolgten Namenserneuerungen (Refresh)
Timeouts		Anzahl der durch Alterung herausgefallenen Namen
B-Knoten		Anzahl der gerade aktiven B-Knoten (Broadcast) im Netz

P-Knoten		Anzahl der gerade aktiven P-Knoten (Peer-to-Peer) im Netz
M-Knoten		Anzahl der gerade aktiven M-Knoten (Mixed-Mode) im Netz
W-Knoten		Anzahl der gerade aktiven W-Knoten (Hybrid) im Netz

B-Knoten Broadcast-Knoten. Ein B-Knoten führt die Namenverhandlung ausschließlich über Broadcasts durch. Ein solcher Rechner ist über eine Routerverbindung hinweg nicht zu sehen, da Broadcasts nicht geroutet werden dürfen.

P-Knoten Point-To-Point-Knoten. Ein P-Knoten benötigt zur Namensverhandlung einen NetBIOS-Nameserver (NBNS) sowie zur Datagrammübermittlung über einen Router hinweg einen NetBIOS-Datagram-Distribution-Server (NBDD).

M-Knoten Mixed-Knoten. Dieser Knoten-Typ stellt eine Mischung aus B- und P-Knoten dar. Im lokalen Netz verhält er sich wie ein B-Knoten, ist der gewünschte Kommunikationspartner nicht im lokalen Netz zu finden, so wird versucht ihn über eine NBNS-Anfrage aufzulösen (P-Knoten-Verhalten).

W-Knoten Diese Art von Knoten ist nach RFC nicht zulässig, trotzdem hat Microsoft sie als Hybrid-Knoten eingeführt.

Status/TCP-IP-Statistik/DNS-Statistik

Der DNS-Statistik können zusätzliche Informationen über das DNS-Modul entnommen werden. Dieses Menü hat den folgenden Aufbau:

LAN-Rx		Anzahl der DNS-Pakete, die vom LAN empfangen wurden
LAN-Tx		Anzahl der DNS-Pakete, die zum LAN gesendet wurden
WAN-Rx		Anzahl der DNS-Pakete, die vom WAN empfangen wurden
WAN-Tx		Anzahl der DNS-Pakete, die zum WAN gesendet wurden
Forwarded		Anzahl der Anfragen, die nicht beantwortet werden konnten und daher über den Forwarding-Mechanismus weitergeleitet wurden
Fehler		Anzahl von ungültigen Anfragen
DNS-Zugriffe		Gibt an, wie viele Namen aus der DNS-Tabelle aufgelöst wurden
DHCP-Zugriffe		Gibt an, wie viele Namen aus der DHCP-Tabelle aufgelöst wurden
NetBIOS-Zugriffe		Gibt an, wie viele Namen aus den NetBIOS-Tabellen aufgelöst wurden
Hit-Liste		In dieser Tabelle tauchen die 16 häufigsten Anfragen auf. Diese können dann unter Umständen über die Filterliste abgeblockt werden.

Die Hitliste hat den folgenden Aufbau

Name	Requests	Zeit	Ip-Adresse
www.elsa.de	1	00.00.0000 00:00:29	10.0.0.123

Die einzelnen Felder dieser Liste haben die folgende Bedeutung

Name	Name des abgefragten Rechners
Requests	Gesamtzahl der Anfragen auf diesen Namen, seit er in die Tabelle steht
Zeit	Zeitpunkt der letzten Abfrage
IP-Adresse	Adresse des Rechners, der diesen Namen zuletzt abgefragt hat

Diese Liste ist nach Anzahl der Anfragen sortiert. Wenn die Tabelle voll ist, wird bei jeder neu eintreffenden Anfrage immer der am längsten nicht nachgefragte Name aus der Tabelle gelöscht.

Status/IP-Router-Statistik

Hier werden die Statistiken aus dem IP-Router-Modul gesammelt.

/IP-Router-Statistik		Statistiken aus dem IP-Router-Bereich
IPr-LAN-Rx		Anzahl vom LAN zu routender Datenpakete
IPr-LAN-Tx		Anzahl zum LAN gerouteter Datenpakete
IPr-LAN-lokales-Routing		Anzahl vom LAN empfangener und zum LAN gerouteter Pakete
IPr LAN-Netzwerk-Fehler		Anzahl LAN-Pakete, die nicht geroutet wurden
IPr-LAN-Routing-Fehler		Anzahl LAN-Pakete, die zu einem anderen Router müssen
IPr-LAN-TTL-Fehler		Anzahl LAN-Pakete mit einem abgelaufenen Time-to-Live-Wert
IPr-LAN-Filter		Anzahl der über die Filtertabelle gefilterten LAN-Pakete
IPr-LAN-verworfen		Anzahl der verworfenen LAN-Pakete
IPr-WAN-Rx		Anzahl vom WAN zu routender Datenpakete
IPr-WAN-Tx		Anzahl zum WAN gerouteter Datenpakete
IPr-WAN-Netzwerk-Fehler		Anzahl WAN-Pakete, die nicht geroutet wurden
IPr-WAN-TTL-Fehler		Anzahl WAN-Pakete mit einem abgelaufenem Time-to-Live-Wert
IPr-WAN-Filter		Anzahl der über die Filtertabelle gefilterten WAN-Pakete
IPr-WAN-verworfen		Anzahl der verworfenen WAN-Pakete

/IP-Router-Statistik	Statistiken aus dem IP-Router-Bereich	
IPr-WAN-Typ-Fehler		Anzahl der Pakete vom WAN ohne IP-Router-Kennung
IPr-ARP-Fehler		Anzahl der nicht erfolgreichen Zugriffe auf den ARP-Cache
Werte löschen		IP-Router-Statistik löschen
Aufbau-Tabelle		Tabelle der letzten 20 Pakete, die eine Verbindung erforderten
Protokoll-Tabelle		Tabelle über geroutete Pakete, protokollabhängig aufgestellt
RIP-Statistik		Statistiken aus dem IP/RIP-Bereich

Aufbau-Tabelle In der **Aufbau-Tabelle** sind die letzten 20 Einträge, die Informationen über die Systemzeit, Ziel-Adresse und Quell-Adresse, IP-Protokoll, Ziel-Port und Quell-Port der Datenpakete enthalten, die zu einem Verbindungsaufbau führen sollten.

Eine IP-Router-Aufbau-Tabelle kann wie folgt aussehen:

Systemzeit	Ziel-Adresse	Quell-Adresse	Protokoll	Z-Port	Q-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

Als 'Systemzeit' wird entweder die Betriebszeit des Geräts angezeigt oder die Systemzeit des ISDN-Netzes (falls diese vom ISDN-Anschluß zur Verfügung gestellt wird). Die Ziel- und Quell-Adressen sind jeweils IP-Adressen, das Protokoll kann zum Beispiel auf tcp, udp oder ähnliches hinweisen und die Ziel- und Quell-Ports definieren näher die betroffenen Dienste (Telnet z.B. über TCP und Z-Port. 23, Nameserver über UDP und Z-Port 53).

Protokoll-Tabelle

Auch die Protokoll-Tabelle liefert wertvolle Daten über das zum LAN oder WAN übertragene Paketvolumen. Diese Werte sind aufgeschlüsselt nach den unterschiedlichen IP-Protokollen, zum Beispiel ICMP, TCP, UDP.

Eine Protokoll-Tabelle kann wie folgt aussehen:

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

Status/IP-Router-Statistik/RIP-Statistik

Hier werden die vom Gerät empfangenen IP-RIP-Pakete angezeigt. In dieser Unterstatistik finden Sie die folgenden Einträge:

RIP-Rx	Anzahl empfangener IP-RIP-Pakete
RIP-Request	Anzahl empfangener IP-RIP-Request-Pakete
RIP-Response	Anzahl empfangener IP-RIP-Response-Pakete
RIP-verworfen	Anzahl verworfener IP-RIP-Pakete
RIP-Fehler	Anzahl fehlerhafter IP-RIP-Pakete
RIP-Eintrag-Fehler	Anzahl fehlerhafter Einträge in IP-RIP-Paketen
RIP-Tx	Anzahl gesendeter IP-RIP-Pakete
Tabelle-RIP	Routing-Tabelle der durch RIP-Broadcast gelernten Routen

Tabelle-RIP

In der zugehörigen RIP-Tabelle stehen alle aus dem Netz gelernten Routen. Diese Tabelle wird vom Router selber verwaltet und kann nicht manuell verändert werden.

Eine IP-RIP-Tabelle kann wie folgt aussehen:

IP-Adresse	IP-Netz-Maske	Zeit	Distanz	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-Statistik

Hier werden die Statistiken aus dem Bereich der Remote-Konfiguration angezeigt. Die Informationen über die Anzahl aller bereits gehaltenen sowie der aktuellen Konfigurationssitzungen sind jederzeit abrufbar. Die Aufschlüsselung geschieht nach LAN-, WAN- und Outband-Anschluß.

/Config-Statistik	Statistiken der Remote-Konfiguration	
LAN-Akt.-Verbindungen		Anzahl aktueller Konfigurationsverbindungen vom LAN
LAN-Ges.-Verbindungen		Anzahl bisheriger Konfigurationsverbindungen vom LAN
WAN-Akt.-Verbindungen		Anzahl aktueller Konfigurationsverbindungen vom WAN
WAN-Ges.-Verbindungen		Anzahl bisheriger Konfigurationsverbindungen vom WAN
Outband-Akt.-Verbindungen		Anzahl aktueller Outband-Konfigurationsverbindungen
Outband-Ges.-Verbindungen		Anzahl bisheriger Outband-Konfigurationsverbindungen
Outband-Bitrate		Bitrate der letzten Outband Konfigurationssitzung
Login-Fehler		Gesamtzahl der fehlerhaften Logins

/Config-Statistik	Statistiken der Remote-Konfiguration	
Login-Sperren		Anzahl der Login-Sperrungen
Login-Ablehnungen		Anzahl der Login-Versuche, während die Login-Sperre aktiv war
Werte löschen		Config-Statistik löschen

Status/Queue-Statistik

In dieser Statistik kann der Durchlauf der einzelnen Pakete in den verschiedenen Modulen der *ELSA LANCOM* beobachtet werden.

/Queue-Statistik	Statistiken über die Queue	
LAN-Heap-Pakete		Anzahl verfügbarer Puffer
LAN-Queue-Pakete		Anzahl belegter Puffer
WAN-Heap-Pakete		Anzahl verfügbarer Puffer
WAN-Queue-Pakete		Anzahl belegter Puffer
Bridge-interne Queue-Pakete		Anzahl der Bridge-Pakete aus dem LAN
Bridge-externe Queue-Pakete		Anzahl der Bridge-Pakete aus dem WAN
ARP-Query-Queue-Pakete		Anzahl der ARP-Pakete in der Query-Queue
ARP-Queue-Pakete		Anzahl der ARP-Pakete in der normalen Queue
IP-Queue-Pakete		Anzahl der IP-Pakete in der normalen Queue
IP-Urgent-Queue-Pakete		Anzahl der IP-Pakete in der gesicherten Queue
ICMP-Queue-Pakete		Anzahl der ICMP-Pakete
TCP-Queue-Pakete		Anzahl der TCP-Pakete
TFTP-Queue-Pakete		Anzahl der TFTP-Pakete
SNMP-Queue-Pakete		Anzahl der SNMP-Pakete
IPX-Queue-Pakete		Anzahl der IPX-Pakete
RIP-Queue-Pakete		Anzahl der RIP-Pakete
SAP-Queue-Pakete		Anzahl der SAP-Pakete
IPX-Watchdog-Queue-Pakete		Anzahl der IPX-Watchdog-Pakete
SPX-Watchdog-Queue-Pakete		Anzahl der SPX-Watchdog-Pakete
IPX-Router-Queue-Pakete		Anzahl der IPX-Router-Pakete
Prot-Heap-Pakete		Anzahl der Prot-Heap-Pakete
IPR-Queue-Pakete		Anzahl der Pakete, die noch durch den IP-Router bearbeitet werden sollen.

/Queue-Statistik	Statistiken über die Queue	
DHCP-Server-Queue-Pakete		Anzahl der Pakete in der Empfangs-Queue des DHCP-Servers.
IPR-RIP-Queue-Pakete		Anzahl der Pakete in der Empfangs-Queue des IP-RIP-Moduls (für RIP-Anfragen, RIP-Propagierungen ...).
DNS-Sende-Queue		Anzahl der Pakete, die zu DNS- oder NBNS-Servern weitergeleitet werden sollen.
DNS-Empfangs-Queue		Anzahl der Pakete, die von DNS- oder NBNS-Servern kommen und an den Host weitergeleitet werden sollen.
IP-Masq. Sende-Queue		Anzahl der Pakete, die maskiert versendet werden sollen (ins Internet).
IP-Masq. Empfangs-Queue		Anzahl der Pakete, die aus dem Internet empfangen wurden und demaskiert werden müssen.

Status/Verbindungs-Statistik

Über dieses Menü können die Verbindungszeiten, alle angefallene Gebühren und weitere nützliche Informationen über die Auslastung des ISDN-Anschlusses angezeigt werden.

Der Menüpunkt **Status/Verbindungs-Statistik** enthält für jedes verfügbare Interface eine Statistik über die auf diesem Interface aufgebauten Verbindungen. Die dort aufgeführte Tabelle hat folgendes Aussehen:

Ifc	Verbindung	aktiv	passiv	Fehler	Verbindungs-Zeit	Gebuehren
Ch01	0	0	0	0	Keine Verbindung	0
Ch02	0	0	0	0	Keine Verbindung	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
Verbindung	gibt die Anzahl der Verbindungen auf dem jeweiligen Kanal an.
aktiv	gibt die Anzahl der aktiven Verbindungsaufbauten für den Kanal an.
passiv	gibt die Anzahl der Verbindungen durch eingegangene Rufe für den Kanal an.
Fehler	gibt die Anzahl der Verbindungsfehler an.
Verbindungs-Zeit	gibt die Zeit an, seit der die aktuelle Verbindung besteht. Besteht keine Verbindung, so wird „Keine Verbindungen.“ ausgegeben.
Gebühren	gibt die Zahl der Gebühren der aktuellen Verbindung an. Dieser Wert wird bei einem erneuten Verbindungsaufbau wieder auf Null gesetzt.

Die gesamten angefallenen Gebühren werden nicht unmittelbar angezeigt. Es wird jedoch intern eine Summierung der Gebühren durchgeführt, um das Gebührenbudget verwalten zu können (siehe auch **Setup/Gebühren-Modul**).

Status/Info-Verbindung

Der Menüpunkt **Status/Info-Verbindung** enthält für jedes verfügbare Interface weitere Informationen über dessen aktuellen Verbindungszustand (logische Gegenstelle etc.). Die dort aufgeführte Tabelle hat folgendes Aussehen:

lfc	Status	Mode	Rufnummer	Gerätename	B1-HZ	B2-HZ
Ch01	Bereit				0	0
Ch02	Bereit				0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	bezeichnet den zugehörigen Kanal.
Status	gibt den Zustand der jeweiligen Verbindung an. Mögliche Werte sind: Initialisierung , Setup-WAN , Bereit , Anwahl , Anliegender-Ruf , Protokoll , Verbindung , Rückruf sowie Bündelung und Reserviert . Der Status Bündelung wird im Display (nur <i>ELSA LANCOM Business 4100</i>) durch Anfügen von „/2“ in Spalte 15 und 16 der zugehörigen Displayzeile ebenfalls angezeigt. Bündelung erscheint für das zweite Interface, wenn entweder auf dem ersten Interface eine Bündelverbindung aktiviert wurde oder eine Festverbindung mit zwei B-Kanälen eingestellt wurde. Reserviert wird das zweite Interface, wenn auf dem ersten B-Kanal eine Verbindung besteht und die Y-Verbindung deaktiviert wurde.
Mode	gibt die Art des Aufbaus wieder. Möglich sind: Akt. (aktiver Verbindungsaufbau = Anwahl) Pas. (passiver Verbindungsaufbau = Anruf) RR (Aufbau durch Rückruf)
Rufnummer	gibt die Rufnummer der Gegenstelle aus der Namenliste an.
Gerätename	gibt den logischen Namen der Gegenstelle an (sofern dieser auflösbar ist). Der Gerätename wird ebenfalls auf dem Display in der entsprechenden Displayzeile mit angezeigt, sobald eine logische Verbindung besteht.
B1-HZ	gibt die Haltezeit (Short-Hold-Zeit) der Verbindung an.
B2-HZ	gibt die Haltezeit (Short-Hold-Zeit) für gebündelte Kanäle dieser Verbindung an.

Status/Layer-Verbindung

Der Menüpunkt **Status/Layer-Verbindung** enthält für jedes verfügbare Interface Informationen über das auf dem jeweiligen Interface benutzte B-Kanal-Protokoll. Die Einträge dieser Tabelle entsprechen denen der Layerliste **Setup/WAN-Modul/Layer-Liste** im WAN-Modul. Zusätzlich existiert noch ein Eintrag für das Interface selbst. Das Menü hat folgendes Aussehen:

lfc	Layername	Encaps	Lay-3	Lay-2	L2-Opt.	Lay-1
Ch01	DEFAULT	ETHER	ELSA TRANS	X.75ELSA	compr.	HDLC64K
Ch02	PPPHDL	TRANS	TRANS	PPP	Keine	HDLC64K

Status/Ruf-Info-Tabelle

In dieser Tabelle werden die letzten zehn angekommenen Rufe angezeigt, und zwar unabhängig davon, ob der Router den Ruf angenommen hat oder nicht.

Dadurch ist es z.B. möglich, beim Betrieb an einer TK-Anlage herauszufinden, welche interne MSN verwendet wird. Die Tabelle hat den folgenden Aufbau:

Systemzeit	Ifc	CLIP-Anrufer	Wahl-Anrufer	Dienst	B-Kanal
OT; 00:20:57	S ₀	5678	1234	HDLC64K	2
OT; 00:20:46	S ₀	4321	1234	HDLC64K	1
OT; 00:19:47	S ₀	4321	1234	HDLC64K	1
OT; 00:11:33	S ₀	5678	1234	HDLC64K	1
OT; 00:01:13	S ₀	4321	1234	HDLC64K	2
OT; 00:01:02	S ₀	4321	1234	HDLC64K	1
OT; 00:00:06	S ₀	5678	1234	HDLC64K	1

Die Einträge haben die folgende Bedeutung:

Systemzeit	Zeitpunkt, zu dem der Ruf ankam. Dabei wird entweder die Betriebszeit des Geräts angezeigt oder die Systemzeit des ISDN-Netzes (falls diese vom ISDN-Anschluß zur Verfügung gestellt wird).
Ifc	Bezeichnet das zugehörige Interface.
CLIP-Anrufer	Die Rufnummer (CLIP) des Anrufers
Wahl-Anrufer	Die vom Anrufer gewählte MSN/EAZ
Dienst	Hier ist der vom Anrufer gewünschte Dienst eingetragen. Mögliche Werte sind HDLC64K, HDLC56K und unbekannt. Ein analoger Ruf wird hier also als unbekannt angezeigt.
B-Kanal	Hier wird der benutzte B-Kanal eingetragen. Ein Wert von 0 bedeutet, daß alle Kanäle bereits belegt sind, es sich also um ein Anklopfen handelt.



Ein Tip für den Fall, daß ein Router in einer Nebenstellenanlage verwendet wird: Nach einem Anruf mit einem beliebigen ISDN-Endgerät unter der Nummer des ISDN-Busses, wird unter 'Wahl-Anrufer' genau die MSN/EAZ angezeigt, die im Router an der Stelle / Setup/WAN-Modul/Router-Interface-Liste/MSN-EAZ eingetragen werden muß, damit ein Ruf von Außen korrekt angenommen werden kann.

Status/Gegenstellen-Statistik

In dieser Tabelle werden die letzten hundert Verbindungen der *ELSA LANCOM* mit Informationen über die Gegenstelle angezeigt.

Die Tabelle hat den folgenden Aufbau:

Verb.-Start	Gegenstelle	Anw.	Ifc	Verb.-Zeit	Gebühren
OT; 00:20:57	BERLIN	Akt.	Ch01	50	5
OT; 00:20:46	CHEMNITZ	Pas.	Ch02	230	10

Die Einträge haben die folgende Bedeutung:

Verbindungsstart	Zeit, zu der die Verbindung zustande gekommen ist. Dabei wird entweder die Betriebszeit des Geräts angezeigt oder die Systemzeit des ISDN-Netzes (falls diese vom ISDN-Anschluß zur Verfügung gestellt wird).
Gegenstelle	Logischer Gegenstellename
Anwahl	Art des Verbindungsaufbaus: Akt. – die Verbindung wurde aktiv vom Gerät aufgebaut Pas. – das Gerät wurde angerufen RR – das Gerät hat die Gegenstelle zurückgerufen
Ifc	Interface, auf dem die Verbindung zustande gekommen ist (Ch01, Ch02).
Verbindungszeit	Dauer der Verbindung in Sekunden
Gebühren	Für diese Verbindung angefallene Gebühren in Einheiten

Eine Verbindung bleibt mindestens für die Dauer ihres Bestehens in der Tabelle. Jede neue Verbindung füllt die Tabelle von oben her auf. Sollte eine bestehende Verbindung als unterster Eintrag der Tabelle stehen, so wird ggf. eine bereits abgebaute Verbindung stattdessen aus der Tabelle entfernt.

Status/Kanal-Statistik

Diese Tabelle zeigt Ihnen Informationen über den aktuellen Zustand der beiden B-Kanäle. Die Informationen aus dieser Tabelle werden hauptsächlich zur Ausgabe über *ELSA LAN-monitor* verwendet. Daher liegen einige Werte in einer reinen Bitdarstellung vor, die hier nicht näher erläutert wird.

Die Tabelle hat folgenden Aufbau:

Kanal	Zustand	App	Mode	Cause	Rufnummer	Subadr.	Geb.	Verb.-Zeit	Extra	ISDN-Anzeige
S ₀ -1-ERR	00000000	Router	akt.	0000	0241123456	00000000	3	0		
S ₀ -1-B1	00000000	a/b	akt.	0000	0241123457	00000000	2	20		
S ₀ -1-B2	00000000	Lancapi	pass.	0000	0241123458	00000000	4	180		

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Kanal	Kanal, für den der Eintrag gilt. Es wird immer nur der letzte Zustand eines Kanals angezeigt. Für Fehlermeldungen auf Kanälen wird ein eigener „Kanal“ geführt.
Zustand	Als Zustand eines Kanals wird hier z.B. 'bereit' angezeigt.
App	Applikation, die den Kanal belegt: Router, <i>LANCAPI</i>
Mode	Art des letzten Verbindungsaufbaus: aktiv oder passiv
Cause	Letzter aufgetretener Fehler
Rufnummer	Rufnummer der Gegenstelle: bei aktivem Aufbau die gewählte Nummer, bei eingehenden Rufen die Nummer, die übermittelt wird.
Subadresse	Zusatz zur Applikation, die für den Router z.B. den logischen Kanal angibt. Für die <i>LANCAPI</i> z.B. die IP-Adresse des Clients, der die CAPI nutzt.
Geb.	Anzahl der Gebühreneinheiten, die für diese Verbindung angefallen sind
Verb.-Zeit	Dauer der letzten Verbindung auf diesem Kanal
Extras	Zusatzinformation zur Verbindung, z.B. der Name der Gegenstelle bei Routerverbindungen
ISDN-Anzeige	Informationen von der Vermittlungsstelle, z.B. Fehlermeldungen, beim Anschluß an TK-Anlage evtl. auch Name des Anrufers etc.

Status/Zeit-Statistik

In diesem Menü finden Sie Informationen über die aktuelle Zeit im Gerät sowie über den Weg, wie der *ELSA LANCOM Business* zu dieser Zeit gekommen ist.

Das Menü hat folgenden Aufbau:

/Zeit-Statistik	Statistiken aus dem Zeit-Modul	
Aktuelle Zeit		Aktuelle Zeit des Geräts
Quelle		Quelle der Zeitangabe. Mögliche Werte sind: 'ISDN' für die Übernahme der Zeit aus dem ISDN-Netz, 'Manuell' für das manuelle Setzen der Zeit mit dem Befehl 'time', 'RAM' für die Übernahme der Zeit aus dem Zwischenspeicher des Gerätes nach einem Bootvorgang.
Übernahme		Anzahl der bisher erfolgten Zeit-Übernahmen aus einer der vorher genannten Quellen
ISDN		Weitere Informationen zur Übernahme der Zeit aus dem ISDN-Netz

Status/Zeit-Statistik/ISDN

In dieser Statistik werden die folgenden Werte angezeigt:

Verbindung	Anzahl der Versuche, eine Zeitinformation aus dem ISDN-Netz abzulesen
Informationen	Anzahl der aus dem ISDN-Netz erhaltenen Zeitinformationen
Infofehler	Anzahl der fehlerhaften Zeitinformationen aus dem ISDN-Netz

Status/LCR-Statistik

In diesem Menü finden Sie Informationen über die aktuelle Zeit im Gerät sowie über den Weg, wie der *ELSA LANCOM Business* zu dieser Zeit gekommen ist.

Das Menü hat folgenden Aufbau:

/LCR-Statistik		Statistiken aus dem Least Cost Router
Gesamtaufrufe		Gesamtzahl der Aufrufe des LCR
Erfolge		Anzahl der Aufrufe, bei denen der LCR eine passende Regel in seinen Tabellen fand und die Nummer erfolgreich umgeleitet wurde
nicht-gefunden-Fehler		Anzahl der Aufrufe, bei denen der LCR keine passende Regel in seinen Tabellen fand und die Nummer deswegen nicht umgeleitet wurde
fehlende-Zeit-Fehler		Anzahl der Aufrufe, bei denen der LCR mangels fehlender Zeit nicht eingreifen konnte
Provider-Statistik		Eine Tabelle mit allen angerufenen Providern (bzw. deren Vorwahlen), die Anzahl der erfolgreichen bzw. fehlgeschlagenen Anrufe

Status/Werte löschen

Hier können alle Werte der untergeordneten Statistiken bis auf die Tabellen gelöscht werden. Dazu geben Sie folgenden Befehl ein:

```
do werte-loeschen
```

Setup

Über dieses Menü können alle Systemparameter, die für die Funktion der Geräte notwendig sind, abgefragt und geändert werden.

/Setup		Konfiguration des Systems
Name		Eingabe des Gerätenamens
WAN-Modul		Einstellungen für das WAN
Gebühren-Modul		Einstellungen für die Gebührenverwaltung
LAN-Modul		Einstellungen für das LAN
IPX-Modul		Einstellungen für das IPX-Modul (IPX-Router)
TCP-IP-Modul		Einstellungen für das TCP/IP-Modul
IP-Router-Modul		Einstellungen für das IP-Router-Modul
SNMP-Modul		Einstellungen für die Konfiguration über SNMP
DHCP-Modul		Einstellungen für den DHCP-Server
NetBIOS-Modul		Einstellungen für den NetBIOS-Proxy
Config-Modul		Einstellungen für das Konfigurationsmodul
DNS-Modul		Einstellungen für den DNS-Server
LANCAPI-Modul		Einstellungen für die <i>ELSA LANCAPI</i>
LCR-Modul		Einstellungen für den Least-Cost-Router
Zeit-Modul		Einstellungen für das Zeit-Modul

Name

Hier kann der Gerätename (maximal 16 Stellen) eingegeben werden. Der zur Verfügung stehende Zeichensatz beinhaltet Klein- und Großbuchstaben sowie einige Sonderzeichen. Den vollen Umfang können Sie sich in einer Konfigurationssitzung über den Befehl

```
set \setup\name ?
```

anzeigen lassen. Standardmäßig ist kein Name eingetragen.

Der Gerätename wird zur Identifikation benötigt und ist Voraussetzung für eine mögliche Verbindung über die IPX- und IP-Router-Module, da die Router nur mit bekannten Gegenstellen Daten austauschen, sowie für die eindeutige Identifizierung einer Bridge-Gegenstelle.

Bei PPP-Verbindungen wird entweder der Benutzername mit dem Paßwort aus der PPP-Liste oder der Gerätename während einer Überprüfung durch PAP oder CHAP als Identifikation des Gerätes zur Gegenstelle übertragen.

Die Gerätenamen sollten außerdem so vergeben werden, daß sie nicht doppelt auftreten. Empfehlenswert wäre zum Beispiel, den Gerätenamen dem Standort anzupassen (z.B. Aachen, Berlin, Provider etc.).

Setup/WAN-Modul

Hier sind alle Einstellungen zusammengefaßt, die für die Inbetriebnahme der WAN-Interfaces und die Steuerung von Verbindungen zu logischen Gegenstellen notwendig sind.

/WAN-Modul		Einstellungen für das WAN
Interface-Liste		Einstellungen für das S ₀ -Interface
Router-Interface-Liste		Einstellungen für das Interface der Routermodule
Kanal-Liste		Einstellungen für die Verwendung der verfügbaren Kanäle
Namenliste		Einstellungen für die Gegenstellen
Round-Robin-Liste		Einstellungen verschiedener Gegenstellen-Nummern
Layerliste		Einstellungen der verwendeten Layer-Kombinationen
PPP-Liste		Einstellung der Parameter für PPP-Verbindungen
Nummernliste		Einstellung der zugangsberechtigten Rufnummern
Script-Liste		Einstellung der Anwahl-Scripte
Manuelle-Wahl		Einstellungen für die manuelle Verbindungssteuerung
Schutz		Schutz für die Annahme von eingehenden Rufen
RR-Versuche		Anzahl der Rückrufversuche, wenn die Gegenstelle besetzt ist

Interface-Liste Diese Tabelle enthält die Interface-Einstellungen, die für alle Betriebsarten (Module) der Geräte gelten.

lfc	Protokoll	FV-B-Kanal	Anwahl-Prae
S0	Auto	1	0

Zusätzlich können für die einzelnen Module noch weitere, spezielle Interface-Einstellungen vorgenommen werden, z.B. die Rufnummern, auf die ein Modul reagieren soll, siehe auch

```
setup/wan-modul/Router-Interface-Liste
setup/lancapi-modul
```

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	Bezeichnet das zugehörige Interface.
Protokoll	Einstellung des D-Kanal-Protokolls. Mögliche Werte sind: Auto : automatische Erkennung des D-Kanal-Protokolls DSS1 : Euro-ISDN 1TR6 : nationales ISDN GRP0 : Festverbindung Gruppe 0 P2P-DSS1 : Anlagenanschluß
FV-B-Kanal	Einstellung des B-Kanals, auf dem eine Festverbindung ablaufen soll. Mögliche Werte sind: kein : Keine Zuweisung der Festverbindung auf einen bestimmten Kanal. 1 oder 2 : Festverbindung läuft über den angegebenen B-Kanal. Bitte beachten Sie auch die Hinweise zur Einstellung dieser Parameter in der Beschreibung der Festverbindung.
Anwahl-Präe	Globales Anwahlpräfix für alle Module des Geräts. Die hier eingetragenen Ziffern (maximal 8) werden automatisch bei jeder Anwahl vor die gewählte Rufnummer gestellt. Verwenden Sie dieses Präfix z.B. dann, wenn Ihr Router an eine TK-Anlage angeschlossen ist.

Router-Interface-Liste

Diese Tabelle enthält die Interface-Einstellungen, die für die Router-Module der *ELSA LANCOM* gelten.

lfc	MSN/EAZ	YV.	CLIP
S0	123456	Aus	Ein

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	Bezeichnet das zugehörige Interface.
-----	--------------------------------------

MSN-EAZ	<p>Wenn Sie Ihr Gerät an einem ISDN-Anschluß mit 1TR6 angeschlossen haben, geben Sie hier die EAZ ein, auf die das Interface reagieren soll.</p> <p>Wenn Sie Ihr Gerät an einem ISDN-Anschluß mit DSS1 angeschlossen haben, so wird hier die MSN angegeben, auf die das Interface reagieren soll. Soll das Interface auf mehrere MSNs reagieren, so können diese hier mit Semikola getrennt angegeben werden. Ein '#' in der Liste erlaubt beliebige eingehende MSNs.</p> <p>Die erste MSN in dieser Liste wird bei abgehenden Rufen an die Gegenstelle gemeldet. Wenn keine MSN eingetragen wird, überträgt die Vermittlungsstelle die Haupt-MSN des Anschlusses.</p>
YV.	<p>Über diesen Eintrag kann die Fähigkeit des Interfaces, Y-Verbindungen aufzubauen, gesteuert werden. Mögliche Einstellungen sind:</p> <p>Ein: Y-Verbindung wird unterstützt, es können mehrere Verbindungen gleichzeitig aufgebaut werden (Default). Eine Verbindung mit Kanalbündelung wird abgebaut, wenn eine zweite Verbindung zu einer anderen Gegenstelle aufgebaut werden soll.</p> <p>Beachten Sie auch die Einstellungen für die Verfügbarkeit der <i>LANCAPI</i>.</p> <p>Aus: Y-Verbindung wird nicht unterstützt, es kann nur eine Verbindungen aufgebaut werden. Die zweite Verbindung wird blockiert. Wenn eine Verbindung zu einer weiteren Gegenstelle aufgebaut werden soll, wird dieser Aufbau zurückgewiesen. Eine Verbindung mit Kanalbündelung wird nicht beeinträchtigt.</p>
CLIP	<p>Calling Line Identification Protocol: Unterdrückung der abgehenden MSN.</p> <p>Mögliche Werte:</p> <p>Ja: CLIR aktivieren, keine MSN übertragen.</p> <p>Nein: CLIR deaktivieren, MSN zur Gegenstelle übertragen.</p> <p>Bitte beachten Sie: Die „Fallweise Unterdrückung der Rufnummernübermittlung“ muß als Dienstmerkmal ggf. bei der Telefongesellschaft beantragt werden.</p>

Kanal-Liste

Die Kanal-Liste regelt die die Anzahl und Reihenfolge der aufzubauenden Kanäle.

Gerätename	Min	Max	Reihenfolge	Backup
BERLIN	2	2	1-1;1-2	1
INTERNET	2	2	1-1;1-2;2-1;2-2	0
DEFAULT	1	2	0	

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Geraetenname	Name der Gegenstelle, der auch in der Namenliste und der PPP-Liste verwendet wird.
Min	Anzahl der statischen Kanäle. Diese Kanäle werden bei jedem Verbindungsaufbau zu der Gegenstelle aufgebaut.

Max	Anzahl der maximal zu benutzenden Kanäle für diese Gegenstelle. Die Differenz Max-Min gibt die Anzahl der dynamischen Kanäle an.
Reihenfolge	Hier wird definiert, welche Kanäle auf welchem S ₀ -Bus aufzubauen sind. Syntax: [<BusNr>-<KanalNr>][:<BusNr>-<KanalNr>].... Mögliche Werte: 1 bis 4 für die Busse, 1 oder 2 für den Kanal. Ist kein Eintrag vorhanden, wird ein beliebiger Wahlkanal auf einem beliebigen Bus benutzt. Soll eine oder mehrere Festverbindung benutzt werden, muß für jede Festverbindung ein Eintrag vorhanden sein.
Backup	Anzahl der möglichen Backup-Verbindungen. Diese werden dann aufgebaut, wenn alle zulässigen Festverbindungs-Kanäle gestört sind. Eine Backup Verbindung benutzt immer einen beliebigen Wahlkanal auf einem beliebigen Bus.

Namenliste

Die in der Namenliste eingetragenen Gerätenamen werden vom Router benötigt, um die richtige Gegenstelle und den entsprechenden Layernamen zu ermitteln. Zusätzlich wird die Namenliste für die Rückruffunktion verwendet.

In der Namenliste können 64 verschiedene Gerätenamen verwaltet werden, die z.B. so aussehen können:

Geraetenname	Rufnummer	B1-HZ	B2-HZ	Layername	Rückruf
AACHEN	875463	180	0	PPPHDL	ein
BERLIN	040785647	20	20	DEFAULT	aus

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Gerätename	In der Spalte Gerätename können Sie einen eigenen Gegenstellen-Namen eintragen, den Sie dann der entsprechenden Gegenstelle über den Menüpunkt Name des Menüs Setup zuweisen müssen.
Rufnummer	In dieser Spalte können Sie die anzurufende Rufnummer hinterlegen und evtl. mit Wahlsonderzeichen ergänzen (s.u., Standard: keine).
B1-HZ	In dieser Spalte können entsprechende Verbindungshaltezeiten (in Sekunden) für den ersten B-Kanal festgelegt werden. Werden nach Ablauf dieser Zeit keine Daten übertragen, wird die Verbindung auf diesem Kanal wieder abgebaut (Standard: 20). Werden dabei über das ISDN-Netz die Gebühreninformationen während der Verbindung übermittelt, nutzt der <i>ELSA LANCOM</i> eine angefangene Gebühreneinheit vollständig aus und beendet die Verbindung erst kurz vor dem Beginn der nächsten Einheit. Diese Funktion wird auch als dynamischer Short-Hold bezeichnet.

B2-HZ	In dieser Spalte können entsprechende Verbindungshaltezeiten für den zweiten B-Kanal festgelegt werden (analog B1-HZ, Standard: 20). Die B2-Haltezeit steuert bei einer Kanalbündelung das Verhalten der Bündelung. Werte von 0 oder 9999 kennzeichnen eine statische Bündelung, Werte dazwischen eine dynamische Bündelung.
Layername	In dieser Spalte wird ein Name hinterlegt, der in der Layerliste ebenfalls eingetragen sein sollte. Damit wird die für diese Verbindung notwendige Einstellung des Übertragungs-Protokolls festgelegt.
Rückruf	In dieser Spalte können Sie festlegen, ob ein Rückruf für die entsprechende Gegenstelle erfolgen soll (Aus/Name/Auto/Looser/ELSA; Standard: Aus).

■ Rückruffoptionen

Aus	Es erfolgt kein Rückruf.
Looser	Der Router bricht eigene Aufbauversuche ab, wenn ein Ruf von dieser Gegenstelle anliegt (gegenseitiger Verbindungsaufbau). Diese Einstellung muß benutzt werden, wenn ein Rückruf von der Gegenstellen erwartet wird.
Auto (nicht Windows 9x oder Windows NT)	Wenn die Gegenstelle in der Nummernliste eingetragen ist, so wird die Verbindung abgelehnt und ein direkter Rückruf gestartet. Dabei fallen für den Anrufer keine Gebühren an. Ist die Gegenstelle nicht in der Nummernliste eingetragen, so wird in einer Protokollverhandlung (ELSA oder PPP) Rückruf ausgehandelt. Dabei fällt eine Gebühr von einer Einheit an.
Name	Diese Einstellung erzwingt eine Protokollverhandlung. Damit kann über die Nummernliste ein Rufnummernschutz eingestellt und zusätzlich über die Protokollverhandlung ein Rückruf gestartet werden. Dabei fällt eine Gebühr von einer Einheit an.
ELSA	Diese Einstellung ermöglicht ein besonders schnelles Rückrufverfahren. Die zurückgerufene Gegenstelle muß die Einstellung 'Looser' verwenden.

- Die Wahlsonderzeichen der folgenden Tabelle können mit den Rufnummern in der Namen- oder Round-Robin-Liste oder im logischen Anwahlpräfix eingegeben werden. Sie steuern die Amtsholung, die Verwendung einer semipermanenten Festverbindung oder bestimmen das für die Verbindung zu verwendende Interface:

#	Amtsholung (nur bei einigen TK-Anlagen)
F	Die Gegenstelle wird über die Festverbindung erreicht. Syntax: F[Kanal:][Rufnummer] Sowohl Angabe von Kanal als auch Rufnummer sind optional. Der Kanal gibt bei mehreren Festverbindungen den zu verwendenden B-Kanal an. Die Rufnummer gibt je nach Einstellung in der Kanalliste an, ob über die Wahlverbindung eine dynamische Kanalbündelung oder eine Backup-Leitung realisiert werden soll.

Durch Anhängen von **S** oder **S2** an die Rufnummer wird die semipermanente Verbindung (SPV) beim D-Kanal-Protokoll 1TR6 aktiviert.

Eine SPV muß bei der Telefongesellschaft beantragt werden und wird pauschal berechnet.

Wird das Anhängen von **S** oder **S2** vergessen, verhält sich eine SPV wie eine normale Wählleitung, und es entstehen unnötig hohe Gebühren. Die Telekom berechnet Ihnen dann die Pauschalgebühr und die entstandenen Wählleitungsgebühren für die Dauer der Leitungsnutzung.

Round-Robin-Liste

Die Round-Robin-Liste ermöglicht es, eine Gegenstelle unter mehreren Rufnummern zu erreichen. Sie ist wie folgt aufgebaut:

Gerätename	Round-Robin	Anf.
AACHEN	4321-5555-6666	last

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Gerätename	In der Spalte Gerätename können Sie einen Gegenstellennamen aus der Namenliste eintragen. Sollte eine Zeile in der Round-Robin-Liste nicht für alle gewünschten Rufnummern ausreichen, kann diese Zeile wie folgt verlängert werden: Der Gerätename wird um das Zeichen # und einen eindeutigen Index (z.B. AACHEN#1) verlängert und in die nächste Zeile aufgenommen.
Round-Robin	Hier sind die Durchwahlnummern aller möglichen Gegenstellen unter dem entsprechenden Gerätenamen einzugeben. Die einzelnen Durchwahlnummern sind hierbei durch Bindestriche getrennt anzugeben.
Anf.	In der Spalte Anf. sind folgende Einträge möglich: last: Der nächste Verbindungsaufbau beginnt mit der Durchwahl, bei der die letzte Verbindung erfolgreich aufgebaut wurde (Default). frst: Der nächste Verbindungsaufbau beginnt immer mit der ersten Durchwahlnummer. Dieses Feld kann für eine logische Gegenstelle nur über deren ersten Eintrag in der Tabelle geändert werden. Bei allen weiteren Einträgen für diese Gegenstelle wird das Feld automatisch angepaßt.

Layerliste

In der Layerliste können durch Kombination unterschiedlicher ISDN-Layer verschiedene B-Kanal-Protokolle frei definiert werden. Hierdurch kann die Kompatibilität zu Geräten anderer Hersteller, die unterschiedliche B-Kanal-Protokolle verwenden, hergestellt werden.

Die folgende Tabelle dient als Beispiel und zeigt gleichzeitig die Standardeinstellungen für ein *ELSA LANCOM Business*:

Layer-Name	Encaps	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	TRANS	PPP	TRANS	bnd+cmpr	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	none	HDLC64K
MLPPP	TRANS	PPP	TRANS	bnd+cmpr	HDLC64K
RAWHDLC	TRANS	TRANS	TRANS	none	HDLC64K

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Layer-Name	<p>In dieser Spalte können Sie einen eigenen Namen für die von Ihnen verwendete Layer-Kombination aufnehmen. Diese Namen können dann entsprechend ihrer Schreibweise in der Spalte 'Layername' der Namenliste verwendet werden, um das Protokoll einzustellen.</p> <p>Ist in dieser Spalte ein Eintrag mit der Bezeichnung DEFAULT festgelegt, werden die dort abgelegten Einstellungen immer verwendet, wenn kein Layername zugeordnet werden kann (z.B. weil ein Anrufer seine Rufnummer nicht übermittelt). Ebenfalls wird dieser Eintrag verwendet, wenn eine Festverbindung der Gruppe 0 aufgebaut wird. Ist der Eintrag DEFAULT nicht vorhanden, wird standardmäßig ein von ELSA entwickeltes B-Kanal-Protokoll verwendet. Jeder der hier vordefinierten Layer ist vom Benutzer löscht- oder veränderbar.</p>	
Encaps	<p>In der Spalte Encaps können zusätzliche Informationen zu den zu übertragenden Daten festgelegt werden. Folgende Eintragungen sind möglich:</p>	
	ETHER	Die Daten werden mit einem Ethernet-Header versehen. Diese Einstellung ist zur Kommunikation mit älteren <i>ELSA LANCOM</i> -Geräten notwendig.
	TRANS	Bei dieser Einstellung wird kein Ethernet-Header ausgegeben. Es werden z.B. reine IP-Datenpakete übertragen. Diese Einstellung sorgt für den größtmöglichen effektiven Datendurchsatz.
Lay-3	<p>In der Spalte Lay-3 können zusätzliche Header für die Datenübertragung im ISDN definiert werden. Folgende Einstellungen sind wählbar:</p>	
	TRANS	Es wird kein zusätzlicher Header eingefügt (größter Datendurchsatz). Diese Einstellung ist immer zu wählen, wenn die Gegenstelle die Daten transparent auf ISDN-Layer-3 verschickt, (z.B. transparent HDLC, transparent X.75LAPB).
	PPP	Es wird eine Verhandlung nach dem Point-to-Point Protocol durchgeführt.
	APPP	Es wird eine Verhandlung nach dem asynchronen PPP durchgeführt. APPP wird dann verwendet, wenn synchrones PPP nicht möglich ist, weil die Verbindung keine synchrone Übertragung zulässt (z.B. beim analogen Modembetrieb).
	SCPPP	Nach Abschluß der Scriptverarbeitung wird eine synchrone PPP-Verhandlung gestartet.
	SCAPPP	Nach Abschluß der Scriptverarbeitung wird eine asynchrone PPP-Verhandlung gestartet.
	SCTrans	Nach Abschluß der Scriptverarbeitung besteht die Verbindung zur Gegenstelle. Es wird keine weitere Protokoll-Verhandlung durchgeführt.
Lay-2	<p>In dieser Spalte wird das Protokoll für ISDN-Layer-2 eingestellt:</p>	
	TRANS	Die Daten werden direkt in HDLC-Pakete verpackt. Diese Einstellung ist immer dann zu wählen, wenn die Kommunikation über transparent HDLC geschehen soll.
	X.75LAPB	Der Datenaustausch erfolgt im X.75-gesicherten Format. Wählen Sie diese Einstellung immer dann, wenn die Gegenstelle mit einer X.75-Datensicherung arbeiten soll.
L2-Opt.	<p>Die Spalte L2-Opt. ermöglicht die Einstellung einer Option für die Datenübertragungseinstellung unter Lay-2 mit einem weiteren <i>ELSA LANCOM</i>.</p>	
	keine	Es erfolgt keine Datenkompression oder Kanalbündelung.

	compr.	Es erfolgt eine Datenkompression nach Stac. Kompression nach Stac (Hi/fn) muß in Verbindung mit PPP oder Multi-link PPP verwendet werden. Stac-Kompression kann auch in Verbindung mit Windows-Gegenstellen genutzt werden.
	bündeln	Es erfolgt eine Kanalbündelung über mehrere B-Kanäle. Die Kanalbündelung ist nur für die Lay-2-Einstellungen 'PPP' möglich.
	bnd+cmpr	Es erfolgt eine Kanalbündelung und Datenkompression über zwei B-Kanäle.
Lay-1		Die Spalte Lay-1 ermöglicht die Festlegung der Geschwindigkeit, mit der die Daten im ISDN geschickt werden.
	HDLC64K	Die Daten werden mit 64.000 bit/s übertragen.
	HDLC56K	Die Daten werden mit 56.000 bit/s übertragen. Diese Einstellung ist besonders für Verbindungen in die USA von Bedeutung.
	V110_9K6	Die Daten werden bei einer V.110-Verbindung mit 9.600 bit/s übertragen, z.B. bei einer Verbindung mit GSM-Mobiltelefonen.
	V110_19K2	Die Daten werden bei einer V.110-Verbindung mit 19.200 bit/s übertragen.
	V110_38K4	Die Daten werden bei einer V.110-Verbindung mit 38.400 bit/s übertragen.

Für die Anbindung an Geräte anderer Fabrikate erkundigen Sie sich bitte bei dem Hersteller nach dem dort verwendeten Datenformat (PPP wird fast immer unterstützt).

Beim Internet-Zugang und Remote-Access ist in der Regel PPP vorgegeben.

PPP-Liste

Die in der PPP-Liste eingetragenen Gerätenamen werden vom Router benötigt, um die zur Verbindung passenden Einstellungen für das Sicherungsverfahren und die PPP-Parameter zu ermitteln. Sie enthält maximal 64 Einträge und ist wie folgt aufgebaut:

Gerätename	Authent.	Paßwort	Zeit	Wdh.	Conf	Fail	Term	Username	Rechte
AACHEN	CHAP	*****	0	5	10	5	2	ELSA	IP

Nicht alle Parameter sind über die Telnet-Konfiguration erreichbar. Verwenden Sie nach Möglichkeit *ELSA LANconfig*.

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Gerätename	In dieser Spalte können Sie den Namen eintragen, mit dem sich die Gegenstelle beim Router anmeldet. Bei Verbindungen über das DFÜ-Netzwerk ist das der als „Benutzername“ eingetragene Name. Beim Remote-Access über DFÜ-Netzwerk wird das Feld 'Username' (s.u.) nicht ausgewertet! Die Groß- und Kleinschreibung wird nicht berücksichtigt!	
Authentifizierung	In dieser Spalte können Sie das Sicherheitsverfahren, mit dem die Gegenstelle überprüft werden soll, eintragen. Standardwert: PAP	
	Keine	Der Router handelt beim Verbindungsaufbau keine Authentifizierung mit der Gegenstelle aus. Diese kann selbst jedoch eine Authentifizierung vom Router verlangen. Das ist z.B. bei der Anwahl an ISP der Fall.
	PAP	Die Gegenstelle wird nach dem Password Authentication Protocol überprüft.
	CHAP	Die Gegenstelle wird nach dem Challenge Handshake Authentication-Protocol überprüft.
Paßwort	In dieser Spalte kann ein Paßwort eingetragen werden, dessen Vorhandensein durch das Symbol * dargestellt wird und der zur Überprüfung der Gegenstelle dient. Er kann aus 95 Zeichen (7-Bit ASCII, auch Leerzeichen) bestehen. Standardwert: keiner. Mit dem Befehl <code>set ?</code> erhalten Sie eine Liste der erlaubten Zeichen.	
Zeit	In dieser Spalte kann der Zeitraum in Minuten zwischen zwei Überprüfungen der Gegenstelle eingetragen werden. Das Protokoll CHAP muß hierbei eingestellt sein. Standardwert: 0	
Wdh.	Hier kann die Anzahl der Wiederholungen von Überprüfungsversuchen eingestellt werden. Bei fehlgeschlagener Überprüfung wird die Verbindung sofort abgebrochen. Standardwert: 5	
Conf, Fail und Term	Durch diese Parameter kann die Arbeitsweise des PPP beeinflußt werden. Diese Parameter sind im RFC 1661 definiert und beschrieben. Die Standardwerte sind für die meisten Gegenstellen ausreichend. Wird hier nichts eingetragen, erscheinen diese Werte in der Anzeige als 0,0,0. In diesem Fall werden trotzdem die Standardwerte 10, 5, 2 benutzt. Diese Parameter können nur über SNMP oder TFTP (mit dem Konfigurationsprogramm <i>ELSA LANconfig</i>) verändert werden!	
Username	Benutzername (max. 64 Zeichen), der der Gegenstelle während der PPP-Verhandlung übermittelt wird. Damit meldet sich der Router bei der Gegenstelle an. Wird kein Username eingetragen, gilt der Gerätename als Benutzername. Berücksichtigen Sie dabei auch die Groß- und Kleinschreibung.	
Rechte	Netzwerkprotokolle, die über diese Verbindung geroutet werden sollen: IP, IPX, NTB (NetBIOS). NetBIOS erfordert immer eines der beiden anderen Protokolle. Das Routing von IP oder NetBIOS über PPP erfordert immer eine entsprechende Route (in der IP-Routing-Tabelle für IP bzw. in der Gegenstellen-Tabelle für NetBIOS).	

Nummernliste Unter diesem Menüpunkt wird eine Nummernliste verwaltet, in der 64 verschiedene Rufnummern mit dazugehörigen Gerätenamen eingetragen werden können. Damit können die von den Gegenstellen übermittelten Rufnummern (CLI) zu den Gegenstellen-Namen zugeordnet werden.

Einträge in der Nummernliste könnten für zwei anrufende Geräte AACHEN und BERLIN wie folgt aussehen, damit über die mitgeteilte Rufnummer deren Name erkannt und ge-

gebenenfalls ein Rückruf (wenn gewünscht) über die Namenliste durchgeführt werden kann:

Rufnummer	Gerätename
875463	AACHEN
040785647	BERLIN

Diese Nummernliste ist für den passiven Verbindungsaufbau nötig. Die Rufnummern der Gegenstellen müssen ohne führende Nullen eingetragen werden.

Bei einem Rufnummerntest wird dann das momentan aktive D-Kanal-Protokoll berücksichtigt.

Falls die Einstellung 'Schutz Nummer' eingestellt ist und ein Anruf einer Gegenstelle erfolgt, wird die dabei übermittelte Rufnummer der Gegenstelle mit den Einträgen in der Nummernliste verglichen. Sind die übermittelte Rufnummer und ein Listeneintrag identisch, ist der Anrufer berechtigt, und die Verbindung wird aufgebaut.

Falls die Einstellung 'Schutz Nummer oder Name' eingestellt ist und ein Anruf einer Gegenstelle erfolgt, wird die dabei übermittelte Rufnummer der Gegenstelle mit den Einträgen in der Nummernliste verglichen. Sind die übermittelte Rufnummer und ein Listeneintrag identisch, ist der Anrufer zum Verbindungsaufbau berechtigt. Aus der Nummernliste kann außerdem der Name der Gegenstelle ermittelt werden und damit der Layer, der für diese Verbindung verwendet werden soll. Mit diesem Layer wird dann die Verbindung aufgebaut und die Namensüberprüfung mit dem gefundenen Layer gestartet (bzw. mit dem Default-Layer, wenn keiner gefunden wurde).

Wenn der Name der Gegenstelle (und damit der zu verwendende Layer) nicht über die Nummernliste ermittelt werden kann, wird der Ruf mit dem DEFAULT-Layer angenommen und nach der Protokoll-Verhandlung (PPP) geprüft, ob ein passender Eintrag in der Namenliste ist.

Script-Liste

Einige Internet-Provider (z.B. CompuServe) führen vor einer PPP-Verhandlung einen scriptgesteuerten Anmeldevorgang durch. Um auch solche Verbindung aufbauen zu können, ist im *ELSA LANCOM* eine einfache Scriptverarbeitung implementiert (siehe 'Script-Verarbeitung').

In dieser Tabelle werden die Scripte definiert und den Gegenstellen zugewiesen. Die Tabelle hat den folgenden Aufbau:

Gerätename	Script
CSERVE	<>[Host]<CIS>[User]\$U[Password]\$P[PPP]\$C

Die Einträge in der Script-Liste haben die folgende Bedeutung:

- Gerätename: Name der logischen Gegenstelle

- Script: Alle auszuführenden Befehle – Maximal 58 Zeichen stehen pro Zeile zur Verfügung. Sollte die notwendige Befehlsfolge länger sein, so kann ähnlich wie in der Round-Robin-Liste ein weiterer Eintrag für die logische Gegenstelle hinzugefügt werden. Die Syntax hierfür ist: GeräteName gefolgt von '#' und einer Zahl. Die Einträge werden von oben nach unten abgearbeitet.

Setup/WAN-Modul/Manuelle-Wahl

Über diesen Menüpunkt kann für Testzwecke eine manuelle Verbindungssteuerung vorgenommen werden.

/Manuelle Wahl	Einstellungen für die manuelle Verbindungssteuerung	
Aufbau		Aufbau einer Verbindung
Abbau		Abbau von Verbindungen
Status		Zeigt den aktuellen Verbindungszustand an

Aufbau

Parameter: Gegenstellengerätename (nur über Remote-Konfiguration).

Mit dem Befehl

`Do /Setup/WAN-Modul/Manuelle-Wahl/Aufbau Gegenstelle` wird ein manueller Verbindungsaufbau über die Remote-Konfiguration initiiert. Der als Parameter angegebene Gegenstellengerätename muß dazu mit Rufnummer in der Namenliste eingetragen sein.

Bei Aktivierung der Funktion von der Tastatur der *ELSA LANCOM* aus erfolgt jeweils unmittelbar die Anzeige der Fehlermeldung 'Keine Gegenst.', weil dabei kein Name eingegeben werden kann. Diese Funktion ist also von der Tastatur der *ELSA LANCOM* nicht zu verwenden! Soll zu einer logischen Gegenstelle eine Verbindung aufgebaut werden, für die in der Namenliste keine Rufnummer angegeben ist, so wird die Fehlermeldung 'Keine Rufnummer' angezeigt.

Abbau

Über diesen Befehl kann eine bestehende Verbindung abgebaut werden. Bei einem manuellen Verbindungsabbau kann in der Remote-Konfiguration zusätzlich der Name einer Gegenstelle angegeben werden. Es wird dann nur die Verbindung zur angegebenen Gegenstelle gelöst. Besteht keine Verbindung zur angegebenen Gegenstelle, erfolgt keine weitere Reaktion. Wird dagegen kein Gegenstellename angegeben, so werden alle bestehenden Verbindungen abgebaut.

Setup/WAN-Modul/Schutz

Hier kann eingestellt werden, unter welchen Voraussetzungen am Übertragungsmodul anliegende Rufe angenommen werden sollen.

- Ist der Schutz auf 'keiner' eingestellt, werden grundsätzlich alle anliegenden Rufe angenommen, solange die Gegenseite das Verbindungsprotokoll unterstützt.

- Mit der Einstellung 'Name' werden nur Rufe von Gegenstellen akzeptiert, für die ein Eintrag in der Namenliste vorhanden ist. Durch diese Überprüfung wird ein zusätzlicher Schutz gewährleistet. Diese Überprüfung steht nur bei Verwendung von PPP zur Verfügung.
- Bei der Einstellung 'Nummer' werden nur solche Gegenstellen akzeptiert, die in der Nummernliste als berechnigte Gegenstellen eingetragen sind.
- Auch ein Kombinationsschutz aus Namenliste oder Nummernliste ist mit 'Nr./Name' einstellbar. Damit wird zunächst geprüft, ob ein Eintrag in der Nummernliste vorhanden ist. Wenn das nicht möglich ist, versucht der Router den Namen über die Protokollverhandlung zu ermitteln.

Setup/WAN-Modul/RR-Versuche

Hierüber kann eingestellt werden, wie oft (von 1 bis 9) ein Rückruf wiederholt werden soll, wenn die Gegenstelle besetzt ist. Bei internationalen Verbindungen sollte ein Wert zwischen 3 und 5 eingegeben werden, um die Rückruffunktionalität zu optimieren. Der Standardwert beträgt 3.

Setup/WAN-Modul/Backup-St.-Sekunden

Die Backup-Startzeit gibt an, nach wieviel Sekunden der erste Backupversuch erfolgt, wenn der Zusammenbruch einer Festverbindung festgestellt wurde. Wird hier der Wert 0 angegeben, so wird aktiv keine Backupverbindung aufgebaut.

Setup/LAN-Modul

Über diesen Menüpunkt werden die für das lokale Netzwerk notwendigen Einstellungen vorgenommen. Das Menü hat folgenden Aufbau:

/LAN-Modul	Einstellungen für das LAN	
Anschluß		Wahl des Netzwerkanschlusses
Node-ID		MAC-Layer-Adresse des Geräts
Heap-Reserve		Pufferspeicher für die Aufnahme von Datenpaketen aus dem lokalen Netzwerk

Anschluß

Hier kann einer der folgenden Netzwerkanschlüsse ausgewählt werden:

Anschluß	Bedeutung
Auto	Standardeinstellung, aktiviert die Autosense-Funktion des Netzwerk-Chips. Dadurch stellt sich der Router automatisch auf den verwendeten Anschluß ein, ohne dass dieser Punkt manuell konfiguriert werden muß.
10BTX	10BASE-T im Halbduplex-Betrieb

Anschluß	Bedeutung
FD10BTX	10BASE-T im Vollduplex-Betrieb
100BTX	100BASE-T im Halbduplex-Betrieb
FD100BTX	100BASE-T im Vollduplex-Betrieb



Bitte beachten Sie, daß bei den Einstellungen für den Fast-Ethernet-Betrieb die entsprechenden weiteren Endgeräte das gewählte Übertragungsverfahren auch unterstützen müssen.

Nach dem Aus- und Einschalten bleibt der zuletzt gewählte Anschluß aktiv.

Node-ID

Unter diesem Menüpunkt wird die eigene Ethernet-Adresse des Routers angezeigt. Der hier angezeigte Wert wurde vom Hersteller festgelegt und kann nicht verändert werden. Die Anzeige der Ethernet-Adresse erfolgt als zwölfstellige Hexadezimalzahl, wobei die ersten sechs Stellen '00a057' für ein ELSA Gerät stehen.

Heap-Reserve

Die Heap-Reserve für das lokale Netzwerk beeinflusst, wieviel Pufferspeicher ständig zur Aufnahme von Frames des lokalen Netzwerks zur Verfügung stehen. Standardmäßig ist hier ein Wert von 10 eingestellt, der garantiert, daß z.B. vier Telnet-Sitzungen jederzeit über das lokale Netzwerk aktiviert werden können.

Setup/IPX-Modul

Über dieses Menü können Einstellungen für das IPX-Modul, insbesondere für den IPX-Router vorgenommen werden. Das Menü hat den folgenden Aufbau:

/IPX-Modul	Einstellungen für das IPX-Modul (IPX-Router)	
Zustand		IPX-Modul ein- oder ausgeschaltet
IPX-Router		IPX-Router ein- oder ausgeschaltet
LAN-Einstellung		Einstellungen für die LAN-Seite
WAN-Einstellung		Einstellungen für die WAN-Seite
RIP-Einstellung		Einstellungen für RIP
SAP-Einstellung		Einstellungen für SAP

Zustand

Hier kann das IPX-Modul ein- bzw. ausgeschaltet werden. Standardmäßig ist das IPX-Modul eingeschaltet.

Die Remote-Konfiguration über DOS/IPX und der IPX-Router können nur benutzt werden, wenn das IPX-Modul eingeschaltet ist. Zur lokalen Konfiguration über LAN muß der Router nicht eingeschaltet sein.

IPX-Router Hier kann der IPX-Router aktiviert bzw. deaktiviert werden. Standardmäßig ist das der IPX-Router ausgeschaltet.

Beim Einschalten des IPX-Routers wird auch das IPX-Modul aktiviert. Der IPX-Router kann nur dann eingeschaltet werden, wenn unter LAN- und WAN-Einstellung unterschiedliche zulässige Netzwerkadressen eingetragen sind.

Setup/IPX-Modul/LAN-Einstellung

Hier können Einstellungen für die Datenpakete des LAN durchgeführt werden. Das Menü hat folgenden Aufbau:

/LAN-Einstellung		Einstellungen für die LAN-Seite
Netzwerk		Logische IPX-Netzwerknummer des LAN-Anschlusses
Binding		Einstellung der Ethernet-Frame-Typen für den LAN-Anschluß
IPX-Watch		Einstellungen für IPX-Watchdog-Verwaltung
SPX-Watch		Einstellungen für SPX-Watchdog-Verwaltung
NetBIOS-Watch		Einstellungen für NetBIOS-Watchdog-Verwaltung
Socket-Filter		Filtertabelle für Zielsocketfilterung
Lok.-Routing		Lokales Routing aktiviert oder deaktiviert
RIP-SAP-Skal.		RIP-SAP-Skalierung aktiviert oder deaktiviert
LOOP-propagieren		Propagieren von redundanten Routen aktiviert oder deaktiviert

Netzwerk Hier wird die IPX Netzwerknummer des Netware-Netzes (8stellig, hexadezimal) eingetragen, die an den LAN-Anschluß unter dem Binding (siehe unten) angeschlossen wird. Ist im lokalen Netzwerk ein NetWare-Server vorhanden, so kann der Router die Netzwerknummer und das Binding automatisch ermitteln.

Der Standardwert beträgt '00000000' und bedeutet, daß der Router die Netzwerknummer automatisch ermitteln soll.

Binding Das Ethernet-Paketformat (Auto, II, 802.3, 802.2, SNAP) kann hiermit für den LAN-Anschluß eingestellt werden. Dieses Format muß zu dem im lokalen Netzwerk gebundenen Ethernetformat unter der eben beschriebenen Netzwerknummer passen.

Der Standardwert beträgt 'Auto' und bedeutet, daß der Router das Binding automatisch ermitteln soll (nur, wenn im lokalen Netzwerk ein NetWare-Server vorhanden ist).

- IPX-Watch* Die Art der Verwaltung von IPX-Watchdog-Paketen wird hiermit festgelegt.
- **Filt.** bedeutet, daß IPX-Watchdog-Pakete weder lokal beantwortet noch übertragen werden. Dadurch wird ein Benutzer nach der im NetWare-Server eingestellten Zeit auf jeden Fall abgemeldet.
 - **Route** bewirkt die Übertragung der Watchdog-Pakete und damit auch einen regelmäßigen Verbindungsaufbau durch Watchdog-Pakete des Servers.
 - **Spoof** (Standard) sorgt dafür, daß IPX-Watchdog-Pakete lokal vom Router beantwortet werden, Benutzer also nicht mehr automatisch abgemeldet werden. Diese Einstellung ist besonders gebührenschonend, allerdings muß im Server eventuell dafür gesorgt werden, daß zu bestimmten Zeiten die Benutzer auf jeden Fall abgemeldet werden, um nicht zu viele Benutzerlizenzen zu belegen.

- SPX-Watch* Die Art der Verwaltung von SPX-Watchdog-Paketen wird hiermit festgelegt.
- **Route** bewirkt die Übertragung der SPX-Watchdog-Pakete und damit auch einen regelmäßigen Verbindungsaufbau durch SPX-Watchdog-Pakete des Servers.
 - **Spoof** (Standard) sorgt dafür, daß SPX-Watchdog-Pakete lokal beantwortet werden. Diese Einstellung ist besonders gebührenschonend.

- NetBIOS-Watch* Dieser Punkt gibt an, wie mit NetBIOS-Watchdog-Paketen verfahren werden soll. NetBIOS-Watchdog-Pakete treten auf, wenn z.B. Windows-Netze auf IPX gebunden werden. Es sind die gleichen Optionen möglich wie bei IPX- oder SPX-Watchdog-Paketen (Filter, Route, Spoof).

- Socket-Filter* Die Socket-Filtertabelle ermöglicht die gezielte Filterung von LAN-Paketen zu bestimmten Ziel-Socket-Bereichen. Die Filterung erfolgt sowohl für einfache IPX-Pakete also auch für Propagated-IPX-Pakete. Folgende Sockets, die im Netzwerk periodisch versandt werden und deshalb zu häufigen Verbindungsaufbauten führen würden, sind bereits defaultmäßig in der LAN-Filter-Tabelle vorhanden (siehe dazu auch FAQs zum 'IPX-Router').

Anfangs-Socket	End-Socket
0455	0457
0550	0555
1401	1402
1480	1481
83ba	83ba
900f	9010

- Lok.-Routing* Mit dieser Einstellung wird die Skalierung von mehreren Routern in einem lokalen Netz unterstützt. Wenn bei einem Router schon alle Kanäle belegt sind, und es kommen trotzdem noch Pakete für andere Gegenstellen bei ihm an, haben möglicherweise andere Router in LAN noch freie Kanäle.

Ist die Option 'Lokales Routing' eingeschaltet, leitet der Router die Pakete auf dem lokalen Netz weiter zu einem Router, der eine Route zur angestrebten Gegenstelle propagiert hat. Der Router hat diese Route gespeichert, obwohl sie schlechter war als die eigene, und mit dem Flag 'Reserve' in der RIP-Tabelle markiert.

Die Default-Einstellung hierfür ist 'Aus', da ein IPX-Client nach einem Timeout einen RIP-Request für die gewünschte Route sendet und damit automatisch andere Router findet, über die das Zielnetz erreichbar ist.

RIP-SAP-Skal. Eine weitere Möglichkeit, die Skalierung zu unterstützen, ist, jede Route, zu der eine aktive Verbindung besteht, mit einem etwas besseren Tic-Count zu propagieren als der tatsächliche. Hierdurch werden alle Clients ihre Pakete für diese Routen an den Router schicken, der die Verbindung hat. Weiterhin können in dem Fall, in dem alle Kanäle belegt sind, die nicht mehr erreichbaren Routen als 'DOWN' propagiert werden. Da hierdurch bei jedem Verbindungsauf- und Abbau ein oder mehrere Broadcasts auf das LAN gesendet werden (durch die sich andere Router zu weiteren Broadcasts veranlaßt sehen könnten und somit eine hohe Netzlast entstehen kann), ist dieses Feature ein- und ausschaltbar. Die Default-Einstellung ist 'Aus'.

LOOP-propagieren Redundante Routen, d.h. Routen mit gleichem Tic- und Hopcount, werden nur den Gegenstellen mitgeteilt, von denen sie nicht empfangen wurden (Split Horizon). Mit dem Einschalten der Funktion 'LOOP-Propagieren' kann das Verbreiten dieser Routen trotzdem ermöglicht werden. Redundante Routen werden in der RIP-Tabelle mit dem Flag 'LOOP' gekennzeichnet.

Da die Verbreitung von redundanten Routen nach den Novell-Spezifikationen zwar nicht verboten ist, aber trotzdem möglichst unterlassen werden sollte, ist die Default-Einstellung 'Aus'.

Setup/IPX-Modul/WAN-Einstellung

Hier können Einstellungen der Datenpakete für den WAN-Anschluß durchgeführt werden. Das Menü hat folgenden Aufbau:

/WAN-Einstellung	Einstellungen für die WAN-Seite	
Routing-Tabelle		Router-Tabelle für die Zuordnung von IPX-Netzwerk und Gegenstelle
Socket-Filter		Filtertabelle für Ziel-Socketfilterung

Routing-Tabelle Die Routing-Tabelle kann bis zu 16 Gegenstellen und Zielnetze aufnehmen. Diese Tabelle hat folgende Einträge:

Gegenstelle	Netzwerk	Binding	Propagate	Backoff
Name der IPX Gegenstelle	Netzwerk-Adresse	802.3, II, 802.2, SNAP	Route / Filter	Ein /Aus

Hierbei bedeuten:

- **Gegenstelle:** Name der logischen Gegenstelle (wie in /Setup/WAN-Modul/ Namenliste angegeben).
- **Netzwerk:** Die Adresse des WAN-seitigen Netzwerk. Es muß ein eigenständiges Netzwerk verwendet werden, für die beiden beteiligten Router jedoch das gleiche!
- **Binding:** Zu verwendendes Ethernet-Binding auf der ISDN-Strecke. Diese Angabe wird nur berücksichtigt, wenn Ethernet-Encapsulation im verwendeten Layer eingestellt ist. Wird kein Binding eingegeben, so wird 802.3 angenommen.
- **Propagate:** Dieser Eintrag gibt an, wie mit IPX-Paketen vom Typ 20 (NetBIOS Propagated Frames) verfahren werden soll. Mögliche Einstellungen sind Route oder Filter. Hat dieses Feld den Eintrag **Filter** werden keine Propagated Frames an diese Gegenstelle weitergeleitet. Hat der Eintrag den Wert **Route**, so werden die Pakete an alle gerade erreichbaren Gegenstellen weitergeleitet, d.h., zu der Gegenstelle muß eine Verbindung bestehen, oder es ist mindestens ein Kanal für einen Verbindungsaufbau zur Gegenstelle verfügbar.

Besteht keine Verbindung und ist kein Kanal verfügbar, so wird das Paket verworfen. Daher können maximal maximal so viele Gegenstellen Propagated-Frames erhalten, wie gleichzeitige Verbindungen möglich sind. Die Default-Einstellung ist 'Filter'.

- **Backoff:** Der IPX-Router benutzt einen speziellen Algorithmus (Exponential Backoff), um bei Fehlkonfigurationen die anfallenden Verbindungskosten so gering wie möglich zu halten (siehe unten).

Wenn im entfernten Netz kein Server vorhanden ist (z.B. bei Remote-Access von einer Workstation), so kann der Router dies nicht erkennen und die entsprechende Gegenstelle wird nach spätestens einem Tag deaktiviert. Damit dies nicht geschieht kann der Exponential-Backoff-Algorithmus für diese Gegenstellen ausgeschaltet werden.

Die Default-Einstellung ist 'Ein'.

Socket-Filter

Die Socket-Filtertabelle ermöglicht die gezielte Filterung von WAN-Paketen zu bestimmten Ziel-Socket-Bereichen. Die Filterung erfolgt sowohl für einfache IPX-Pakete also auch für Propagated-IPX-Pakete.

Setup/IPX-Modul/RIP-Einstellung

Hier können Einstellungen für RIP-Datenpakete (Router-Informationen) hinterlegt werden. Das Menü hat folgenden Aufbau:

/RIP-Einstellung		Einstellungen für das RIP
Tabelle-RIP		Anzeigen der RIP-Tabelle
LAN-Filtertab.		Filterbereiche für IPX-Netzwerkadressen (LAN)
WAN-Filtertab.		Filterbereiche für IPX-Netzwerkadressen (WAN)

/RIP-Einstellung	Einstellungen für das RIP	
Routen/Frm		Max. # RIP-Einträge pro gesendeten RIP-Frame
Aging		Aging-Zeitraum in Update-Einheiten
Spoofing		RIP-Spoofing-Verfahren einstellen
WAN-Update-Zeit		RIP-Update-Zeitraum, je nach Spoofing wirksam

Tabelle-RIP

Über diesen Menüpunkt werden die Einträge der aktuellen RIP-Tabelle angezeigt. Die Tabelle umfaßt maximal 256 Einträge.

Die Einträge in der RIP-Tabelle können wie folgt aussehen, wenn es zum Beispiel die Netzwerke 00000001, 00000002, 00000010, 00000081 gibt und diese über verschiedene Router erreicht werden können. Über die Flags kann ermittelt werden, wo diese Netzwerke, vom jeweiligen Router aus gesehen, liegen (**lokal** oder **remote**). Der Zusatz **direkt** gibt einen Hinweis darauf, daß dieses Netz direkt das lokale oder entfernte Netz ist. **DOWN** weist auf ein Netz hin, das bekannt, aber momentan nicht erreichbar ist. Die Tabelle ist nach den Netzwerknummern sortiert.

Netzwerk	Hops	Tics	Node-Id	Zeit	Flags
00000001	0	1	00a05702000a	0	lokal, direkt
00000002	1	2	00608c70ab56	1	lokal
00000010	2	7	00a057020014	1	lokal, DOWN
00000081	1	6	00a05702000b	0	remote, direkt

LAN-Filtertab.

Die LAN-Filtertabelle ermöglicht die gezielte Filterung von Routen, die über das lokale Netzwerk „gelernt“ werden. Gefilterte Routen erscheinen nicht in der IPX-RIP-Tabelle.

Eine LAN-Filtertabelle zur Filterung der Routen im Bereich 00001000 bis 00001fff sieht z.B. wie folgt aus:

Startnetz	Endnetz
00001000	00001fff

WAN-Filtertab.

Die WAN-Filtertabelle ermöglicht die gezielte Filterung von Routen, die über das Weitverkehrsnetzwerk „gelernt“ werden. Gefilterte Routen erscheinen nicht in der IPX-RIP-Tabelle.

Eine WAN-Filtertabelle zur Filterung der Routen im Bereich 00002000 bis 00002fff sieht z.B. wie folgt aus:

Startnetz	Endnetz
00002000	00002fff

- Routen/FRM* Dieser Parameter setzt die maximale Anzahl von Routen, die in einem RIP-Frame enthalten sein können. Der ursprünglich von Novell definierte Vorgabewert ist 50. Heutzutage ist es jedoch üblich, eine höhere Anzahl von Routen in jeden Frame zu packen, da dies die Netzwerklast senkt. Falls alle beteiligten Geräte im Netzwerk eine höhere Anzahl unterstützen, kann dieser Wert auf bis zu 182 erhöht werden.
- Aging* Hier kann die Anzahl der Updates (Aktualisierungsvorgänge der RIP-Tabelle) eingestellt werden, die durchgeführt werden, bis ein Eintrag in der RIP-Tabelle altert, d.h. die dort vermerkte Route als „nicht erreichbar (down)“ markiert wird. Die Eingabemöglichkeiten reichen von 1 bis 60 bei einem Standardwert von 3.
- Spoofing* Hiermit kann das Verhalten des Routers für RIP-Pakete eingestellt werden.
- Bei der Einstellung **Ohne** werden RIP-Pakete auf dem WAN genauso wie auf lokalen Netzwerken behandelt. Bei neuen Informationen und im Minutenabstand werden RIP-Daten zur Remote-Seite geschickt, also eine Verbindung wird aufgebaut.
 - Die **Trig**-Einstellung bewirkt eine Verschickung der RIP-Daten zur Remote-Seite immer dann, wenn Änderungen anfallen.
 - Die **Zeit**-Einstellung bewirkt eine Verschickung der RIP-Daten zur Remote-Seite in einem einzustellenden Zeitabstand (siehe unten).
 - **pBack** (Standard) ist die gebührenschonendste Einstellung, wodurch RIP-Daten nur zur Gegenseite verschickt werden, wenn eine Verbindung aktiv ist.
- Bei der Spoofing-Einstellung **pBack** altern Einträge aus der RIP-Tabelle nur dann, wenn eine Verbindung neu aufgebaut wird und gezielt ein Eintrag als „nicht erreichbar“ gekennzeichnet wurde.*
- WAN-Update-Zeit* Hier wird für eine Spoofing-Zeitsteuerung der zeitliche Übertragungsabstand angegeben, in dem RIP-Daten zur Gegenseite übertragen werden. Die Eingabemöglichkeiten reichen von 1 bis 60 Minuten bei einem Standardwert von 5.

Setup/IPX-Modul/SAP-Einstellung

Hier werden Einstellungen für SAP-Datenpakete (Server-Informationen) hinterlegt.

/SAP-Einstellung		Einstellungen für das SAP
Tabelle-SAP		Anzeigen der SAP-Tabelle
LAN-Filtertab.		Filterbereiche für IPX-Service-Adressen (LAN)
WAN-Filtertab.		Filterbereiche für IPX-Service-Adressen (WAN)
Server/Frm		Max. # SAP-Einträge pro gesendeten SAP-Frame
Aging		Aging-Zeitraum in Update-Einheiten
Spoofing		SAP-Spoofing-Verfahren einstellen
WAN-Update-Zeit		SAP-Update-Zeitraum, je nach Spoofing wirksam

Tabelle-SAP Über diesen Menüpunkt werden die Einträge der aktuellen SAP-Tabelle angezeigt. Die Tabelle umfaßt maximal 512 Einträge. Die Tabelle ist nach dem Service-Typ und bei gleichem Typ nach Server-Namen sortiert. Eine beispielhafte SAP-Tabelle könnte wie folgt aussehen:

Typ	Server-Name	Netzwerk	Node-Id	Socket	Hops	Zeit	Flags
0004	Y	000000c1	000000000001	0451	1	1	lokal
0047	X	00000001	0000c0123456	8060	1	0	lokal
0107	Z	000000c1	000000000001	8104	2	1	lokal

Verschiedene SAP-Typen sind dort abgelegt. Nachzulesen ist der Server-Name, das zuständige Netzwerk, die MAC-Adresse des Servers (bei internen Server-Netzwerken 000000000001), die Socket-Nummer und Informationen über die Lokalität des Servers.

LAN-Filtertab. Durch Einträge in der LAN-Filtertabelle ist es möglich, bestimmte Bereiche der Service-Informationen eines Novell-Netzwerks von der Aufnahme in die SAP-Tabelle auszuschließen und so die Ressourcen des IPX-Routers besser zu nutzen. Außerdem werden ungewünschte Verbindungsaufbauten durch diese SAPs (Dienste) verhindert.

Alle Service-Informationen, die sich innerhalb eines Filterbereiches der LAN-Filtertabelle befinden, werden nicht vom lokalen Netzwerk in die SAP-Tabelle des IPX-Routers übernommen. Sie werden ebenfalls nicht an die Gegenstelle des IPX-Routers übertragen und stehen daher dort auch nicht zur Verfügung.

Häufig sind z.B. die Service-Informationen der Printer-Server für die Gegenstelle des IPX-Routers nicht notwendig. Sollen diese Informationen durch die LAN-Filtertabelle von der Aufnahme in die SAP-Tabelle ausgeschlossen werden, ist folgender Eintrag notwendig:

Anfangsservice	Endservice
030c	030c

Eine Liste von SAP-Services mit Beschreibung finden Sie im Kapitel 'Novell-SAP-Nummern'.

WAN-Filtertab. Analog zur LAN-Filtertabelle ist es durch die WAN-Filtertabelle möglich, Bereiche von Service-Informationen aus dem WAN von der Aufnahme in die SAP-Tabelle auszuschließen.

Die gesperrten Dienste haben damit allerdings auf der Gegenstelle schon zu einem Verbindungsaufbau geführt, bevor der Zielrouter sie WAN-seitig filtern konnte.

Aufbau und Funktion der WAN-Filtertabelle sind dabei völlig analog zur LAN-Filtertabelle. Eine WAN-Filtertabelle zur Filterung der File-Services sieht z.B. wie folgt aus:

Startservice	Endservice
0004	0004

- Server/FRM* Dieser Parameter setzt die maximale Anzahl von Services, die in einem SAP-Frame enthalten sein können. Der ursprünglich von Novell definierte Vorgabewert ist 7. Heutzutage ist es jedoch üblich, eine höhere Anzahl von Services in jeden Frame zu packen, da dies die Netzwerklast senkt. Falls alle beteiligten Geräte im Netzwerk eine höhere Anzahl unterstützen, kann dieser Wert auf bis zu 22 erhöht werden.
- Aging* Hier kann die Anzahl der Updates (Aktualisierungsvorgänge der SAP-Tabelle) eingestellt werden, die durchgeführt werden, bis ein Eintrag in der SAP-Tabelle altert, d.h. der dort vermerkte Service als „nicht erreichbar (down)“ markiert wird. Die Eingabemöglichkeiten reichen von 1 bis 60 bei einem Standardwert von 3.
- Spoofing* Hiermit kann das Verhalten des Routers für SAP-Pakete eingestellt werden.
- Bei der Einstellung **Ohne** werden SAP-Pakete auf dem WAN genauso wie auf lokalen Netzwerken behandelt. Bei neuen Informationen und im Minutenabstand werden SAP-Daten zur Remote-Seite geschickt, also eine Verbindung wird aufgebaut.
 - Die **Trig**-Einstellung bewirkt eine Verschickung der SAP-Daten zur Remote-Seite immer dann, wenn Änderungen anfallen.
 - Die **Zeit**-Einstellung bewirkt eine Verschickung der SAP-Daten zur Remote-Seite in einem einzustellenden Zeitabstand (siehe unten).
 - **pBack** (Standard) ist die gebührenschonendste Einstellung, wodurch SAP-Daten nur zur Gegenseite verschickt werden, wenn eine Verbindung aktiv ist.
- Bei der Spoofing-Einstellung **pBack** altern Einträge aus der RIP-Tabelle nur dann, wenn eine Verbindung neu aufgebaut wird und gezielt ein Eintrag als „nicht erreichbar“ gekennzeichnet wurde.*
- WAN-Update-Zeit* Hier wird für eine Spoofing-Zeitsteuerung der zeitliche Übertragungsabstand eingegeben, in dem SAP-Daten zur Gegenseite übertragen werden. Die Eingabemöglichkeiten reichen von 1 bis 60 Minuten bei einem Standardwert von 5.

Setup/TCP-IP-Modul

Über dieses Menü können Einstellungen für das TCP-IP-Modul vorgenommen werden. Das Menü hat den folgenden Aufbau:

/TCP-IP-Modul		Einstellungen für das TCP/IP-Modul
Zustand		TCP/IP-Modul ein- oder ausgeschaltet
IP-Adresse		Eigene IP-Adresse
IP-Netz-Maske		Passende IP-Netzmaske des lokalen Netzes
Intranet-Adresse		Eigene Intranet-Adresse
Intranet-Maske		Passende Intranet-Netzmaske des lokalen Netzes
Zugangsliste		Einschränkung des Zugriffs auf interne Funktionen über TCP/IP
DNS-Default		Domain Name Server
DNS-Backup		Backup Domain Name Server
NBNS-Default		NetBIOS Name Server
NBNS-Backup		Backup NetBIOS Name Server
Tabelle-ARP		ARP-Tabelle für Abb. einer IP-Adresse auf eine MAC-Adresse
ARP-Aging-Min		Verweildauer für Einträge in der ARP-Tabelle
TCP-Aging-Min		Zeitbeschränkung für Konfigurations-Verbindungen, die inaktiv sind
TCP-Max.-Verbindungen.		Max. Anzahl gleichzeitiger Konfigurations-Verbindungen zum <i>ELSA LANCOM</i>

Zustand Hier kann das TCP/IP-Modul des Routers ein- oder ausgeschaltet werden. Standardmäßig ist das TCP/IP-Modul aktiviert.

Die Konfiguration über TCP/IP durch Telnet und der IP-Router können nur benutzt werden, wenn das TCP/IP-Modul eingeschaltet ist.

IP-Adresse Hier kann die IP-Adresse für den Router eingegeben werden. Die Standardadresse bei der Auslieferung ist die '0.0.0.0'.

Bei Verwendung von IP-Masquerading bekommt diese Adresse in Verbindung mit der Intranet-Adresse eine besondere Bedeutung:

Wird dem Router vom Internet-Provider die hier eingestellte IP-Adresse per PPP zugewiesen, so werden alle Rechner, die sich im durch IP-Adresse und IP-Netzmaske aufgespannten Netz befinden, normal geroutet. Diese Rechner sind dann auch direkt aus dem Internet heraus erreichbar.

IP-Netzmaske Hier muß die zur IP-Adresse gehörende Netzmaske eingegeben werden. Die Standardeinstellung ist 255.255.255.0 (Klasse C Netz). Eine Netzmaske von 255.255.255.255 bedeutet, daß sich in diesem Netz nur ein einziger Rechner befindet (nämlich der Router

selber). Diese Einstellung (eine im Internet registrierte IP-Adresse mit voll besetzter Netzmaske) kann für das Masquerading über einen Raw-IP-Zugang, wie ihn z.B die Provider des Individual Network anbieten, verwendet werden. Bei einem solchen Zugang wird dem Router keine IP-Adresse über eine PPP-Verhandlung zugewiesen, sondern er muß eine feste, im Internet registrierte IP-Adresse besitzen.

Intranet-Adresse

Hier kann eine zweite IP-Adresse für den Router eingegeben werden. Dadurch kann der Router einerseits für zwei logische IP-Netze als Router dienen, andererseits erhält diese Adresse eine besondere Bedeutung bei Verwendung von IP-Masquerading:

In diesem Fall werden alle Rechner, die sich im durch Intranet-Adresse und Intranet-Maske aufgespannten Netz befinden, hinter der vom Provider zugewiesenen Adresse (bzw. der Internet-Adresse (IP-Adresse)) versteckt.

Die Standardadresse bei der Auslieferung ist die '0.0.0.0'.

Intranet-Maske

Hier muß die zur IP-Adresse gehörende Netzmaske eingegeben werden. Die Standard-einstellung ist 255.255.255.0 (Klasse C Netz).



Wurde weder eine IP- noch eine Intranet-Adresse angegeben, reagiert das Gerät auf eine Standard-IP-Adresse, deren erste drei Stellen identisch sind mit den ersten drei Stellen des Sendegeräts XXX.XXX.XXX.YYY. Das Gerät ist dann durch Anwahl der IP-Adresse XXX.XXX.XXX.254 zu erreichen.

Existiert im Netz bereits eine solche IP-Adresse, muß über die Outband-Konfiguration (Terminal-Programm) eine andere Adresse eingegeben werden.



Wurden sowohl IP- als auch Intranet-Adresse eingegeben, so dürfen sich in dem durch IP-Adresse und IP-Netzmaske aufgespannten Netz nur Workstations (also keine Router) befinden.

Zugangsliste

Der Zugang zu „internen Funktionen“ der Router kann in TCP/IP-Anwendungen durch eine Zugangsliste gesteuert werden.



Zwar sind die Konfigurationsdaten der Geräte durch ein Paßwort geschützt, jedoch wird dieses immer im Klartext übertragen, wodurch es prinzipiell möglich ist, dieses auszuspähen und von jedem beliebigen Rechner aus die Konfiguration auszulesen oder gar zu zerstören. Um dies zu verhindern, kann über die Zugriffsliste eingestellt werden, von welchen Rechnern oder aus welchen Netzen herauf auf die Konfiguration zugegriffen werden darf.

Die Zugangskontrolle bezieht sich aus Konsistenzgründen auf alle „internen Funktionen“ der Router. Unter dem Begriff „interne Funktionen“ sind folgende zu verstehen:

- Telnet-Server: die Konfigurations-Schnittstelle auf Basis des Telnet-Protokolls.
- TFTP-Server: die Konfigurations-Schnittstelle auf Basis des TFTP-Protokolls.
- SNMP: die Konfigurations-Schnittstelle auf Basis von SNMP.

Jeder der maximal 16 Einträge in der Zugangsliste besitzt folgenden Aufbau:

IP-Adresse	IP-Netz-Maske
IP-Adresse des berechtigten Teilnehmers (oder Teilnehmerkreises)	IP-Netzwerk-Maske des Teilnehmerkreises

Sobald eine IP-Workstation mit ihrer IP-Adresse und der Netzmaske 255.255.255.255 in die Liste eingetragen ist, kann nur noch von diesem Rechner aus auf die internen Funktionen der Router zugegriffen werden. Alle Anforderungen von Geräten mit anderen IP-Adressen bleiben unbeantwortet.

Soll einem kompletten Netzwerk der Zugang zu einem *ELSA LANCOM* ermöglicht werden, kann dies für ein Netzwerk der Klasse C etwa wie folgt geschehen:

IP-Adresse	IP-Netz-Maske
192.234.222.0	255.255.255.0

Durch diesen Eintrag sind alle IP-Adressen im Klasse-C-Netzwerk 192.234.222.0 berechtigt, interne Funktionen des Routers zu benutzen.

DNS-Default

Der Eintrag **DNS** (Domain Name Server) wird benötigt, um Rechnern, die über PPP direkt auf den Router zugreifen, den für das eigene Netz zuständigen Name-Server bekanntzugeben.

Wenn der Router für den Zugang zum Internet über einen Internet-Service-Provider konfiguriert ist, wird der DNS-Server meist vom Provider übermittelt. Für die Einstellung im Router gibt es dann zwei verschiedene Möglichkeiten:

- Als Adresse des DNS-Servers wird die '0.0.0.0' eingetragen. Dann können alle Rechner im lokalen Netz den DNS-Server des Providers nutzen.
- Die eigene IP-Adresse des Routers wird als DNS-Server eingetragen. Dann nutzt er die DNS-Informationen des Providers nicht nur für das eigene lokale Netz, sondern gibt diese Informationen selbst weiter (DNS-Forwarding). Entfernte Gegenstellen wie z.B. Rechner, die sich über Remote-Access einwählen, können dann auch auf den DNS-Server des Providers zugreifen. Dieser Mechanismus wird auch als DNS-Forwarding bezeichnet.

DNS-Backup

Durch den Eintrag **DNS-Backup** kann ein zweiter Name-Server benannt werden, der bei Ausfall des DNS benutzt wird.

NBNS-Default

Der Eintrag **NBNS** (NetBIOS Name Server) wird benötigt, um Rechnern, die über PPP direkt auf den Router zugreifen, den für das eigene Netz zuständigen NBNS bekanntzugeben.

NBNS-Backup

Durch den Eintrag **NBNS-Backup** kann ein zweiter Server benannt werden, der bei Ausfall des NBNS benutzt wird.

ARP-Tabelle Hier wird die ARP-Tabelle (ARP-Cache), die zur Abbildung von IP-Adressen auf physikalische Endgeräteadressen automatisch verwaltet wird, angezeigt. Einzelne Einträge können aus dieser Tabelle entfernt, jedoch können keine neuen Einträge manuell eingegeben werden.

Die Einträge in der ARP-Tabelle könnten z.B. wie folgt aussehen, wenn verschiedene Geräte mit unterschiedlichen IP-Adressen (192.168.139.20, 192.168.130.30) mit dem Router kommuniziert haben:

IP-Adresse	Node-ID	Letzter Zugriff	Anschluß
192.168.130.20	0000c0717860	6780443 tics	lokal
192.168.130.30	0800091eebf4	6214514 tics	lokal

ARP-Aging-Min Hier kann eine Zeit (von 1 bis 99 Minuten) eingegeben werden, nach der die ARP-Tabelle automatisch aktualisiert wird, d.h., alle nicht angesprochenen IP-Adressen seit der letzten automatischen Aktualisierung werden entfernt. Der Standardwert beträgt 15 Minuten.

TCP-Aging-Min Erfolgt während einer TCP-Verbindung zum Router keine Übertragung mehr, wenn z.B. während der Remote-Konfiguration keine Daten mehr vom Benutzer eingegeben werden, baut er die TCP-Verbindung automatisch nach der hier angegebenen Zeit ab. Gültige Werte sind 1 bis 99 Minuten. Der Standardwert beträgt 15 Minuten.

TCP-Max.-Verbindungen Hier kann die Anzahl der maximal zulässigen, gleichzeitig möglichen Verbindungen eingestellt werden. DEFAULT-Einstellung ist '0', was gleichbedeutend ist mit „beliebig viele“.

Setup/IP-Router-Modul

Über dieses Menü können Einstellungen für das IP-Router-Modul vorgenommen werden. Das Menü hat den folgenden Aufbau:

/IP-Router-Modul		Einstellungen für das IP-Router-Modul
Zustand		IP-Router-Modul ein- oder ausgeschaltet
IP-Routing-Tabelle		Router-Tabelle für Zuordnung IP-Netzwerk und Gegenstelle
LAN-Filtertabelle		Negativ/Aufb.-Filtertabelle für TCP/UDP-Zielports von LAN-Pak.
WAN-Filtertabelle		Negativ-Filtertabelle für TCP/UDP-Zielports von WAN-Paketen
Proxy-ARP		Aktivierung/Deaktivierung der Proxy-ARP-Funktion
Lok.-Routing		Ein- und Ausschalten des lokalen Routings
Start-WAN-Pool		Anfang des Adreßpools für die dynamische Adreßzuweisung beim Remote Access
Ende-WAN-Pool		Ende des Adreßpools

/IP-Router-Modul	Einstellungen für das IP-Router-Modul	
Routing-Methode		Routing-Verfahren für IP-Pakete
RIP-Einstellungen		Einstellungen für den Betrieb von IP-RIP
Masquerading		Einstellungen für das IP-Masquerading

Zustand

Hier kann das IP-Router-Modul ein- oder ausgeschaltet werden. Standardmäßig ist das IP-Router-Modul aktiviert.



IP-Routing-
Tabelle

Beim Einschalten des IP-Router-Moduls wird auch das TCP/IP-Modul aktiviert.

In der Router-Tabelle können maximal 128 Einträge von Zielnetzwerkadressen oder direkten IP-Adressen mit dazugehörigen Netzwerkmasken und Router-Namen bzw. IP-Adressen anderer lokaler Router aufgenommen werden. Alternativ können Sie einstellen, daß Pakete zu bestimmten Ziel-IP-Adressen verworfen und auch nicht durch Proxy-ARP beantwortet werden. Dies erreichen Sie durch den Eintrag 0.0.0.0 bei dem zuständigen Router-Namen.

Das Feld 'Maskierung' gibt an, ob die Route maskiert werden soll oder nicht. Dabei werden folgende Möglichkeiten unterschieden:

- **Ein:** IP-Masquerading ist eingeschaltet und funktioniert mit dynamischer Zuweisung der IP-Adresse durch die Gegenstelle. Bei diesem Verfahren fragt der Router bei der Gegenstelle die IP-Adresse '0.0.0.0' an und bekommt daraufhin eine beliebige IP-Adresse der Gegenstelle zugewiesen, die im weiteren verwendet wird.
- **Aus:** Masquerading ist ausgeschaltet.
- **Statisch:** Masquerading ist eingeschaltet und funktioniert mit Zuweisung einer statischen, vorher vereinbarten IP-Adresse durch die Gegenstelle. Bei diesem Verfahren fragt der Router bei der Gegenstelle die unter 'Setup/TCP-IP-Modul' eingetragene IP-Adresse an und bekommt daraufhin genau diese Adresse von der Gegenstelle zugewiesen. Verwenden Sie diese Einstellung, wenn Ihnen die Gegenstelle (z.B. Ihr Internet-Provider) mit den Zugangsdaten eine feste IP-Adresse mitgeteilt hat. Dieses Verfahren funktioniert natürlich nur dann, wenn Sie diese Adresse auch als IP-Adresse im Router eingetragen haben.

Die IP-Routing-Tabelle ist im allgemeinen wie folgt sortiert:

- Die längste Netzmaske steht oben.
- Bei gleicher Netzmaske steht die kleinste IP-Adresse oben.

Zur Identifizierung der richtigen Gegenstelle durchsucht der Router anhand der empfangenen Ziel-IP-Adresse die Routing-Tabelle von oben nach unten. Wurde ein passender Eintrag gefunden, wird der gefundene Router-Name für die Verbindung verwendet.

Im Internet verbotene Adreßbereiche werden über voreingestellte Einträge in der IP-Routing-Tabelle von der Übertragung ausgeschlossen (Router-Name 0.0.0.0 bedeutet:

Pakete an diese Adressen nicht übertragen). Die folgende IP-Routing-Tabelle dient als Beispiel und zeigt gleichzeitig die Standardeinträge:

IP-Adresse	IP-Netz-Maske	Router-Name	Distanz	Maskierung
192.168.0.0	255.255.0.0	0.0.0.0	0	Aus
172.16.0.0	255.240.0.0	0.0.0.0	0	Aus
10.0.0.0	255.0.0.0	0.0.0.0	0	Aus
224.0.0.0	224.0.0.0	0.0.0.0	0	Aus

Sollten diese Adressen trotzdem z.B. für Intranet-Benutzung benötigt werden, ist es möglich, diese vordefinierten Einträge jederzeit zu löschen. Erscheinen in dieser Routing-Tabelle keine Einträge mit Router-Namen 0.0.0.0, werden vom Router alle IP-Adressen mit gültigen Routen verarbeitet.

■ Beispiel

- Die lokale Netzwerkadresse ist 192.120.130.0.
- Drei Endgeräte sollen über Proxy-ARP mit den IP-Adressen 192.120.130.10, 192.120.130.11 und 192.120.130.12 über einen *ELSA LANCOM* 'Dresden' erreichbar sein.
- Es gibt zwei erreichbare Zielnetze 192.120.131.0 und 192.120.132.0 für die Gegenstellen 'AACHEN' und 'BERLIN'.
- Datenpakete für das Zielnetz 193.140.300.0 sollen zu einem weiteren lokalen Router mit der IP-Adresse 192.120.130.200 geschickt werden.
- Zu einem Zielnetzwerk 193.140.200.0 soll überhaupt nichts übertragen werden.
- Alle anderen nicht lokalen Datenpakete sollen zum Router 'PROVIDER' beim Internet-Service-Provider geschickt werden.

Die Router-Tabelle müßte in diesem Beispiel folgende Einträge beinhalten:

IP-Adresse	IP-Netz-Maske	Router-Name	Distanz	Maskierung
192.120.130.10	255.255.255.255	DRESDEN	0	Aus
192.120.130.11	255.255.255.255	DRESDEN	0	Aus
192.120.130.12	255.255.255.255	DRESDEN	0	Aus
192.120.131.0	255.255.255.0	AACHEN	0	Aus
192.120.132.0	255.255.255.0	BERLIN	0	Aus
193.140.200.0	255.255.255.0	0.0.0.0	0	Aus
193.140.300.0	255.255.255.0	192.120.130.200	0	Aus
255.255.255.255	0.0.0.0	PROVIDER	0	Ein



Wenn die Verbindung zur gewählten Gegenstelle über eine PPP-Verbindung realisiert wird, müssen in der PPP-Tabelle für den entsprechenden Eintrag die Rechte für IP aktiviert sein!

Die letzte Zeile ist ein Eintrag für die „Standard-Route“. Die IP-Adresse 255.255.255.255 ist gleichbedeutend mit 0.0.0.0 (0.0.0.0 kann in der ersten Spalte aus technischen Gründen nicht eingegeben werden). Durch die IP-Netzmaske 0.0.0.0 paßt diese Zeile immer, wenn alles vorher durchsucht wurde. Der Router schickt also alles, was er über andere Routen nicht übertragen kann und nicht verwerfen soll bzw. was von einem WAN-Anschluß kommt und nicht lokal ist, an den Router beim Provider.

LAN-Filtertab.

Mit dieser Tabelle können bestimmte Ziel-Port-Bereiche gefiltert werden. Darüber hinaus kann bestimmt werden, wie diese Pakete gefiltert werden. Treffen von der LAN-Seite Pakete mit den eingetragenen Ports ein, so werden sie nicht weitergeroutet (Immer-Filter), nur, wenn die Verbindung gerade steht (Aufbau-Filter) oder nur, wenn sie über eine andere als die DEFAULT-Route gerouted werden können (I-Net-Filter).

Die LAN-Portfilter sind in einer Tabelle mit dem folgenden Aufbau definiert:

Idx.	Z-von	Z-bis	Q-von	Q-bis	Quell-Adresse	Quell-Netzmaske	Prot	Typ
WIN	0	0	137	139	255.255.255.255	0.0.0.0	TCP und UDP	Immer

Die Felder der Tabelle haben folgende Bedeutung:

- **Idx.**
Eindeutiger Index. Dieser Eintrag ist nötig, um die Filter unterscheiden zu können. Der Index kann vier Zeichen lang sein und beliebig gewählt werden.
- **Z-von, Z-bis**
Ziel-Port-Bereich, der gefiltert werden soll. Ein Bereich von 0 bis 0 bedeutet, daß kein Ziel-Port von diesem Filter beeinflußt wird.
- **Q-von, Q-bis**
Quell-Port-Bereich, der gefiltert werden soll. Ein Bereich von 0 bis 0 bedeutet, daß kein Quell-Port von diesem Filter beeinflußt wird.
- **Quell-Adresse, Quell-Netzmaske**
Hiermit kann ein Subnetz des lokalen Netzes angegeben werden, für das der Filter gelten soll. Ist die Quell-Adresse 0.0.0.0 so bedeutet das, daß der Filter auf jeden Rechner angewendet wird. Eine Netzmaske von 0.0.0.0 bedeutet, daß der Filter auf alle Netze angewendet wird (was ebenfalls alle Rechner bedeutet).
- **Prot**
Protokoll, das gefiltert werden soll. Möglich sind **TCP, UDP, ICMP** und **alle**.

Die Einstellung **alle** filtert jedes Paket aus dem spezifizierten Quell-Netz bzw. zum Ziel-Netz.

■ Typ

Art des Filters. Möglich sind Immer, Aufbau und I-Net.

- **Immer**-Filter: Das Paket wird verworfen.
- **Aufbau**-Filter: Das Paket wird verworfen, wenn keine Verbindung zur Gegenstelle besteht.
- **I-Net**-Filter: Das Paket wird verworfen, wenn sein Ziel nur über die DEFAULT-Route erreichbar ist.

In der vorhergehenden Tabelle ist der Default-Filter eingetragen, der den unerwünschten und kostenintensiven Verbindungsaufbau bei Windows-Netzen auf IP unterbindet. Diese Netze senden regelmäßig z.B. DNS-Anfragen ins lokale Netz, die ohne diesen Filter ins Internet geleitet werden.

WAN-Filtertab. Mit dieser Tabelle können bestimmte Ziel-Port-Bereiche angegeben werden. Treffen von der WAN-Seite Pakete mit den eingetragenen Ports ein, werden sie nicht weitergeroutet (Firewall-Funktion).

Die WAN-Portfilter sind in einer Tabelle ähnlich der LAN-Filter-Tabelle definiert:

Idx.	Z-von	Z-bis	Q-von	Q-bis	Ziel-Adresse	Ziel-Netzmaske	Prot
WIN	53	53	137	139	0.0.0.0	0.0.0.0	TCP und UDP

Die Felder der Tabelle haben die gleiche Bedeutung wie in der LAN-Filter-Tabelle, mit folgendem Unterschied:

■ Ziel-Adresse, Ziel-Netzmaske

Hiermit kann ein Subnetz des lokalen Netzes angegeben werden, für das der Filter gelten soll. Die Ziel-Adresse 0.0.0.0 bedeutet, daß der Filter auf jeden Rechner angewendet wird. Eine Netzmaske von 0.0.0.0 bedeutet, daß der Filter auf alle Netze angewendet wird (was ebenfalls alle Rechner bedeutet).

Die Tabelleneinträge sind ähnlich der IP-Router-Tabelle sortiert:

- Die längsten Netzmasken stehen oben.
- Bei gleicher Netzmaske steht die größte IP-Adresse oben.

Damit können Netzmasken und IP-Adressen von 0.0.0.0 als „Wildcard“ eingesetzt werden. Gleichzeitig können bestimmte Rechner und Netze gezielt gefiltert werden, während andere ungefiltert den Router passieren.

Die Tabellen werden von oben nach unten abgearbeitet. Sobald ein Filter paßt, wird das Paket entsprechend behandelt.

Proxy-ARP Hier kann der Proxy-ARP-Mechanismus aktiviert bzw. deaktiviert werden (Standard: 'Aus'). Diese Funktion erlaubt die Datenübertragung zu IP-Adressen im gleichen logischen Netz wie der Absender, z.B. bei der Anbindung von einzelnen Arbeitsplatzrechnern (Teleworkern) über TCP-IP an das Firmen-Netz.

Lok.-Routing Das lokale Routing ermöglicht es dem Router, Datenpakete über das lokale Netz weiterzuleiten. Das lokale Routing wird dann nötig, wenn der Router als Standard-Gateway der Arbeitsplatzrechner Pakete für Zielnetze empfängt, zu denen er selbst keine Verbindung aufbauen kann. Wenn dieser Router die Adresse des eigentlich zuständigen Routers nicht über IMCP an die Arbeitsplatzrechner zurückmelden kann, leitet er die Daten selbst zu dem entsprechenden Router weiter (siehe auch 'Lokales Routing'). Da diese Einstellung zu einer erhöhten Netzlast im LAN führt, ist die Standardeinstellung 'Aus'.

Start-Adreß-Pool Beginn des Adreß-Pools, aus dem die IP-Adressen für einwählende Geräte dynamisch zugewiesen werden. Diese Funktion wird auch als IP-Pooling bezeichnet und z.B. für Remote Access von mehreren Außendienstmitarbeitern verwendet.

Der Adreß-Pool sollte im selben Adreßbereich wie der Router liegen. Legen Sie den Adreßpool nach Möglichkeit so groß aus, daß alle einwählenden Geräte eine IP-Adresse zugewiesen bekommen können (z.B. je eine Adresse für die verfügbaren B-Kanäle).

Wenn das einwählende Gerät bei der Anwahl zunächst eine Verbindung aufbauen kann, diese Verbindung dann jedoch direkt während der Protokollverhandlung wieder getrennt wird, deutet das auf fehlende freie IP-Adressen im IP-Pool hin.

Ende-Adreß-Pool Ende des Adreß-Pools für IP-Pooling.

Setup/IP-Router-Modul/Routing-Methode

Der Router bietet zwei Methoden für das IP-Routing an, die für IP- und ICMP-Pakete getrennt eingestellt werden können. Beide Methoden setzen auf der Auswertung des Feldes 'Type-of-Service' innerhalb des IP-Headers auf.

Das Menü hat den folgenden Aufbau:

/Routing-Methode	Einstellungen der Routing-Methode	
Routing-Methode		Routing-Methode für IP-Pakete
ICMP-Routing-Methode		Routing-Methode für ICMP-Pakete

Routing-Methode Mit diesem Eintrag legen Sie die Routing-Methode für IP-Pakete fest:

- Durch die Einstellung 'normal' werden alle IP-Pakete gleich behandelt, entsprechend den Routing-Vorschriften des Internet-Protocols.
- Durch die Einstellung 'TOS' werden IP-Pakete je nach Inhalt des 'TOS'-Feldes in die Urgent-Queue oder in die gesicherte Queue gestellt. Alle anderen Pakete werden in der normalen Sende-Queue abgelegt. Die Übertragung ist also garantiert, sofern sie grundsätzlich möglich ist.

ICMP-Routing-
Methode

Mit diesem Eintrag legen Sie die Routing-Methode für ICMP-Pakete fest:

- Durch die Einstellung 'normal' werden ICMP-Pakete wie alle anderen IP-Pakete behandelt, entsprechend den Routing-Vorschriften des Internet-Protocols.
- Durch die Einstellung 'gesichert' werden alle empfangenen ICMP-Pakete in die gesicherte Queue gestellt.

Setup/IP-Router-Modul/RIP-Einstellungen

Hierüber können Einstellungen für die Verwaltung von IP-RIP-Paketen vorgenommen werden. Das Menü hat den folgenden Aufbau:

/RIP-Einstellungen	Einstellungen für den Betrieb von IP-RIP	
Typ		RIP-Kompatibilitätsschalter
R1 Maske		Verwaltung von Netzwerkmasken
Tabelle-RIP		Dynamische IP-Routing-Tabelle

Typ

Es kann eingestellt werden, nach welchem Verfahren die IP-RIP-Pakete behandelt werden sollen. Dabei bedeutet die Einstellung:

- **Aus:** IP-RIP wird nicht unterstützt (Standard).
- **RIP-1:** RIP-1- und RIP-2-Pakete werden empfangen, aber nur RIP-1-Pakete gesendet.
- **R1komp:** Es werden ebenfalls RIP-1- und RIP-2-Pakete empfangen. Gesendet werden RIP-2-Pakete als IP-Broadcast.
- **RIP-2:** Wie **R1komp**, nur werden alle RIP-Pakete an die IP-Multicast-Adresse 224.0.0.9 gesendet.

R1-Maske

Über diesen Menüpunkt kann, bei Verwendung von **RIP-1**, die Verwaltung der Netzwerkmasken beeinflusst werden. Diese Einstellungen werden daher nur bei Subnetting unter **RIP-1** benötigt. Dabei bedeutet die Einstellung:

- **Klasse** (Standard): Die im RIP-Paket verwendete Netzwerkmaske ergibt sich direkt aus der IP-Adresse-Klasse, d.h., für die Netzwerkklassen werden folgende Netzwerkmasken verwendet:
 - Klasse A: 255.0.0.0
 - Klasse B: 255.255.0.0
 - Klasse C: 255.255.255.0
- **Adresse:** Die Netzwerkmaske ergibt sich aus dem 1. gesetzten Bit der eingetragenen IP-Adresse. Dieses und alle höherwertigen Bits innerhalb der Netzwerkmaske

werden gesetzt. Aus der IP-Adresse 127.128.128.64 ergibt sich so z.B. die IP-Netzmaske 255.255.255.192.

- **KI+Adr:** Die Netzwerkmaske wird aus der IP-Adressen-Klasse und einem angefügten Teil nach dem Adreßverfahren gebildet. Aus obiger Adresse und der Netzmaske 255.255.0.0 ergibt sich somit die IP-Netzmaske 255.128.0.0.

Tabelle-RIP

Über diesen Menüpunkt werden die Einträge der aktuellen dynamischen IP-Routing-Tabelle angezeigt.

Eine IP-RIP-Tabelle kann z.B. wie folgt aussehen:

IP-Adresse	IP-Netz-Maske	Zeit	Distanz	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200

Setup/IP-Router-Modul/Masquerading

In diesem Menü werden die Einstellungen für die Maskierungsfunktion vorgenommen. Das Menü hat den folgenden Aufbau:

/Masquerading	Einstellungen für das IP-Masquerading	
TCP-Aging		Zeit in Sekunden bis eine TCP-Maskierung ungültig wird
UDP-Aging		Zeit in Sekunden bis eine UDP-Maskierung ungültig wird
ICMP-Aging		Zeit in Sekunden bis eine ICMP-Maskierung ungültig wird
Service-Tabelle		statische Masquerading-Tabelle
Tabelle-Masquerade		dynamische Masquerading-Tabelle

Service-Tabelle

Bei der Verwendung des inversen Masqueradings werden durch den Eintrag bestimmter Ports in der Service-Tabelle 'Dienste' (z.B. ein Fileserver) im IP-Netz gezielt im Internet sichtbar gemacht, während alle anderen Dienste und Rechner aus dem lokalen Netz unsichtbar bleiben (siehe auch 'IP-Masquerading (NAT, PAT)'). Die Service-Tabelle (auch statische Masquerading-Tabelle) hat max. 16 Einträge nach folgendem Aufbau:

Z-Port	Intranet-Adresse
20	10.1.1.10
21	10.1.1.10

Hierbei bedeuten:

- Z-Port: Ziel-Port für diesen Eintrag
- Intranet-Adresse: Ziel-IP-Adresse des Rechners im lokalen Netz

Durch diese Zuweisung kann der entsprechende Dienst z.B. über Telnet direkt angesprochen werden. Geben Sie dazu die IP-Adresse des Routers ein und hängen die Port-Nummer, durch Doppelpunkt getrennt, an die Adresse an.

Mit dem Befehl

```
telnet 192.38.50.100:27
```

verbinden Sie sich direkt mit einem News-Server, der über einen Router mit der IP-Adresse 192.38.50.100 zu erreichen ist.

Tabelle-Masquerade

Beim IP-Masquerading werden die IP-Adressen von Rechnern im lokalen Netz durch eine Umsetzung der Adressen und Ports im Router nach außen hin unsichtbar gemacht. In der dynamischen Masquerading-Tabelle werden die IP-Adressen aus dem lokalen Netz angezeigt, die aktuell vom Router maskiert werden. Die dynamische Masquerading-Tabelle hat maximal 2048 Einträge nach folgendem Aufbau:

Intranet-Adresse	Q-Port	Protokoll	Zeit
10.1.1.10	1234	TCP	10

Hierbei bedeuten:

- Intranet-Adresse: IP-Adresse des Rechners im lokalen Netz
- Q-Port: Quell-Port für diesen Eintrag
- Protokoll: verwendetes Protokoll (TCP/UDP/ICMP)
- Zeit: Zeit in Sekunden, bis der Eintrag aus der Tabelle entfernt wird

Setup/SNMP-Modul

Über dieses Menü können Einstellungen für Konfiguration des Routers über SNMP vorgenommen werden. Das Menü hat den folgenden Aufbau:

/SNMP-Modul		Einstellungen für das SNMP-Modul
Traps-senden		Schalter für die Ausgabe von SNMP-Traps
IP-Trap-Tabelle		Tabelle mit 20 Ziel-Adressen für Trap-Nachrichten
Administrator		Geräte-Administrator
Standort		Geräte-Standort
Register-Monitor		Befehl zum Anmelden einer Zieladresse, zu der Traps gesendet werden sollen
Loesche-Monitor		Befehl zum Löschen einer Adresse, die mit 'Register-Monitor' gesetzt wurde
Monitor-Tabelle		Tabelle mit allen aktuell aktiven Zieladressen, die mit 'Register-Monitor' gesetzt wurden

Traps-senden

Dieser Eintrag steuert die Ausgabe von Traps (ein/aus).

IP-Trap-Tabelle Gibt die IP-Adressen an, zu der Trap-Nachrichten gesendet werden.

Administrator Name des Administrators

Standort Standort des Gerätes

Die letzten beiden Parameter können auch über SNMP (MIB-2) abgefragt werden.

Register-Monitor Mit diesem Befehl melden sich Applikationen beim Router an, um gezielte Trap-Informationen zu erhalten. Der *ELSA LANmonitor* fragt so z.B. die Kanalstatistiken ab und setzt sie (unter Windows) in eine grafische Darstellung um.

Im Prinzip können beliebige SNMP-Manager diesen Befehl nutzen, um Informationen aus dem Router zu erhalten. Mit der Syntax:

```
register-monitor ip-adresse:port mac-adresse timeout
```

wird der Router angewiesen, die angegebene Adresse in die Monitor-Tabelle aufzunehmen und Traps an sie zu senden. Bleiben die Traps für die eingestellte Haltezeit aus, wird die Adresse automatisch aus der Tabelle gelöscht. Eine Haltezeit von '0' behält den Eintrag dauerhaft in der Tabelle.

Loesche-Monitor Mit diesem Befehl werden die Einträge aus der Monitor-Tabelle entfernt.

Monitor-Tabelle Die Monitor-Tabelle hat folgenden Aufbau:

IP-Adresse	Port	MAC-Adresse	Timeout
10.0.0.53	1057	0080c76da46e	1

Mit diesem Eintrag hat sich z.B. ein *ELSA LANmonitor* bei dem Router angemeldet.

Setup/DHCP-Server-Modul

Über dieses Menü können Einstellungen für den DHCP-Server vorgenommen werden. Das Menü hat den folgenden Aufbau:

/DHCP-Server-Modul		Einstellungen für den DHCP-Server
Zustand		Schalter für die Aktivierung des DHCP-Moduls
Start-Adreß-Pool		Start-Adresse für den Adreßpool
Ende-Adreß-Pool		End-Adresse für den Adreßpool
Netzmaske		Netzmaske für den Adreßpool
Broadcast-Adresse		Broadcast-Adresse für das LAN
Max.-Gültigkeit-Minute(n)		Maximal-Gültigkeit der Adreßzuweisung über DHCP
Default-Gültigkeit-Minute(n)		Standard-Gültigkeit der Adreßzuweisung über DHCP
Tabelle-DHCP		Tabelle mit den aktuellen Zuweisungen über DHCP

<i>Zustand</i>	<p>Ein: Das Gerät arbeitet als DHCP-Server</p> <p>Aus: Das Gerät arbeitet nicht als DHCP-Server</p> <p>Auto: Das Gerät überprüft regelmäßig, ob ein anderer DHCP-Server im LAN vorhanden ist. Wenn nicht, dann arbeitet es als DHCP-Server und verteilt IP-Adresse an lokale Clients.</p>
	<p><i>Falls im TCP/IP-Modul keine IP- oder Intranet-Adresse eingetragen ist (z.B. Auslieferungszustand), dann verteilt der Router im Auto-Modus IP-Adressen aus dem Adreßbereich 10.0.0.2—10.0.0.253 an alle DHCP-Clients.</i></p>
<i>Start-Adreß-Pool</i> <i>Ende-Adreß-Pool</i>	<p>Die zugewiesene IP-Adresse wird aus dem eingestellten Adreß-Pool genommen ('Start-Adress-Pool' bis 'Ende-Adress-Pool'). Hier können beliebige im lokalen Netz gültige Adressen eingegeben werden.</p> <p>Wird stattdessen '0.0.0.0' eingegeben, so ermittelt das Gerät die jeweiligen Adressen (Start bzw. Ende) aus den Einstellungen unter 'Setup/TCP-Modul'. Dabei wird wie folgt vorgegangen:</p> <ul style="list-style-type: none">■ Ist nur die IP-Adresse oder nur die Intranet-Adresse eingegeben, so wird über die zugehörige Netzmaske der Start bzw. das Ende des Pools bestimmt.■ Sind beide angegeben, so hat die Intranet-Adresse den Vorrang bei der Bestimmung des Pools.■ Als Start-Adresse des Pools wird entweder die im DHCP-Modul eingegebene Adresse verwendet oder die erste gültige Adresse im lokalen Netz.■ Als End-Adresse des Pools wird entweder die im DHCP-Modul eingegebene Adresse verwendet oder die letzte gültige Adresse im lokalen Netz. <p>Als IP-Adresse wird dann eine gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit bereits schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.</p> <p>Der DHCP-Server prüft zusätzlich, ob die Adresse, die dem Rechner zugewiesen werden soll, eindeutig im lokalen Netz ist. Dies geschieht mit einem ARP-Request auf die Adresse. Wird dieser ARP-Request beantwortet, so beginnt der DHCP-Server den Vorgang mit einer neuen Adresse. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.</p>
<i>Netzmaske</i>	<p>Die Zuweisung der Netzmaske erfolgt analog zur Adreßzuweisung:</p> <p>Entweder wird die im DHCP-Modul eingetragene Netzmaske zugewiesen, oder es wird die zum (bei der Adreßzuweisung bestimmten) lokalen Netz gehörende Netzmaske verwendet.</p>
<i>Broadcast</i>	<p>Die Zuweisung der Broadcast-Adresse erfolgt analog zur Adreßzuweisung:</p>

Entweder wird die im DHCP-Modul eingetragene Broadcast-Adresse zugewiesen, oder es wird die zum (bei der Adreßzuweisung bestimmten) lokalen Netz gehörende Broadcast-Adresse verwendet.

Max.-Gültigkeit-Minute(n) Hier kann die maximale Gültigkeitsdauer eingetragen werden, die der DHCP-Server einem Host zuweist.

Der DEFAULT-Wert von 6000 Minuten entspricht ca. 4 Tagen.

Default-Gültigkeit-Minute(n) Hier kann die Gültigkeitsdauer eingetragen werden, die zugewiesen wird, wenn der Host überhaupt keine Gültigkeitsdauer anfordert.

Der DEFAULT-Wert von 500 Minuten entspricht ca. 8 Stunden.

Tabelle-DHCP Im DHCP-Modul kann über den Punkt 'Tabelle-DHCP' die Zuweisung von IP-Adressen an die jeweiligen Rechner überprüft (bzw. nachgeschaut) werden. Diese Tabelle hat den folgenden Aufbau:

IP-Adresse	MAC-Adresse	Timeout	Rechnername	Typ
10.1.1.10	00a0570308e1	500	ELSA	neu

- IP-Adresse: zugewiesene IP-Adresse
- MAC-Adresse: Ethernet-Adresse des Rechners
- Timeout: Restzeit bis die Zuweisung ungültig wird
- Rechnername: Klartextname des Rechners, wenn er diesen in der Anfrage übermittelt
- Typ: Dieses Feld enthält weitere Informationen zu der Zuweisung.

Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:

- **neu**: Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.
- **unbek.**: Bei der Überprüfung der Eindeutigkeit wurde festgestellt, daß die Adresse bereits an einen anderen Rechner vergeben wurde. Der DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.
- **stat.**: Ein Rechner hat dem DHCP-Server mitgeteilt, daß er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr verwendet werden.
- **dyn.**: Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

Setup/NetBIOS

Im Menü Setup/NetBIOS werden die Einstellungen für das NetBIOS-Modul vorgenommen. Das Menü hat den folgenden Aufbau

Zustand		Ein oder aus
Scope-ID		NetBIOS-Scope, in dem sich der Router befindet.
NT-Domaene		Arbeitsgruppe/Domain, in dem sich der Router befindet.
Gegenstellen-Tab.		In der Gegenstellen-Tabelle werden alle Gegenstellen eingetragen, mit denen NetBIOS-Informationen ausgetauscht werden.
Gruppen-Liste		In der Gruppen-Liste werden alle über NetBIOS bekannten Arbeitsgruppen abgelegt.
Host-Liste		In der Host-Liste werden alle über NetBIOS bekannten Rechner-Namen abgelegt.
Server-Liste		In der Server-Liste werden alle Server abgelegt, die sich im Netz bekannt gemacht haben.

Scope-ID

Im Menüpunkt Scope-ID kann der NetBIOS-Scope angegeben werden, in dem sich das Gerät befindet. Es sieht dann nur noch NetBIOS-Pakete, die aus dem selben NetBIOS-Scope kommen. Alle anderen Pakete werden stillschweigend verworfen. Die Scope-ID wird nur in Verbindung mit Windows-Name-Servern (WINS) verwendet. Im allgemeinen kann dieser Eintrag frei bleiben.

NT-Domaene

Im Punkt NT-Domaene kann eine Arbeitsgruppe/Domain angegeben werden, um den Such-Vorgang beim Start des NetBIOS-Moduls anzustoßen. Dies ist notwendig, wenn sich im Netz keine Rechner mit Windows 95 oder Windows 98 befinden.

Gegenstellen-Tab.

In der Gegenstellen-Tabelle werden alle Gegenstellen eingetragen, die NetBIOS Informationen erhalten sollen, bzw. von denen NetBIOS-Information angenommen werden. Wenn das NetBIOS-Modul eingeschaltet ist, werden NetBIOS-Pakete von anderen als den angegebenen Gegenstellen stillschweigend verworfen. Die Gegenstellen-Tabelle hat den folgenden Aufbau

Name	Typ
AACHEN	Router oder Workstation



Wenn die Verbindung zur gewählten Gegenstelle über eine PPP-Verbindung realisiert wird, müssen in der PPP-Tabelle für den entsprechenden Eintrag die Rechte für NetBIOS aktiviert sein!

Typ

Das Feld 'Typ' gibt an, ob die Gegenstelle ein Router oder eine Workstation ist. Ist die Gegenstelle eine Workstation, so werden alle von dieser Gegenstelle bekannten Namen und Server im lokalen Netz und allen anderen verbundenen Routern abgemeldet und aus

den jeweiligen Tabellen gelöscht, sobald die Verbindung zu der Gegenstelle abgebaut wird.

Host-Tabelle Die Host-Tabelle hat den folgenden Aufbau:

Name	Typ	IP-Adresse	Gegenstelle	Timeout	Flags
REMOTE	00	10.0.1.100	AACHEN	5000	xx20
WORKSTATION	00	10.0.0.10		5000	xx00

Gruppentabelle Die Gruppentabelle sieht entsprechend so aus:

Gruppe/ Domaene	Typ	IP-Adresse	Gegenstelle	Timeout	Flags
WORKGROUP	1e	10.0.0.10		5000	xx00
WORKGROUP	1e	10.0.1.100	AACHEN	5000	xx20

Die Felder der Tabellen haben dabei die folgende Bedeutung:

Name	Name des Hosts in der Host-Tabelle
Gruppe/ Domaene	Name der Gruppe bzw. Domain in der Gruppenliste. Gruppen und NT-Domains werden aus NetBIOS-Sicht gleich behandelt.
Typ	WINS-Typ des Host. Der Typ ist aus NetBIOS-Sicht uninteressant, jedoch ist ordnen Windows-Netze anhand des Typs dem Namen bestimmte Eigenschaften zu.
IP-Adresse	IP-Adresse des Besitzers des Namens. In der Gruppenliste können mehrere IP-Adressen dem gleichen Namen zugeordnet sein
Gegenstelle	Name der Gegenstelle, über die der Name bekannt wurde.
Timeout	Zeit bis der Name ungültig wird. Der Timeout ist zusätzlich mit einem Aging-Counter in den Flags verknüpft.
Flags	In den Flags werden bestimmte Zusatzinformationen zu dem Namen gehalten.

Flags Die Flags haben folgende Bedeutung:

0x0003	Dieser Zähler wird nach jedem Ablauf der Gültigkeit erhöht. Wenn den Name nicht spätestens nach dem zweiten ablaufen erneuert wurde, so wird der Eintrag gelöscht.
0x0004	Dies kennzeichnet einen Eintrag, der noch übertragen werden muß.
0x0008	Dies kennzeichnet einen Eintrag, der zum Löschen ansteht, d.h. der Name wurde nach einem Verbindungsaufbau noch nicht erneuert
0x0010	reserviert
0x0020	Dies kennzeichnet eine remote Gegenstelle.
0x0040	reserviert
0x0080	reserviert

Die Server-Liste hat den folgenden Aufbau

Host	Gruppe/ Domaene	UPD	IP- Adresse	OS- Ver	SMB- Ver	Server- Typ	Gegen- stelle	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

Diese Tabelle füllt sich im Gegensatz zur Host- und Gruppen-Liste nur allmählich, da das NetBIOS-Modul darauf angewiesen ist, daß sich die Server von sich aus melden.

Dabei haben die einzelnen Felder die folgende Bedeutung:

Host	Name des Servers
Gruppe/ Domaene	Arbeitsgruppe bzw. Domain, in der sich der Server befindet
UPD	Update-Counter: gibt an wie oft der Server sich bereits propagiert hat
IP-Adresse	Adresse des Servers
OS-Ver	Versions-Nummer des Betriebssystems
SMB-Ver	Versions-Nummer des verwendeten SMB-Protokolls
Server-Typ	Bitmaske, in der die Dienste des Servers codiert sind
Gegenstelle	Name der Gegenstelle von der der Server bekannt gegeben wurde
Timeout	Zeit bis zum ungültig werden des Eintrags (bei Einträgen vom LAN) bzw. Zeit bis der Router einen Remote-Eintrag propagiert.
Flags	Entspricht den Flags in der Host- bzw. Gruppentabelle.

Setup/Config-Modul

Über dieses Menü können Einstellungen für Konfigurationsmöglichkeiten des Routers vorgenommen werden. Das Menü hat den folgenden Aufbau:

/Config-Modul		Einstellungen für das Konfigurationsmodul
LAN-Config		Schalter für Konfiguration von der LAN-Seite
WAN-Config		Schalter für Konfiguration von der WAN-Seite
Passwort-Zwang		Paßwortzwang ein/aus, wenn kein Paßwort vorhanden ist
Fernconfig-(EAZ-MSN)		Rufnummer für die Fernkonfiguration über PPP
Maximale-Verbindungen.		Maximale Anzahl gleichzeitiger Verbindungen
Conf.-Haltezeit		Zeitbeschränkung für Remote-Konfigurationsverbindungen

/Config-Modul	Einstellungen für das Konfigurationsmodul	
Login-Fehler		Anzahl für Login-Fehlversuche, bevor die Login-Sperre greift
Sperr-Minuten		Dauer der Sperrung und Zeitraum, bis alte Login-Fehler vergessen sind
Sprache		Sprache für die Konfiguration

LAN-Config Mit dieser Einstellung kann festgelegt werden, ob eine Konfiguration von der LAN-Seite möglich ist (**Ein**), nicht möglich ist (**Aus**) oder nur im Lese-Betrieb möglich ist (**Lese**). Standardmäßig ist die Option **Ein** aktiviert.

WAN-Config Mit dieser Einstellung kann festgelegt werden, ob eine Konfiguration von der WAN-Seite möglich ist (**Ein**), nicht möglich ist (**Aus**) oder nur im Lese-Betrieb möglich ist (**Lese**). Standardmäßig ist die Option **Aus** aktiviert.

Passw.Zwang Hier wird festgelegt, ob bei nicht vorhandenem Paßwort bei jedem Konfigurationsbeginn nach einem neuen Paßwort gefragt werden soll (**Ein**), oder ob die Paßwortabfrage unterdrückt werden soll (**Aus**). Standardmäßig ist die Option **Ein** aktiviert.

Fernconfig-(EAZ-MSN) Diese Rufnummer erlaubt die Fernkonfiguration über PPP. Solange keine Nummer eingetragen ist, werden Rufe auf beliebige Nummern für die Fernkonfiguration angenommen.

Maximale-Verbindungen Hier kann die maximale Anzahl der gleichzeitigen Remote-Konfigurationssitzungen zum Gerät abgelesen werden.

Conf.-Haltezeit Erfolgt während einer Remote-Konfiguration keine Übertragung mehr, wenn z.B. keine Daten mehr vom Benutzer eingegeben werden, baut das Gerät die Verbindung automatisch nach der hier angegebenen Zeit ab. Gültige Werte sind 1 bis 99 Minuten. Der Standardwert beträgt 5 Minuten.

Login-Fehler Dieser Eintrag gibt an, wie viele Fehlversuche gemacht werden dürfen, bevor die Login-Sperre aktiviert wird. Dabei wird ein leeres Paßwort (am Paßwort-Prompt einfach nur <ENTER> drücken) nicht als Versuch gewertet und löst daher auch nicht die Sperre aus.



Der Default-Wert ist 5. Bei einem niedrigeren Wert kann es passieren, daß bei einem Zugriff über ein älteres ELSA LANconfig die Login-Sperre greift! In diesem Fall erhalten Sie eine aktuelle ELSA LANconfig-Version über unsere Online-Medien.

Sperr-Minuten Dieser Eintrag hat zwei Bedeutungen. Zum einen gibt er an, wie lange der Zugang gesperrt ist, wenn die Login-Sperre aktiviert wurde. Zum zweiten wird hiermit die Zeit eingestellt, nach der das Gerät alle vorherigen Login-Fehler vergißt.

Sprache Stellen Sie hier ein, ob Sie die Konfiguration mit der deutschen oder der englischen Fassung der Software durchführen wollen.

Setup/LANCAPI-Modul

Bei der Einstellung der *LANCAPI* werden im Prinzip folgende Fragen geregelt:

- Auf welche Rufnummer aus dem Telefonnetz soll die *LANCAPI* reagieren?
- Welche der Rechner im lokalen Netz sollen über die *LANCAPI* Zugang zum Telefonnetz erhalten?
- Über welchen UDP-Port kommunizieren *LANCAPI*-Server und *LANCAPI*-Clients?

Das *LANCAPI*-Modul hat folgenden Aufbau:

/LANCAPI-Modul		Einstellungen für die <i>LANCAPI</i>
Zugangsliste		Liste der Rechner, die die <i>LANCAPI</i> nutzen dürfen
Interface-Tabelle		Aktivierung der <i>LANCAPI</i> für die verschiedenen Interfaces und Einstellung der Rufnummern, auf die die <i>LANCAPI</i> reagieren soll.
Prioritäten-Tabelle		Priorität für die <i>LANCAPI</i> gegenüber Routerverbindungen
UPD-Port		UDP-Port für die Kommunikation zwischen <i>LANCAPI</i> -Server und -Clients

Zugangsliste

Grenzen Sie hier den Kreis der Rechner ein, die die *LANCAPI* nutzen dürfen. Diese Tabelle kann maximal 16 Einträge aufnehmen. Ist die Tabelle leer, können alle Rechner auf die *LANCAPI* zugreifen.

Interface-Tabelle

Die Interface-Tabelle sieht so aus:

lfc	Zustand	EAZ-MSN(s)	Erzw.-Out-MSN
S0-1	Abgehend	123456	nein

Die Felder der Tabellen haben dabei die folgende Bedeutung:

lfc	Bezeichnet das zugehörige Interface
Zustand	Dieser Punkt legt fest, ob auf diesem Interface <i>LANCAPI</i> -Betrieb mit ausgehenden Rufen (Abgehend), mit ein- und ausgehenden Rufen (Ein) oder kein <i>LANCAPI</i> -Betrieb (Aus) zugelassen ist.
EAZ-MSN(s)	Hier werden die EAZs bzw. MSNs eingetragen, auf die die <i>LANCAPI</i> bei einkommenden Rufen reagieren soll, bzw. die bei ausgehenden Rufen ggf. als abgehende EAZ/MSN der Vermittlungsstelle gemeldet werden soll.
Erzw.-Out-MSN	Wenn die CAPI-Applikation keine abgehende MSN konfiguriert hat, kann hier eingestellt werden, ob die <i>LANCAPI</i> in diesem Fall die erste EAZ/MSN aus der Liste übermittelt.

Prioritäten-Tabelle

Mit der Priorität steuern Sie die Möglichkeit, für abgehende Verbindungen über die *LANCAPI* Routerverbindungen zu unterbrechen. Mit der Option '1' werden keine Routerverbindungen unterbrochen, mit der Einstellung '2' werden nur Nebenkanäle einer Routerverbindung mit Kanalbündelung unterbrochen, mit der Auswahl '3' werden auch Hauptkanäle einer Routerverbindung unterbrochen.

Setup/LCR-Modul

Bei der Einstellung des Least-Cost-Routers geben Sie folgende Informationen an:

- Für welche Module im Gerät sollen die Funktionen des LCR aktiv sein?
- Welche Vorwahlen sollen wann über welchen Call-by-Call-Provider umgeleitet werden?

Das LCR-Modul hat folgenden Aufbau:

/LCR-Modul		Einstellungen für den Least-Cost-Router
Router-Nutzung		LCR für die Routermodule aktivieren, Ein oder Aus
Lancapi-Nutzung		LCR für die <i>LANCAPI</i> aktivieren, Ein oder Aus
Zeittabelle		Tabelle der Rufumleitungen
Feiertagstabelle		Liste der Feiertage, die von der Zeittabelle berücksichtigt werden müssen.

Zeittabelle

Die Zeittabelle hat 256 Einträge mit folgenden Aufbau:

Index	Praefix	Tage	Start	Stop	Nummernliste	Rueckfall
1	0171	192	0:00	23:59	01013;01070	Ein

Die einzelnen Einträge haben die folgende Bedeutung:

Index	Durchlaufender Index für die Einträge in der Tabelle
Praefix	Vorwahl, die umgeleitet werden soll
Tage	Gültigkeit des Eintrags für Wochen- und Feiertage in Darstellung einer 8-Bit-Maske: Bit 0 steht für Montag, Bit 7 für Feiertage. Der Eintrag '31' bezeichnet also alle Werkzeuge, '192' die Sonn- und Feiertage
Start	Anfangszeit für die Gültigkeit des Eintrags an den definierten Tagen
Stop	Endzeit für die Gültigkeit des Eintrags an den definierten Tagen
Nummernliste	Netzkennzahl des Call-by-Call-Providers
Rueckfall	Automatischer Rückfall auf die eigene Telefongesellschaft, falls alle Call-by-Call-Nummern besetzt sind

Beispiel:

```
set 1 02 31 1:00 11:59 01030;01090;01070 Ein
```

leitet alle Fernverbindungen in die Region '02' zwischen ein und zwölf Uhr um auf den Provider mit der Netzkennzahl '01030'. Falls da besetzt ist, werden die Netzkennzahlen '01090' und '01070' versucht. Sind die auch nicht verfügbar, wird die Verbindung über die normale Telefongesellschaft aufgebaut.

Feiertagstabelle Die Feiertagstabelle hat 256 Einträge mit folgendem Aufbau:

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

Die einzelnen Einträge haben die folgende Bedeutung:

Index	Durchlaufender Index für die Einträge in der Tabelle
Datum	Datum der einzelnen Feiertage Geben Sie den Index und das Datum vollständig ohne Trennzeichen ein, also z.B. 'set 8 13041999' für den 13. April 1999 als achten Listeneintrag. Geben Sie als Jahr '0000' für jährlich wiederkehrende Feiertage ein.

Setup/DNS-Modul

Hier werden die Einstellungen des DNS-Servers vorgenommen. Das Menü enthält die folgenden Einträge (inkl. Default-Einstellungen):

Zustand		Ein (Default) oder aus
Domaene		Eigene Domain, optional, maximal 32 Zeichen
DHCP-verwenden		Ja (Default) oder nein
NetBIOS-verw.		Ja (Default) oder nein
DNS-Tabelle		Statische DNS-Tabelle zur manuellen Zuweisung von IP-Adressen und Namen, 64 Einträge
Filter-Liste		Filter-Liste zum Ausschließen verbotener Domains, 64 Einträge
Gültigkeit		Gibt an, welche Gültigkeit einem anfragenden Rechner für einen Namen mitgeteilt wird. Default: 2000

DNS-Tabelle Die DNS-Tabelle enthält eine einfache Zuordnung von lokalen Namen zu IP-Adressen. Dabei ist diese alphabetisch nach Namen sortiert.

Die Tabelle ist auf 64 Einträge beschränkt, da man größere Netze besser über den DHCP-Server konfiguriert und daher diesen zur Auflösung heranziehen kann. Die Tabelle hat den folgenden Aufbau:

Rechnername	Ip-Adresse
HOST10	10.0.0.10

Der Name ist hierbei auf 32 Zeichen begrenzt. Längere Namen sind im lokalen Netz auch nicht sinnvoll.

Filter-Liste

Die Filter-Liste nimmt Einträge für zu sperrende Domains auf. Weiterhin kann konfiguriert werden, für wen diese Domain gesperrt sein soll. Dies wird über ein Paar IP-Adresse/Netzmaske angegeben. Eine IP-Adresse von 0.0.0.0 bedeutet dabei, daß diese Domain für alle Rechner gesperrt ist. Ebenso bedeutet eine Netzmaske von 0.0.0.0, daß die Domain für alle Netze gesperrt ist. Die Tabelle hat den folgenden Aufbau:

Name	Domain	Ip-Adresse	Netzmaske
F001	*xxx*	0.0.0.0	0.0.0.0

Im Feld 'Name' kann eine eindeutige ID für den jeweiligen Filter frei gewählt werden.

Das Feld 'Domain' nimmt den Namen der zu sperrenden Domain auf. Dabei sind auch Wildcards wie '?' und '*' möglich. Der Wildcard '?' ersetzt dabei genau ein Zeichen, während '*' für beliebig viele Zeichen steht. Der Wildcard '*' kann dabei öfters verwendet werden. So filtert *xxx* z.B. alle Namen, in denen xxx vorkommt.

Über die Felder IP-Adresse und Netzmaske kann angegeben werden, für welches Subnetz diese Domain gesperrt wird.

Die Filtertabelle ist absteigend nach Netzmasken (die längste steht oben) und bei gleicher Netzmaske aufsteigend nach IP-Adressen sortiert. Bei gleichen IP-Adressen wird sie dann noch aufsteigend nach zu sperrender Domain sortiert.

Beim Durchsuchen der Tabelle wird diese nun von oben nach unten abgearbeitet. Sobald ein Filter paßt, wird eine Fehlermeldung an den anfragenden Rechner ausgegeben.

Setup/Zeit-Modul

Der Least-Cost-Router im Gerät benötigt korrekte Zeitinformationen für die Berechnung der Rufnummernumleitungen über Call-by-Call-Provider. Auch bei einigen Statistiken ist die Anzeige einer präzisen Zeitinformation wünschenswert.

Die Zeit kann entweder manuell gesetzt werden (mit dem Befehl 'time') oder automatisch aus dem ISDN-Netz abgelesen werden.

Für den automatischen Zeitabgleich wird beim Einschalten des Moduls direkt eine vorher bestimmte Gegenstelle angerufen und dabei die Zeitinformation aus dem ISDN-Netz übernommen. Solange das Zeit-Modul eingeschaltet ist, wird bei jeder Verbindung erneut die Zeit aus dem ISDN übernommen.

Das Zeit-Modul hat folgenden Aufbau:

/Zeit-Modul		Einstellungen für das Zeit-Modul
Zustand		Aktivierung des Moduls: Ein, Aus
Aktuelle-Zeit		Anzeige der aktuellen Zeit im Gerät
Time EAZ-MSN		Rufnummer, zu der eine Verbindung aufgebaut werden soll, um eine Zeitinformation aus dem ISDN-Netz zu erhalten
Anwahl-Versuche		Anzahl der möglichen Versuche, eine Zeitinformation zu erhalten.

Firmware

Über dieses Menü können die verschiedenen Firmwareparameter abgerufen werden und ein Firmware-Upload gestartet werden:

/Firmware		Einstellungen für Display-Anzeige und Tastatur
Versions-Tabelle		Anzeige der Hardware-Releases und Seriennummern des Routers
Tabelle-Firmsafe		Informationen über die beiden im Gerät gespeicherten Firmware-Versionen und über den Bootloader.
Modus-Firmsafe		Modus der Firmware-Aktivierung
Timeout-Firmsafe		Zeit in Minuten für den Test einer neuen Firmware
Test-Firmware		Testet die inaktive Firmware
Firmware-Upload		Starten eines Firmware-Uploads

Versions-Tabelle

In der Versions-Tabelle werden die Firmware-Version des Gerätes und die Seriennummer angezeigt.

lfc	Modul	Version	Seriennummer
lfc	LANCOM Business 4100	1.60.0012 / 30.06.1999	8427.000.020

Table-Firmsafe

In dieser Tabelle finden Sie für jede der beiden im Gerät gespeicherten Firmware-Versionen die Angaben über die Position im Speicherbereich (1 oder 2), die Angabe des Zustan-

des (aktiv oder inaktiv), die Versionsnummer, das Datum, die Größe und den Index (fortlaufende Nummer).

Position	Status	Version	Datum	Große	Index
1	inaktiv	1.60	23061999	690	6
2	aktiv	1.60	30061999	692	7
3	<Lader>	1.60	07061999	64	0

Um eine inaktive Firmware zu aktivieren, geben Sie den Befehl

```
set <Positionsnummer> aktiv  
ein.
```

Modus-Firmsafe Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firmware überschrieben. Sie können selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll:

- 'Unmittelbar': Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:
 - Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.
 - Arbeitet die neue Firmware jedoch nicht korrekt, ist das Gerät evtl. nach dem Neustart nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit das Gerät neu.
- 'Login': Um den Problemen einer fehlerhaften Firmware zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.
 - Im Unterschied zur ersten Variante wartet Firmsafe anschließend auf einen erfolgreichen Login über Outband oder Inband (per Telnet). Im Unterschied zur ersten Variante wartet Firmsafe anschließend auf einen erfolgreichen Login (per Telnet). Nur wenn dieser Login während der unter 'Timeout-Firmsafe' eingestellten Zeit erfolgt, wird die neue Firmware auch dauerhaft aktiviert.
 - Wenn das Gerät nicht mehr ansprechbar ist und ein Login somit unmöglich ist, aktiviert Firmsafe automatisch wieder die bisherige Firmware und startet damit das Gerät neu.
- 'Manuell': Auch bei der dritten Möglichkeit können Sie vorher selbst eine Zeit bestimmen (Timeout-Firmsafe), in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, daß die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird.

Sonstiges

Über das Menü **Sonstiges** werden nachfolgende Funktionen verwaltet:

/Sonstiges	Verschiedene Funktionen	
Manuelle Wahl		Test einer Verbindung
System-Boot		Neustart des Gerätes
System-Reset		Rücksetzen auf Werkseinstellung
System-Upload		Neue Firmware laden

Sonstiges/Manuelle-Wahl

Über diesen Menüpunkt kann für Testzwecke eine manuelle Verbindungssteuerung vorgenommen werden.

System-Boot

Über diesen Menüpunkt kann das Gerät neu gestartet werden.



Vor der Ausführung des Befehls werden alle offenen Verbindungen (ISDN oder TCP) abgebaut bzw. geschlossen.

System-Reset

Über diesen Menüpunkt werden alle vorgenommenen Einstellungen rückgängig gemacht. Das Gerät wird in den Auslieferungszustand zurückversetzt.

Zur Sicherheit wird dabei das Paßwort zum Schutz der Konfiguration abgefragt, um eine Verwechslung mit dem Befehl `system-boot` zu vermeiden. Ist kein Paßwort vergeben, muß ein zweites Mal die Enter-Taste gedrückt werden.

System-Upload

Über diesen Menüpunkt kann ein Firmware-Upload gestartet werden (siehe Kapitel 'So spielen Sie eine neue Software ein').

Die Flash-ROM-Technologie ermöglicht eine flexible und servicefreundliche Handhabung der Systemsoftware durch Einspielen unterschiedlicher Firmware-Versionen. Hierdurch können die Geräte auch auf alle zukünftigen Optionen nachgerüstet werden.

Novell SAP-Nummern

Dezimal	hexa-dezimal	SAP-Beschreibung
1	0001	User
2	0002	User Group
3	0003	Print Queue or Print Group
4	0004	File Server (SLIST source)
5	0005	Job Server
6	0006	Gateway
7	0007	Print Server or Silent Print Server
8	0008	Archive Queue
9	0009	Archive Server
10	000a	Job Queue
11	000b	Administration
15	000F	Novell TI-RPC
23	0017	Diagnostics
32	0020	NetBIOS
33	0021	NAS SNA Gateway
35	0023	NACS Async Gateway or Asynchronous Gateway
36	0024	Remote Bridge or Routing Service
38	0026	Bridge Server or Asynchronous Bridge Server
39	0027	TCP/IP Gateway Server
40	0028	Point to Point (Eicon) X.25 Bridge Server
41	0029	Eicon 3270 Gateway
42	002a	CHI Corp
44	002c	PC Chalkboard
45	002d	Time Synchronization Server or Asynchronous Timer
46	002e	ARCserve 5.0 / Palindrome Backup Director 4.x (PDB4)
69	0045	DI3270 Gateway
71	0047	Advertising Print Server
74	004a	NetBlazer Modems

Dezimal	hexa-dezimal	SAP-Beschreibung
75	004b	Btrieve VAP/NLM 5.0
76	004c	Netware SQL VAP/NLM Server
77	004d	Xtree Network Version Netware XTree
80	0050	Btrieve VAP 4.11
82	0052	QuickLink (Cubix)
83	0053	Print Queue User
88	0058	Multipoint X.25 Eicon Router
96	0060	STLB/NLM
100	0064	ARCserve
102	0066	ARCserve 3.0
114	0072	WAN Copy Utility
122	007a	TES-Netware for VMS
146	0092	WATCOM Debugger or Emerald Tape Backup Server
149	0095	DDA OBGYN
152	0098	Netware Access Server (Asynchronous gateway)
154	009a	Netware for VMS II or Named Pipe Server
155	009b	Netware Access Server
158	009e	Portable Netware Server or SunLink NVT161
161	00a1	Powerchute APC UPS NLM
170	00aa	LAWserve
172	00ac	Compaq IDA Status Monitor
256	0100	PIPE STAIL
258	0102	LAN Protect Bindery
259	0103	Oracle DataBase Server
263	0107	Netware 386 or RSPX Remote Console
271	010f	Novell SNA Gateway
273	0111	Test Server
274	0112	Print Server (HP)
276	0114	CSA MUX (f/Communications Executive)

Dezimal	hexa-dezimal	SAP-Beschreibung
277	0115	CSA LCA (f/Communications Executive)
278	0116	CSA CM (f/Communications Executive)
279	0117	CSA SMA (f/Communications Executive)
280	0118	CSA DBA (f/Communications Executive)
281	0119	CSA NMA (f/Communications Executive)
282	011a	CSA SSA (f/Communications Executive)
283	011b	CSA STATUS (f/Communications Executive)
286	011e	CSA APPC (f/Communications Executive)
294	0126	SNA TEST SSA Profile
298	012a	CSA TRACE(f/Communications Executive)
299	012b	Netware for SAA
301	012e	IKARUS virus scan utility
304	0130	Communications Executive
307	0133	NNS Domain Server or Netware Naming Services Domain
309	0135	Netware Naming Services Profile
311	0137	Netware 386 Print Queue or NNS Print Queue
321	0141	LAN Spool Server (Vap, Intel)
338	0152	IRMLAN Gateway
340	0154	Named Pipe Server
358	0166	NetWare Management
360	0168	Intel PICKIT Comm Server or Intel CAS Talk Server
371	0173	Compaq
372	0174	Compaq SNMP Agent
373	0175	Compaq
384	0180	XTree Server or XTree Tools
394	018A	NASI services broadcast server (Novell)
432	01b0	GARP Gateway (net research)

Dezimal	hexa-dezimal	SAP-Beschreibung
433	01b1	Binview (Lan Support Group)
447	01bf	Intel LanDesk Manager
458	01ca	AXTEC
459	01cb	Shiva NetModem/E
460	01cc	Shiva LanRover/E
461	01cd	Shiva LanRover/T
462	01ce	Shiva Universal
472	01d8	Castelle FAXPress Server
474	01da	Castelle LANPress Print Server
476	01dc	Castille FAX/Xerox 7033 Fax Server/Excel Lan Fax
496	01f0	LEGATO
501	01f5	LEGATO
563	0233	NMS Agent or Netware Management Agent
567	0237	NMS IPX Discovery or LANtern Read/Write Channel
568	0238	NMS IP Discovery or LANtern Trap/Alarm Channel
570	023a	LABtern
572	023c	MAVERICK
575	023f	Used by eleven various Novell Servers / Novell SMDR
590	024e	Netware Connect
591	024f	NASI server broadcast (Cisco)
618	026a	Network Management (NMS) Service Console
619	026b	Time Synchronization Server (Netware 4.x)
632	0278	Directory Server (Netware 4.x)
640	0280	Novell File and Printer Sharing Service for PC
989	03dd	Banyan ENS for Netware Client NLM
772	0304	Novell SAA Gateway
776	0308	COM or VERMED 1
778	030a	Galacticomm's Worldgroup Server

Dezimal	hexa-dezimal	SAP-Beschreibung
780	030c	Intel Netport 2 or HP JetDirect or HP Quicksilver
800	0320	Attachmate Gateway
807	0327	Microsoft Diagnostiocs
808	0328	WATCOM SQL server
821	0335	MultiTech Systems Multi-synch Comm Server
835	0343	Xylogics Remote Access Server or LAN Modem
853	0355	Arcada Backup Exec
858	0358	MSLCD1
865	0361	NETINELO
894	037e	Twelve Novell file servers in the PC3M family
895	037f	Virusafe Notify
902	0386	HP Bridge
903	0387	HP Hub
916	0394	NetWare SAA Gateway
923	039b	Lotus Notes
951	03b7	Certus Anti Virus NLM
964	03c4	ARCserve 4.0 (Cheyenne)
967	03c7	LANspool 3.5 (Intel)
983	03d7	lexmark printer server (type 4033-011)
984	03d8	lexmark XLE printer server (type 4033-301)
990	03de	Gupta Sequel Base Server or NetWare SQL
993	03e1	Univel Unixware
996	03e4	Univel Unixware
1020	03fc	Intel Netport
1021	03fd	Print SErver Queue
1196	04ac	On-Time Scheduler NLM
1034	040A	ipnServer Running on a Novell Server
1037	040D	LVERRMAN Running on a Novell Server
1038	040E	LVLIC Running on a Novell Server
1044	0414	Kyocera

Dezimal	hexa-dezimal	SAP-Beschreibung
1065	0429	Site Lock Virus (Brightworks)
1074	0432	UFHELP R
1075	0433	Synoptics 281x Advanced SNMP Agent
1092	0444	Microsoft NT SNA Server
1096	0448	Oracle
1100	044c	ARCserve 5.01
1111	0457	Canon GP55 Running on a Canon GP55 network printer
1114	045a	QMS Printers
1115	045b	Dell SCSI Array (DSA) Monitor
1169	0491	NetBlazer Modems
1200	04b0	CD-Net (Meridian)
1299	0513	Emulux NOA Something from Emulux
1312	0520	Site Lock Checks
1321	0529	Site Lock Checks (Brightworks)
1325	052d	Citrix OS/2 App Server
1343	0535	Tektronix
1344	0536	Milan
1387	056b	IBM 8235 modem server
1388	056c	Shiva LanRover/E PLUS
1389	056d	Shiva LanRover/T PLUS
1408	0580	McAfee's NetShield anti-virus
1466	05BA	Compatible Systems Routers
	05B8	NLM to workstation communication (Revelation Software)
	0606	JCWatermark Imaging
1569	0621	IBM AntiVirus NLM
1600	0640	Microsoft Gateway Services for NetWare
1614	064e	Microsoft Internet Information Server
1900	076C	Xerox
1947	079b	Shiva LanRover/E 115
1958	079c	Shiva LanRover/T 115

Dezimal	hexa-dezimal	SAP-Beschreibung
1972	07B4	Cubix WorldDesk
	07c2	Quarterdeck IWare Connect V2.x NLM
	07c1	Quarterdeck IWare Connect V3.x NLM
2084	0824	Shiva LanRover Access Switch/E
2154	086a	ISSC collector NLMs
2175	087f	ISSC DAS agent for AIX
2857	0b29	Site Lock
3113	0c29	Site Lock Applications
3116	0c2c	Licensing Server
9088	2380	LAI Site Lock
9100	238c	Meeting Maker
18440	4808	Site Lock Server or Site Lock Metering VAP/NLM
21845	5555	Site Lock User
25362	6312	Tapeware
28416	6f00	Rabbit Gateway (3270)
30467	7703	MODEM??
32770	8002	NetPort Printers (Intel) or LANport
32776	8008	WordPerfect Network Version
34238	85BE	Cisco Enhanced Interior Routing Protocol (EIGRP)
34952	8888	WordPerfect Network Version or Quick Network Management
36864	9000	McAfee's NetShield anti-virus
38404	9604	CSA-NT_MON
46760	b6a8	Ocean Isle Reachout Remote Control
61727	f11f	Site Lock Metering VAP/NLM
61951	f1ff	Site Lock
62723	f503	Microsoft SQL Server
63749	f905	IBM Time and Place/2 application
64507	fbfb	TopCall III fax server
65535	ffff	Any Service or Wildcard

TCP/IP-Ports

Dienst	Port-Nr.	Protokoll
echo	7	tcp
echo	7	udp
discard	9	tcp
discard	9	udp
systat	11	tcp
systat	11	tcp
daytime	13	tcp
daytime	13	udp
netstat	15	tcp
qotd	17	tcp
qotd	17	udp
chargen	19	tcp
chargen	19	udp
ftp-data	20	tcp
ftp	21	tcp
telnet	23	tcp
smtp	25	tcp
time	37	tcp
time	37	udp
rlp	39	udp
name	42	tcp
name	42	udp
whois	43	tcp
domain	53	tcp
domain	53	udp
nameserver	53	tcp
nameserver	53	udp
mtp	57	tcp
bootp	67	udp
tftp	69	udp
rje	77	tcp
finger	79	tcp
www	80	tcp

Dienst	Port-Nr.	Protokoll
www	80	udp
link	87	tcp
supdup	95	tcp
hostnames	101	tcp
iso-tsap	102	tcp
dictionary	103	tcp
x400	103	tcp
x400-snd	104	tcp
csnet-ns	105	tcp
pop	109	tcp
pop2	109	tcp
pop3	110	tcp
portmap	111	tcp
portmap	111	udp
sunrpc	111	tcp
sunrpc	111	udp
auth	113	tcp
sftp	115	tcp
path	117	tcp
uucp-path	117	tcp
nntp	119	tcp
ntp	123	udp
nbname	137	udp
nbdatagram	138	udp
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

Dienst	Port-Nr.	Protokoll
sytek	500	udp
biff	512	udp
exec	512	tcp
login	513	tcp
who	513	udp
shell	514	tcp
syslog	514	udp
printer	515	tcp
talk	517	udp
ntalk	518	udp
efs	520	tcp
route	520	udp
timed	525	udp
tempo	526	tcp
courier	530	tcp
conference	531	tcp
rvd-control	531	udp
netnews	532	tcp
netwall	533	udp
uucp	540	tcp
klogin	543	tcp
kshell	544	tcp
new-rwho	550	udp
remotefs	556	tcp
rmonitor	560	udp
monitor	561	udp
garcon	600	tcp
maitrd	601	tcp
busboy	602	tcp
acctmaster	700	udp
acctslave	701	udp
acct	702	udp
acctlogin	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctslave2	706	udp

Dienst	Port-Nr.	Protokoll
acctdisk	707	udp
kerberos	750	tcp
kerberos	750	udp
kerberos_master	751	tcp
kerberos_master	751	udp
passwd_server	752	udp
userreg_server	753	udp
krb_prop	754	tcp
erlogin	888	tcp
kpop	1109	tcp
phone	1167	udp
ingreslock	1524	tcp
maze	1666	udp
nfs	2049	udp
knetd	2053	tcp
eklogin	2105	tcp
rmt	5555	tcp
mtb	5556	tcp
man	9535	tcp
w	9536	tcp
mantst	9537	tcp
bnews	10000	tcp
rscs0	10000	udp
queue	10001	tcp
rscs1	10001	udp
poker	10002	tcp
rscs2	10002	udp
gateway	10003	tcp
rscs3	10003	udp
remp	10004	tcp
rscs4	10004	udp
rscs5	10005	udp
rscs6	10006	udp
rscs7	10007	udp
rscs8	10008	udp
rscs9	10009	udp
rscsa	10010	udp

Dienst	Port-Nr.	Protokoll
rscsb	10011	udp
qmaster	10012	tcp
qmaster	10012	udp

ELSA LANCOM Business intern

In diesem Kapitel finden Sie Informationen über die internen Funktionen der Router, die bei der täglichen Arbeit mit den ISDN-Routern nicht immer benötigt werden, die Spezialisten in besonderen Situationen jedoch gut unterstützen können.

Script-Verarbeitung

Allgemeines

Einige Internet-Provider (z.B. Compuserve) führen vor einer PPP-Verhandlung einen script-gesteuerten Anmeldevorgang durch. Um auch solche Verbindung aufbauen zu können, wurde im *ELSA LANCOM* eine einfache Scriptverarbeitung implementiert.

Ein Script kann aus den folgenden Elementen bestehen:

Element	Beschreibung
<>	Sende den eingeschlossenen Text mit einem abschließenden Carriage-Return.
[]	Warte auf den Empfang des eingeschlossenen Textes. Dabei wird die Groß- und Kleinschreibung ignoriert. Es genügt die Angabe eines eindeutigen Subtextes.
\$U	Sende den User-Namen (aus der PPP-Tabelle) mit einem abschließenden Carriage-Return.
\$P	Sende das Paßwort (aus der PPP-Tabelle) mit einem abschließenden Carriage-Return.
\$C	Ende des Scripts

Wie bereits aus der Übersicht hervorgeht, werden Username und Paßwort aus der PPP-Tabelle entnommen, wenn sich dort ein passender Eintrag befindet. Gibt es den User-Namen in der PPP-Tabelle nicht, so wird der Gerätenamen der *ELSA LANCOM* als Username übermittelt.

Nach Abschluß des Scripts wird eine PPP-Verhandlung gestartet bzw. der Login-Vorgang abgeschlossen.

Zur Festlegung, ob nach der Script-Bearbeitung eine PPP-Verhandlung gestartet wird, dient der Layer-3-Eintrag in der Layerliste. Es existieren drei mögliche Einträge:

SCPPP	Nach Abschluß der Scriptverarbeitung wird eine synchrone PPP-Verhandlung gestartet.
SCAPP	Nach Abschluß der Scriptverarbeitung wird eine asynchrone PPP-Verhandlung gestartet.
SCTrans	Nach Abschluß der Scriptverarbeitung besteht die logische Verbindung zur Gegenstelle. Es erfolgt keine weitere Protokollverhandlung.

Die Script-Liste

Scripte werden in einer dafür vorgesehenen Tabelle der Script-Liste eingegeben. Diese Tabelle befindet sich unter /Setup/WAN-Modul und hat den folgenden Aufbau:

Gerätename	Script
CSERVE	<>[Host]<CIS>[User]\$U[Password]\$P[PPP]\$C

Die Einträge in der Script-Liste haben die folgende Bedeutung:

Gerätename:	Name der logischen Gegenstelle
Script:	Alle auszuführenden Befehle – Maximal 58 Zeichen stehen pro Zeile zur Verfügung. Sollte die notwendige Befehlsfolge länger sein, so kann ähnlich wie in der Round-Robin-Liste ein weiterer Eintrag für die logische Gegenstelle hinzugefügt werden. Die Syntax hierfür ist: Gerätename gefolgt von '#' und einer Zahl. Die Einträge werden von oben nach unten abgearbeitet.

Beispiel:

Gerätename	Script
CSERVE#1	<>[Host]<CIS>[User]
CSERVE#2	\$U[Password]\$P[PPP]\$C

Im *ELSA LANconfig* ist die Script-Liste auf der Registerkarte 'Kommunikation' zu finden.

Compuserve-Anwahl

Im folgenden werden an einem Beispiel die nötigen Einstellungen für die Anwahl an das Compuserve-Netzwerk über X.75, asynchrones PPP und Script-Steuerung vorgestellt.

Layerliste:

Layername	Encaps.	Lay-1	Lay-2	L2-Opt.	Lay-3
CSERVE	TRANS	SCAPPP	X.75LAPB	keine	HDLC64K

Namenliste:

Gerätename	Rufnummer	B1-HZ	B2-HZ	Layername	Rückruf
CSERVE	0021194260	60	60	CSERVE	Aus

PPP-Liste:

Gerätename	Authent.	Paßwort	Zeit	Wdh.	Username
CSERVE	keine	*	0	0	xxxxxx,xxxx/PPP:CISPPP

Für xxxxxx,xxxx ist der Compuserve-Account einzutragen.

Script-Liste:

Gerätename	Script
CSERVE	<>[Host]<CIS>[User]\$U[Passwort]\$P[PPP]\$C

Wobei die Elemente des Scripts folgende Bedeutung haben:

Element	Bedeutung
<>	Starte Script auf der Gegenstelle durch senden von Carriage-Return.
[Host]	Warte auf die Antwort vom Compuserve-Einwahlknoten. In der Antwort taucht irgendwann 'Host Name' auf.
<CIS>	Sende 'CIS' gefolgt von Carriage-Return.
[User]	Warte auf die Antwort. Compuserve fragt nach der 'User ID'.
\$U	Sende den Usernamen. Bei Compuserve besteht dieser aus der Compuserve-User-ID mit angehängtem '/PPP:CISPPP'. Der Username wird aus der PPP-Tabelle geholt und mit einem abschließenden Carriage-Return an die Gegenstelle gesendet.
[Password]	Warte auf die Abfrage des Paßworts.
\$P	Sende das Paßwort mit einem abschließenden Carriage-Return. Das Paßwort wird aus der PPP-Tabelle geholt.
[PPP]	Warte auf die Connect-Meldung der Gegenstelle.
\$C	Das Script ist vollständig bearbeitet. Es wird die in der Layerliste eingestellte asynchrone PPP-Verhandlung (SCAPP) gestartet.

Online-Trace-Ausgaben

Allgemeines

Durch sogenannte 'Online-Trace-Ausgaben' (Kontrollausgaben) kann der Anwender Informationen über interne Vorgänge der arbeitenden *ELSA LANCOM* erhalten. Mit Hilfe solcher Informationen können Fehlkonfigurationen, sowohl vom *ELSA LANCOM* als auch von anderen mit einem *ELSA LANCOM* verbundenen Geräten, einfach und sicher aufgespürt werden.

Die Online-Trace-Ausgaben können dabei flexibel für einzelne Protokolle bzw. Funktionen innerhalb der Firmware und einzelne Konfigurations-Sitzungen verwaltet werden.

Durch sitzungsbezogene „Trace-Profile“ werden jeweils nur die innerhalb einer Sitzung aktivierten Trace-Informationen angezeigt.

Die Steuerung der Online Trace-Ausgaben erfolgt über ein neu implementiertes Kommando der Remote-Konfiguration, welches vom Kommando-Interpreter ausgewertet wird und dem Benutzer eine direkte Rückmeldung der vorgenommenen Einstellungen gibt. Änderungen dieser Einstellungen werden sofort wirksam und erzeugen bzw. unterdrücken direkt die entsprechenden Ausgaben.

Die Anzeige der Online-Trace-Ausgaben erfolgt dabei zeitverzögert zum eigentlichen Ereignis durch die Remote-Konfiguration. Der optional anzuzeigende Zeitstempel spiegelt dabei den Zeitpunkt der Ausgabe, nicht jedoch den Zeitpunkt des tatsächlichen Ereignisses wieder. Im Regelfall differieren diese Zeiten nicht wesentlich, bei einer Analyse der Ausgaben sollte dieser Punkt dennoch immer berücksichtigt werden.

Alle Anzeigen innerhalb der Online-Trace-Ausgaben erfolgen soweit möglich im Klartext. Da die Analyse von Netzwerkprotokollen nicht vollständig auf die Darstellung von numerischen Parametern verzichten kann und ein Trace-System nur dann sinnvoll anwendbar ist, wenn die angezeigte Information auch verstanden wird, werden im folgenden für alle Protokolle und Funktionen genaue Beschreibungen der Trace-Informationen nachgereicht.

Sind Anzeigen für ein Protokoll aktiviert, so überschreibt die nächste Ausgabe den aktuellen System-Prompt; jeder weiteren Ausgabe wird ein <Return> <LineFeed> vorangestellt. Betätigt der Anwender eine Taste, wird die gesamte gepufferte Eingabe zusammen mit dem aktuellen System-Prompt erneut dargestellt. Der Anwender erhält so einen visuellen Feedback und Eingaben müssen nicht „blind“ vorgenommen werden.

Bedienung der Trace-Ausgaben

Die Bedienung der Trace-Ausgaben erfolgt in gewohnter Weise kommandozeilenorientiert. Dazu wurde die Remote-Konfiguration um den Befehl `trace` erweitert; dieser besitzt folgende Befehlsyntax:

<code>trace [Schlüssel] [Parameter] ...[Parameter]</code>	zeigt, oder beeinflusst den Zustand der Trace-Ausgaben einzelner Protokolle oder Funktionen.
Schlüssel	<ul style="list-style-type: none"> <code>?</code> Anzeige einer Hilfeseite <code>+</code> Einschalten der Trace-Ausgaben <code>-</code> Ausschalten der Trace-Ausgaben <code>#</code> Umschalten der Trace-Ausgaben (toggle) (kein) Anzeige des Zustands
Parameter	symbolischer Name des Protokoll bzw. der Funktion.

Schlüssel und Parameter sind durch Leerzeichen voneinander zu trennen. Die Schlüssel werden vom Kommando-Interpreter nur erkannt, wenn sie eindeutig sind, d.h., sie bestehen aus einem der oben aufgeführten Zeichen ohne Prä- oder Suffix. Für die Eingabe der

symbolischen Namen von Protokollen oder Funktionen genügt wie üblich die Eingabe eines eindeutigen Präfixes.

Es können in einer Kommandozeile beliebig viele Schlüssel und Parameter angegeben werden, maßgebend als Obergrenze ist lediglich die Größe des Zeileneingabepuffers. Die Parameter werden entsprechend dem letzten vorhergehenden Schlüssel bearbeitet. Ist vor Parametern kein Schlüssel angegeben, so wird der Zustand der jeweiligen Trace-Funktion (ON oder OFF) ausgegeben.

Zu beachten ist außerdem, daß die Kommandozeile von links nach rechts abgearbeitet wird. So kann die Trace-Ausgabe eines Parameters durchaus innerhalb einer Zeile mehrfach ein- und ausgeschaltet werden, da die Umschaltung während des Einlesens der Token aus dem Eingabepuffer erfolgt (siehe auch Beispiele).

Zusätzlich zur Aktivierung von Online-Trace-Ausgaben kann über die Schlüsselwörter „Time“ und „Source“ die vorangestellte Ausgabe der Systemzeit und des Protokoll-Namens ein- bzw. ausgeschaltet werden. Ohne diese beiden Anzeigen wird jede Trace-Ausgabe um 21 Zeichen verkürzt.

Beispiele zur Bedienung der Trace-Ausgaben

Die folgende Tabelle soll einige praktische Beispiele aufzeigen, wie das Kommando für die Trace-Ausgaben genutzt werden kann:

Eingabe	Wirkung
trace	Ausgabe aller Protokolle, die in der Konfigurationssitzung Trace-Ausgaben erzeugen können, und des Zustandes der Ausgaben (ON, OFF).
trace + all	schaltet alle Trace-Ausgaben in der jeweiligen Sitzung ein.
trace + protocol display	schaltet alle Verbindungs-Aufbauprotokolle und die Anzeige der Display-Ausgaben ein.
trace + all - icmp	schaltet alle Trace-Ausgaben ein, jedoch Ausgaben des ICMP-Protokolls aus.
trace ppp els	zeigt den Zustand der PPP- und ELSA Trace-Ausgaben an.
trace # ipx-rt display	schaltet die Trace-Ausgaben des IPX-Routers und der Display-Ausgaben um.
trace - time	schaltet die Angabe der Betriebszeit vor der eigentlichen Ausgabe aus.

Unterstützte Protokolle und Funktionen

Folgende symbolische Namen für Protokoll-Stacks werden unterstützt:

Status	Anzeige von Status-Meldungen über Verbindungen
Error	Anzeige von Fehlermeldungen über Verbindungen
PPP	Anzeige der PPP-Verhandlungen

SCRPT	Anzeige der Script-Verhandlung
IPX-Rt.	Anzeige des IPX-Routings
RIP	Anzeige des IPX Routing Information Protocols
SAP	Anzeige des IPX Service Advertising Protocols
IPX-Wd.	Anzeige des IPX Watchdog-Spoofings
SPX-Wd.	Anzeige des SPX Watchdog-Spoofings
NetBIOS	Anzeige der IPX NetBIOS-Verwaltung
IP-Rt.	Anzeige des IP-Routings
IP-RIP	Anzeige des IP Routing Information Protocols
ICMP	Anzeige des Internet Control Message Protocols
IP-MASQ	Anzeige der Vorgänge im Masquerading Modul
ARP	Anzeige des Address Resolution Protocols
DHCP	Anzeige des Dynamic Host Configuration Protocols (nur LANCOM Office-Router)
Paket-Dump	Anzeige der ersten 64 Bytes eines Pakets in Hexadezimal-Darstellung (nur LANCOM Office-Router)

Außer diesen Parametern existieren noch folgende „Sammelparameter“ (das sind Parameter für eine bestimmte Protokoll-Art), mit deren Hilfe die Online Trace-Ausgaben für eine komplette, logisch zusammenhängende, Protokoll-Familie aktiviert bzw. deaktiviert werden können:

All	Anzeige aller Online Trace-Ausgaben
Display	Anzeige von 'Status' und 'Error'
Protocol	Anzeige von 'ELSA' und 'PPP' und 'SCRPT'
TCP-IP	Anzeige von 'IP-Rt.', 'IP-RIP', 'ICMP', 'ARP' und 'IP-MASQ'
IPX-SPX	Anzeige von 'IPX-Rt.', 'RIP', 'SAP', 'IPX-Wd.', 'SPX-Wd.' und 'NetBIOS'

Schließlich werden noch weitere Parameter erkannt, über welche das Darstellungsformat der Trace-Ausgaben beeinflusst werden kann:

Time	Anzeige der Systemzeit als Präfix
Source	Anzeige des erzeugenden Protokolls als Präfix

Durch Abschalten der Präfix-Ausgaben 'Time' und 'Source' wird jede Trace-Ausgabe um 21 Zeichen verkürzt. Standardmäßig ist die Ausgabe der Präfixe aktiviert.

Präfix-Ausgabe 'Time'

Durch Aktivierung der Präfix-Ausgabe 'Time' wird jeder Trace-Ausgabe die Systemzeit (zum Zeitpunkt der Erzeugung der Ausgabe!) in folgender Form vorangestellt:

- Format: [Tage]t; _[Stunden]:[Minuten]:[Sekunden]_

- Beispiel:

```
12t; 07:23:15
```

entspricht der Systemzeit von 12 Tagen, 7 Stunden, 23 Minuten und 15 Sekunden.

Präfix-Ausgabe 'Source'

Durch Aktivierung der Präfix-Ausgabe 'Source' wird jeder Trace-Ausgabe der symbolische Name des Protokolls vorangestellt, welches diese Trace-Ausgabe verursacht hat. Die Anzeige erfolgt dabei immer 9stellig (wenn notwendig durch Auffüllen von Leerzeichen).

- Beispiel: ICMP

d.h. die folgende Trace-Ausgabe wurde vom ICMP-Protokoll verursacht.

Online-Trace 'Status'

Die Ausgaben unter 'Status' beschreiben Zustandsänderungen auf einem WAN-Interface (momentan nur der interne S₀-Anschluß). Sie werden in folgendem Format angezeigt:

- Format: [Interface] [Zustand]

- Beispiel:

```
Ch01: Anwahl 8700
```

Auf dem ersten B-Kanal des internen S₀-Anschlusses wird die Rufnummer 8700 angewählt.

Online-Trace 'Error'

Die Ausgaben unter 'Error' beschreiben Fehler, die auf einem WAN-Interface aufgetreten sind. Sie werden in folgendem Format angezeigt:

- Format: [Interface] [Fehler]

- Beispiel:

```
Ch01: Keine Antwort
```

Die angewählte Gegenstelle hat auf den Ruf nicht reagiert.

Online-Trace 'PPP'

Das Point-to-Point-Protocol besteht aus einer Sammlung von Subprotokollen, von denen der *ELSA LANCOM* folgende erkennt und verwaltet:

LCP	Das Link-Control-Protocol
PAP	Das Password Authentication Protocol
CHAP	Das Challenge Handshake Protocol
IPXCP	Das IPX Control Protocol
IPCP	Das IP Protocol

Diese Subprotokolle des PPPs werden gezielt in einzelnen Phasen während einer Protokollverhandlung angesprochen. Innerhalb der ESTABLISH-Phase wird das Link-Control-Protocol ausgehandelt; zu diesem Zeitpunkt sind nur LCP-Pakete innerhalb des PPP zulässig. Wurde durch das LCP eine Authentifizierung ausgehandelt, geht PPP in die AUTHENTICATE-Phase über; ab diesem Zeitpunkt dürfen LCP-, PAP- und CHAP-Pakete übertragen werden. Nach Abschluß der (optionalen) Authentifizierung wechselt PPP in die NETWORK-Phase; ab sofort dürfen LCP-, Authentifizierungs- und Network-Control-Protocol-Pakete (wie IPXCP und IPCP) beliebig gemischt übertragen werden. Zum Abbau einer PPP-Verbindung wird in die TERMINATE-Phase gewechselt, in der wieder nur LCP-Pakete zulässig sind. Nach Abbau der Verbindung befindet sich PPP in der DEAD-Phase, aus der es nur durch einen erneuten Verbindungsaufbau in die ESTABLISH-Phase übergeht. Jeder Phasenwechsel des PPPs wird in der Form

```
Change Phase to [Neue Phase]
```

etwa wie folgt angezeigt:

```
Change Phase to AUTHENTICAT
```

Für alle oben aufgeführten Subprotokolle des PPP werden empfangene und gesendete Pakete, wichtige Parameter und Optionen sowie durchgeführte Aktionen angezeigt. Ein empfangener Frame wird immer in folgendem Format angezeigt:

- Format: [Interface] Rx [Protokoll] [Pakettyp] [Pakettyp] [Länge des Pakets]

- Beispiel:

```
Ch01: Rx IPXCP ConfReq ID=00 Length=22
```

In obigem Beispiel wurde also auf dem ersten B-Kanal ein Configure-Request für das IPX Control Protocol mit der ID '00' und einer Länge von 22 Byte empfangen. Kann ein Paket keinem der fünf Subprotokolle zugeordnet werden, erscheint die Meldung:

- Format: [Interface] Rx Unknown Protocol [Protokoll-ID]

- Beispiel:

```
Ch01: Rx Unknown Protocol 8029
```

Ein Paket mit der Protokoll-ID 8029 (= Appletalk Control Protocol) wurde empfangen.

Online-Trace 'IPX-Rt.'

Die Ausgaben unter 'IPX-Rt.' beschreiben die Verarbeitung von IPX-Frames durch den IPX-Router. Sie werden in folgendem Format angezeigt:

- Format: [Quell-Interface] [IPX-Ziel-Adresse] [IPX-Quell-Adresse] [Ziel/Aktion]
- Beispiel:

Intern-Rx

DstAddr: 00000002 ffffffff 0453

SrcAddr: 00000002 00a057123456 0453

WAN-Tx Peer: ELSA.SUP.TEST

Der IPX-Router hat von einem internen Prozeß (hier von der Instanz des Routing-Information-Protokolls) einen Frame empfangen, dessen Ziel-Adresse einer logischen Gegenstellen (ELSA.SUP.TEST) zugeordnet ist und daher auf ein WAN-Interface gesendet wird.

LAN-Rx

DstAddr: 00000001 ffffffff 0455

SrcAddr: 00000001 0123456789ab 0455

Filter

Der IPX-Router hat vom lokalen Netzwerk einen NetBIOS-Frame (IPX-Socket 455) empfangen, der als Broadcast ffffffff an alle Stationen im Netz 00000001 weitergeleitet werden soll. Da auf den Socket ein Filter gelegt wurde, wird der Frame vom Router verworfen.

Online-Trace 'RIP'

Die Ausgaben unter 'RIP' beschreiben die Verarbeitung von IPX RIP-Frames durch den RIP-Prozeß des IPX-Routers. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format

- Format: [Quell-Interface] [Receive/Transmitt/Aktion] [Quell-Node-Adresse] [Frame-typ] [Parameter] [Netzwerkadresse] [Hops] [Tics] [Aktion] ... [Netzwerkadresse] [Hops] [Tics] [Aktion]

- Beispiel:

LAN-Rx Node: 0000c0123456 Req: 00000002

Vom lokalen Netzwerk wurde ein RIP-Request für das IPX-Netzwerk 00000002 empfangen. Der RIP-Request wurde vom IPX-Node 0000c0123456 gesendet.

- Beispiel:

LAN-Rx Node: 00a057123456 Resp

Route: 00000002 Hops: 0001 Tics: 0002 Up

Vom lokalen Netzwerk (erzeugt vom IPX-Node 00a057123456) wurde ein RIP-Response empfangen. Durch diesen Response wird die Route 00000002, mit einer Hop-Distanz (Anzahl der Zwischenstationen) von 1 und einer Tic-Distanz von 2 als weiterhin verfügbar in der RIP-Tabelle eingetragen.

LAN-Update

Der RIP-Prozeß sendet alle notwendigen Routing-Informationen auf das lokale Netzwerk.

Online-Trace 'SAP'

Die Ausgaben unter 'SAP' beschreiben die Verarbeitung von IPX-SAP-Frames durch den SAP-Prozeß des IPX-Routers. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format:

- Format: [Quell-Interface] [Receive/Transmitt/Aktion] [Quell-Node-Adresse] [Frame-typ] [Parameter] [Service-Typ] [Server-Name] [Aktion] ... [Service-Typ] [Server-Name] [Aktion]
- Beispiel:

```
LAN-Rx Node: 00a057123456 Response
```

```
0004 FS_Entwicklung Up
```

```
0107 FS_Entwicklung Up
```

```
023f FS_Entwicklung Up
```

```
0511 FS_Entwicklung Up Change
```

```
030c 08000912345678CGNP-Entwicklung Filtered
```

Vom lokalen Netzwerk wurde ein SAP-Response empfangen (ausgesendet vom IPX-Node 00a057123456). Durch diesen Response werden die Server 'FS_Entwicklung' (File-Server), 'FS_Entwicklung' (NetWare-386-Server), 'FS_Entwicklung' (DNS-Server) und 'FS_Entwicklung' (Time-Sync-Server) als weiterhin verfügbar in die SAP-Tabelle aufgenommen. Dabei hat sich der Zustand des Time-Sync-Servers 'FS_Entwicklung' innerhalb der SAP-Tabelle geändert (d.h., der Server war vorher nicht verfügbar). Der letzte angezeigte Server ist ein Printer-Server; da dieser Server-Typ mit einem SAP-Filter belegt ist, wird er nicht in die SAP-Tabelle aufgenommen, sondern verworfen.

LAN-Trigger

Durch einen empfangenen SAP-Response ist eine Zustandsänderung innerhalb der SAP-Tabelle aufgetreten, die vom SAP-Prozeß unmittelbar ins lokale Netzwerk gemeldet wird; die Änderung kann also nur durch die Auswertung eines SAP-Responses vom WAN eingetreten sein.

LAN-Age

Der SAP-Prozeß des Routers „altert“ alle vom lokalen Netzwerk ermittelten Server/ Services im Minutentakt. Nach einer einstellbaren Zeit wird ein SAP-Eintrag gelöscht (Setup/IPX-Modul/SAP-Einstellungen/Aging-Minuten).

Online-Trace 'IPX-Watchdogs'

Die Ausgaben unter 'IPX-Watchdogs' beschreiben die Verarbeitung sogenannter „IPX-Watchdog“-Pakete. Dies sind Pakete, welche in regelmäßigen Abständen von einem Novell-Server zu einer Workstation gesendet werden, um die Verbindung zu dieser Workstation zu verifizieren. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format:

- Format: [Quell-Interface] [Receive/Transmitt] [Quell-Adresse] [Ziel-Adresse] [Aktion]
- Beispiel:

LAN-Rx

DstAddr: 12345678 00a057654321 0451

SrcAddr: 00000002 00a057123456 0451

Spoof

Der *ELSA LANCOM* hat vom Node 00a057123456 einen IPX-Watchdog empfangen, der zur Überprüfung einer entfernten Workstation gedacht war. Da das entfernte Netzwerk, in welchem sich die Workstation befindet, aktiv ist, wird der IPX-Watchdog vom *ELSA LANCOM* lokal beantwortet, um einen unnötigen Verbindungsaufbau zu vermeiden. Alternativ können noch folgende Anzeigen für Aktionen erscheinen:

- **Route:** Der IPX-Watchdog wird weitergeleitet (Verbindungsaufbau).
- **Filter:** Der IPX-Watchdog wird verworfen und nicht beantwortet.
- **Dst Net DOWN Error:** Das Zielnetz des IPX-Watchdogs ist nicht verfügbar.

Online-Trace 'SPX-Watchdogs'

Analog zu den Trace-Ausgaben für IPX-Watchdogs wird durch die Ausgaben unter 'SPX-Watchdogs' die Verarbeitung von SPX-Watchdog-Paketen beschrieben. Dies sind Pakete, die von einem Novell-Server zur Überprüfung einer SPX-Verbindung (z.B. R-Console) in regelmäßigen Abständen zur beteiligten Workstation gesendet werden. Die Anzeige der Trace-Ausgaben geschieht in folgender Weise:

- Format: [Quell-Interface] [Receive/Transmitt] [Quell-Adresse] [Ziel-Adresse] [Aktion]
- also völlig analog zu den Anzeigen der IPX-Watchdog-Pakete.

Online-Trace 'IPX-NetBIOS'

Die Ausgaben unter NetBIOS beschreiben die Verarbeitung von IPX-NetBIOS- und IPX-Propagated-Paketen. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format

- Format: [Quell-Interface] [Receive/Transmitt] [Quell-Adresse] [Ziel-Adresse] [Aktion]
- Beispiel:

```

LAN-Rx
DstAddr: 12345678 00a057654321 0455
SrcAddr: 00000002 00a057123456 0455
Route

```

Online-Trace 'IP-Rt.'

Die Ausgaben unter 'IP-Rt.' beschreiben die Verarbeitung von IP-Frames durch den IP-Router. Sie werden in folgendem Format angezeigt:

- Format: [Quell-Interface] [IP-Ziel-Adresse] [IP-Quell-Adresse] [Protokoll] [Ziel-Port] [Quell-Port] [Type of Service] [Aktion] [Ziel]
- Beispiel:

```

LAN-Rx
DstIP: 195.162.38.161, SrcIP: 194.162.38.162
Prot.: TCP, DstPort: 23, SrcPort: 1197, TOS: ----
Route: WAN-Tx Peer: R1

```

Der IP-Router hat vom Rechner mit der IP-Adresse 194.162.38.162 ein TCP-Paket erhalten, das an den Rechner 195.162.38.161 gesendet werden soll.

Der Quell-Port ist 1197, der Ziel-Port 23 (Telnet), es ist kein Bit im TOS gesetzt. Das Feld TOS kann die folgenden Werte (bzw. Eine Kombination hiervon) annehmen:

D---	Low Delay
-T--	High Troughput
--R-	High Reliability
---C	Low Costs

Das Paket wird geroutet und der Zielrechner ist unter der logischen Gegenstelle **R1** erreichbar. Daher wird das Paket auf ein WAN-Interface gesendet.

```

LAN-Rx
DstIP: 195.162.38.161, SrcIP: 194.162.38.162
Prot.: ICMP, DstPort: ---, SrcPort: ---, TOS: --R-
Route: WAN-Tx Peer: R1

```

Der IP-Router hat vom Rechner mit der IP-Adresse 194.162.38.162 ein ICMP-Paket erhalten, das an den Rechner 195.162.38.161 gesendet werden soll.

Da ICMP keine Ports kennt, wird als Ziel- bzw. Quell-Port --- ausgegeben. Im TOS ist das Feld **High Reliability** gesetzt.

Online-Trace 'IP-RIP'

Die Ausgaben unter 'IP-RIP' beschreiben die Verarbeitung von IP-RIP-Frames durch den RIP-Prozeß des IP-Routers. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format:

- Format: [Quell-Interface] [Receive/Transmitt/Aktion] [Quell-Adresse] [RIP-Version] [Routing-Domain] [Netzwerk-Adresse] [Netzmaske] [Beste Route] [Distanz] [Aktion] ... [Netzwerk-Adresse] [Netzmaske] [Beste Route] [Distanz] [Aktion]

- Beispiel:

```
LAN-Rx Src: 194.162.38.252
Vers.: RIP-1      Routg.Dom.: 0000
190.254.0.0255.255.0.0194.162.38.1623Store
195.126.38.0255.255.255.0194.162.38.1623update
255.255.255.2550.0.0.0194.162.38.1622Discard
194.162.38.0255.255.255.0194.162.38.1622Discard
```

Vom lokalen Netz wurde ein RIP-1-Frame empfangen. Dieser Frame enthält die Routen zu den Netzen 190.254.0.0, 195.126.38.0, 255.255.255.255 (DEFAULT-Route) und 194.162.38.0. Mit diesen Routen wurde wie folgt verfahren:

Die Route 190.254.0.0 wird gespeichert, da sie entweder besser als die bisherige oder noch unbekannt ist.

Die Route 195.126.38.0 wird überarbeitet, d.h., die Route ist unverändert, nur die Distanz kann sich geändert haben. In jedem Fall wird der Aging-Timer zurückgesetzt.

Die DEFAULT-Route wurde verworfen, da eine bessere Route bekannt ist.

Die Route zum Netz 194.162.38.0 wird verworfen, da es sich um eine Route zum lokalen Netz handelt (Split Horizon).

Die Trace-Ausgabe empfangener RIP-Frames erfolgt immer, nachdem sie vom RIP-Prozess ausgewertet und dadurch Netzmasken (RIP-1) sowie beste Route bestimmt wurden. Bei gesendeten RIP-Frames werden die Pakete so angezeigt, wie sie gesendet wurden. Dies bedeutet, daß z.B. bei RIP-1-Frames die Netzmaske immer als 0.0.0.0 ausgegeben wird.

Online-Trace 'ARP'

Die Ausgaben unter 'ARP' beschreiben die Verarbeitung Adress-Resolution-Protocol-Frames durch das TCP-IP-Modul. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format:

- Format: [Quell-Interface] [Receive/Transmitt/Aktion] [Quell-Adresse] [Ziel-Adresse] [Ziel/Aktion]

- Beispiel:

```
LAN-Rx Request
```

SrcIP: 194.162.38.162, DstIP: 194.162.38.171

Cache-Update: 194.162.38.162 : 0000c0717860

Response LAN-Tx

Es wurde ein ARP-Request für die IP-Adresse 194.162.38.171 vom Rechner 194.162.38.162 empfangen. Die MAC-Adresse des Quell-Rechners wird in der ARP-Tabelle gespeichert. Weiterhin ist der *ELSA LANCOM* der nachgefragte Rechner. Daher wird ein ARP-Response auf das LAN-Interface zurückgeschickt.

Online-Trace 'ICMP'

Die Ausgaben unter 'ICMP' beschreiben die Verarbeitung Internet-Control-Message-Protocol-Frames durch das TCP-IP-Modul. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format:

- Format [Quell-/Ziel-Interface] [Receive/Transmitt] [Quell-/Ziel-Adresse] [Message] [Aktion]

- Beispiel:

LAN-Rx

SrcIP: 194.162.38.162: Echo Request

LAN-Tx

DstIP: 194.162.38.162: Echo Reply

Auf dem LAN-Interface wurde ein ICMP Echo-Request (**ping**) vom Rechner 194.162.38.162 empfangen. Der *ELSA LANCOM* beantwortet dies mit einem ICMP-Echo-Reply.

Online-Trace 'IP-MASQ'

Die Ausgaben unter 'IP-MASQ' beschreiben die Vorgänge im Masquerading-Modul. Es wird das Öffnen sowie das Schließen einer maskierten Verbindung ausgegeben. Die Anzeige erfolgt in folgendem Format:

- Format: [Open/Close]: [Protokoll] [IP-Quelladresse] [Quell-Port] [Mapped-Port] [Grund]

Als Protokoll kommt TCP, UDP oder ICMP in Frage. Wenn das Protokoll ICMP ist, so gibt der Quell-Port den Identifier des Request-Pakets an. Das Feld Mapped-Port gibt an, wie

der Quell-Port ersetzt wurde. Im Feld 'Grund' wird die Ursache eines Close angegeben. Mögliche Gründe sind:

Timeout	Der eingestellte Protokoll-Timeout ist abgelaufen.
TCP finish	Eine TCP-Verbindung wurde normal beendet.
TCP reset	Eine TCP-Verbindung wurde aufgrund eines Fehlers von einer der beteiligten Maschinen abgebrochen.
Port assigned	Einer „passiven“ TCP-Verbindung wurde ein Quell-Port zugewiesen. Beispiel: FTP im passive Mode.

■ Beispiele:

```
Open: TCP SrcIP: 10.0.0.44, 1121 -> 64107
Open: TCP SrcIP: 10.0.0.44, 1122 -> 64104
Open: TCP SrcIP: 10.0.0.44, 1123 -> 64105
Close: TCP SrcIP: 10.0.0.44, 1121 -> 64107 TCP reset
```

Online-Trace 'SCRPT'

Die Ausgaben unter „SCRPT“ beschreiben den Fortschritt einer Script-Verhandlung. Die Ausgaben erfolgen in folgendem Format:

■ Format: [Quell-Interface] [Receive/Transmit/Error] [Text] [Aktion]

■ Beispiel:

```
CH01: Rx: Password -> Tx: * \r
```

In obigem Beispiel wird von der Gegenstelle das Paßwort erfragt. Dieses wird an die Gegenstelle zurückgeschickt, verborgen unter einem '*’.

Online-Trace 'DHCP'

Die Ausgaben unter 'DHCP' beschreiben die Vorgänge im Dynamic Host Configuration Protocol. Dabei werden die Anfragen von DHCP-Clients und die entsprechende Antwort des DHCP-Servers im *ELSA LANCOM* angezeigt. Die Anzeige erfolgt in folgendem Format:

■ Format: [DHCP Client Message] [DHCP Server Message]

Online-Trace 'Paket-Dump'

Der Online-Trace 'Paket-Dump' ergänzt die Trace-Ausgaben, die z.B. vom IP-Router erzeugt werden. Dabei werden die ersten 64 Bytes eines Pakets in hexadezimaler Darstellung ausgegeben.

Policy Based Routing

Allgemeines

Der Begriff „Policy Based Routing“ beschreibt die Möglichkeit, zusätzlich zum Standard-Routing-Verfahren für IP-Pakete, weitere Routing-Methoden (eben diese „Policies“) zu verwenden.

Um die Inband-Konfiguration über Weitverkehrsnetzwerke bei starker Datenübertragung zu erleichtern und die Zusammenarbeit vom *ELSA LANCOM* mit 'ping' und 'traceroute'-Mechanismen zu verbessern, wurden zwei Methoden für das IP-Routing eingeführt. Beide Methoden setzen auf der Auswertung des Feldes 'Type of Service' innerhalb des IP-Headers auf.

Das Feld 'Type of Service' (kurz TOS) beschreibt, wie IP-Pakete vorzugsweise behandelt werden sollen (aber nicht müssen). D.h., es spiegelt die gewünschte Verarbeitungsweise wieder, die der Erzeuger diesem IP-Paket zugedacht hat. TOS besitzt dabei folgenden Aufbau:

Bit 7, 6	Bit 5	Bit 4	Bit 3	Bit 2, 1, 0
Unbenutzt	Reliable-Transmission	High-Throughput	Low-Delay	Precedence

Durch die Routing-Methoden werden das **R**- und das **D**-Bit ausgewertet und das Verhalten an deren Zustände angepaßt.

Ein gesetztes **R**-Bit fordert eine gesicherte Übertragung des zugehörigen IP-Pakets an. Derart gekennzeichnete Pakete werden entsprechend ihrer Empfangsreihenfolge über eine „gesicherte“ Queue immer übertragen. Im Extremfall kann dies dazu führen, daß ein bereits in einer Sende-Queue befindliches „normales“ Paket wieder aus dieser entnommen und in den Heap zurückgestellt wird, um Platz für das zu sendende Paket zu schaffen. Dies geschieht, wenn die maximale Anzahl an Pufferspeichern für die zugehörige Verbindung bereits verbraucht ist. Die Übertragungsreihenfolge zwischen Paketen mit gesetztem **R**-Bit und „normalen“ Bits wird durch diesen Mechanismus jedoch nicht verändert.

Die gesicherte Übertragung kann für alle ICMP-Pakete unabhängig vom Eintrag im TOS-Feld aktiviert werden. Da ein derart gekennzeichnetes ICMP-Paket ohne Änderung der Übertragungsreihenfolge gesendet wird, können weiterhin durch 'ping' oder 'traceroute' die Durchlaufverzögerungen der *ELSA LANCOM* ermittelt werden.

Durch ein gesetztes **D**-Bit fordert der Erzeuger eines IP-Pakets dessen schnellstmögliche Übermittlung an. Derart gekennzeichnete IP-Pakete werden entsprechend ihrer Empfangsreihenfolge über eine Urgent-Queue vor den Paketen der Sende-Queue übertragen. Dies führt zum einen zu Veränderungen in der Übertragungsreihenfolge, da ein so gekennzeichnetes IP-Paket als letztes empfangen aber als erstes gesendet wird. Zum anderen besteht ebenfalls die Möglichkeit, daß ein bereits in der Sende-Queue befindli-

ches Paket wieder aus dieser entnommen wird, um Platz für das zu sendende IP-Paket zu schaffen (s.o.).

Pakete, die sich bereits in der gesicherten oder der Urgent-Queue befinden, werden nicht verworfen. Befindet sich kein Paket mehr in der normalen Sende-, der gesicherten oder der Urgent-Queue, können keine Pakete mehr gesendet werden. Empfangene IP-Pakete werden daher auch mit gesetztem **D**- oder **R**-Bit verworfen.

Beispiele

Durch die Einstellung

`Setup/IP-Router-Modul/Routing-Methode/IP TOS`

wird das TOS-Feld des IP-Headers eines empfangenen Pakets wie oben beschrieben ausgewertet, d.h., daß IP-Pakete mit gesetztem **D**-Bit in die Urgent-Queue und Pakete mit gesetztem **R**-Bit in die gesicherte Queue gestellt werden. Alle anderen Pakete werden in der normalen Sende-Queue abgelegt.

Dies bedeutet gleichzeitig, daß evtl. „normale“ IP-Pakete von „gesicherten“ oder „Urgent“-Paketen verdrängt werden können (bei maximaler Füllung der Sende-Queue dieser Verbindung) oder es zu Veränderungen in Paketreihenfolgen kommen kann!

Durch die Einstellung 'normal' werden alle IP-Pakete gleich behandelt, entsprechend den Routing-Vorschriften des Internet-Protocols.

Durch die Einstellung

`Setup/IP-Router-Modul/Routing-Methode/ICMP gesichert`

werden alle empfangenen ICMP-Pakete so übertragen, als hätten sie das **R**-Bit im TOS-Feld des IP-Headers gesetzt. (s.o.).

Das bedeutet, daß die gesicherte Übertragung von ICMP-Paketen evtl. zu Störungen in anderen Datenflüssen führen kann! Die Latenzzeit des Routers wird jedoch nicht beeinflusst, da das ICMP-Paket trotzdem als letztes in die Sende-Queue aufgenommen wird.

Durch die Einstellung 'normal' werden ICMP-Pakete wie alle anderen IP-Pakete behandelt, entsprechend den Routing-Vorschriften des Internet-Protocols.

