

Inhalt

Benutzer-Handbuch

Einleitung	Kap. 1.1
Das <i>LANCOM</i> stellt sich vor	Kap. 2.1
Konfigurationsmöglichkeiten	Kap. 3.1
<i>LANCOM</i> -Betriebsarten	Kap. 4.1
Feste Verbindungen	Kap. 5.1
Point-to-Point Protocol	Kap. 6.1

Workshop

Vorbemerkung	Kap. 2.1
Internet-Anwendungen	Kap. 2.2
LAN-LAN-Kopplungen	Kap. 2.3
Remote Access	Kap. 2.4
Zugang zum ELSA-Testnetz	Kap. 2.5
Fehlersuche	Kap. 2.6

Referenz-Handbuch

Beschreibung der Menüpunkte	Kap. 3.1
<i>LANCOM</i> intern	Kap. 3.2
Meldungen, Nummern, Ports	Kap. 3.3
Häufig gestellte Fragen und Antworten	Kap. 3.4

Anhang

Copyright © 1996-98 ELSA AG, Aachen (Germany)

Alle Angaben in diesem Handbuch 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 dieses Handbuchs und die Verwertung seines Inhalts sowie der zum Produkt gehörenden Software sind nur mit schriftlicher Erlaubnis von ELSA gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

ELSA ist DIN-EN-ISO-9001-zertifiziert. Mit der Urkunde vom 16.05.1995 bescheinigt die akkreditierte Zertifizierungsstelle TÜV CERT die Konformität mit der weltweit anerkannten Norm DIN EN ISO 9001. Die an ELSA vergebene Zertifikatsnummer lautet 09 100 5069.

Marken

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

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

Internet <http://www.elsa.de>

Aachen, im April 1998

Art.-Nr. 20549/0498

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Mit dem *ELSA MicroLink LANCOM MPR* haben Sie sich für einen ISDN-Router entschieden, mit dem Sie lokale Netzwerke mit anderen Netzwerken ebenso einfach und komfortabel verbinden wie mit einzelnen, entfernten Arbeitsplatzrechnern oder dem Internet. Höchste Qualitätsanforderungen in der Fertigung und eine enggefaßte Qualitätskontrolle bilden die Basis für den hohen Produktstandard und sind Voraussetzung für gleichbleibende Produktqualität.

Lieferumfang

Bevor Sie mit der Inbetriebnahme Ihres ISDN-Router beginnen, vergewissern Sie sich bitte, daß Ihre Lieferung vollständig ist:

- ISDN-Router *ELSA MicroLink LANCOM MPR*
- ISDN-Anschlußkabel
- Netzteil
- Kabel für die Konfigurationsschnittstelle
- BNC-T-Verbindungsstück für Thin Ethernet
- Dokumentation
- Disketten mit Konfigurationsprogramm *LANconfig* für Windows 95 und Windows NT sowie LANCOM-Firmware

Dokumentation

Die beiliegende Dokumentation besteht aus:

- Installation Guide
Hardware-Installation und erste Beispiele zur Konfiguration
- Handbuch
Ausführliche Beschreibung des *LANCOM*, weitere Konfigurationsbeispiele, Referenzteil zum Nachschlagen

Online-Dienste



Sollten Sie darüber hinaus noch Fragen haben oder zusätzliche Hilfe benötigen, stehen Ihnen unsere Online-Dienste rund um die Uhr zur Verfügung. Den gesamten Umfang der von ELSA bereitgestellten Unterstützung und Service-Leistungen können Sie in den Kapiteln „Rat & Hilfe“ und „ELSA-Service“ im Handbuch nachschlagen.

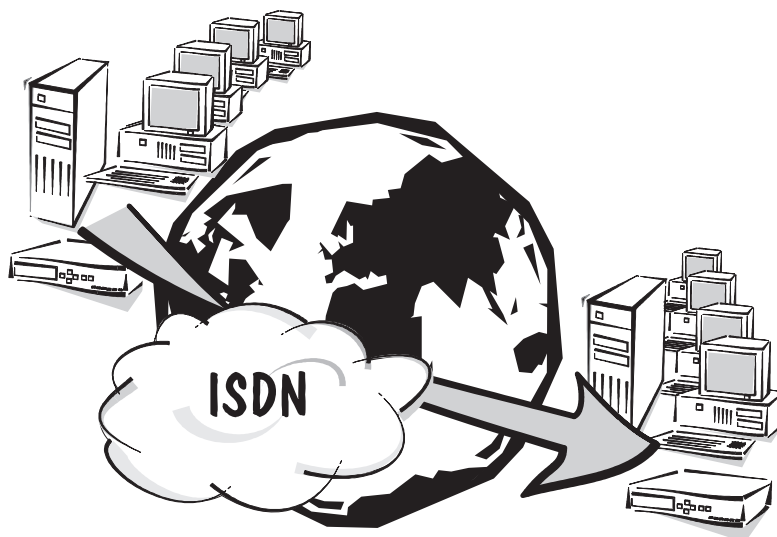


Benutzer-Handbuch

Einleitung	1.1.1
Was macht ein Router überhaupt?	1.1.2
Was bietet das <i>ELSA MicroLink LANCOM MPR</i> ?	1.1.4
Was finden Sie in diesem Handbuch?	1.1.7
Das <i>LANCOM</i> stellt sich vor	1.2.1
Vorhang auf für das <i>LANCOM</i>	1.2.2
Wie sieht das <i>LANCOM</i> aus?	1.2.2
Wie können Sie das <i>LANCOM</i> anschließen?	1.2.4
Sicherheit für Ihr LAN	1.2.5
Die Kontrolle	1.2.5
Der Rückruf	1.2.6
Das Versteck – IP Masquerading (Single User Access, NAT, PAT)	1.2.7
Kosten unter Kontrolle	1.2.8
Wir müssen leider draußen bleiben	1.2.8
Schnell schnell – Datenkompression und Kanalbündelung	1.2.10
Die Kosten im Griff – Gebührenmanagement	1.2.10
Kompatible Kommunikation	1.2.11
Online oder Offline – Die Leitung für die Verbindung	1.2.11
Übertragungsprotokolle	1.2.11
Das Chamäleon	1.2.12
<i>LANCOM</i> -Verbindungen sind zuverlässig	1.2.14
Gesicherte Protokolle	1.2.14
Die Backup-Leitung	1.2.14
Konfigurationsmöglichkeiten	1.3.1
Viele Wege führen zum <i>LANCOM</i>	1.3.2
Fingertips – Die Tastaturbedienung	1.3.3
Das Display	1.3.3
Die Tasten	1.3.3
Erlaubte Zeichen für die Eingabe	1.3.4
Der direkte Weg: Outband	1.3.5
Der komfortable Weg: Inband	1.3.7
Befehle für die Konfiguration	1.3.10
Konfiguration über SNMP	1.3.11
Allgemeines	1.3.11
Zugriff auf Tabellen und Parameter über SNMP	1.3.11
Die Management Information Base (MIB)	1.3.13
Was ist los auf der Leitung? – Trace-Ausgaben	1.3.14

So starten Sie einen Trace.....	1.3.14
Beispiele:.....	1.3.15
So spielen Sie eine neue Software ein	1.3.16
LANCOM-Betriebsarten	1.4.1
Bridge oder Router?	1.4.2
Die Brücke im Netz	1.4.4
Der IP-Router.....	1.4.6
IP-Adressierung.....	1.4.6
Die IP-Routing-Tabelle	1.4.7
Was passiert bei der Datenübertragung im IP-Netz?.....	1.4.9
Filter für die TCP/IP-Pakete.....	1.4.10
Proxy-ARP.....	1.4.11
Lokales Routing.....	1.4.11
Dynamisches Routing mit IP-RIP.....	1.4.12
IP-Masquerading (Single User Access, NAT, PAT).....	1.4.15
DNS-Forwarding.....	1.4.17
Zugangskontrolle.....	1.4.18
Policy Based Routing.....	1.4.18
Der IPX-Router	1.4.19
IPX-Adressierung.....	1.4.19
Informationen über das LAN.....	1.4.19
IPX-Routing-Tabelle	1.4.19
Was passiert bei der Datenübertragung im IPX-Netz?.....	1.4.21
RIP- und SAP-Tabellen	1.4.21
So viele LANCOMs hier... ..	1.4.22
Redundante Routen.....	1.4.22
Exponential Backoff	1.4.22
Filter für die IPX-Pakete	1.4.23
Feste Verbindungen	1.5.1
Ein oder zwei Kanäle, mit oder ohne D-Kanal?	1.5.2
So stellen Sie die Festverbindung ein	1.5.3
Einstellungen in der Interface-Tabelle.....	1.5.3
Einstellungen in der Namenliste.....	1.5.4
Einstellungen in der Layer-Liste.....	1.5.5
Die Backup-Leitung	1.5.7
Wann wird die Backup-Verbindung aktiviert?	1.5.7
Einstellungen für den Backup-Betrieb	1.5.7
Point-to-Point Protocol	1.6.1
Das Protokoll	1.6.2
Die PPP-Liste	1.6.4
Alles o.k.? Leitungsüberprüfung mit LCP	1.6.5

Zuweisung von IP-Adressen	1.6.6
Rückruf-Funktionen	1.6.7
Rückruf nach Microsoft CBCP	1.6.7
Rückruf nach RFC 1570 (PPP LCP Extensions).....	1.6.9



Einleitung

Wenn es um den Aufbau unternehmensweiter Infrastrukturen geht, rückt der Einsatz von ISDN-Routerlösungen zunehmend in den Vordergrund. Mit hohen Übertragungsraten und umfangreichen Sicherheitsmechanismen bietet das ISDN-Netz die wirtschaftlich attraktivste Basis zur Überbrückung der Entfernungen im Wide-Area-Verbund. An verschiedenen Standorten gewachsene lokale Netzwerke (LANs) und Einzel-PCs lassen sich mit Routern kostengünstig verbinden. Filialen und Niederlassungen können via ISDN transparent in das Netzwerk der Zentrale eingebunden werden und verfügen über die gleiche Datenbasis wie die Zentrale.

Was macht ein Router überhaupt?	2
Was bietet das <i>ELSA MicroLink LANCOM MPR</i> ?	4
Was finden Sie in diesem Handbuch?	7

Was macht ein Router überhaupt?

Mit einem ISDN-Router wie dem *LANCOM* werden lokale Netzwerke (Local Area Networks, LANs) und Einzel-PCs über ISDN-Leitungen verbunden. Jeder Rechner in diesem Wide Area Network (WAN) kann dann je nach Berechtigung auf die Rechner und Dienste im gesamten Netz zugreifen. Der Router sucht dabei einen Weg (eine Telefonverbindung), über den die Daten zwischen den Rechnern ausgetauscht werden können.

Das *LANCOM* wird wie ein normaler PC in das lokale Netz eingebunden. Alle Daten, die über die Verkabelung des Netzwerkes fließen, kommen damit auch beim *LANCOM* an. Das *LANCOM* entscheidet dann selbständig, ob Daten in ein anderes Netzwerk übertragen werden müssen und stellt bei Bedarf die Verbindung zur Gegenstelle über die ISDN-Leitung her. Bei der Verwendung von ISDN-Standleitungen entfällt natürlich der Verbindungsaufbau.

Wann setzen Sie das *LANCOM* 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 eMail sind nur einige der Anwendungen, die den Anwendern am PC die Arbeit erleichtern sollen.

Das *LANCOM* 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 Verbindung 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 wer-

den über das *LANCOM* im lokalen Netz der Zentrale ermöglicht. Auch beim Remote-Access tut das *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.

Was bietet das *ELSA MicroLink LANCOM MPR*?

Um Ihnen einen kleinen Überblick über die Leistungsfähigkeit des ISDN-Routers zu geben, sind im folgenden die wesentlichen Eigenschaften des *LANCOMs* aufgeführt.

Einfache Installation

LANCOM-ISDN-Router von ELSA sind besonders einfach zu installieren:

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

LAN-Anschluß

ISDN-Router von ELSA arbeiten im Ethernet. Über die Anschlüsse 10Base-5, 10Base-2 oder 10Base-T verbinden Sie das *LANCOM* mit dem LAN.

WAN-Anschluß

Das *LANCOM* wird an die S_0 -Schnittstelle eines ISDN-Mehrgeräteanschlusses oder einer Nebenstellenanlage (TK-Anlagen) angeschlossen. Anlagenanschlüsse, auch Punkt-zu-Punkt-Konfiguration genannt, werden nicht unterstützt.

Auf der ISDN-Leitung unterstützt das *LANCOM* natürlich auch die Kanalbündelung. Wählverbindungen mit DSS1 oder 1TR6 können ebenso verwendet werden wie Festverbindungen.

Zusätzlich ist der Anschluß eines analogen Modems oder eines ISDN-Terminaladapters an die serielle Schnittstelle des *LANCOMs* möglich.

Kompatibilität

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

Statusanzeigen

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

Konfiguration mit *LANconfig*

Die Einstellung und Anpassung des *LANCOMs* an Ihre spezielle Aufgabe erfolgt schnell und komfortabel über das mitgelieferte Konfigurationstool *LANconfig* für Windows® 95 und Windows NT® 4.0. Benutzer anderer Betriebssysteme verwenden ein beliebiges Telnet oder Terminalprogramm. Der Zugriff auf das *LANCOM* 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.

Leitungsaufbau und -verwaltung

Das *LANCOM* überprüft alle Daten in einem Netzwerk daraufhin, ob sie in ein anderes Netz oder zu einem anderen Rechner übertragen werden müssen. Ist eine Übertragung notwendig, baut das *LANCOM* selbständig die Verbindung auf und beendet diese nach der Übertragung auch wieder.

Um Übertragungskosten zu sparen, bietet das *LANCOM* je nach Betriebsart verschiedene Filter-Möglichkeiten. Damit werden die Daten aus ganzen Netzen oder Teilen von Netzen von der Übertragung ausgeschlossen. Ebenso können die Daten, die zu bestimmten Diensten (wie z.B. Druck-Dienste) gehören, aus der Übertragung herausgefiltert werden.

Zugriffsschutz

Zum Schutz vor unberechtigtem Zugriff auf das Firmen-Netz bietet das *LANCOM* neben dem Paßwortschutz und der Rufnummernerkennung auch eine Rückruf-Funktion, die nur den Verbindungsaufbau vom *LANCOM* aus zu vorher festgelegten Telefon-Anschlüssen zuläßt.

Gebührenschatz

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.

Software-Update

Damit Sie immer auf dem neuesten Stand der Technik in Sachen Software bleiben, hat *LANCOM* einen Flash-ROM-Speicher. Eine neue Firmware kann so komfortabel in das Gerät eingespielt werden, ohne daß man das Gerät öffnen muß. Die aktuelle Version steht z.B. immer in unseren Online-Medien für Sie bereit (siehe 'An wen können Sie sich wenden?' auf Seite A-5) und kann über das LAN, das WAN oder über die Konfigurationsschnittstelle in das *LANCOM* eingespielt werden.

Statistiken

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

Betriebsarten

Netzwerke mit beliebigen Protokollen werden vom *LANCOM* auf Ebene der MAC-Adressen mit der Bridge verbunden. Netze mit TCP/IP oder IPX/SPX können die Routerfunktionen nutzen. Alle Betriebsarten laufen dabei auf Wunsch auch parallel und gleichzeitig in einem Gerät.

Was finden Sie in diesem Handbuch?

Benutzer-Handbuch

Im allgemeinen Teil dieses Handbuchs finden Sie zunächst eine ausführliche Beschreibung der Funktionen und Eigenschaften des *LANCOMs*. Anschließend erklären wir Ihnen, wie das *LANCOM* arbeitet und mit welchen Hilfsmitteln Sie es konfigurieren können.

Workshop

Der Workshop stellt Ihnen die praktischen Dinge vor. Neben den speziellen Funktionen und Möglichkeiten von Bridge, IPX- und IP-Router erfahren Sie alles über die umfangreichen Filtermechanismen des *LANCOMs*. Anwendungsbeispiele wie LAN-LAN-Kopplung, Internet-Anbindung, Remote-Access und der Zugang zu den ELSA-Testnetzen runden den praktischen Teil ab. Dazu finden Sie noch einige Hinweise zur analytischen Fehlersuche mit den speziellen Hilfsmitteln des *LANCOMs* (z.B. Statistiken und Trace-Ausgaben).

Referenz-Handbuch

Der Referenzteil des Handbuchs ist das Nachschlagewerk. Hier finden Sie alle Befehle der *LANCOM*-Software. Für alle, die nicht zu den Profis in Sachen Netzwerktechnik oder ISDN zählen, gibt es in den Grundlagen leicht verständliche Erklärungen, die kein großes Vorwissen erfordern. Hinweise zur Scriptverarbeitung und zu den Trace-Ausgaben runden das Referenz-Handbuch zusammen Antworten auf häufig gestellt Fragen und Antworten (FAQs) ab.

Anhang

Im Anhang finden Sie neben den technischen Daten des *LANCOMs* Kontaktadressen, Service- und Garantiebedingungen. Im Glossar werden die verwendeten Fachbegriffe erläutert, der Index hilft Ihnen beim schnellen Zugriff auf die gesuchten Informationen.



Das **LANCOM** stellt sich vor

Die Kernfunktion des *LANCOMs* ist die Datenübertragung. Weil diese Übertragung über öffentliche Telefonleitungen abläuft, müssen die Verbindungen des *LANCOMs* vor allem sicher, zuverlässig, kostengünstig und kompatibel sein.

Darüber hinaus soll es natürlich in den verschiedensten Rechnerumgebungen einfach zu konfigurieren sein und dem Benutzer zu jedem Problem die bestmögliche Lösung bieten ...

In diesem Kapitel zeigen wir Ihnen die Anzeige- und Bedienungselemente des *LANCOMs*, welche Anschlußmöglichkeiten es bietet und mit welchen Eigenschaften und Funktionen es die oben aufgeführten Anforderungen erfüllt.

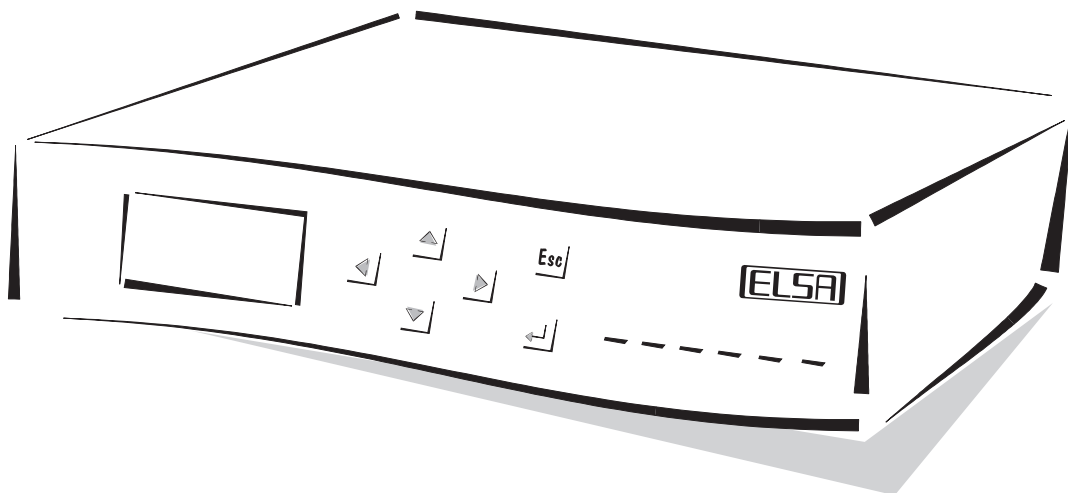
Die genaue Verwendung der *LANCOM*-Features erläutern wir in den nachfolgenden Kapiteln und anhand der Beispiele im Workshop.

Vorhang auf für das <i>LANCOM</i>	2
Sicherheit für Ihr LAN.....	5
Kosten unter Kontrolle.....	8
Kompatible Kommunikation.....	11
<i>LANCOM</i> -Verbindungen sind zuverlässig.....	14

Vorhang auf für das **LANCOM**

Wie sieht das **LANCOM** aus?

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



Das Display zeigt die verschiedenen Betriebszustände, Meldungen, Menüs und Eingabemöglichkeiten des Gerätes an, wenn es nicht von einem Rechner aus bedient wird.

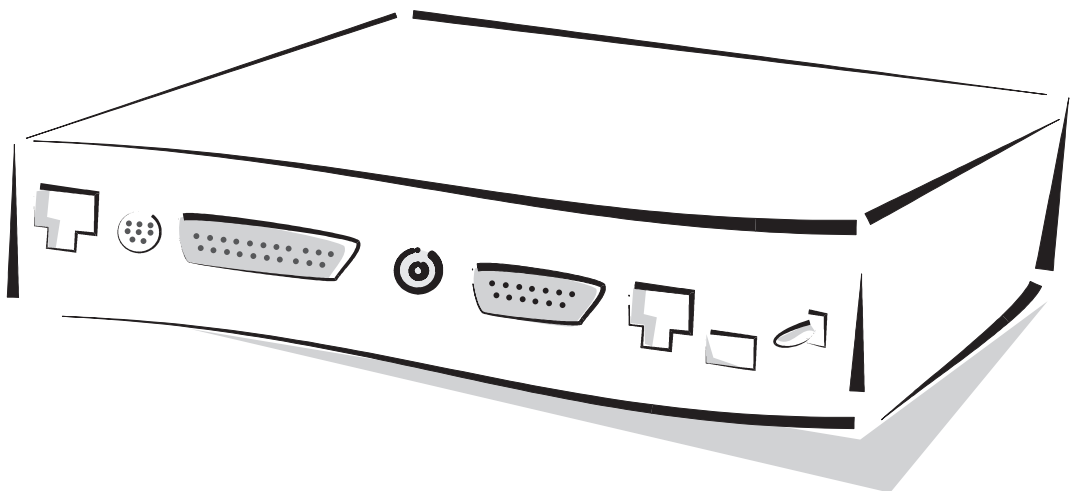
Mit den Tasten wählen Sie die Menüs aus und geben Werte oder Befehle ein. Die genaue Funktion der einzelnen Tasten in den verschiedenen Betriebszuständen des **LANCOMs** ist im Kapitel 'Konfigurationsmöglichkeiten' auf Seite 1.3.1 beschrieben.

Die LEDs schließlich zeigen Ihnen, was auf dem LAN und auf dem WAN los ist. Fangen Sie von links an und sehen sich die Dioden im einzelnen an:

Diese LED in diesem Zustand zeigt folgendes an:
NetTx	gelb	<i>LANCOM</i> sendet Daten an das LAN
NetRx	grün	<i>LANCOM</i> empfängt Daten
Coll	rot	<i>LANCOM</i> sendet Daten an das LAN und stellt dabei eine Datenkollision fest
Conn	gelb	<i>LANCOM</i> hat eine Verbindung über die serielle Schnittstelle zur Gegenstelle aufgebaut

Diese LED in diesem Zustand zeigt folgendes an:
S ₀ -Status	aus	keine Spannung am S ₀ -Bus oder Bus nicht aktiviert
	blinkt schnell	Spannung am S ₀ -Bus mit D-Kanal erkannt oder Bus mit D-Kanal aktiviert, keine TEI
		Spannung am S ₀ -Bus ohne D-Kanal erkannt, Bus nicht aktiviert
	grün	Spannung am S ₀ -Bus mit D-Kanal erkannt oder Bus mit D-Kanal aktiviert, TEI zugewiesen
		Spannung am S ₀ -Bus ohne D-Kanal erkannt, Bus aktiviert
S ₀ -Line	aus	Kein Anruf, keine Verbindung
	blinkt langsam (1x pro Sek., insgesamt 2 bis 3x)	Ankommender Ruf, LANCOM ist jedoch nicht zuständig oder LANCOM baut selbst eine Verbindung auf
	blinkt schnell (3x pro Sek.)	Ruf liegt an, LANCOM ist zuständig, hat aber (noch) nicht angenommen
	gelb	Verbindung wird/ist hergestellt

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



- ISDN-S₀-Anschluß
- V.24-Konfigurationsschnittstelle
- Serielle Schnittstelle (V.24)
- 10Base-2 (BNC)
- 10Base-5 (AUI-15-polig)
- 10Base-T (RJ45)
- Anschluß für das Netzteil
- Ein/Aus-Schalter

Wie können Sie das *LANCOM* anschließen?

Das *LANCOM* wird in Ihrem lokalen Netz (Ethernet) ganz einfach wie ein Arbeitsplatz-rechner angeschlossen. Das *LANCOM* bietet Ihnen 10Base-T, 10Base-2 und 10Base-5 Anschlüsse an. Bei anderen Netzwerkverkabelungen verwenden Sie einen geeigneten Transceiver an der 10Base-5 Buchse.

Zusätzlich benötigt das *LANCOM* auch einen ISDN-Anschluß in Punkt-zu-Mehrpunkt-Konfiguration. *LANCOM* unterstützt DSS1 und 1TR6 als D-Kanal-Protokolle. Zur Übertragung großer Datenmengen bieten sich Festverbindungen nach D64S, D64S2, (T)S01 und (T)S02 an.

Sicherheit für Ihr LAN

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

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

Die Kontrolle

Ein Anrufer kann über zwei Eigenschaften identifiziert werden: Den Namen oder die Rufnummer. Welcher der beiden „Identifizier“ zur Erkennung des Anrufers verwendet werden soll, wird im Menü '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 der Name bzw. die Rufnummer vom Anrufer auch übermittelt wird.

Zusätzlich kann in der Namenliste eingestellt werden, ob der Anrufer zurückgerufen werden soll. Damit werden die Gebühren für die Verbindung vom angerufenen *LANCOM* getragen, allerdings können ggf. auch nur bestimmte, mit Rufnummer bekannte Gegenstellen Zugriff auf das Netz bekommen. Bei Verwendung von 'PPP' als Protokoll auf dem B-Kanal kann optional auch der Anrufer angegeben, an welcher Rufnummer er zurückgerufen werden möchte.

Horch, was kommt von draußen rein

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 Identifizier).

Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückge-

rufen. Ist ein Schutz des *LANCOMs* über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekannten Rufnummern abgelehnt.

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

Sag mir Deinen Namen ...

Bei Verwendung des ELSA- bzw. PPP-Layers für den B-Kanal kann auch der Name der anrufenden Gegenstelle übertragen werden. Dazu muß allerdings zunächst eine Verbindung aufgebaut werden, weil der Name nicht über den D-Kanal ausgetauscht werden kann.

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

Bei Verwendung des ELSA-Protokolls wird überprüft, ob der von der Gegenstelle übermittelte Name in der Namenliste vorhanden ist.

Beim PPP-Protokoll wird überprüft, ob der Name der Gegenstelle in der PPP-Liste (als Gerätenamen) vorhanden ist.

Kein Paßwort? Doch, diese besonderen Möglichkeiten gibt es beim PPP-Layer: 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 *LANCOM* von der Gegenstelle verlangt.



Die Sicherungsverfahren PAP oder CHAP wenden Sie natürlich nicht an, wenn Sie selber mit dem 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?

- Wenn das ELSA-Protokoll für den B-Kanal verwendet wird, läuft die Identifizierung ja nur über den Namen, ohne Paßwort ab. Der Name ist dabei der Gerätenamen des anrufenden Routers.
- Bei PPP werden Name und Paßwort beim Verbindungsaufbau mit der Gegenstelle eingegeben, z.B. im entsprechenden Fenster einer Verbindung im DFÜ-Netzwerk. Wenn das *LANCOM* selbst eine Verbindung aufbaut, werden Gerätenamen, Paßwort und Benutzername aus der PPP-Liste verwendet.

Der Rückruf

Eine besondere Variante des Zugriffsschutzes wird mit der Rückruf-Funktion 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 (ELSA oder PPP) können Sie das Rückrufverhalten Ihres *LANCOMs* steuern:

- Das *LANCOM* 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 das rückrufende *LANCOM* alle Gebühren bis auf eine, die für die Namensübermittlung benötigt wird. Ebenfalls eine Einheit fällt für das *LANCOM* an, wenn der Anrufer nicht über CLIP identifiziert wird. Ist dagegen eine Identifizierung über die Rufnummer des Anrufers erlaubt und möglich, kommt der Anrufer sogar ganz ohne Kosten weg.

Das Versteck – IP Masquerading (Single User Access, NAT, PAT)

Eine der häufigsten Aufgaben für ISDN-Router wie das *LANCOM* 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 *LANCOM* mit seiner IP-Adresse (fest oder vom Provider zugewiesen) im Internet bekannt gemacht. Die Rechner im LAN nutzen das *LANCOM* dann als Gateway und können selbst nicht erkannt werden. Das *LANCOM* trennt dabei Internet und Intranet wie eine Wand. IP-Masquerading wird daher auch als „Firewall-Technik“ bezeichnet.

Kosten unter Kontrolle

Eines war Ihnen ja schon von Anfang an klar: Zu den reinen Investitionskosten für das *LANCOM* werden auch die Gebühren für die Datenübertragung via ISDN (oder analoges Telefon) kommen. Und weil wir bei ELSA das natürlich auch wissen, wollen wir Ihnen auch beim Sparen helfen.

Aber wie können wir gemeinsam die Kosten reduzieren und in Grenzen halten? Folgende Überlegungen helfen uns auf die Sprünge:

- Die geringsten Kosten verursachen Daten, die gar nicht übertragen werden. Also versuchen Sie nur die wichtigen Datenpakete über die Leitung zu schicken. Die bestimmen Sie z.B. mit Hilfe von Routing-Tabellen, die nur bestimmte Daten rauslassen. Die anderen bremsen Sie mit Filtern, die ganze Datengruppen von der teuren ISDN-Leitung ausschließen oder „Spoofing-Mechanismen“, die Anfragen an ein entferntes Netz lokal im eigenen Netz beantworten.
- Wenn Sie schon Daten übertragen müssen, dann sollen die möglichst klein sein und schnell ankommen. Dazu gibt es die Datenkompression.
- Außerdem soll die Leitung nur dann bezahlt werden, wenn auch Daten fließen. Intelligentes Line-Management baut die notwendigen Verbindungen selbständig auf und anschließend wieder ab, wenn die Übertragung erfolgreich war.
- Zum guten Schluß setzen Sie dem *LANCOM* eine Grenze: bis hierher und nicht weiter. Mit dem Gebührenbudget verhindern Sie überhöhte und vor allen Dingen unerwartete Telefonrechnungen.

Wir müssen leider draußen bleiben ...

Die Suche nach den wirklich wichtigen Datenpaketen, die auch tatsächlich eine Gegenstelle erreichen müssen, gehört zu den Hauptaufgaben bei der Router-Konfiguration. Schauen Sie die drei verschiedenen Betriebsarten des *LANCOMs* doch einmal an und sehen, wie Sie die überflüssigen Datenpakete zu fassen bekommen.

IP-Router

Hier ist die Auswahl der übertragungswürdigen Daten recht einfach. Der IP-Router überträgt nur die Datenpakete zu den Ziel-IP-Adressen, die nicht in seinem lokalen Netz zu finden sind **und** für die er in der Routing-Tabelle einen Weg findet. Also legen Sie mit den Einträgen in der IP-Routing-Tabelle selbst genau fest, welche Daten übertragen werden und welche nicht. Mit Adreß- und Port-Filtern für die WAN- und die LAN-Seite können Sie außerdem noch gezielt Gruppen von Datenpaketen von der Übertragung ausschließen.

IPX-Router

Etwas schwieriger ist die Situation beim IPX-Router. Eine Eigenschaft der IPX-Netzwerke ist im Hinblick auf das Routing besonders wichtig: Zur Kommunikation untereinander versenden die einzelnen Geräte in einem IPX-Netz regelmäßig spezielle Datenpakete, mit denen sie z.B. die verfügbaren Dienste in einem Netz bekannt machen (Service Advertising Protocol SAP), sich gegenseitig über Routen ins andere Netz informieren (Routing Information Protocol RIP) oder einfach nur nachfragen, ob andere Geräte noch aktiv sind (Watchdogs). Wird ein IPX-Netz über einen Router mit einem anderen Netz verbunden, so werden prinzipiell auch diese Daten über die ISDN-Leitung übertragen und bauen permanent Verbindungen auf.

Um das zu verhindern, können einzelne RIP- oder SAP-Informationen (oder ganze Gruppen von ihnen) von der Aufnahme in die RIP/SAP-Tabellen ausgeschlossen werden. Eine weitere Möglichkeit besteht darin, SAP oder RIP nur zu bestimmten Zeiten zu übertragen, nur wenn sich Änderungen in den Informationen ergeben haben oder nur wenn die Verbindung ohnehin schon besteht.

Zur Reduzierung der Watchdogs auf der WAN-Strecke bietet sich das „Spoofing“ an. Dabei beantwortet das LANCOM lokal die Watchdogs, die eigentlich an ein Gerät in einem entfernten Netz gerichtet sind und verhindert so den Verbindungsaufbau.

Ähnlich den Port-Filtern beim IP-Routing können beim IPX-Router für die WAN- und die LAN-Seite Filter-Tabellen gepflegt werden. Alle Pakete aus dem lokalen oder entfernten Netz, die einem der Sockets aus der entsprechenden Tabelle zugeordnet sind, werden nicht übertragen.

Bridge

Eine Bridge verbindet genau zwei lokalen Netzwerke. Dabei hat sie die besondere Eigenschaft, zunächst einmal alle Datenpakete zu übertragen, die lokal nicht zugeordnet werden können. Das ist, zumindest bei Verwendung von Wählleitungen, eine recht teure und unerwünschte Angelegenheit. Daher können Sie auch hier die zu übertragenden Datenpakete etwas eingrenzen.

Für Broadcast-Datenpakete (an alle erreichbaren Geräte in einem Netz gerichtet) und Multicast-Datenpakete (an eine bestimmte Gruppe von Geräten in einem Netz gerichtet) bieten sich drei Möglichkeiten: immer übertragen, nie übertragen, nur dann übertragen, wenn die Leitung schon besteht.

Ein weitergehende Eingrenzung erreichen Sie durch die Filter-Tabellen. Für die Filter-Tabelle kann zunächst entschieden werden, ob die Pakete zu den in ihr eingetragenen Adressen übertragen werden sollen oder ob gerade diese Pakete ausgeschlossen werden sollen (positiver oder negativer Filter). In der Tabelle werden dann die physikalischen, fest eingetragenen Adressen der betreffenden Netzwerkkarten eingetragen.

Schnell schnell – Datenkompression und Kanalbündelung

Wenn Sie auf beiden Seiten einer ISDN-Verbindung ein *LANCOM* verwenden, können Sie Ihren Daten Beine machen: Sie können die Daten komprimieren und/oder zwei B-Kanäle zur Übertragung verwenden (Kanalbündelung).

Datenkompression und Kanalbündelung sind an das verwendete B-Kanal-Protokoll geknüpft: Nur bei X.75LAPB und bei X.75ELSA stehen diese Funktionen zur Verfügung.

Zur Verwendung der beiden „Hochgeschwindigkeits-Funktionen“ des *LANCOMs* stellen Sie die Optionen auf Layer 2 des B-Kanal-Protokolls in der Layer-Liste ein:

- **compr.** nach V.42bis reduziert das Datenvolumen (theoretisch um den Faktor 4-5), wenn die Daten nicht schon vorher komprimiert waren.
- **Buendeln** verwendet zwei B-Kanäle für eine Verbindung. Die Haltezeiten einer Verbindung für B1 und B2 in der Layer-Liste legen fest, ob eine statische oder dynamische Kanalbündelung verwendet wird.
- **bnd+compr** nutzt beides: Komprimierung und Kanalbündelung

Die Kosten im Griff – Gebührenmanagement

Daß Ihr *LANCOM* selbst entscheiden kann, wann es Verbindungen aufbauen will, ist ja schön und gut. Aber wie schützen Sie sich gegen zu häufigen Verbindungsaufbau?

Um die Kostenexplosion auf der Telefonrechnung (z.B. durch eine Fehlkonfiguration) zu vermeiden, geben Sie dem *LANCOM* ein bestimmtes Budget: In sieben Tagen darf es z.B. 830 Einheiten verbrauchen (Voreinstellung). Sowohl die Tage als auch die Anzahl der Gebühren können frei gewählt werden.

Wenn Sie Gebühren für das *LANCOM* völlig freigeben wollen, stellen Sie Einheiten auf Null. Aber Vorsicht: das *LANCOM* kann jetzt so viele Verbindungen aufbauen, wie es will!

Die Gebührenüberwachung des LANCOMs können Sie nur bei freigeschalteter „Gebühreninformation während der Verbindung“ im ISDN-Netz (nach AOCD) nutzen. Beantragen Sie ggf. die Freischaltung dieses Merkmals bei Ihrer Telefongesellschaft.



Kompatible Kommunikation

Online oder Offline – Die Leitung für die Verbindung

Die *LANCOM*-Router verbinden Netzwerke und Einzel-PCs über ISDN-Leitungen, beim Anschluß eines analogen Modems an die serielle Schnittstelle des *LANCOMs* auch über normale Telefon-Leitungen. Dabei können sowohl Wählverbindungen als auch Standleitungen zum Einsatz kommen.

■ Festverbindung

Die Festverbindung oder Standleitung verbindet vor allem Netzwerke, zwischen denen ein permanenter Datenaustausch stattfindet. Ab einer bestimmten Größe des zu übertragenden Datenvolumens ist eine Standleitung kostengünstiger als eine Wählverbindung und durch den Wegfall der Anwahlvorgänge auch schneller.

Das *LANCOM* unterstützt Festverbindungen mit einem oder zwei B-Kanälen, jeweils mit oder ohne D-Kanal.

■ Wählverbindung

Wenn über das *LANCOM* nicht permanent, sondern eher sporadisch Daten übertragen werden sollen, reicht eine Wählverbindung meist aus.

Die Wählverbindung wird vom *LANCOM* selbständig verwaltet, d.h. bei Bedarf automatisch aufgebaut und nach Ablauf der Haltezeit wieder beendet.

Übertragungsprotokolle

Damit sich zwei Geräte zur Datenübertragung über eine ISDN-Leitung verständigen können, müssen Sie zunächst einmal die gleiche Sprache sprechen. Diese Sprache wird im ISDN-Netz mit Hilfe von Protokollen geregelt. Nur wenn beide das gleiche Protokoll verwenden, können sie sich auch verstehen.

Das ISDN verwendet immer zwei Protokolle für die Verbindung: ein D-Kanal- und ein B-Kanal-Protokoll.

D-Kanal

Der D-Kanal überträgt in der Regel nur die Steuerinformationen, die zum Aufbau und zur Verwaltung der Verbindung benötigt werden. Das *LANCOM* unterstützt DSS1 (Euro ISDN) und 1TR6 (das ältere, nationale ISDN in Deutschland), SPV (semipermanente Festverbindungen) und Festverbindungen (D64S, D64S2, D64SY, S01, S02). Die Gegenstellen einer Verbindung können dabei durchaus unterschiedliche D-Kanal-Protokolle verwenden.

B-Kanal

Der B-Kanal überträgt die eigentlichen Nutzdaten der Verbindung. Auf drei Ebenen (Layern) wird beim B-Kanal-Protokoll in der Layer-Liste festgelegt, wie die Datenübertragung ablaufen soll. So kann die Übertragung auch zwischen Geräten unterschiedlicher Hersteller genau angepaßt werden.

- Auf Layer 1 können 64 oder 56 kbit/s, beide mit HDLC eingesetzt werden.
- Layer 2 bietet Transparent, X.75UI, X.75BUI, X.75LAPB und X.75ELSA zur Auswahl an.
- Auf Layer 3 stehen neben den firmeneigenen Protokollen von ELSA und CISCO die Auswahlmöglichkeiten Transparent, synchrones und asynchrones PPP bereit.

Mit diesen Protokollen in der Layer-Liste können Sie sich mit den meisten anderen Routern verständigen. Verwenden Sie nach Möglichkeit das transparente HDLC, dabei erreichen Sie den größten Datendurchsatz.

Aus den Kombinationen der unterschiedlichen Werte für die Einstellungen der Kommunikations-Layer ergeben sich beim *LANCOM* viele verschiedene B-Kanal-Protokolle. Einige gängige Möglichkeiten haben wir schon für Sie vorbereitet und in der Layer-Liste abgelegt. Sie können aber jederzeit Änderungen daran vornehmen oder neue B-Kanal-Protokolle (Layer) hinzufügen.

Das *LANCOM* unterstützt neben der Datenkompression nach V.42bis sowohl statische als auch dynamische Kanalbündelung. Natürlich können die B-Kanäle auch gleichzeitig für verschiedene Verbindungen verwendet werden. Mit einem ISDN-Terminal-Adapter oder Modem an der seriellen Schnittstelle des *LANCOMs* können so drei Verbindungen zu verschiedenen Gegenstellen gleichzeitig aufgebaut werden.

Das Chamäleon

Eine der ganz großen Stärken des *LANCOMs*: es paßt sich überall an die entsprechende Umgebung an. In jedem Ethernet findet es einen Weg zur Datenübertragung, unter jedem Betriebssystem findet sich ein passender Weg zur Konfiguration.

Netzwerke

Daten aus Netzwerken mit TCP/IP oder IPX/SPX überträgt das *LANCOM* als Router und findet so immer einen Weg zwischen verschiedenen entfernten Netzen. Netzwerke, die auf andere Protokolle setzen, werden mit der Bridge-Funktion zu einem Netz zusammengeschaltet.

Betriebssysteme

Auch bei den eingesetzten Betriebssystemen gibt sich das *LANCOM* gar nicht wählerisch: Unter Windows, Unix, OS/2 oder MacOS findet sich immer ein geeignetes Programm zur Anpassung der *LANCOM*-Software an Ihre Aufgabenstellung. Windows 95-

oder Windows NT-User haben es besonders leicht: Mit dem Konfigurations-Tool *LAN-config* steht Ihnen eine intuitiv zu erfassende Oberfläche mit vielen nützlichen Assistenten und Hilfen zur Verfügung. Unter anderen Betriebssystemen erreicht man mit Terminal- oder Telnet-Programmen ebenso sein Ziel.

SNMP

Mit dem Simple Network Management Protocol (SNMP) bietet sich eine weitere, moderne Möglichkeit zur Konfiguration des *LANCOMs*. Mit diesem Protokoll können alle SNMP-fähigen Geräte in einem Netz, also auch das *LANCOM*, komfortabel von einer zentralen Stelle aus überwacht und eingestellt werden.

LANCOM-Verbindungen sind zuverlässig

Nichts ist ärgerlicher bei der Datenübertragung als Daten, die nicht oder nicht korrekt übertragen werden. Und weil Sie mit dem *LANCOM* auch ganze Netze von Unternehmen verbinden wollen, hat die Zuverlässigkeit der Verbindung einen hohen Stellenwert. Aber mit welchen Maßnahmen können Sie die Sicherheit der Datenübertragung verbessern?

Gesicherte Protokolle

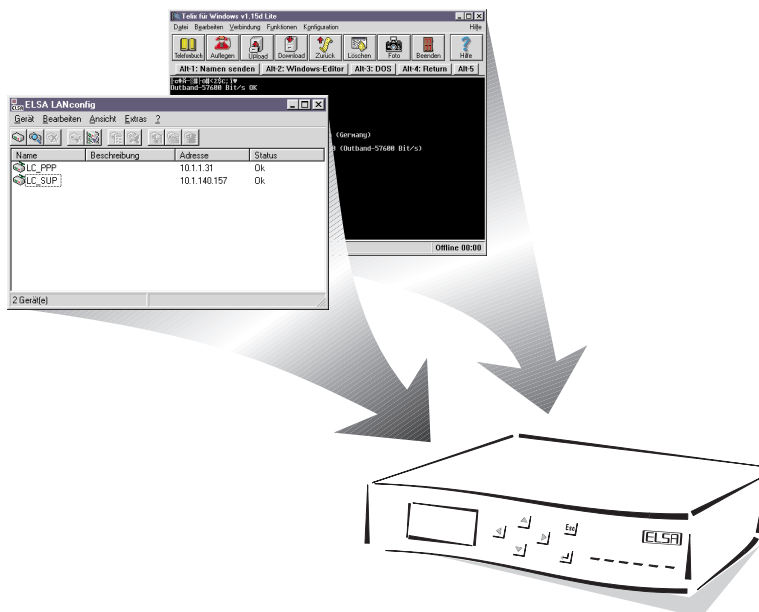
Zunächst bietet sich die Verwendung von bestimmten Protokollen auf dem B-Kanal an: X.75LAPB, X.75ELSA und PPP. Diese Protokolle prüfen während der Übertragung in regelmäßigen Abständen, ob die Gegenstelle noch aktiv ist. Das geschieht im Prinzip durch ein Frage-Antwort-Spiel neben der Übertragung der eigentlichen Nutzdaten. Bleibt die Gegenstelle bei einer Festverbindung die Antwort für eine längere (einstellbare) Zeit schuldig, legt das *LANCOM* auf und versucht, die Übertragung über eine Backup-Leitung zu starten. Gleichzeitig versucht das *LANCOM* jedoch auch die eigentliche Verbindung wiederherzustellen.

Die Backup-Leitung

Mit dem Anschluß eines ISDN-Terminal-Adapters oder eines analogen Modems an die serielle Schnittstelle des *LANCOMs* eröffnet sich die Möglichkeit einer Backup-Leitung für Festverbindungen. Damit gewinnen sehr wichtige Datenleitungen ein weiteres Stück an Sicherheit gegen den Ausfall der Verbindung.

Die Backup-Leitung hat alle Eigenschaften einer normalen Wählleitung, z.B. Haltezeiten, nach deren Ablauf die Verbindung beendet wird, wenn keine Daten mehr fließen. Also könnte man doch eigentlich die Backup-Funktion einfach durch den Eintrag einer weiteren Rufnummer für diese Gegenstelle (in der Round-Robin-Liste) realisieren? Nicht ganz. Die Backup-Verbindung hat die besondere Eigenschaft, normale Wählverbindungen auf der seriellen Schnittstelle beenden zu können, wenn die Leitung benötigt wird. Sie ist also quasi immer verfügbar.

Wird die Backup-Verbindung durch die Gegenstelle oder das Ablaufen der Haltezeit beendet, gibt sie die Aufgabe der Datenübertragung wieder an die normalerweise zuständige Leitung zurück. Nur wenn diese Leitung beim Eintreffen neuer Datenpakete immer noch gestört ist, wird die Backup-Verbindung erneut aktiviert.



Konfigurationsmöglichkeiten

Das neue *LANCOM* wird immer mit einer aktuellen Software ausgeliefert, in der schon einige Einstellungen für Sie vorbereitet sind.

Trotzdem ist aber 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 *LANCOM* zugreifen können, um die Einstellungen vorzunehmen.

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

Viele Wege führen zum <i>LANCOM</i>	2
Fingertips – Die Tastaturbedienung	3
Der direkte Weg: Outband.....	5
Der komfortable Weg: Inband	7
Befehle für die Konfiguration	10
Konfiguration über SNMP	11
Was ist los auf der Leitung? – Trace-Ausgaben .	14
So spielen Sie eine neue Software ein	16

Viele Wege führen zum *LANCOM*

Prinzipiell gibt es drei Möglichkeiten, auf des *LANCOM* zuzugreifen:

- Über die eingebaute Tastatur und das Display an der Front
- Über die Konfigurations-Schnittstelle (Config-Schnittstelle) an der Rückseite des *LANCOM* (auch Outband genannt)
- Über das angeschlossene Netzwerk, LAN oder WAN (Inband)

Was unterscheidet nun diese Möglichkeiten?

Zuerst einmal die Anforderungen an weitere Soft- oder Hardware. Bei der Konfiguration über die Tastatur brauchen Sie keine weiteren Hilfsmittel: Sie können die Befehle direkt eingeben und auf dem Display ablesen. Das ist weniger komfortabel als andere Varianten, gelingt aber immer! 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 (im LAN) und das entsprechende Konfigurationskabel.

Ein weiterer Unterschied ist die Berechtigung, überhaupt Änderungen in der Konfiguration vornehmen zu dürfen.

- Die Inband-Konfiguration kann durch die Einstellungen in der *LANCOM*-Software eingeschränkt werden (siehe 'Setup/Config-Modul' auf Seite 3.1.61). Zugriffe auf das *LANCOM* aus dem WAN oder LAN können ganz verhindert oder nur auf das Lesen beschränkt werden. Inband können gleichzeitig vier konfigurationswillige Mitarbeiter das *LANCOM* anwählen, aber nur der erste darf neue Einstellungen schreiben. Alle anderen starten mit dem Attribut 'Nur Lesen'.
- Der Outband-Konfigurator oder der Finger an der Tastatur sind im Prinzip jederzeit berechtigt, Änderungen in den Einstellungen vorzunehmen. Allerdings kann der Zugriff über die Konfigurationsschnittstelle oder die Tastatur mit einem Paßwort geschützt werden (siehe 'Setup/Sonstiges' auf Seite 3.1.62).

Fingertips – Die Tastaturbedienung

Alle notwendigen Einstellungen beim *LANCOM* können mit Hilfe der Tastatur vorgenommen werden. Dazu stehen Ihnen die Tasten , , , ,  und  zur Verfügung.

Das Display





Im Display gibt es drei verschiedene Anzeige-Zustände:

In der **Status-Anzeige** wird entweder die aktuelle Verbindungssituation des *LANCOMs* mit beiden B-Kanäle angezeigt oder die bisherige Betriebszeit des *LANCOMs*. Welcher Status angezeigt wird, stellen Sie im Menü 'Status' ein.

In der **Menü-Anzeige** wird entweder ein Untermenü des aktuellen Menüs angezeigt, ein Eintrag in einem Menü oder der aktuelle Wert des Eintrags.

Im **Editier-Modus** blinkt der Cursor im Display, Sie können den Wert des aktuellen Eintrags ändern.

Die Tasten

Diese Taste bewirkt bei diesem <i>LANCOM</i> -Display folgende Aktion:
	Status-Anzeige	Wechsel in die Menü-Anzeige
	Menü-Anzeige	Wechsel in die Status-Anzeige
	Editier-Modus	Wechsel auf die vorige/nächste Stelle des aktuellen Eintrags In Tabellen Wechsel in die vorige/nächste Spalte.
	Status-Anzeige	Wechsel ins Hauptmenü
	Menü-Anzeige	Wechsel in das übergeordnete Menü
	Editier-Modus	Bricht die Eingabe ab
	Status-Anzeige	Wechsel in das Menü, das in der Menü-Anzeige nach dem → steht
	Menü-Anzeige	Wechsel in das Menü, das nach dem → steht
	Editier-Modus	Bestätigt eine Eingabe
	Status-Anzeige	Bringt weitere Zeilen der Status-Anzeige in das Display
	Menü-Anzeige	Bringt das nächste/vorhergehende Untermenü auf das Display
	Editier-Modus	Wechselt auf das nächste/vorhergehende zulässige Zeichen

Erlaubte Zeichen für die Eingabe

Folgende Zeichen stehen je nach Eingabefeld zur Verfügung:

Bei der Eingabe von folgenden Werten können Sie diese Zeichen verwenden:
Namen (Geräte, Gegenstellen, Layer)	16 Zeichen aus: ABCDEFGHIJKLMNOPQRSTUVWXYZ @{}~!\$%&'()+-./:;<=>?[]^_`.0123456789 (keine Leerzeichen!)
Paßwörter	16 Zeichen aus: ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz @{}~!\$%&'()+-./:;<=>?[]^_`.0123456789 (keine Leerzeichen!)
Rufnummern	21 Zeichen aus: 0123456789 Die ebenfalls gültigen Wahlsonderzeichen S#-F:IEB werden an den Stellen erläutert, wo Sie verwendet werden.
Haltezeiten	4 Zeichen aus: 0123456789
MAC-Adressen	12 Zeichen aus: 0123456789abcdef
IP-Adressen	15 Zeichen aus: .0123456789



Mit dem Befehl `set parameter ?` können Sie jederzeit den gültigen Wertebereich für die Eingabe eines Parameters abfragen.

Der direkte Weg: Outband

Mit der Outband-Konfiguration greifen Sie direkt über die Konfigurations-Schnittstelle auf das *LANCOM* zu.

Voraussetzungen für die Outband-Konfiguration

Was brauchen Sie dazu?

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

Outband-Konfiguration mit *LANconfig*

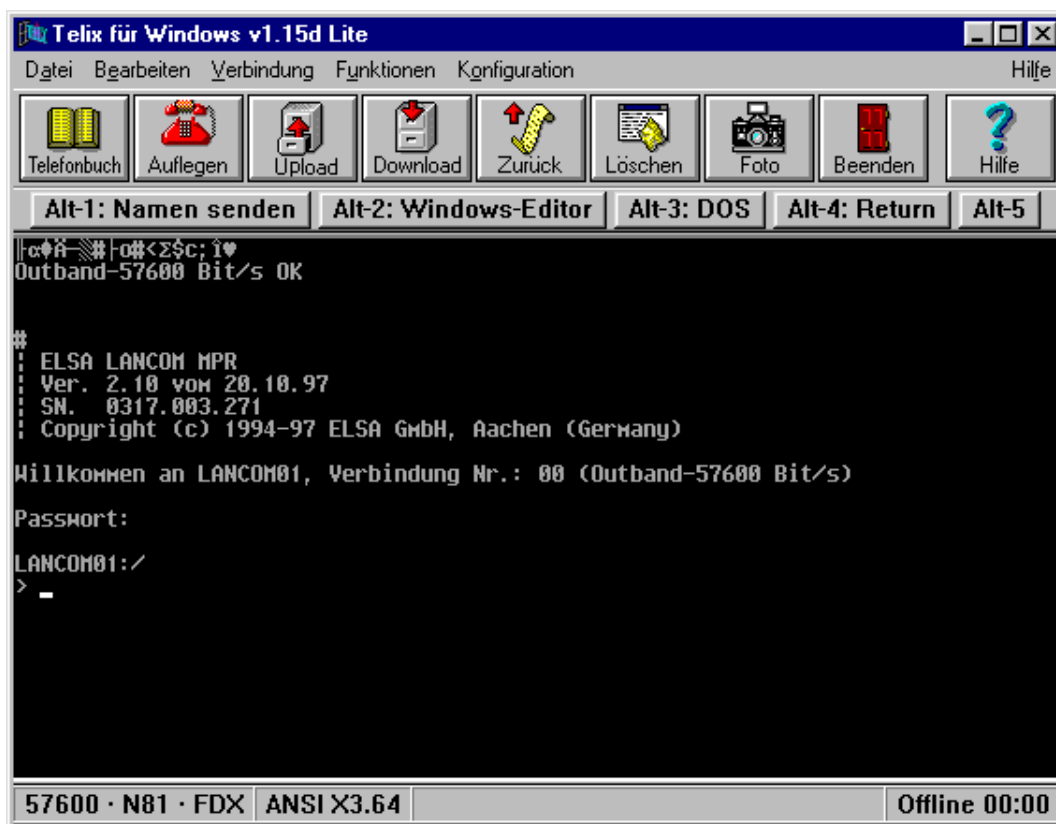
Starten Sie *LANconfig* z.B. aus der Windows-Startleiste mit **Start ► Programme ► ELSAlan ► LANconfig**. *LANconfig* sucht nun automatisch im lokalen Netz und an der seriellen Schnittstelle nach *LANCOM*-Geräten. *LANconfig* zeigt ein neues *LANCOM* in der Liste mit der Bezeichnung 'Ohne Name' an.

Für ein neues, noch nicht konfiguriertes *LANCOM* 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 das *LANCOM* für die ausgewählte Aufgabe eingestellt. Die Assistenten geben Ihnen außerdem noch Hinweise darauf, welche Einstellungen Sie ggf. bei den einzelnen Arbeitsplatzrechnern im Netz vornehmen müssen.

Alternativ können Sie mit einem Doppelklick auf 'Ohne Name' die aktuelle Konfiguration des *LANCOMs* zur Bearbeitung öffnen.

Outband-Konfiguration mit *Telix*

Wenn das Terminalprogramm gestartet ist, drücken Sie nur einige Male die Return-Taste, dann erscheinen z.B. bei *Telix* folgende Zeilen auf dem Bildschirm:



Nach der Eingabe des Paßworts stehen Ihnen alle Befehle aus dem Abschnitt 'Befehle für die Konfiguration' auf Seite 1.3.10 zur Konfiguration zur Verfügung.

Der komfortable Weg: Inband

Mit der Inband-Konfiguration haben Sie von jedem Rechner aus dem WAN oder LAN aus Zugriff auf das *LANCOM*. Allerdings nur, wenn das *LANCOM* dies zuläßt, denn der Zugang aus dem WAN oder LAN kann über die IP-Zugangsliste eingeschränkt werden. Für die Inband-Konfiguration verwenden Sie entweder Telnet (gehört zum Lieferumfang der meisten Betriebssysteme) oder das Konfigurationsprogramm *LANconfig* für Windows 95 oder Windows NT. *LANconfig* ist im Lieferumfang Ihres *LANCOMs* enthalten. Aktuelle Versionen stehen immer in unseren Online-Medien <Querverweis> für Sie bereit.

Voraussetzungen für die Inband-Konfiguration

Die Konfiguration mit Telnet oder *LANconfig* läuft über TCP/IP bzw. TFTP ab. Dazu muß also auf dem verwendeten Rechner das TCP/IP-Protokoll installiert sein, und das *LANCOM* benötigt eine IP-Adresse, mit der Sie es ansprechen können. Ein noch nicht konfiguriertes *LANCOM* hat 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 das *LANCOM* 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 LANCOM mit der Tastatur oder über die Outband-Konfiguration eine neue Adresse, bevor Sie es im LAN installieren.

Starten der Inband-Konfiguration über *LANconfig*

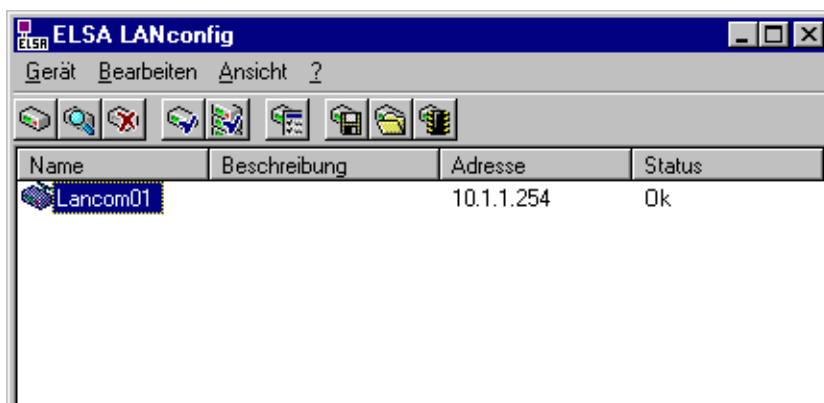
Nach der Installation (mit Doppelklick auf die 'setup.exe') rufen Sie das Konfigurations-Tool *LANconfig* z.B. aus der Windows-Startleiste auf **Start ▶ Programme ▶ ELSA!an ▶ LANconfig**. *LANconfig* sucht nun automatisch im lokalen Netz und an der Konfigurationsschnittstelle nach *LANCOM*-Geräten. Wird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

Wählen Sie einen der angebotenen Assistenten aus und beantworten Sie einfach seine Fragen. Anschließend ist das *LANCOM* für die ausgewählte Aufgabe eingestellt. Die Assistenten geben Ihnen außerdem noch Hinweise darauf, welche Einstellungen Sie ggf. bei den einzelnen Arbeitsplatzrechnern im Netz vornehmen müssen.

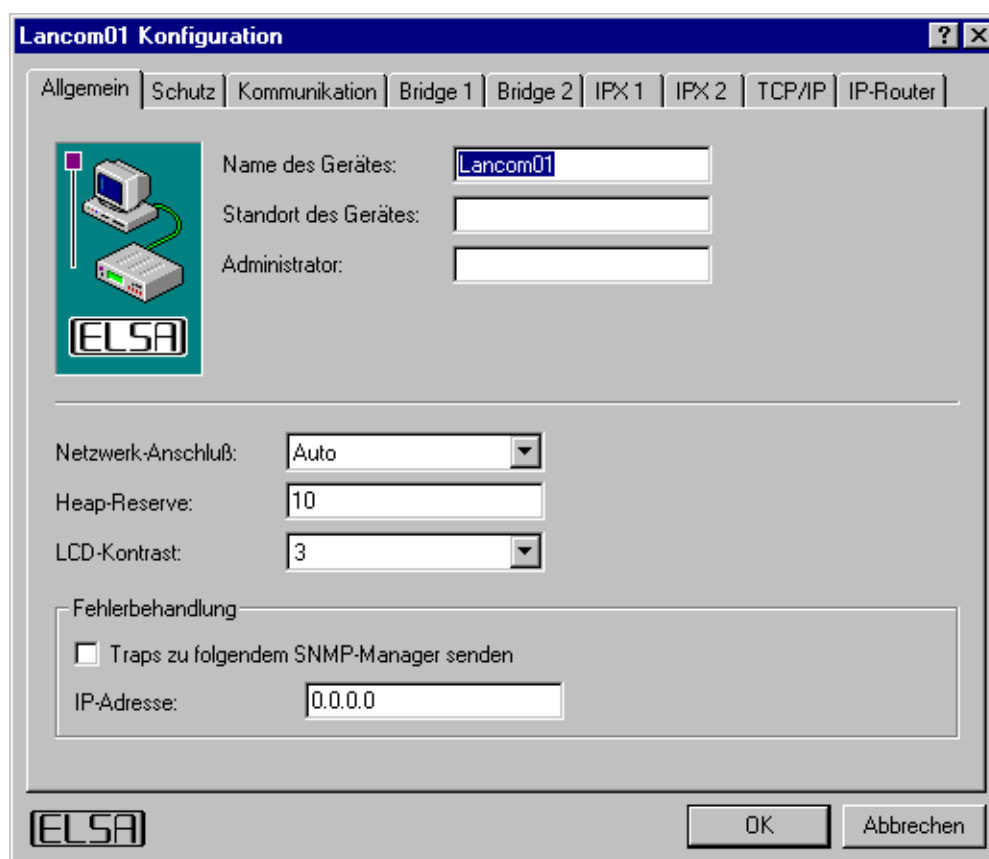


Um die Suche eines neuen *LANCOMs* manuell einzuleiten, klicken Sie nur auf die Schaltfläche **Suchen** oder rufen den Befehl über **Gerät ▶ Suchen** auf. *LANconfig* erkundigt sich dann, wo es suchen soll. Bei der Inband-Lösung reicht hier die Auswahl des lokalen Netzes, und los geht's.

Sobald *LANconfig* mit der Suche fertig ist, zeigt es uns 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 *LANCOM*, der Klick auf die Schaltfläche **Konfigurieren** oder den Menüeintrag **Bearbeiten ► Konfiguration bearbeiten** liest die aktuellen Einstellungen aus dem Gerät aus und zeigt die Registerkarte 'Allgemein'.



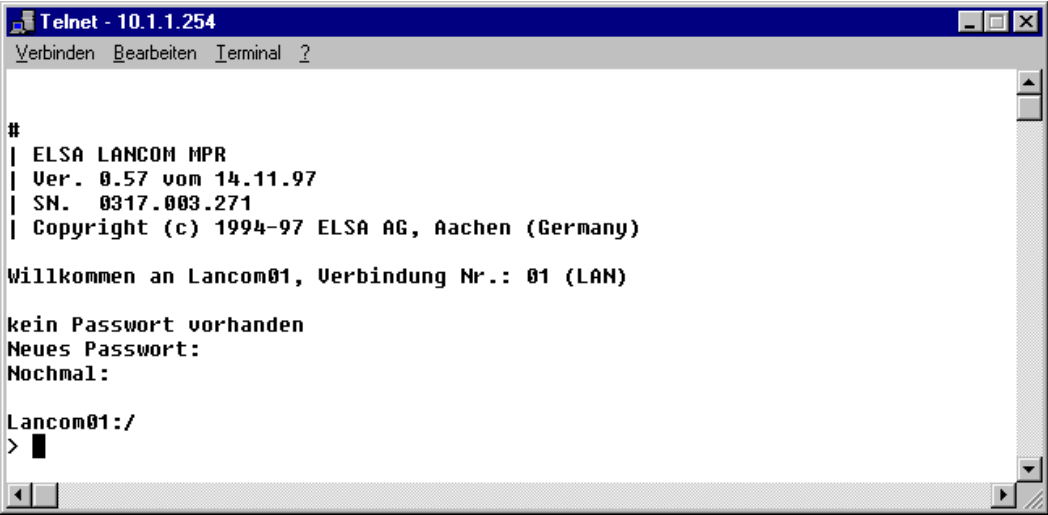
Die weitere Bedienung des Programms *LANconfig* erklärt sich im Prinzip selbst bzw. über die Online-Hilfe. Mit einem Klick auf das Fragezeichen oben rechts in jedem Fenster bzw. mit einem rechten Mausklick auf einen unklaren Begriff können Sie jederzeit die kontext-sensitive Hilfe aufrufen.

Starten der Inband-Konfiguration über Telnet

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

```
telnet 192.168.130.254
```

Telnet baut dann eine Verbindung zum *LANCOM* mit der IP-Adresse 192.168.130.254 auf, und z.B. folgende Zeilen erscheinen im Bildschirm:



```
Telnet - 10.1.1.254
Verbinden Bearbeiten Terminal ?

#
| ELSA LANCOM MPR
| Ver. 0.57 vom 14.11.97
| SN. 0317.003.271
| Copyright (c) 1994-97 ELSA AG, Aachen (Germany)

Willkommen an Lancom01, Verbindung Nr.: 01 (LAN)

kein Passwort vorhanden
Neues Passwort:
Nochmal:

Lancom01:/
> █
```


Nach der Eingabe des Paßworts stehen Ihnen alle Befehle aus dem Abschnitt 'Befehle für die Konfiguration' auf Seite 1.3.10 zur Verfügung.

Befehle für die Konfiguration

Bei der Verwendung von Telnet (Inband) oder einem Terminalprogramm (Outband) zur LANCOM-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 müssen nicht vollständig ausgeschrieben werden, eine eindeutige Abkürzung reicht aus.

Bei der Konfiguration LANCOM 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/t) 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 namenliste/Lancom04 123456 90 30 erzeugt in der Namenliste einen Eintrag für das Lancom04 mit der Rufnummer 123456 und den haltezeiten 90 und 30 Sekunden.
set <WERT> ?	Zeigt Ihnen, welche Werte Sie hier eingeben können	
del <WERT>	Löscht den angegebenen WERT (oder die ganze Zeile)	
do <AKTION> (Parameter)	Führt die AKTION aus, evtl. mit den angegebenen Parametern	do sonstiges/manuelle-wahl/aufbau ELSA.SUP.1 (kurz do/so/m/au ELSA.SUP.1) baut manuell eine Verbindung zum ELSA-Testnetz auf
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 wie Wiederholung.	repeat 3 dir/status/wan-statistik zeigt alle 3 Sekunden die aktuelle WAN-Statistik
exit, quit, x	Konfiguration wird beendet.	

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).

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 des *LANCOMs* 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 ein *LANCOM* 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 *LANCOM*-Remote-Konfiguration in einem eigenen Ast des SNMP-Management-Baums zur Verfügung: iso.org.dod.internet.private.enterprises.elsa.lancom oder 1.3.6.1.4.1.2356.1 .

Zugriff auf Tabellen und Parameter über SNMP

Alle Tabellen und Parameter des *LANCOMs* 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 Stati '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 *LANCOM* 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 *LANCOMs* zu verwenden. Wenn für ein *LANCOM* kein Paßwort eingegeben wurde, ist prinzipiell kein Schreibzugriff über SNMP erlaubt.

Beim Zugriff auf das *LANCOM* 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 Read-Only. 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 Read-Only. 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.

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

IP-Adresse	IP-Netz-Maske	Router-Name	Distanz
10.0.0.0	255.0.0.0	ROBERT	0
224.0.0.0	224.0.0.0	0.0.0.0	0
255.255.255.255	0.0.0.0	T-ONLINE	1

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 sechsten Spalte 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.

Die Management Information Base (MIB)

Um SNMP-Management-Systemen Zugriff auf die Konfiguration im *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 Diskette zu finden, als auch auf den ELSA Online-Medien.

Was ist los auf der Leitung? – Trace-Ausgaben

Zur Kontrolle der internen Abläufe im *LANCOM* 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 PPP angezeigt. Erfahrene Anwender können durch die Interpretation dieser Ausgaben evtl. Fehler beim Verbindungsaufbau aufspüren. Besonders positiv: Die aufzuspürenden Fehler können sowohl in der Konfiguration des eigenen *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
IPX-Rt.	IPX-Routing
RIP	IPX Routing Information Protocol
SAP	IPX Service Advertising Protocol
IPX-Wd.	IPX Watchdog-Spoofing
SPX-Wd.	SPX Watchdog-Spoofing
NetBIOS	IPX NetBIOS-Verwaltung
IP-Rt.	IP-Routing

Dieser Parameter ruft beim Trace die folgende Anzeige hervor:
IP-RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
SCRPT	Script-Verhandlung
IP-Masq	Vorgänge im Masquerading-Modul

Dieser Kombinations-Befehl ruft beim Trace die folgende Anzeige hervor:
All	alle Traceausgaben
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 elsa	Zeigt den Zustand der Verbindungsprotokolle PPP und ELSA 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.



So spielen Sie eine neue Software ein

Die Software zum *LANCOM* wird ständig weiterentwickelt. Damit Sie auch in den Genuß von neuen Features und Funktionen kommen, haben wir das *LANCOM* 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!

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

- Konfigurations-Tool *LANconfig*
- Terminal-Programme
- TFTP

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

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

LANconfig

Beim Konfigurations-Tool *LANconfig* markieren Sie das gewünschte *LANCOM* in der Auswahlliste und klicken auf **Bearbeiten ► Firmware-Upload** oder direkt die Schaltfläche **Firmware-Upload**. Dann wählen Sie das Verzeichnis, in dem sich die neue Version befindet, und klicken (nur einmal!) auf die entsprechende Datei. *LANconfig* informiert Sie dann in der Fußzeile über Versions-Nr. und Datum der Firmware und bietet das Upload an. Mit **Öffnen** ersetzen Sie die vorhandene Firmware durch die ausgewählte Version.

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

Terminal-Programme nutzen im Menü 'Sonstiges' den Befehl 'System-Upload'. Damit wird das *LANCOM* in Empfangsbereitschaft versetzt. Starten Sie anschließend den Upload-Vorgang von Ihrem Terminalprogramm aus:

- Bei *Telix* 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 **writelflash** eingespielt werden. Um eine neue Firmware, die in der Datei LCMPRGU.220 vorliegt, in ein LANCOM 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 lcmprgu.220 writelflash
```



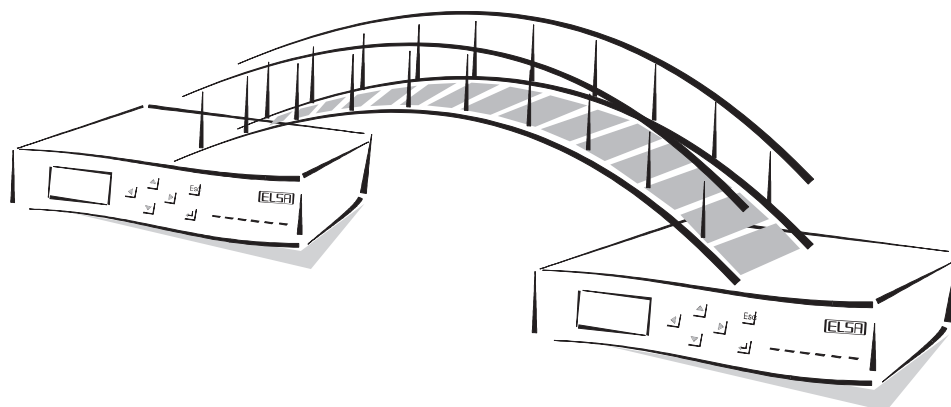
*Durch diesen Befehl wird die Datei „lcmprgu.220“ mit dem Kommando **writelflash** an das LANCOM gesendet. Dabei muß für TFTP die binäre Dateiübertragung eingestellt werden. Auf vielen Systemen ist jedoch das ASCII-Format voreingestellt. In diesem Beispiel für Windows NT erreichen Sie das durch den Parameter '-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 oder ein Fehler im Upload-File) 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 LANCOM einen Firmware-Upload über die serielle Schnittstelle.



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



LANCOM-Betriebsarten

Dieses Kapitel stellt Ihnen die drei verschiedenen Betriebsarten Ihres ISDN-Routers vor.

Wir zeigen Ihnen die unterschiedlichen Möglichkeiten und Anforderungen von Bridge, IP-Router und IPX-Router. Zusätzlich werden Sie sehen, welche Möglichkeiten zur Filterung von Daten es bei den einzelnen Konfigurationen gibt.

Neben der Beschreibung der Betriebsart geben wir Ihnen auch Hinweise, die Sie bei der Konfiguration unterstützen.

Bridge oder Router?	2
Die Brücke im Netz	4
Der IP-Router.....	6
Der IPX-Router	19

Bridge oder Router?

Das LANCOM kann als Bridge oder als Router arbeiten. Was aber ist der Unterschied zwischen den beiden, oder besser gefragt: Was macht eine Bridge, was ein Router?

Um die Unterschiede zu verstehen, müssen wir uns kurz mit dem OSI-Referenzmodell (auch 7-Schichten-Modell) beschäftigen. Dieses Modell gliedert die verschiedenen Aufgaben, die beim Transport von Informationen in einem Netzwerk oder zwischen mehreren Netzwerken anfallen, in sieben Bereiche oder Ebenen. Jede Ebene baut dabei auf die darunterliegende Schicht auf.

Weitere Informationen zum OSI-Modell finden Sie im Referenzteil des Handbuchs.

Für das Verständnis von Bridges oder Routern sind nur die drei untersten Schichten wichtig. In diesen drei Schichten wird folgendes geregelt:

- Schicht 1 (physikalische Schicht):

Hier wird der rein physikalische Transport der Daten vereinbart. Welche Kabel werden verwendet, und wie wird eine digitale Information aus Nullen und Einsen mit Hilfe der elektrischen Möglichkeiten dargestellt? Auf solche Fragen finden wir in der untersten Ebene die Antworten.

- Schicht 2 (Datensicherungs-Schicht):

Jetzt kommt etwas Ordnung in die Daten. Die einzelnen Bits werden auf dieser Ebene zu Einheiten zusammengefaßt. Das sind dann die Datenpakete oder auch Frames, von denen die Netzwerker immer reden. Die 2. Ebene sagt uns also, wieviele Bits z.B. zu einem Frame gehören.

Außerdem werden den Datenpaketen nun auch Adressen (von Absender und Adressat) zugewiesen, damit sie richtig weitergeleitet werden können. Mit Adressen sind hier die festen Adressen der einzelnen Netzwerk-Komponenten gemeint. Diese Adressen heißen auch Media-Access-Control (MAC)-Adressen, sind einmalig auf der Welt und fest in jeder Komponente verankert.

- Schicht 3 (Netzwerk-Schicht):

Die Organisation eines Netzwerks mit Hilfe der MAC-Adressen kann zuweilen etwas schwierig und unübersichtlich werden. So sieht man z.B. an der MAC-Adresse nicht, ob sich ein Server oder Arbeitsplatzrechner dahinter verbirgt oder zu welcher Arbeitsgruppe der Rechner gehört. Dazu werden auf der Netzwerkschicht Möglichkeiten vereinbart, auch logische Adressen zu verwenden, die vom Netzwerkbetreuer festgelegt werden. Der Administrator kann dann also Rechner zu Gruppen zusammenfassen, die man auch sehr einfach gemeinsam ansprechen kann.

Die 3. Schicht ist also die Ebene der Netzwerkprotokolle, wie z.B. IP oder IPX.

Eine Bridge verwendet bei der Adressierung der Datenpakete nur die physikalischen Adressen aus der 2. OSI-Ebene. Die Bridge ist unabhängig von den Protokollen der

schicht 3 (IP, IPX, Apple Talk ...) und kann daher Ethernet-Netzwerke mit beliebigen Protokollen auf Layer 3 verbinden.

Der zentrale Unterschied von Routern zur Bridge: Router verwenden logische Adressen zur Übertragung der Datenpakete. Logische Adressen werden – innerhalb bestimmter Adressierungs-Regeln – vom Systembetreuer nach logischen Gesichtspunkten vergeben, haben also mit den MAC-Adressen direkt nichts zu tun. Die Art der logischen Adressen wird in der dritten OSI-Ebene festgelegt, daher ist ein Router abhängig vom dort vereinbarten Netzwerk-Protokoll. Ein IP-Router arbeitet also mit anderen Adressen als ein IPX-Router.

Die Brücke im Netz

In der Betriebsart als Bridge überträgt das *LANCOM* alle Daten, deren MAC-Adresse nicht lokal zugeordnet werden können, zwischen einem lokalen Netz (LAN) und einem anderen LAN oder einem Arbeitsplatzrechner. Dabei lernt die Bridge relativ schnell, welche MAC-Adressen im eigenen Netz liegen und welche auf der anderen Seite gefunden wurden. Nach einem anfänglich recht hohen Datenverkehr, mit dem sich die beiden Netze bekanntmachen, geht die Netz-Last dann stark zurück, und die Verbindung wird nicht mehr so oft aufgebaut.

Mit der Bridge verbinden Sie die beteiligten Rechner so, als ob sie tatsächlich in einem Netz stehen würden. Daher sind aber auch nur solche Rechner zu verbinden, die theoretisch auch in ein Netz zu integrieren wären. Das heißt: Beide Netze bzw. das Netz und die Arbeitsplatzrechner müssen gleiche Netzwerkadressen haben.

Die Bridge ist unabhängig von dem auf Layer 3 verwendeten Protokoll. Sie arbeitet nur mit Ethernet-Adressen (MAC-Adressen). Achten Sie deshalb darauf, in der Layerliste nur solche B-Kanal-Protokolle zu verwenden, die in der Spalte ENCAPS die Einstellung ETHER haben.

Was müssen Sie zur Konfiguration der Bridge einstellen?

Zuerst legen Sie fest, auf welche Rufnummer das *LANCOM* hören und welche es selber nach außen weitergeben soll (Setup/WAN-Modul/Interface).

Damit das *LANCOM* die Gegenstelle erreichen kann, muß es in der Namenliste einen Eintrag mit Name und Rufnummer geben (Setup/WAN-Modul/Namenliste).

Da im *LANCOM* im Laufe der Zeit wahrscheinlich mehrere Gegenstellen eingetragen werden, teilen Sie der Brücke noch mit, welche denn jetzt die richtige ist (Setup/Bridge-Modul/Gegenstelle). Denn die Bridge verbindet genau zwei Netze miteinander, während ein Router mehrere Gegenstellen verwalten kann. Damit die Brücke funktioniert, müssen Sie sie dann auch einschalten (Setup/Bridge-Modul/Zustand:Ein).

Damit ist erst mal alles getan. Die Brücke überträgt nun fleißig alle Datenpakete für nicht lokale MAC-Adressen zur eingestellten Gegenstelle.



Weitere Hinweise zur Konfiguration des LANCOMs als Bridge finden Sie im entsprechenden Abschnitt im Workshop und in der ausführlichen Beschreibung der einzelnen Menüs im Referenz-Teil des Handbuchs.

Welche zusätzlichen Möglichkeiten gibt es?

Daß alle Daten übertragen werden, ist oft unerwünscht. Viele Daten, die sich im Netz tummeln, sind für entfernte Netze oder Workstations uninteressant. Daher können Sie folgende Datenpakete von der Übertragung ausschließen oder sie nur dann übertragen, wenn die Leitung ohnehin schon steht:

- Broadcast-Pakete: Daten, die sich an alle erreichbaren Geräte in einem Netz wenden (Setup/Bridge-Modul/LAN-Einstellung/Broadcast).
- Multicast-Pakete: Daten, die sich an alle erreichbaren Geräte einer Gruppe wenden (Setup/Bridge-Modul/LAN-Einstellung/Multicast).
- Unicast-Pakete: Das sind Daten, die nur an ein bestimmtes Gerät (also eine feste MAC-Adresse) gerichtet sind.

Für diese Daten können spezielle Filterlisten eingerichtet werden, in denen bestimmte Adressen von der Übertragung ausgeschlossen werden oder nur bestimmte Adressen zugelassen werden. Die Bridge-Filter unterscheiden dabei Ziel- und Quell-Adressen. Für beide Adreß-Typen können Sie zunächst festlegen, ob die zugehörige Tabelle die Adressen enthält, die übertragen werden sollen (Setup/Bridge-Modul/LAN-Einstellung/Ziel-Adresse/Filter-Typ/pos) oder die Adressen, die nicht übertragen werden sollen (.../Filter-Typ/neg). In der Tabelle selbst tragen Sie dann die MAC-Adressen ein, die gefiltert werden sollen.



Diese Filterung mit der genauen Angabe der MAC-Adressen verlangt natürlich auch einen gewissen Pflegeaufwand. Ändern sich die Adressen z.B. durch den Tausch einer Netzwerkkarte, dann müssen die neuen Adressen eingetragen werden, um die Funktion der Bridge aufrechtzuerhalten.

Der IP-Router

Der IP-Router arbeitet zwischen Netzen, die TCP/IP als Netzwerk-Protokoll verwenden. Dabei werden nur Daten übertragen, deren Zieladressen im Router eingetragen sind. Für einen IP-Router können bis zu 64 verschiedenen Gegenstellen als Ziele vereinbart werden.

IP-Adressierung

In TCP-IP-Netzen werden IP-Adressen zur Kommunikation zwischen verschiedenen Geräten verwendet. Um Irrtümer zu vermeiden, müssen die Adressen innerhalb eines zusammenhängenden Netzes eindeutig sein. Da auch das Internet mit seinen vielen Millionen angeschlossener Rechner auf TCP/IP aufsetzt und damit IP-Adressen verwendet, müssen auch alle Adressen im Internet eindeutig sein. Zur Kontrolle dieser öffentlich zugänglichen Adressen gibt es Stellen, die die IP-Adressen verwalten, verteilen und sich auch bezahlen lassen.

Damit eine Firma mit einem lokalen TCP-IP-Netzwerk aber nicht für jeden Arbeitsplatz eine IP-Adresse kaufen muß, sind bestimmte Bereiche der IP-Adressen für die private Verwendung reserviert (Private Address Spaces). Diese Adressen können in einem abgeschlossenen Netz beliebig benutzt werden, müssen nur wieder innerhalb dieses Netzes eindeutig sein und dürfen nicht nach außen (ins Internet) bekannt gemacht werden.

Wie sieht nun eine IP-Adresse aus? Sie besteht aus vier Bytes, die durch Punkte getrennt sind, insgesamt also aus 32 Bits. Jedes der vier Bytes kann Werte von 0 bis 255 annehmen, z.B. 192.168.130.124. In dieser Adresse ist sowohl die Adresse des Netzwerks enthalten als auch die des Rechners.

Wie unterscheidet man nun den Teil, der das Netz bestimmt, und den Teil, der den Rechner identifiziert? Mit Hilfe der Netzmaske. Masken kennen Sie alle: Die decken einen Teil von etwas ab und lassen nur den anderen Teil sichtbar werden. Genau so verhält es sich mit der Netzmaske. Das ist eine Zahl mit dem gleichen Aufbau wie die IP-Adresse, also 32 Nullen oder Einsen. Die Netzmaske fängt meistens vorne mit Einsen an und hört hinten mit Nullen auf. Die Nullen am Ende decken dabei den Teil der IP-Adresse ab, der nicht zur Netzadresse gehört. Beispiele:

Diese Adresse...	...in Bytes...	...sieht in Bits so aus:
IP-Adresse	192.168.120.253	11000000.10101000.01111000.11111101
Netzmaske	255.255.255.0	11111111.11111111.11111111.00000000
Netzwerk-Adresse	192.168.120.0	11000000.10101000.01111000.00000000

Diese Adresse...	...in Bytes...	...sieht in Bits so aus:
IP-Adresse	192.168.120.253	11000000.10101000.01111000.11111101
Netzmaske	255.255.0.0	11111111.11111111.00000000.00000000
Netzwerk-Adresse	192.168.0.0	11000000.10101000.00000000.00000000

Sie sehen also: eine IP-Adresse alleine ist noch nicht eindeutig. Mit verschiedenen Netzmasken gehören die Rechner in andere logische Netze. Und Sie sehen weiter: Je weniger Bits in der Netzmaske eine Eins enthalten, um so mehr Bits bleiben übrig zur Identifizierung der einzelnen Rechner. Während im ersten Beispiel mit der Netzmaske 255.255.255.0 nur 254 (die Endziffern '0' und '255' sind reserviert) verschiedene Adressen vergeben werden können, sind es im zweiten Beispiel schon $254 \times 254 = 64516$ verschiedene Adressen!

Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem *LANCOM*, an welche Gegenstelle (also welchen anderen Router oder Rechner) es die Daten für bestimmte IP-Adressen oder IP-Adressbereiche 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 (siehe auch 'Dynamisches Routing mit IP-RIP' auf Seite 1.4.12). 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 *LANCOM* in der IP-Routing-Tabelle noch, 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 ISDN-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 (siehe auch 'Proxy-ARP' auf Seite 1.4.11) 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.

So sieht eine IP-Routing-Tabelle also z.B. aus:

IP-Adresse	IP-Netzmaske	Router-Name	Distanz
192.168.120.0	255.255.255.0	LANCOM01	2
192.168.125.0	255.255.255.0	LANCOM02	3
192.168.130.0	255.255.255.0	191.168.140.123	0

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 das *LANCOM*, ob das Paket in das Zielnetz gehört.

■ Router-Name

An diese Gegenstelle überträgt das *LANCOM* 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 das eigene *LANCOM* die Gegenstelle nicht selbst erreichen, steht hier die IP-Adresse eines anderen Routers, der den Weg ins Zielnetz kennt.

■ Distanz

Anzahl der zwischen *LANCOM* und Ziel liegenden Routern. Dieser Wert wird 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 über das ISDN-Netz 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 Kanal 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.

■ 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, daß über IP-Masquerading (siehe auch 'IP-Masquerading (Single User Access, NAT, PAT)' auf Seite 1.4.15) nur mit einer IP-Adresse nach außen hin sichtbar ist.
- Router-Name 0.0.0.0: Ausschluß-Routen. Datenpakete für diese „Null-Routen“ werden vom *LANCOM* 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:
10.0.0.0	255.0.0.0	0.0.0.0	0	Schließt die Übertragung aller Datenpakete in 10er-Netze aus.
192.168.120.0	255.255.255.0	LANCOM01	2	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.120.x werden an Lancom01 übertragen.
192.168.125.0	255.255.255.0	LANCOM02	3	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.125.x werden an Lancom02 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.
192.168.1.9	255.255.255.255	AUSSENDIENST	2	Die Gegenstelle AUSSENDIENST ist unter der IP-Adresse 192.168.1.9 zu erreichen.
255.255.255.255	0.0.0.0	INTERNET	2	Alle Datenpakete, die nicht den zuvorstehenden Einträgen zugeordnet werden können, werden an die Gegenstelle INTERNET übertragen.



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

Was passiert bei der Datenübertragung im IP-Netz?

Wenn ein Gerät in einem IP-Netz ein Datenpaket an ein anderes Gerät schicken möchte, braucht es dazu seine physikalische MAC-Adresse. Mit Hilfe der IP-Adresse und der Netzmaske kann es herausfinden, ob sich das Ziel im gleichen Netz wie das sendende Gerät selbst befindet. Wenn das so ist, fragt es zunächst einmal bei allen Geräten im Netz nach, welche MAC-Adresse hinter der gewünschten IP-Adresse steckt. Diese Rundfrage nennt man auch ARP-Request (Address Resolution Protocol Request). Wenn die Antwort darauf eintrifft, weiß das sendewillige Gerät, an welche MAC-Adresse es das Datenpaket schicken muß. Außerdem merkt es sich diese Zuordnung von IP- und MAC-Adresse für das nächste Mal in seiner internen ARP-Tabelle, um so unnötige Anfragen zu verhindern und das Netz zu entlasten.

Findet der Sender mit Hilfe der Netzmasken jedoch heraus, daß das Ziel in einem anderen Netz steht, muß ein Router her. Der Router muß dazu eine IP-Adresse im gleichen Netz

wie der Absender haben, damit dieser ihn überhaupt erreichen kann. Auf die Anfrage nach einer IP-Adresse, zur der das *LANCOM* eine Route kennt, antwortet das *LANCOM* mit seiner eigenen IP-Adresse. Das *LANCOM* kennt die Routen zu anderen IP-Adressen aus der Routing-Tabelle, in der hinterlegt ist, welche Datenpakete wohin geschickt werden. Die Routing-Tabelle sieht z.B. so aus:

IP-Adresse	IP-Netzmaske	Router-Name	Distanz
192.168.120.0	255.255.255.0	LANCOM01	2
192.168.125.0	255.255.255.0	LANCOM02	2
192.168.130.0	255.255.255.0	192.168.140.123	0

Empfängt der Router (mit IP-Adresse 192.168.110.50, Netzmaske 255.255.255.0) nun ein Paket mit der Ziel-Adresse 192.168.125.123, so erkennt er, daß diese Adresse in einem anderen Netz liegt. Deshalb sucht er in der Routing-Tabelle von oben nach unten nach einer IP-Adresse für das passende Zielnetz. In diesem Beispiel wäre das der zweite Eintrag, der das Ziel-Netz 192.168.125.0 enthält. Der Eintrag in der Spalte 'Router-Name' zeigt an, unter welchem Namen in der Namenliste das *LANCOM* nun die Informationen für den Verbindungsaufbau findet, der Eintrag der Distanz zeigt an, wieviele Router auf dem Weg zu passieren sind.

Wenn der Router das Ziel über eine ISDN-Verbindung direkt erreichen kann, steht die Distanz auf '2'. Wenn der Router eine Verbindung aufgebaut hat, wird die Distanz auf '1' herabgesetzt. Damit können die Router (über IP-RIP, siehe auch 'Dynamisches Routing mit IP-RIP' auf Seite 1.4.12) in einem Netz untereinander Informationen darüber austauschen, welches Gerät schon eine Verbindung zu einer Gegenstelle aufgebaut hat, die vielleicht auch von anderen Geräten genutzt werden kann.

Findet der Router im Feld 'Router-Name' eine IP-Adresse (und keinen Gegenstellen-Namen) wie im letzten Eintrag des Beispiels, dann ist dieser Router nicht für das Zielnetz zuständig und leitet die Pakete an die eingetragene IP-Adresse weiter.

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' auf Seite 3.3.14). Die Quell-Ports hingegen werden in bestimmten Bereichen frei gewählt.

Das *LANCOM* kann sich i.d.R. die Ziel-Ports von solchen Datenpakete ansehen, die TCP oder UDP als Protokoll verwenden. Aus diesen Ziel-Ports kann es dann ableiten, für wel-

chen 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 Datenpakete für bestimmte Portbereiche 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).

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 ISDN 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 lokalen 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 auf der Registerkarte 'IP-Router' oder im Menü setup/IP-Router-Modul bei anderen Konfigurationsmöglichkeiten).

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

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

Da das LANCOM 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.

Das LANCOM 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 LANCOM geschickt, das die Daten zum Rechner auf der anderen Seite der ISDN-Verbindung weiterleitet.

Lokales Routing

In den vorhergehenden Abschnitten haben Sie folgendes Verhalten der Arbeitsplatzrechner in einem lokalen Netz kennengelernt: 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 unbekannten IP-Adressen erreichen können soll. Manchmal kann dieser Standard-Router jedoch selbst das Zielnetz nicht erreichen, er kennt aber einen anderen Router, der zu diesem Ziel findet.

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

Standardmäßig schickt das *LANCOM* 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 (*Setup* / *IP-Router-Modul* / *Lok. -Routing: Ein*). Dadurch weisen Sie das *LANCOM* 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 (siehe auch 'Die IP-Routing-Tabelle' auf Seite 1.4.7) gibt es im *LANCOM* auch eine dynamische Routing-Tabelle mit bis zu 128 Einträgen. Diese Tabelle füllen Sie im Gegensatz zu der statischen nicht selbst aus, das erledigt das *LANCOM* selbst. Dazu nutzt das *LANCOM* 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 *LANCOM* 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 (siehe auch 'Proxy-ARP' auf Seite 1.4.11).

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

- Solange das *LANCOM* 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 *LANCOM* eine bestehende Verbindung zu dieser Gegenstelle genutzt werden kann. So können also Gebühren gespart werden oder zusätzliche Verbindungsaufbauten von Routern verhindert werden, die ebenfalls eine Route zum Ziel kennen.
- Wenn darüber hinaus in diesem *LANCOM* 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 *LANCOM* neben der bestehenden Verbindung keine weitere aufbauen kann, liegt an einer der folgenden Ursachen:
 - Auf dem anderen Kanal ist schon eine andere Verbindung hergestellt.
 - Die Y-Verbindungen für den S₀-Anschluß sind in der Interface-Tabelle ausdrücklich ausgeschlossen.
 - Die bestehende Verbindung benutzt beide B-Kanäle (Kanalbündelung).
 - Bei der bestehenden Verbindung handelt es sich um eine Festverbindung. Dann kann parallel dazu keine Wählverbindung aufgebaut werden.



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

RIP-fähige Router versenden die RIP-Pakete ungefähr alle 30 Sekunden. Das *LANCOM* ist nur dann auf das Versenden und Empfangen von RIPs eingestellt, wenn es 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 das *LANCOM* aus empfangenen IP-RIP-Paketen?

Wenn das *LANCOM* solche IP-RIP-Pakete empfängt, baut es 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 min wird die Distanz auf '16' gesetzt (Route nicht erreichbar), nach 5,5 min wird die Route gelöscht.

Wenn das *LANCOM* nun ein IP-RIP-Paket empfängt, muß es entscheiden, ob es die darin enthaltenen Routen in seine dynamische Tabelle aufnehmen soll oder nicht. Dazu geht es 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 Distanz 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, siehe unten), dann glaubt das *LANCOM* 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 das *LANCOM* sich dann die eigentliche IP-Routing-Tabelle zusammen, mit der es den Weg für die Datenpakete bestimmt. Dabei nimmt es zu den Routen aus der eigenen statischen Tabelle die Routen aus der dynamischen Tabelle auf, die es 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 Verbindun-

gen aufgebaut. Um das zu vermeiden, kann der RIP-Port sowohl in der WAN- als auch in der LAN-Filtertabelle 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.

Weitere Hinweise zur Skalierung von mehreren LANCOMs in einem Netz finden Sie im Workshop.



IP-Masquerading (Single User Access, 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 Eingriffe aus dem Internet auf das lokale Netz.

Zwei Adressen für das LANCOM

Bei Masquerading treffen zwei gegensätzliche Forderungen an das LANCOM aufeinander: Zum einen soll es eine im lokalen Netz gültige IP-Adresse haben, damit es aus dem LAN erreichbar ist, zum anderen soll es 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. Das LANCOM bekommt also nun eine **Internet**-Adresse und eine **Intranet**-Adresse, jeweils natürlich mit passender Netzmaske. Mit dem Einschalten der Option 'Masquerading' in der Routing-Tabelle informieren Sie das LANCOM darüber, welche der beiden Adressen es bei der Weitergabe der Pakete verwenden soll.

Mit dem Eintrag der Internet-Adresse (in der LANCOM-Software auch IP-Adresse) beeinflussen Sie maßgeblich das Verhalten bei der Maskierung.

- IP-Adresse '0.0.0.0' und IP-Netz-Maske '0.0.0.0': Mit diesem Eintrag fordern Sie von Ihrem Provider die Zuweisung einer im Internet gültigen IP-Adresse an, die Sie im weiteren für die Verbindung und die Maskierung verwenden wollen.

- 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 des *LANCOM* 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 *LANCOM* 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.

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 das *LANCOM* nun ein Datenpaket zur Übertragung, merkt es sich die IP-Adresse und den Port des Absenders in einer internen Tabelle. Dann gibt das *LANCOM* 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 des *LANCOMs* mit der neuen Absender-Portnummer. Mit dem Eintrag in der internen Tabelle kann das *LANCOM* diese Antwort nun wieder dem ursprünglichen Absender zuordnen.

In den Statistiken des LANCOMs können Sie sich diese Tabellen genau ansehen (siehe auch 'Status' auf Seite 3.1.3).



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 *LANCOMs* maskiert (einfaches Masquerading).

Schickt umgekehrt ein Rechner aus dem Internet ein Paket z.B. an einen FTP-Server im Intranet, so werden aus der Sichtweise des FTP-Servers alle Adressen aus dem Internet hinter der IP-Adresse des *LANCOMs* versteckt (inverses Masquerading).

Der kleine Unterschied:

- Der Zugriff von außen auf einen Dienst (Port) im Intranet muß vorher durch Angabe einer Port-Nr. 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 das *LANCOM* selbst vorgenommen.

Die entsprechende Tabelle kann max. 32 Einträge aufnehmen, also **gleichzeitig** 32 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

Nach einer einstellbaren Zeit geht das *LANCOM* jedoch davon aus, daß der Eintrag nicht mehr benötigt wird und löscht ihn selbständig wieder aus der Tabelle. Dadurch können auch mehr als 32 Arbeitsplatzrechner ohne allzu lange Wartezeiten z.B. auf das Internet zugreifen.

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 das *LANCOM* 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.elsa.de' verbirgt? Der DNS-Server!

DNS heißt Domain Name Service und bezeichnet die Zuordnung von Domain-Namen (wie elsa.de) 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 die Homepage von ELSA aufrufen möchte, sendet er zunächst einen DNS-Request aus: „Welche IP-Adresse gehört zu www.elsa.de?“ Wenn das *LANCOM* bei den Arbeitsplatzrechnern als DNS-Server eingetragen ist, wird diese Anfrage folgendermaßen behandelt:

- Das *LANCOM* sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist. Wird es dort fündig, baut es eine Verbindung zu diesem Server auf und holt die gewünschte Information.
- Gibt es keinen eingetragenen DNS-Server im *LANCOM*, versucht das *LANCOM* 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 das *LANCOM* 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 *LANCOMs* als DNS-Server bei den Ar-

beitsplatzrechnern 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 das *LANCOM* stets die aktuellen Informationen.

Zugangskontrolle

Mit einer speziellen Filterliste kann der Zugriff auf die internen Funktionen des *LANCOMs* über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Telnet- oder TFTP-Sitzungen zur Konfiguration des *LANCOMs* 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 das *LANCOM* 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 des *LANCOMs* zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen.

Policy Based Routing

Das 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 eines *LANCOMs* über das WAN erleichtern, wenn gleichzeitig viele Daten übertragen werden sollen.



Weitere Informationen zum Policy Based Routing finden Sie in der 'Beschreibung der Menüpunkte' auf Seite 3.1.1.

Der IPX-Router

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 das *LANCOM* 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 das *LANCOM* die Adresse und das Binding selbst. Dazu sucht es sich auf dem angeschlossenen Kabel das Netz aus, auf dem es die meisten SAP-Replies erhält.

IPX-Routing-Tabelle

In der IPX-Routing-Tabelle sagen Sie dem *LANCOM*, 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 Services 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' auf Seite 1.4.22).

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 im *LANCOM* fertig konfiguriert ist und eingeschaltet wird, baut das *LANCOM* zunächst einmal zu allen über die Routing-Tabellen erreichbaren Gegenstellen Verbindungen auf und tauscht dann mit diesen Netzen SAP- und RIP-Informationen aus. Das *LANCOM* 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 das *LANCOM* 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 das *LANCOM* anhand der Tabellen den Weg mit den wenigsten Tics und dem kleinsten Hop-Count 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 eine 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 **LANCOMs** hier...

Ist in einem Netz der Aufbau zu mehr als drei Gegenstellen gleichzeitig erwünscht, reichen die beiden B-Kanäle und die serielle Schnittstelle am **LANCOM** nicht mehr aus. 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 **LANCOM** dann auch die gleichen Routing-Informationen übermittelt, allerdings mit höherem Tic- und Hop-Count. Dadurch werden diese Routen quasi als Reserve markiert, wenn auf dem angesprochenen **LANCOM** alle Kanäle besetzt sind.

Redundante Routen

Empfängt ein **LANCOM** mit einem RIP-Paket Informationen über Routen mit gleichem Tic- und Hopcount wie die eigenen Routen (redundante Routen), muß es dem Absender diese Routen natürlich nicht selbst wieder bekanntgeben. Das **LANCOM** 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 **LANCOM** 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 Verbindungsaufbauten gestartet werden und spart damit Gebühren.

Gelingt der erste Verbindungsversuch zu einer Gegenstelle nicht, versucht das **LANCOM** 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 eine 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 das LANCOM 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 das *LANCOM* von anderen Routern gelernt hat. Das *LANCOM* lernt dabei sowohl von Routern aus lokalen als auch aus entfernten Netzen. Alle verfügbaren Routing-Informationen trägt das *LANCOM* 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. Das *LANCOM* 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 das *LANCOM* 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) des LANCOMs 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 das *LANCOM* 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 von unserem *LANCOM* 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 wird.

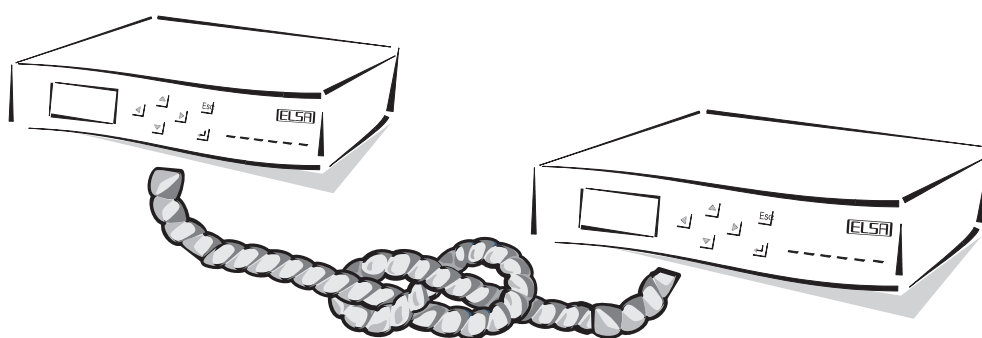
■ IPX- und SPX-Watchdogs:

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. Das *LANCOM* 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' auf Seite 3.1.42.



Feste Verbindungen

Für häufig benutzte Strecken kann die Nutzung einer Festverbindung wirtschaftlich sein. In Deutschland werden mehrere Festverbindungsarten mit und ohne D-Kanal zu unterschiedlichen Konditionen angeboten.

Die folgenden Abschnitte zeigen kurz die verschiedenen Arten auf. Anschließend geben wir Ihnen Hinweise zur Konfiguration des *LANCOMs* für den Betrieb an Festverbindungen. Den Abschluß bildet die Einrichtung einer Backup-Verbindung als Sicherheit für die Festverbindung.

Ein oder zwei Kanäle, mit oder ohne D-Kanal?	2
So stellen Sie die Festverbindung ein	3
Die Backup-Leitung	7

Ein oder zwei Kanäle, mit oder ohne D-Kanal?

Wird tagsüber 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-Leistungsverhältnis.

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. Die Wahl einer GRP2-Festverbindung zu entsprechend höheren Kosten scheint nur sinnvoll, falls der dabei vorhandene D-Kanal unabhängig von der *LANCOM*-Verbindung für weitere ISDN-Dienste genutzt werden soll.

Zur Zeit werden in Deutschland drei verschiedene Varianten von ISDN-Festverbindungen ohne D-Kanal (Gruppe 0) angeboten:

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 *LANCOM* als Gruppe-0-Festverbindung in der Interface-Tabelle (/Setup/WAN-Modul/Interface) eingestellt. Unterschieden werden die Varianten durch das „YV-Flag“ in der Interface-Tabelle bzw. durch den Eintrag 'Layer-2-Optionen' in der Layerliste. Festverbindung werden ausschließlich auf dem internen S₀-Interface unterstützt.

Zusätzlich gibt es zwei Varianten von ISDN-Festverbindungen mit D-Kanal (Gruppe 2):

Festverbindung	Ausführung
(T)S01	Ein B-Kanal, ein D-Kanal
(T)S02	Zwei B-Kanäle, ein D-Kanal

Weiterhin existiert an älteren 1TR6-Anschlüssen die Möglichkeit einer pauschal abgerechneten Dauerwählverbindung, der „semipermanenten Verbindung“. Diese muß, nach Einrichtung durch die Telekom, im *LANCOM* durch ein der Rufnummer nachgestelltes „S“ aktiviert werden.

So stellen Sie die Festverbindung ein

Die folgenden Einstellungen sind erforderlich, um das *LANCOM* auf den Betrieb an den verschiedenen Festverbindungen vorzubereiten.

Einstellungen in der Interface-Tabelle

D64S (ein B-Kanal, kein D-Kanal)

- In der Interface-Tabelle wird als Protokoll **Grp0** eingegeben.
- Als FV-Mode wird ein Gerät als **Master**, das andere als **Slave** konfiguriert.
- Als **B-Kanal** wird der verwendete Kanal (1 oder 2) angegeben. Diese Angabe muß bei beiden Geräten gleich sein.
- Das **YV-Flag** muß den Wert **Aus** besitzen.
- Im verwendeten Layer wird als Layer-2-Option **compr.** oder **keine** eingetragen.

D64S2 (zwei B-Kanäle, kein D-Kanal, eine Gegenstelle)

- In der Interface-Tabelle wird als Protokoll **Grp0** eingegeben.
- Als FV-Mode wird ein Gerät als **Master**, das andere als **Slave** konfiguriert.
- Als **B-Kanal** wird der verwendete Hauptkanal (1 oder 2) angegeben. Diese Angabe muß bei beiden Geräten gleich sein. Der Haupt-Kanal ist der Kanal, auf dem die erste Verbindung aufgebaut wird.
- Das **YV-Flag** muß den Wert **Aus** besitzen.
- Im verwendeten Layer wird als Layer-2-Option **buendeln** oder **bnd+compr** eingetragen.

D64SY (zwei B-Kanäle, kein D-Kanal, zwei Gegenstellen)

- In der Interface-Tabelle wird als Protokoll **Grp0** eingegeben.
- Als FV-Mode wird das Gerät, daß zwei Verbindungen aufbauen soll, als **Master**, die anderen als **Slave** oder umgekehrt (ein Slave, zwei Master) konfiguriert. Eine unterschiedliche Master/Slave-Konfiguration für die zwei Gegenstellen ist nicht möglich. Hierdurch ergibt sich, daß eine „Dreiecks-Konfiguration“ nicht möglich ist
- Die Einstellung im Feld **B-Kanal** wird ignoriert. Für die Gegenstellen ist jeweils eine einfache **D64S** auf dem entsprechenden B-Kanal zu konfigurieren. Falls bei einer Gegenstelle der zweite Kanal ebenfalls zu einer anderen Gegenstelle führt, so kann dort auch wieder eine D64SY eingestellt werden. Zu beachten ist nur, daß eine „Dreiecks-Konfiguration“ nicht möglich ist.
- Das **YV-Flag** muß den Wert **Ein** besitzen.
- Im verwendeten Layer wird als Layer-2-Option **compr.** oder **keine** eingetragen. Eine eingetragene Bündelungs-Option wird automatisch beim Verbindungsaufbau unterdrückt.

(T)S01 (ein B-Kanal, ein D-Kanal)

- In der Interface-Tabelle wird als Protokoll **Grp2** eingegeben.
- Als FV-Mode wird ein Gerät als **Master**, das andere als **Slave** konfiguriert.
- Als **B-Kanal** wird der verwendete Hauptkanal (1 oder 2) angegeben. Diese Angabe muß bei beiden Geräten gleich sein. Der Haupt-Kanal ist der Kanal, auf dem die erste Verbindung aufgebaut wird.
- Das **YV.-Flag** muß den Wert **Aus** besitzen.
- Im verwendeten Layer wird als Layer-2-Option **compr.** oder **keine** eingetragen. Eine eingetragene Bündelungs-Option wird automatisch beim Verbindungsaufbau unterdrückt.

(T)S02 (zwei B-Kanäle, ein D-Kanal)

- In der Interface-Tabelle wird als Protokoll **Grp2** eingegeben.
- Als FV-Mode wird ein Gerät als **Master**, das andere als **Slave** konfiguriert.
- Als **B-Kanal** wird der verwendete Hauptkanal (1 oder 2) angegeben. Diese Angabe muß bei beiden Geräten gleich sein. Der Haupt-Kanal ist der Kanal, auf dem die erste Verbindung aufgebaut wird.
- Das **YV.-Flag** muß den Wert **Aus** besitzen.
- Im verwendeten Layer wird als Layer-2-Option **buendeln** oder **bnd+cmpr** eingetragen.

Einstellungen in der Namenliste**D64S, D64S2, D64SY**

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

Soll ein anderer Layer oder der Dial-Backup-Mechanismus verwendet werden, so muß die Gegenstelle in der Namenliste auftauchen und mit einem 'F' im Feld Rufnummer als Festverbindungs-Gegenstelle gekennzeichnet werden. Bei einer D64S- oder einer D64S2-Festverbindung genügt diese Angabe, da es bei diesen Einstellungen nur eine Gegenstelle geben kann.

Geraetenname	Rufnummer	B1-HZ	B2-HZ	Layername	Rueckruf
FVG0	F1234	20	0	PPPHDL	Aus

Ist jedoch D64SY konfiguriert, so wird zusätzlich eine B-Kanal-Angabe benötigt, um sowohl einen Layer als auch evtl. eine Backup-Rufnummer der Gegenstelle zuordnen zu können. Die Kanalangabe folgt direkt dem 'F' in Form einer dezimalen Ziffer, die von ei-

nem Doppelpunkt abgeschlossen wird. Diese Angabe wird nur bei einer D64SY ausgewertet. Bei einer D64S-Festverbindung gilt der Eintrag in der Interface-Tabelle.

Im Anschluß an das 'F' (D64S, D64S2) bzw. hinter die Kanalvorgabe 'Fx:' (D64SY) kann die Rufnummer für eine Backup-Verbindung über ein Gerät an der seriellen Schnittstelle (s.u.) eingetragen werden.

Geraetenname	Rufnummer	B1-HZ	B2-HZ	Layername	Rueckruf
FVG0-B1	F1:	0	0	X75compr	Aus
FVG0-B2	F2:123456	20	0	PPPHDL	Aus

(T)S01, (T)S02

Für Festverbindungen der Gruppe 2 muß dem Gerät auf der Gegenseite über den D-Kanal signalisiert werden, daß ein Verbindungswunsch vorliegt. Das erfolgt über das Wählen einer beliebigen Nummer. Dazu ist bei beiden Geräten in der Namenliste ein Eintrag für die jeweilige Gegenstelle mit einer beliebigen Rufnummer aufzunehmen. Damit erfolgt der Verbindungsaufbau automatisch, sobald ein Paket übertragen werden soll.

Geraetenname	Rufnummer	B1-HZ	B2-HZ	Layername	Rueckruf
DEFAULT	1	0	0	DEFAULT	Aus

Einstellungen in der Layer-Liste

D64S, D64S2, D64SY

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	ETHER	ELSA	X.75LAPB	compr.	HDL

(T)S01, (T)S02

Für Festverbindungen der Gruppe 2 wird die Auswahl des Layers über den Eintrag in der Namenliste vorgenommen. Dabei kann natürlich auch der DEFAULT-Layer verwendet werden.



Wird für den Verbindungsaufbau kein ELSA-Protokoll verwendet, muß der Layer mit dem Namen 'DEFAULT' mit den gewünschten B-Kanal-Optionen angepaßt werden, da bei Festverbindungen die anrufende Gegenstelle nicht über die CLIP erkannt werden kann.

Die Backup-Leitung

Mit dem Anschluß eines ISDN-Terminal-Adapters oder eines analogen Modems an die serielle Schnittstelle des *LANCOMs* eröffnet sich die Möglichkeit einer Backup-Leitung für Festverbindungen. Damit gewinnen sehr wichtige Datenleitungen ein weiteres Stück an Sicherheit gegen den Ausfall der Verbindung.

Wann wird die Backup-Verbindung aktiviert?

Die gesicherten Protokolle X.75LAPB, X.75ELSA und PPP prüfen in regelmäßigen Abständen, ob die Gegenstelle noch aktiv ist. Wenn die Gegenstelle eine längere Zeit nicht antwortet, oder die Leitung defekt ist, so wird die Verbindung getrennt. Danach wird versucht, die Verbindung zur Gegenstelle erneut zu etablieren. Wenn dies nach einer einstellbaren Zeit von 10...999 Sekunden nicht zum Erfolg geführt hat, dann tritt der Backup-Mechanismus in Kraft. Hierbei wird versucht, die Verbindung zur Gegenstelle über die externe Schnittstelle aufzubauen.

Gleichzeitig wird weiter versucht, die Gegenstelle erneut über den internen S_0 -Bus zu erreichen. Sobald die Verbindung wieder hergestellt ist, wird die Backup-Verbindung wieder getrennt.

Die Backup-Leitung hat alle Eigenschaften einer normalen Wählleitung, z.B. Haltezeiten, nach deren Ablauf die Verbindung beendet wird, wenn keine Daten mehr fließen. Zusätzlich hat diese Verbindungsart die besondere Eigenschaft, normale Wählverbindungen auf der seriellen Schnittstelle beenden zu können, wenn die Leitung benötigt wird. Sie ist also quasi immer verfügbar.

Einstellungen für den Backup-Betrieb

Folgende Einstellungen sind notwendig, um die serielle Schnittstelle als Backup-Leitung für eine Festverbindung zu aktivieren:

- In der Interface-Tabelle wird die serielle Schnittstelle mit den an- und abgehenden MSNs eingetragen:

Ifc	Protokoll	EAZ	MSN-an	MSN-ab	FV-Mode	B-Kanal	YV.
S0	GRPO	0			Master	2	Aus
Ser1	DSS1	0	123456	123456	Master	1	Ein

- In der Namenliste wird für die Gegenstelle ein F (für Festverbindung) eingetragen, gefolgt von der (ersten) Rufnummer der Gegenstelle, die über das Gerät an der seriellen Schnittstelle im Backup-Fall angewählt werden soll. Weitere Rufnummern bzw. Durchwahlen für die Wahl über die serielle Schnittstelle werden wie gewohnt

in der Round-Robin-Liste eingetragen (siehe auch 'RoundRobin-Liste' auf Seite 3.1.30):

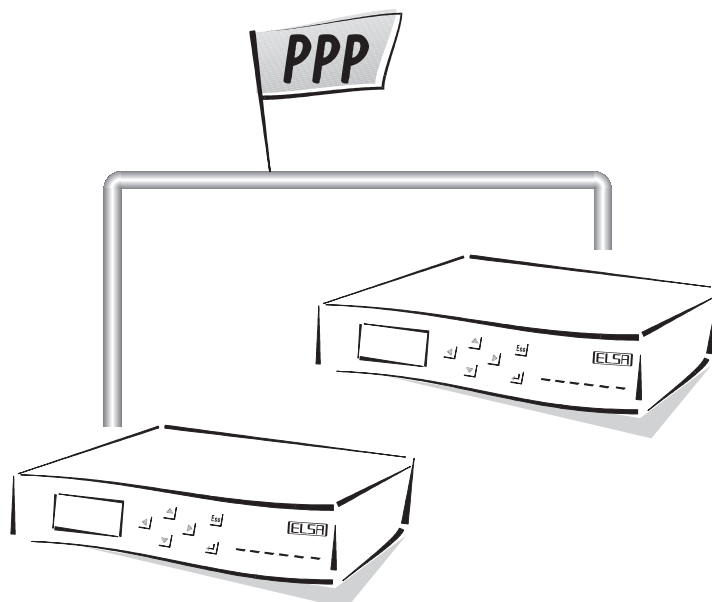
Geraetenname	Rufnummer	B1-HZ	B2-HZ	Layername	Rueckruf
AACHEN	F12345	180	180	MY_LAYER	Aus

In diesem Fall wird die Gegenstelle 'AACHEN' für die Festverbindung benutzt. Es wird der angegebene Layer 'MY_LAYER' und bei Festverbindung Gruppe 2 die Haltezeiten verwendet. Bei einer Festverbindung Gruppe 0 werden die Haltezeiten ignoriert.

Im Backup-Fall wird dann eine Verbindung zur Gegenstelle 'AACHEN' über die externe Schnittstelle aufgebaut. Hierzu wird die in der Namenliste angegebene Rufnummer, sowie die in der Namenliste angegebenen Haltezeiten und Layer verwendet.



Wenn an der externen Schnittstelle ein analoges Modem angeschlossen ist, müssen die Einstellungen von 'MY_LAYER' und 'V.24_DEF' übereinstimmen.



Point-to-Point Protocol

Wie im Kapitel 'Übertragungsprotokolle' auf Seite 1.2.11 erwähnt, unterstützt das *LANCOM* 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. PPP wird im *LANCOM* sowohl mit dem IP-Router als auch mit dem IPX-Router verwendet.

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

Das Protokoll	2
Die PPP-Liste	4
Alles o.k.? Leitungsüberprüfung mit LCP	5
Zuweisung von IP-Adressen	6
Rückruf-Funktionen	7

Das Protokoll

Was ist PPP?

Das Point-to-Point Protokoll (PPP) wurde speziell für Netzwerkverbindungen über serielle Kanäle entwickelt und hat sich als Standard für Verbindungen zwischen ISDN-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 Link Control Protocol (LCP)

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 einem gemeinsamen Nenner über standardisierte Steuerungsprotokolle (LCP, IPCP, IPXCP), die im PPP enthalten sind.

Wozu wird PPP verwendet?

Das Point-to-Point-Protokoll 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 *LANCOM* implementierte PPP kann sowohl über eine transparente HDLC-Verbindung (synchrones PPP) als auch über eine X.75- oder Modem-Verbindung (nur V.24) verwendet werden (asynchrones PPP).

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 Link Control Protokoll (LCP).

Es wird festgestellt, ob die Gegenstelle auch bereit ist, PPP zu benutzen, die Paketgrößen und das Authentifizierungsprotokoll (PAP, CHAP oder keines) werden festge-

legt. Danach wechselt das LCP in den „Opened“ Zustand (siehe auch 'Status/PPP-Statistik' auf Seite 3.1.7).

■ 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 *LANCOM* sind die Protokolle IPCP (IP Control Protocol) und IPXCP (IPX Control Protocol) 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, wechselt das PPP von der „Establish-Phase“ in die „Network-Phase“ und es können von den Router-Modulen IP- und/oder IPX-Pakete auf der geöffneten Leitung übertragen werden.

■ Terminate-Phase

In der letzten Phase wird die Leitung geschlossen.

Die PPP-Verhandlung im *LANCOM*

Der Verlauf einer PPP-Verhandlung wird in der PPP-Statistik des *LANCOM* 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.

Für den Remote-Access über PPP via ISDN-Terminal-Adapter oder ISDN-PC-Karte und einen Rechner mit Windows 95 oder Windows NT existieren ausführliche Solution-Guides in den Online-Medien, die als Leitfaden bei der Konfiguration solcher Verbindungen dienen können.

Die PPP-Liste

In der PPP-Liste können wir für jede Gegenstelle, die mit unserem *LANCOM* Kontakt aufnimmt, eine eigene Definition der PPP-Verhandlung festlegen.

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

In dieser Spalte der PPP-Liste tragen Sie folgende Werte ein:
Gerätename	Name der Gegenstelle, mit dem sie sich bei Ihrem <i>LANCOM</i> anmeldet
Sicherung	Verfahren zur Sicherung der PPP-Verbindung ('PAP', 'CHAP' oder 'keine'). Ihr eigenes <i>LANCOM</i> 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 <i>LANCOM</i> an die Gegenstelle übertragen wird (falls gefordert). * in der Liste zeigen an, daß ein Eintrag vorhanden ist.
Zeit	Zeit zwischen zwei Überprüfungen der Verbindung. Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z.B. 2 für 20 Sek.). Dieser Parameter wird nur bei der Sicherung nach CHAP verwendet. Für Gegenstellen mit Windows 95 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.
Conf, Fail, Term	Mit diesen Parametern wird die Arbeitsweise des PPP 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 <i>LANCOMs</i> Hinweise zur Behebung der Störung. Im Allgemeinen sind die Default-Einstellungen ausreichend. Diese Einstellungen können nur mit dem Konfigurations-Tool <i>LANconfig</i> verändert werden!
Username	Name, mit dem sich Ihr <i>LANCOM</i> bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Gerätenamen Ihres <i>LANCOMs</i> verwendet.

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 Link Control Protokolls (LCP) 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 über einen ISDN-Terminal-Adapter an der seriellen Schnittstelle des *LANCOMs* gefunden werden (siehe auch 'Die Backup-Leitung' auf Seite 1.5.7).



Beim Remote-Access von einzelnen Arbeitsplatzrechnern mit Windows 95 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 wir in der PPP-Liste für jede Verbindung einzeln ein. Mit dem Eintrag in die Felder 'Zeit' und 'Wdh.' legen wir 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 wir die LCP-Requests ganz ab.

Zuweisung von IP-Adressen

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 das *LANCOM* ihm für die Dauer der Verbindung eine IP-Adresse zuweisen und so die Kommunikation ermöglichen.



Die Zuweisung einer IP-Adresse wird nur dann möglich, wenn das 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 *LANCOM* anmelden muß.

Neben der IP-Adresse werden der Gegenstelle bei dieser Konfiguration auch die Adressen der DNS- und NBNS-Server (**D**omain **N**ame **S**erver und **N**et**B**IOS **N**ame **S**erver) incl. 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 Namens-Server (DNS und NBNS) vom *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 das *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 das *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 das *LANCOM* während der PPP-Verhandlung auch Informationen über DNS-Server beim Provider.

Im lokalen Netz ist das *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.

Rückruf-Funktionen

Das *ELSA MicroLink LANCOM MPR* unterstützt 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).

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

Mit diesem Eintrag stellen Sie den Rückruf so ein:
Aus	Es erfolgt kein Rückruf
Looser	Das <i>LANCOM</i> bricht eigene Aufbauversuche ab, wenn ein Ruf von dieser Gegenstelle anliegt (gegenseitiger Verbindungsaufbau).
Auto (nicht Windows 95 oder Windows NT, s.u.)	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 werden und zusätzlich über die Protokollverhandlung ein Rückruf gestartet werden. Dabei fällt eine Gebühr von einer Einheit an.



Die Einstellung 'Name' bietet die höchste Sicherheit, wenn sowohl ein Eintrag in der Nummerliste als auch in der PPP-Liste konfiguriert ist.

*Bei Windows 95- oder Windows NT-Gegenstellen **muß** die Einstellung 'Name' gewählt werden.*

Rückruf nach Microsoft CBCP

Das Microsoft CBCP (Callback Control Protocol) 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- oder Windows NT-PC eine Verbindung zum *LANCOM* aufzunehmen und sich von diesem zurückrufen zu lassen. Die drei möglichen Einstellungen werden über den Rückruf-Eintrag sowie den Rufnummern-Eintrag in der Namenliste ausgewählt.

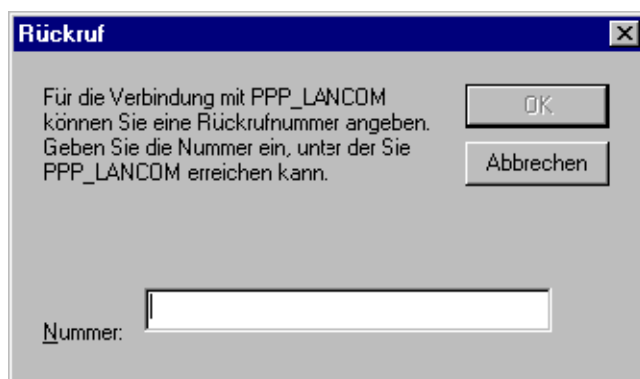
Kein Rückruf

Für diese Einstellung muß der Rückruf-Eintrag den Wert 'Aus' haben.

Rückrufnummer selbst wählen

Für diese Einstellung muß der Rückruf-Eintrag den Wert 'Name' haben, in der Namenliste darf **keine** Rufnummer angegeben sein.

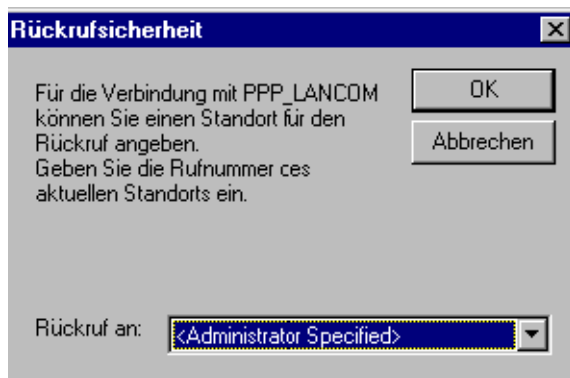
Nach der Authentifizierung erscheint bei Windows 95 die folgende Dialogbox, in der der Anwender seine Rufnummer angeben kann:



Rückrufnummer vom LANCOM bestimmt

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-oder Windows-NT-Workstation erfolgt ca. 15 Sekunden, nachdem die Verbindung abgebaut wurde. Diese Zeit kann nicht verkürzt werden, da sie vom Windows vorgegeben wird.

Sollen zwei LANCOMs miteinander kommunizieren, wobei das eine zurückgerufen wird, so muß die Rückrufnummer vorgegeben werden. Hier beträgt die Wartezeit wie beim Rückruf über das ELSA-Protokoll etwa drei Sekunden.

Rückruf nach RFC 1570 (PPP LCP Extensions)

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

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

