

ELSA LANCOM™ Business 6000

© 2000 ELSA AG, Aachen (Germany)

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

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

ELSA ist DIN-EN-ISO-9001-zertifiziert. Mit der Urkunde vom 15.06.1998 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.

Alle Erklärungen und Urkunden zur Zulassung der Produkte finden Sie im Anhang dieser Dokumentation, sofern sie zum Zeitpunkt der Drucklegung vorlagen.

Marken

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

Cisco ist eine eingetragene Marke von Cisco Systems, Inc.

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

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

52070 Aachen

Deutschland

www.elsa.de

Aachen, Januar 2001

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Mit dem *ELSA LANCOM Business* haben Sie sich für einen Router entschieden, mit dem Sie lokale Netzwerke über eine 2-Mbit-Verbindung anschließen können.

Modellvarianten

Diese Dokumentation beschreibt verschiedene Modellvarianten aus der Serie *ELSA LANCOM Business*, die in Hard- und Softwareausstattung unterschiedlich sind:

- *ELSA LANCOM Business 6001*
- *ELSA LANCOM Business 6011*
- *ELSA LANCOM Business 6021*

Modell-
Einschränkungen

Die Teile der Dokumentation, die sich nur auf einen Teil der Modelle beziehen, sind entweder im Text selbst oder durch entsprechende Hinweise neben dem Text gekennzeichnet.

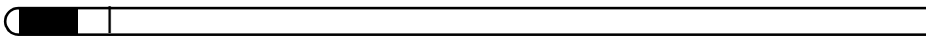
An der Erstellung dieser Dokumentation haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres ELSA-Produktes anzubieten.

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

editorial@elsa.de



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



1 Einleitung	9
1.1 Was bietet ein <i>ELSA LANCOM Business</i> ?	9
2 Beschreibung des Gerätes	11
2.1 Vorderseite	11
2.2 Rückseite	12
2.3 Statusanzeigen der WAN-Schnittstellen	13
3 Installation von Hard- und Software	15
3.1 Lieferumfang	15
3.2 So schließen Sie das Gerät an	15
3.2.1 Anschluss an das lokale Netzwerk (LAN)	16
3.2.2 Anschluss an entfernte Netzwerke (WAN)	16
3.2.3 Anschluss an ISDN	17
3.2.4 Verbindung über die serielle Schnittstelle (COM)	18
3.3 Einschalten des Routers	18
3.4 Installation der Zubehörprogramme	18
3.5 Assistenten machen das Leben leichter	19
4 Konfiguration und Management	21
4.1 Mittel und Wege für die Konfiguration	21
4.1.1 Konfigurations-Zugänge des <i>ELSA LANCOM Business</i>	21
4.1.2 Software zur Konfiguration	22
4.2 Konfiguration über <i>ELSA LANconfig</i>	23
4.3 Konfiguration mit <i>ELSA WEBconfig</i>	24
4.4 Konfiguration über Telnet	24
4.5 Konfiguration über SNMP	25
4.6 Die Basiskonfiguration	25
4.6.1 Basis-Konfiguration unter Windows mit <i>ELSA LANconfig</i>	25
4.6.2 Basis-Konfiguration über Browser mit <i>ELSA WEBconfig</i>	26
4.7 Weitergehende Einstellungen	28
4.8 <i>ELSA LANmonitor</i> – wissen, was läuft	29
4.8.1 <i>ELSA LANmonitor</i> installieren	29
4.8.2 Internet-Verbindung kontrollieren	30
4.9 Die Fernkonfiguration über DFÜ-Netzwerk	31
4.9.1 Das brauchen Sie für die Fernkonfiguration	31
4.9.2 Die erste Fernverbindung mit DFÜ-Netzwerk	32

4.9.3 Die erste Fernverbindung mit PPP-Client und Telnet	32
4.9.4 Fernkonfiguration einschränken	33
4.10 Trace-Ausgaben – Infos für Profis	34
4.10.1 So starten Sie einen Trace	35
4.11 Neue Firmware mit ELSA FirmSafe	37
4.11.1 So funktioniert ELSA FirmSafe	37
4.11.2 So spielen Sie eine neue Software ein	38
5 Anschluss über 2-Mbit-Schnittstelle	41
5.1 Einsatzgebiete	41
5.2 Technische Grundlagen	42
5.2.1 Die 2-Mbit-Schnittstellen Ihres Gerätes	42
5.2.2 G.703 – einfache Basis für 2-Mbit-Verbindungen	43
5.2.3 G.704 bringt Struktur in den Datenstrom	43
5.2.4 Welche Methode für Ihren Zweck?	45
5.2.5 Einstellung der Basisprotokolle	47
5.3 Bündelung von 2-Mbit-Verbindungen	49
6 Funktionen und Betriebsarten	53
6.1 Sicherheit für Ihre Konfiguration	53
6.1.1 Passwortschutz	54
6.1.2 Die Login-Sperre	54
6.1.3 Zugangskontrolle über TCP/IP	54
6.2 Sicherheit für Ihr LAN	55
6.2.1 Die Identifikationskontrolle	55
6.2.2 Der Rückruf	57
6.2.3 Filterung von Datenpaketen – Firewall	58
6.2.4 Das Versteck – IP-Masquerading (NAT, PAT)	62
6.3 Automatische IP-Adressverwaltung mit DHCP	62
6.3.1 Der DHCP-Server	63
6.3.2 DHCP – 'Ein', 'Aus' oder 'Auto'?	63
6.3.3 So werden die Adressen zugewiesen	64
6.3.4 Konfiguration des DHCP-Servers	68
6.4 DNS	71
6.4.1 Was macht ein DNS-Server?	71
6.4.2 So stellen Sie den DNS-Server ein	73
6.5 NetBIOS-Proxy	75
6.5.1 Kurz und bündig: Was ist NetBIOS?	75
6.5.2 Behandlung von NetBIOS-Paketen	76
6.5.3 Welche Voraussetzungen müssen erfüllt sein?	77

6.5.4	So verbinden Sie zwei Windows-Netze	80
6.5.5	So wählt sich ein Remote-Access-Rechner ein	82
6.5.6	Gesucht – Gefunden: Die Netzwerkumgebung	82
6.6	Das SYSLOG-Modul	84
6.6.1	Einrichten des SYSLOG-Moduls	84
6.6.2	Beispielkonfiguration mit <i>ELSA LANconfig</i>	85
6.7	ISDN-Verbindungen	87
6.7.1	ISDN-Namenliste	89
6.7.2	Interface-Einstellungen	90
6.7.3	Einstellungen für Wählverbindungs-Interfaces	90
6.7.4	Interface-Einstellungen für <i>LANCAPI</i>	91
6.7.5	Layer-Liste	92
6.7.6	Round-Robin-Liste	93
6.7.7	Kanal-Liste	94
6.7.8	Script	95
6.7.9	Rufannahme	95
6.7.10	Nummernliste	96
6.8	Bürokommunikation und <i>ELSA LANCAPI</i>	96
6.8.1	Die <i>ELSA LANCAPI</i>	96
6.9	<i>ELSA CAPI Faxmodem</i>	102
6.10	Gebührenmanagement	103
6.10.1	Gebührenabhängige ISDN-Verbindungsbegrenzung	103
6.10.2	Zeitabhängige ISDN-Verbindungsbegrenzung	103
6.10.3	Einstellungen im Gebührenmodul	104
6.11	Accounting	105
6.11.1	Konfiguration des Accountings	106
6.11.2	Ablesen der Accounting-Informationen	106
6.12	Der Least-Cost-Router	107
6.12.1	So arbeitet der Least-Cost-Router im <i>ELSA LANCOM</i>	108
6.12.2	So stellen Sie den Least-Cost-Router ein	110

7 Technische Grundlagen **115**

7.1	Netzwerktechnik	115
7.1.1	Das Netzwerk und seine Komponenten	115
7.1.2	Verbindungsarten	116
7.1.3	Netzwerk-Arten	117
7.2	IP-Adressierung	118
7.2.1	IP-Routing und hierarchische IP-Adressierung	121
7.2.2	Erweiterung durch lokale Netze	124
7.3	Point-to-Point Protocol	130

7.3.1	Das Protokoll	131
7.3.2	Die PPP-Liste	133
7.3.3	Alles o.k.? Leitungsüberprüfung mit LCP	134
7.3.4	Zuweisung von IP-Adressen über PPP	135
7.3.5	Rückruf-Funktionen	137
7.3.6	Kanalbündelung mit MLPPP	140
7.4	IPX-Routing	143
7.4.1	IPX-Adressierung	143
7.4.2	Informationen über das LAN	143
7.4.3	IPX-Routing-Tabelle	144
7.4.4	Was passiert bei der Datenübertragung im IPX-Netz?	145
7.4.5	RIP- und SAP-Tabellen	146
7.4.6	So viele Router hier	146
7.4.7	Redundante Routen	147
7.4.8	Exponential-Backoff	147
7.4.9	Filter für die IPX-Pakete	148
7.5	IP-Routing	150
7.5.1	Die IP-Routing-Tabelle	150
7.5.2	Filter für die TCP/IP-Pakete	154
7.5.3	Proxy-ARP	155
7.5.4	Lokales Routing	155
7.5.5	Dynamisches Routing mit IP-RIP	156
7.6	IP-Masquerading (NAT, PAT)	159
7.7	DNS-Forwarding	162
7.7.1	Policy Based Routing	163
8	Technische Daten	165
8.1	Leistungs- und Kenndaten	165
8.2	Anschlussbelegung	167
8.2.1	X.21-Schnittstelle	167
8.2.2	G.703-Schnittstelle	167
8.2.3	ISDN-S ₀ -Schnittstelle	168
8.2.4	Ethernet-Schnittstelle 10/100Base-T	168
8.2.5	Konfigurationsschnittstelle (Outband)	168
8.2.6	Wichtiger Hinweis zum Recycling	169
9	Anhang	171
9.1	Konformitätserklärung	171
9.2	Allgemeine Garantiebedingungen	172
10	Index	175

1

Einleitung

Wenn es um den Aufbau unternehmensweiter Infrastrukturen geht, rückt der Einsatz von Routerlösungen zunehmend in den Vordergrund. Der Bedarf an Bandbreite – speziell für den Internet-Zugang oder die Kopplung von Filialnetzwerken – wächst stetig und unaufhaltsam. 2-Mbit-Festverbindungen sind heute für kleine und mittelständische Unternehmen eine Selbstverständlichkeit. An verschiedenen Standorten gewachsene lokale Netzwerke (LANs) und Einzel-PCs lassen sich mit Routern kostengünstig verbinden. Filialen und Niederlassungen können transparent in das Netzwerk der Zentrale eingebunden werden und verfügen über die gleiche Datenbasis wie die Zentrale.

Eine ausführliche Beschreibung der Funktionen des *ELSA LANCOM Business*, der Software und ihre Bedienung sowie eine Einführung in die technischen Grundlagen finden Sie in den nachfolgenden Kapiteln.

1.1

Was bietet ein *ELSA LANCOM Business*?

Um Ihnen einen Überblick über die Leistungsfähigkeit Ihres Geräts zu geben, sind im folgenden die wesentlichen Eigenschaften aufgeführt. Eine detaillierte Beschreibung finden Sie in Kapitel 5.

- Betrieb an 2-Mbit-Festverbindungen
- Anschluss an das lokale Netzwerk (LAN)
- Einfache Installation mit Hilfe von Software-Assistenten
- Komfortable Administration mit *ELSA LANconfig* und *WEBconfig*
- Professionelle Gerätekontrolle mit *ELSA LANmonitor*
- Einfaches und sicheres Software-Update mit *ELSA FirmSafe*
- Umfassende Sicherheits- und Firewall-Funktionen
- Flexibler ISDN-Anschluss inklusive Dial-Backup
- Netzwerkfähige *ELSA LANCAPI*
- Optionale Unterstützung von *ELSA Dynamic VPN*

2

Beschreibung des Gerätes

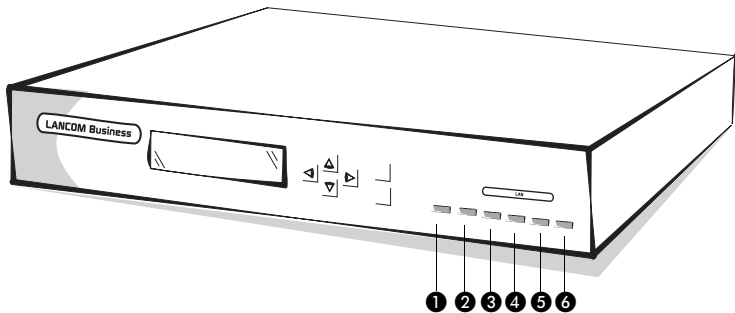
DE

In diesem Abschnitt werden die Schnittstellen und Anzeigeelemente des *ELSA LANCOM Business* vorgestellt.

2.1

Vorderseite

An der Vorderseite finden Sie die Anzeige- und Bedienungselemente: eine Anzeige, einige Tasten und Leuchtdioden (LEDs).



Das Display zeigt die verschiedenen Betriebszustände und Meldungen des Gerätes an. Es werden Betriebszustände und Meldungen in drei verschiedenen Darstellungsarten angezeigt.

Mit den Tasten wählen Sie die Darstellungsart aus, bestätigen Meldungen und scrollen ggf. durch die mehrzeilige Anzeige.

❶ Power/Msg

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

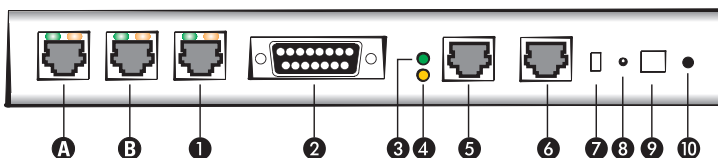
aus		Gerät abgeschaltet
rot	1 x kurz	Bootvorgang (Test und Laden) begonnen
rot	blinkend	Anzeige eines Bootfehlers (im Blinkcode kodiert)
rot		Gerät betriebsbereit
rot	unterbr.	Fehlermeldung oder eine Gebührensperre verhindert abgehende Rufe

- ② **Rx/Tx** – Datenpaket vom Gerät an das LAN oder vom LAN an das Gerät gesendet
- ③ **Coll** – Sendekollision
- ④ **Link** – Der Anschluss zum LAN ist hergestellt und bereit
- ⑤ **FDpx** – Der Router sendet und empfängt Daten gleichzeitig
- ⑥ **Fast** – Das Gerät befindet sich im 100-Mbit-Betrieb

2.2

Rückseite

Auf der Rückseite des Gerätes finden Sie mehrere Schnittstellen zum Anschluss an verschiedenste Geräte und Netze.



- A** G.703-Schnittstelle (nur *ELSA LANCOM Business 6021*) – diese Schnittstelle wird vom Router als zweite G.703-Schnittstelle angesprochen: 'G.703-2' bzw. Kanal 4-1 in der Kanaltabelle.
- B** G.703-Schnittstelle (nur *ELSA LANCOM Business 6011* und *ELSA LANCOM Business 6021*) – diese Schnittstelle wird vom Router als erste G.703-Schnittstelle angesprochen: 'G.703-1' bzw. Kanal 3-1 in der Kanaltabelle.
- ① ISDN-S₀-Anschluss
- ② X.21-Schnittstelle

- ③ Status-LED der X.21-Schnittstelle
- ④ Line-LED der X.21-Schnittstelle
- ⑤ V.24-Konfigurationsschnittstelle (COM), belegungskompatibel zu Cisco
- ⑥ 10/100Base-TX für 10-Mbit- oder 100-Mbit-Netze
- ⑦ Node/Hub-Umschalter
- ⑧ Reset-Taster, führt einen Hardware-Reset durch oder setzt das Gerät in den Auslieferungszustand zurück (nach ca. 5 Sek. Drücken).
- ⑨ Anschluss für das Netzteil
- ⑩ Ein/Aus-Schalter

2.3

Statusanzeigen der WAN-Schnittstellen

Der *ELSA LANCOM Business* verfügt an jeder seiner WAN-Schnittstellen (X.21, G.703, ISDN) über jeweils zwei LEDs zur kontinuierlichen Ausgabe von Statusinformationen. Dabei wird der Zustand der Schnittstelle auf der grünen LED mit der Bezeichnung 'Status' angezeigt. Die orangene LED mit der Bezeichnung 'Line' zeigt den Zustand der logischen Verbindung auf Router-Ebene an.

X.21-Schnittstelle

Status-LED (grün)	aus	Schnittstelle nicht aktiv
	blinkt	Schnittstelle aktiv, kein Signal von externem Gerät
	an	Schnittstelle aktiv, Gerät angeschlossen
Line-LED (orange)	aus	Keine Verbindung aufgebaut
	blinkt	Verbindungsaufbau/Protokollverhandlung (z. B. über PPP)
	an	Aktive Verbindung zur Gegenstelle

G.703-Schnittstelle (nicht beim *ELSA LANCOM Business 6001*)

Status-LED (grün)	aus	Schnittstelle nicht aktiv
	blinkt	Nur bei strukturierter Verbindung: G.704-Framing-Fehler oder RAI (R emote A larm I ndicator)
	an	Schnittstelle aktiv, G.703-Signal OK, bei strukturierter Verbindung: G.704-Framing OK

**Line-LED
(orange)**

aus	Keine Verbindung aufgebaut
blinkt	Verbindungsaufbau/Protokollverhandlung (z.B. über PPP)
an	Aktive Verbindung zur Gegenstelle

ISDN-S₀-Schnittstelle**Status-LED
(grün)**

aus	Schnittstelle oder S ₀ -Bus nicht aktiv
blinkt	Nur Wählverbindung; kein TEI (T erminal E ndpoint Identifier) zugeteilt
an	S ₀ -Bus aktiv

**Line-LED
(orange)**

aus	Keine Verbindung aufgebaut
blinkt	Verbindungsaufbau/Protokollverhandlung (z.B. über PPP)
an	Aktive Verbindung zur Gegenstelle

3

Installation von Hard- und Software



Dieses Kapitel wird Ihnen helfen, möglichst schnell Verbindung aufzunehmen. Sie sehen zunächst, was im Lieferumfang Ihres Produktes enthalten ist. Danach zeigen wir Ihnen, wie Sie das Gerät anschließen und schnell in Betrieb nehmen können.

3.1

Lieferumfang

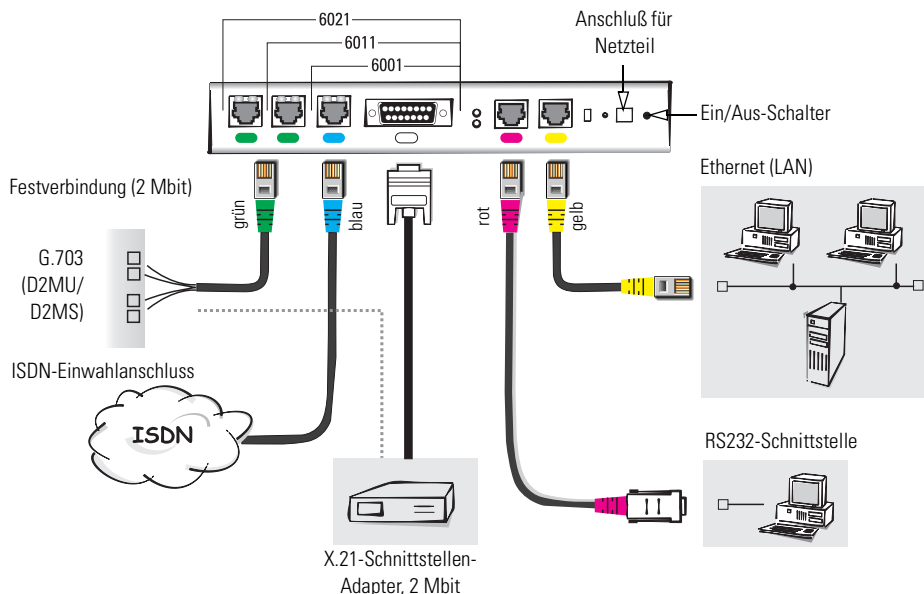
Bitte prüfen Sie den Inhalt der Verpackung auf Vollständigkeit, bevor Sie mit der Installation beginnen. Folgende Komponenten sollte der Karton für Sie bereithalten:

- *ELSA LANCOM Business*
- Netzteil
- LAN-Anschlusskabel, 100Base-TX, gelber Stecker
- Kabel für G.703-Schnittstelle (nur *ELSA LANCOM Business 6011* und *6021*), grüner Stecker
- Kabel für X.21-Schnittstelle
- ISDN-Anschlusskabel, blauer Stecker
- Anschlusskabel für serielle Konfigurationsschnittstelle (RJ45-RJ45) mit Adapter RJ45-D-Sub-9 (nicht nach Kategorie 5), roter Stecker
- Dokumentation
- *ELSA LANCOM Business*-CD mit *ELSA LANconfig*, weiterer Software und elektronischer Dokumentation

3.2

So schließen Sie das Gerät an

Für den Anschluss des *ELSA LANCOM Business 6000* finden Sie alle erforderlichen Kabel im Lieferumfang des Gerätes. Zur Orientierung sind die Kabelstecker und Buchsen am Gerät farblich gekennzeichnet, so dass die Kabel den entsprechenden Buchsen eindeutig zugeordnet werden können.



3.2.1 Anschluss an das lokale Netzwerk (LAN)

Verbinden Sie Ihren *ELSA LANCOM Business* mit dem LAN. Stecken Sie dazu das mitgelieferte Netzkabel in den 10/100Base-TX-Anschluss des Geräts und in eine freie Netzwerkanschlussdose Ihres lokalen Netzes (oder in eine freie Buchse eines Hubs in Ihrem LAN). Das Kabel für den LAN-Anschluss ist mit einem farbigen Knickschutz gekennzeichnet.

Die LED 'LAN-Link' auf der Vorderseite des Gerätes zeigt an, dass eine korrekte Verbindung mit dem LAN hergestellt ist.

Falls diese LED nicht leuchten sollte, schalten Sie den Node/Hub-Umschalter um. Falls die LED dann noch immer nicht leuchtet, liegt evtl. ein Problem mit Netzwerkkarte oder der Verkabelung vor.



3.2.2 Anschluss an entfernte Netzwerke (WAN)

Je nach Gerätetyp haben Sie bis zu drei 2-Mbit-Schnittstellen für den Anschluss an entfernte Netzwerke bzw. Internet:

- *ELSA LANCOM Business 6001*
 - Eine X.21-Schnittstelle für den Anschluss an einen Schnittstellen-Adapter

- *ELSA LANCOM Business 6011*
 - Eine X.21-Schnittstelle für den Anschluss an einen Schnittstellen-Adapter
 - Eine G.703-Schnittstelle für die direkte Installation an einen Festverbindungsanschluss (D2MU oder D2MS)
- *ELSA LANCOM Business 6021*
 - Eine X.21-Schnittstelle für den Anschluss an einen Schnittstellen-Adapter
 - Zwei G.703-Schnittstellen für direkte Installation an Festverbindungsanschlüsse (D2MU oder D2MS)

Anschluss an die X.21-Schnittstelle

Die X.21-Schnittstelle erlaubt den Anschluss an eine 2-Mbit-Festverbindung mittels (D2MU oder D2MS) eines externen Terminaladapters. Der X.21-Terminaladapter wird über eine eigene G.703-Schnittstelle an einen Festverbindungsanschluss gelegt.

Anschluss an eine Festverbindung über G.703

Über die G.703-Schnittstelle können Sie das *ELSA LANCOM Business 6011* oder *6021* direkt an einen Festverbindungsanschluss (in Deutschland unter den Bezeichnungen D2MU oder D2MS) anschließen. Stecken Sie dazu das passende Verbindungskabel in die G.703-Buchse des Geräts. Die Litzen am anderen Ende des Kabels befestigen Sie an den D2MU- bzw. D2MS-Klemmen des entsprechenden Netzabschlussgerätes (in Deutschland NTPMKU oder NTPMKS).

In einigen Ländern werden für den Anschluss an G.703 auch andere Kabel beigelegt, etwa mit Stecker statt Litzen.

Nur für ELSA
LANCOM Business
6011 und 6021!



3.2.3

Anschluss an ISDN

Die ISDN-Schnittstelle ist der direkte Zugang für entfernte Rechner, beispielsweise für die Fernkonfiguration. Außerdem können Sie über die ISDN-Schnittstelle allen Rechnern im angeschlossenen LAN auch verschiedene Office-Funktionen, wie beispielsweise den Versand von Faxen, zur Verfügung stellen. Als Software verwenden Sie dazu die mitgelieferte *ELSA LANCAPI*.

Verbinden Sie die ISDN-Schnittstelle des Routers mit dem ISDN-Netz. Stecken Sie dazu das mitgelieferte ISDN-Anschlusskabel in den ISDN/S₀-Bus-Anschluss (BRI) des Geräts und an einen ISDN/S₀-Mehrgeräteanschluss oder

Anlagenanschluss (Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Konfiguration) an.

3.2.4 Verbindung über die serielle Schnittstelle (COM)

Über die serielle Schnittstelle können Sie das Gerät außerhalb des Netzwerkes konfigurieren. Entweder mit Hilfe von *ELSA LANconfig* oder mit einem Terminalprogramm.

Die serielle Konfigurations-Schnittstelle (COM) der *ELSA LANCOM Business*-Geräte ist belegungskompatibel zu Cisco-Geräten. Entsprechende Anschlusskabel oder Adapter können also auch mit *ELSA LANCOM Business*-Routern verwendet werden.

Die serielle Schnittstelle stellt sich automatisch auf Datenraten im Bereich von 9.600–230.400 bit/s ein.

3.3 Einschalten des Routers

Zu guter Letzt schließen Sie den Router mit dem mitgelieferten Netzteil an das Stromnetz an und schalten das Gerät am Ein/Aus-Schalter auf der Rückseite ein.

Nach dem Einschalten durchläuft der Router einige Testroutinen, um die Funktionsfähigkeit des Gerätes sicherzustellen. Den Verlauf der Testroutinen können Sie auf dem Display auf der Vorderseite des Gerätes verfolgen. Nach erfolgreichem Abschluss der Testroutinen erscheint der Gerätenamen 'LANCOM BUSINESS 6000' auf dem Display. Das Gerät ist betriebsbereit.

3.4 Installation der Zubehörprogramme

Auf der beiliegenden CD finden Sie ein Setup-Programm, mit dem Sie die ELSA-Software installieren. Legen Sie die CD in Ihr CD-Laufwerk. Falls das Setup-Programm nicht automatisch startet, können Sie es manuell aufrufen. Sie finden die Datei SETUP.EXE im Stammverzeichnis der CD.

Befolgen Sie die einzelnen Schritte, und bestätigen Sie die Abfragen des Setup-Programms.

Es werden die folgenden Programme installiert:

- *ELSA LANconfig* zur Administration des Gerätes unter Windows
- *ELSA LANmonitor* zur Überwachung des Gerätes unter Windows

- *ELSA LANCAPI* stellt Office-Funktionen im LAN zur Verfügung

Außerdem finden Sie auf der CD eine Beta-Version der Linux-Variante von *LANconfig*. Dieses Programm heisst *xLANconfig* und bietet alle Funktionen von *LANconfig*. Bislang steht *xLANconfig* für Linux auf x86- und Alpha-Prozessoren zur Verfügung. *xLANconfig* setzt auf dem X-Windows-Standard auf, der unter UNIX-Systemen weit verbreitet ist. Über einen X-Windows-Server kann die gesamte Funktionalität von *xLANconfig* für beliebige X-Windows-Clients im Netz bereitgestellt werden. Diese Clients können *xLANconfig* benutzen, ohne dass auf ihnen *xLANconfig* installiert sein muss. Dank dieser Eigenschaft ist *xLANconfig* besonders interessant für den Einsatz in größeren Netzwerken.

3.5

Assistenten machen das Leben leichter

Im folgenden Kapitel erfahren Sie, wie Sie Ihren *ELSA LANCOM Business* konfigurieren. Früher war diese Konfiguration eine verzwickte Angelegenheit, bei der auch Spezialisten leicht ins Schwitzen gerieten. ELSA entwickelte zur Vereinfachung der Konfiguration Software-Assistenten, mit denen auch schwierige Konfigurationen in kurzer Zeit erfolgreich und sicher vorgenommen werden können.

Die Assistenten können auf zwei Wegen aufgerufen werden:

① ***ELSA LANconfig***

Steht unter allen Windows-Betriebssystemen zur Verfügung. Neuerdings als *xLANconfig* auch für Linux auf x86- oder Alpha-Prozessoren.

② ***ELSA WEBconfig***

Fest im Router eingebaute Software. Kann mit jedem Web-Browser (auch reine Text-Browser) von jedem Betriebssystem aus aufgerufen werden. Voraussetzung: Zugriff über das Netzwerk auf den Router.

In beiden Varianten werden dieselben Assistenten angeboten. Es hängt also vom Betriebssystem auf Ihrem Konfigurationsrechner ab, welche der beiden Varianten Sie verwenden. Im folgenden Überblick werden wir *WEBconfig* als Anschauungsbeispiel anführen. Die Angaben gelten aber auch für *LANconfig* und *xLANconfig*.

Es ist uns ein Anliegen, Ihnen die Konfiguration so einfach wie möglich zu machen. Deshalb weisen wir Sie schon frühzeitig auf die Assistenten hin. Im folgenden Kapitel finden Sie eine vollständige Aufzählung aller möglichen Konfigurationsmethoden. Die Assistenten unter *LANconfig* und *WEBconfig*

sind eine Möglichkeit. Allerdings die einfachste und sicherste zugleich – daher diese frühzeitige Erwähnung.

Es lohnt sich daher, schon jetzt einen kurzen Blick auf die Assistenten zu werfen, die Ihnen für die Konfiguration eines *ELSA LANCOM Business 6000* angeboten werden:



Neben den Grund- und Sicherheitseinstellungen können Sie mit den Assistenten auch den Internet-Zugang konfigurieren, die Einwahlzugänge für den Fernzugang einrichten und eine direkte Verbindung zweier lokaler Netzwerke aufbauen. Natürlich stehen Ihnen nicht nur die Assistenten, sondern auch alle Optionen der Experten-Konfiguration zur Verfügung. Der Einsatz dieser Optionen ist allerdings nur noch in wenigen Fällen notwendig.

Die Assistenten sind so aufgebaut, dass sich der Router für die typischen Anwendungsfälle ausschließlich mit ihnen einfach, sicher und schnell konfigurieren lässt. Die Benutzung der Assistenten ist selbsterklärend. Sie finden eine ausführliche Beschreibung aller notwendigen Eingaben direkt an Ort und Stelle, also im Eingabefenster. Das spart Ihnen den Blick ins Handbuch. Aus diesem Grund sind die einzelnen Schritte der Assistenten in diesem Handbuch auch nicht mehr eingehend beschrieben.

Die Erfahrung zeigt, dass bei Anwendung der Assistenten kaum noch Probleme mit fehlerhaften Konfigurationen auftreten. Seien Sie bequem und machen Sie sich Ihr Leben durch Benutzung der Assistenten einfacher!

4

Konfiguration und Management



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

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

In diesem Kapitel geben wir Ihnen einen Überblick, mit welchen Programmen und über welche Wege Sie auf das Gerät zugreifen können, um erweiterte Einstellungen vorzunehmen.

Im weiteren Verlauf zeigen wir Ihnen dann, wie Sie mit wenigen Eingaben die wichtigsten Einstellungen im Gerät (die Basis-Konfiguration) vornehmen.

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

4.1

Mittel und Wege für die Konfiguration

ELSA LANCOM Business sind flexible Geräte, die verschiedene Mittel (sprich Software) und Wege (in Form von Kommunikationszugängen) für die Konfiguration unterstützen. Zunächst ein Blick auf die möglichen „Wege“.

4.1.1

Konfigurations-Zugänge des *ELSA LANCOM Business*

Einen *ELSA LANCOM Business* können Sie über drei verschiedene Zugänge erreichen:

- über die Konfigurations-Schnittstelle (Config-Schnittstelle) an der Rückseite des Routers (auch Outband genannt)
- über das angeschlossene Netzwerk, LAN oder WAN (Inband)
- über eine Wahlverbindung oder Standleitung am ISDN-Anschluss des Gerätes (Fernkonfiguration)

Was unterscheidet nun diese drei Wege?

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

Zum anderen die Anforderungen an weitere Hard- und Software: Die Inband-Konfiguration benötigt einen der ohnehin vorhandenen Rechner im LAN oder WAN und nur noch eine geeignete Software, beispielsweise *ELSA LANconfig* (vgl. folgender Abschnitt). Die Outband-Konfiguration braucht zusätzlich zur Konfigurationssoftware noch einen Rechner mit serieller Schnittstelle und entsprechendem Konfigurationskabel. Für die Fernkonfiguration sind die Voraussetzungen am umfangreichsten: Eine ISDN-Karte oder ein ISDN-Modem sind ebenso notwendig wie eine PPP-Zugangssoftware, die aber z.B. bei Windows als DFÜ-Netzwerk mitgeliefert wird.

4.1.2 Software zur Konfiguration

Beim Blick auf die Konfigurationszugänge wurde schon klar: Zur Konfiguration bedarf es geeigneter Software.

Die Situationen, in denen konfiguriert wird, unterscheiden sich – aber auch die persönlichen Ansprüche und Vorlieben der Ausführenden. *ELSA LANCOM Business*-Router verfügen daher über ein breites Angebot von Konfigurationssoftware:

- **ELSA LANconfig** – menügeführt, übersichtlich und einfach lassen sich nahezu alle Parameter eines *ELSA LANCOM Business* einstellen. Zusätzlich bietet *ELSA LANconfig* Einblick in interne Vorgänge im Router. *ELSA LANconfig* ist ein vollwertiger Router-Manager unter Windows. Unterstützt Outband, Inband und Fernkonfiguration.
- **ELSA WEBconfig** – diese Software ist fest eingebaut im Router. Auf dem Konfigurationsrechner wird nur ein Web-Browser vorausgesetzt. *WEBconfig* ist dadurch betriebssystemunabhängig. Unterstützt werden Inband- und Fernkonfiguration.
- **SNMP** – Programme zum Management von IP-Netzwerken basieren üblicherweise auf dem Protokoll SNMP. Über SNMP können Sie auf *ELSA LANCOM Business* inband und mittels Fernkonfiguration zugreifen.
- **Terminalprogramm, Telnet** – ein *ELSA LANCOM Business* kann mit einem Terminalprogramm über die Config-Schnittstelle (z.B. HyperTerminal) oder innerhalb eines IP-Netzwerks (z.B. Telnet) konfiguriert werden.
- **TFTP** – innerhalb von IP-Netzwerken (Inband und Fernkonfiguration) kann auch das Dateiübertragungs-Protokoll TFTP verwendet werden.

4.2

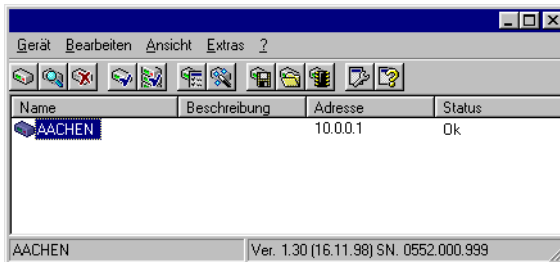
Konfiguration über *ELSA LANconfig*

Rufen Sie *ELSA LANconfig* z.B. aus der Windows-Startleiste auf mit **Start ► Programme ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* sucht nun automatisch im lokalen Netz nach Geräten. Wird dabei ein noch nicht konfiguriertes Gerät im lokalen Netz gefunden, startet *ELSA LANconfig* selbständig den Setup-Assistenten. Die Beschreibung der Basiskonfiguration mit Hilfe des Setup-Assistenten finden Sie im Abschnitt 'Basis-Konfiguration unter Windows mit ELSA LANconfig' auf Seite 25.



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

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



Für die Konfiguration der Geräte mit *ELSA LANconfig* stehen zwei verschiedene Darstellungsmöglichkeiten zur Auswahl:

- In der 'einfachen Darstellung' werden nur die Einstellungen angezeigt, die für übliche Anwendungsfälle benötigt werden.
- In der 'vollständigen Darstellung' werden alle verfügbaren Einstellungen angezeigt. Einige davon sollten nur von erfahrenen Benutzern verändert werden.

Wählen Sie den Darstellungsmodus im Menü **Ansicht ► Optionen**.



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

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

4.3 Konfiguration mit *ELSA WEBconfig*

Sie können die Einstellungen des Gerätes über einen beliebigen (auch text-basierten) Web-Browser vornehmen. Im *ELSA LANCOM Business* ist die Konfigurationssoftware *ELSA WEBconfig* integriert. Sie benötigen lediglich einen Web-Browser, um auf *ELSA WEBconfig* zuzugreifen.

ELSA WEBconfig bietet ähnliche Setup-Assistenten wie *ELSA LANconfig* an und bietet damit optimale Voraussetzungen für eine komfortable Konfiguration von *ELSA LANCOM Business* – im Unterschied zu *ELSA LANconfig*, aber unter allen Betriebssystemen, für die es einen Web-Browser gibt.

Für die Verwendung von *ELSA WEBconfig* muss ein LAN-Anschluss über TCP/IP (bei Fernkonfiguration über PPP) aufgebaut sein. Der Zugriff auf *ELSA WEBconfig* erfolgt über die IP-Adresse des *ELSA LANCOM Business*.

Im Abschnitt 'Basis-Konfiguration über Browser mit *ELSA WEBconfig*' auf Seite 26 lesen Sie, wie Sie das erste Mal mit *WEBconfig* auf ein unkonfiguriertes Gerät zugreifen und die Basiskonfiguration vornehmen.

4.4 Konfiguration über Telnet

Über Telnet starten Sie die Konfiguration z.B. aus einer DOS-Box mit dem Kommando:

```
C:\>telnet 10.0.0.1
```

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

Nach der Eingabe des Passworts (sofern Sie eines zum Schutz der Konfiguration vereinbart haben) stehen Ihnen alle Befehle aus dem Abschnitt 'Befehle für die Konfiguration' zur Verfügung.

4.5

Konfiguration über SNMP

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.

Es gibt eine ganze Reihe von Konfigurations- und Management-Programmen, die über SNMP laufen, beispielsweise OpenView von Hewlett-Packard oder in einfacher Ausgabe der SNMP-Agent, den Sie auch auf der CD finden.

4.6

Die Basiskonfiguration

Zu den wichtigsten Einstellungen, die Sie bei Ihrem neuen Gerät vornehmen können und sollten, gehören:

- Vergabe einer festen IP-Adresse
- Aktivierung des DHCP-Server im Router
- die Sicherheitseinstellungen
- die Einrichtung des Internet-Zugangs oder der Festverbindung
- die Konfiguration der ISDN-Schnittstelle

Für alle diese Konfigurationen stehen Ihnen sogenannte Assistenten zur Verfügung. Das sind gesteuerte Eingabemenüs, die Ihnen bei jedem Konfigurationsschritt Rat und Hilfe geben. Die Grundkonfiguration mit den Assistenten erleichtert Ihnen die Eingabe der Basisdaten. Selbst Laien gelingt mit den Assistenten die Konfiguration eines komplexen Routers. Aber auch Profis machen von den Assistenten Gebrauch.

Die Assistenten stehen Ihnen in zwei Programmen zur Verfügung:

- in *ELSA LANconfig* unter Windows-Betriebssystemen
- in *ELSA WEBconfig* mit jedem Web-Browser

4.6.1

Basis-Konfiguration unter Windows mit *ELSA LANconfig*

Starten Sie zunächst *ELSA LANconfig* mit dem Befehl **Start ► Programme ► ELSAlan ► LANconfig**.

LANconfig durchsucht das Netzwerk nach vorhandenen Geräten. Sobald der neue *ELSA LANCOM Business 6000* gefunden wurde, wird der Assistent für die Grundeinstellungen aufgerufen.

In diesem Assistenten können Sie die wichtigsten Grundeinstellungen vornehmen: die feste IP-Adresse des Gerätes mit anzuwendender Netzmaske.

Außerdem bestimmen Sie, ob im Router der DHCP-Server eingeschaltet werden soll oder nicht.

Im Anschluss an diese Grundeinstellungen werden Ihnen die verfügbaren Assistenten für die typischen Gerätefunktionen, wie Internet-Zugang, Netzwerkverkopplung, Sicherheitsoptionen etc., angeboten. Starten Sie die gewünschten Assistenten, und nehmen Sie die angefragten Einstellungen vor. Anschließend ist der Router für die ausgewählten Aufgaben bereit.

Im Listenfenster von *LANconfig* sehen Sie nun Ihr Gerät mit der dazugehörigen IP-Adresse. Sie können nun auch mit einem Browser auf das Gerät zugreifen. *WEBconfig* bietet Ihnen den Zugriff auf alle Assistenten und das interne Menüsystem für die erweiterte Konfiguration des Rechners.



Für Linux existiert eine Beta-Version von xLANconfig, die Sie auf der ELSA LANCOM Business-CD finden oder in der aktuellsten Version vom Treiberbereich der ELSA-Webseite herunterladen können.

4.6.2

Basis-Konfiguration über Browser mit **ELSA WEBconfig**

Wie Sie wissen, können Sie mit *ELSA WEBconfig* mit jedem Web-Browser Ihren *ELSA LANCOM Business* konfigurieren. Sie sind also nicht wie bei *ELSA LANconfig* auf das Betriebssystem Windows angewiesen.

Einzige Voraussetzung für den Zugriff: Sie müssen die IP-Adresse des Routers kennen.

Welche IP-Adresse hat der Router?

Ein unkonfiguriertes *ELSA LANCOM Business 6000* meldet sich in Ihrem Netzwerk auf der IP-Adresse x.x.x.254. Bei einem Class-A-Netz mit der Subnet-Maske 255.255.0.0 und der Netz-Adresse 10.1.x.x ist dies die Adresse 10.1.0.254. Um die effektive IP-Adresse Ihres Routers herauszufinden, müssen Sie demnach Ihre Netzwerknummer und die Netzmaske kennen.

Mit der IP-Adresse lässt sich das Gerät nun über einen Web-Browser oder über Telnet innerhalb des Netzwerks ansprechen.

Aufruf der Assistenten in **WEBconfig**

Öffnen Sie also Ihren Web-Browser (Internet Explorer, Netscape Navigator) und rufen Sie dort als Internet-Adresse auf:

```
http://<IP-Adresse des LANCOM>
```

Es erscheint folgendes Hauptmenü:



Eine umfangreiche, kontextsensitive Dokumentation zu den einzelnen *WEB-config*-Seiten und -feldern ist jederzeit im *WEBconfig* über den Link 'Hilfe (Referenzhandbuch)' zu erreichen.

Die Hilfedateien für *ELSA WEBconfig* (HTTP-Modul)

Hinter dem Link 'Hilfe (Referenzhandbuch)' befindet sich ein Verweis auf Hilfedateien im HTML-Format. In der Voreinstellung verweist der Hilfe-Link auf die ELSA-Webseiten.

Sie können die Hilfedateien aber auch von den ELSA-Webseiten herunterladen und an einem anderen Speicherplatz Ihrer Wahl ablegen. Idealerweise legen Sie die Hilfedateien lokal auf Ihrem Rechner ab oder auf einen Server, zu dem Sie ständigen Zugriff haben. Dabei kann es sich ebenso um einen File-server wie um einen Web-Server (HTTP) handeln.

Die lokale Variante bietet den Vorteil, dass Sie auf die Hilfe auch bei gestörter Netzwerkfunktion zugreifen können. Wenn Sie die Daten hingegen auf einem Server in Ihrem Netzwerk installieren, können Sie von jedem Rechner auf die Hilfe-Funktion zugreifen, ohne dass Sie die Hilfedateien auf jedem Rechner vorher installieren müssen. In diesem Fall benötigen Sie natürlich einen funktionierenden Netzwerkzugriff auf den entsprechenden Server.

Wenn Sie sich für eine Variante entschieden und die Hilfedateien bereits am gewünschten Ort abgelegt haben, müssen Sie *ELSA WEBconfig* diesen Ort bekannt geben. Wählen Sie dazu in *ELSA WEBconfig* **Experten-Konfiguration ► Setup ► HTTP-Modul ► Dokumentenwurzel**.

Zur Syntax sind zwei wichtige Feststellungen zu machen:

- ① Geben Sie den Pfad nur bis zu dem Verzeichnis an, unter dem Sie die komplette Hilfedateien-Struktur abgelegt haben.

Wenn Sie beispielsweise in einem lokalen Verzeichnis 'C:\ELSA\HTML-Ref' die Hilfedateien-Struktur '\400\1\6001\' angelegt haben, dann geben Sie als Dokumentenwurzel nur 'file://C:/ELSA/HTMLRef' an.

- ② Der Aufbau des Pfades unterscheidet sich nach verwendeter Variante (lokal, Fileserver, HTTP-Server) und Betriebssystem geringfügig. In der Tabelle werden Beispiele angegeben, wobei die verwendeten Namen und Pfade frei wählbar sind.

Variante	Betriebssysteme	Beispiel
Lokal	Windows	file://C:/ELSA/HTMLRef
	Linux	file://usr/lib/ELSA/HTMLRef
Fileserver	Windows NT, Windows 2000, Novell, UNIX	file://Server1/ELSA/HTMLRef
HTTP-Server	alle	http://<IP-Adresse>/ELSA/HTMLRef

Statt des Platzhalters <IP-Adresse> wird die gültige IP-Adresse des HTTP-Servers im Format 'x.x.x.x' erwartet, also beispielsweise '128.7.9.155'.

Die jeweils aktuelle Version der HTML-Hilfe finden Sie zum Download auf den ELSA-Webseiten.



4.7

Weitergehende Einstellungen

Nach der Basis-Konfiguration sind in den meisten Fällen die notwendigen Einstellungen am *ELSA LANCOM Business 6000* für den konkreten Einsatzbereich vorgenommen.

Sie können natürlich auch eine Vielzahl weitergehender Einstellungen vornehmen. Eine ausführliche Beschreibung dieser Optionen finden Sie im Kapitel 'Funktionen und Betriebsarten'.

4.8

ELSA LANmonitor – wissen, was läuft

Mit dem Überwachungstool *ELSA LANmonitor* können Sie sich unter Windows-Betriebssystemen die wichtigsten Informationen über den Status Ihrer Router auf dem Bildschirm anzeigen lassen. Und zwar den Status aller *ELSA LANCOM Business* im Netz.

Viele der internen Meldungen der Geräte werden dabei in Klartext umgewandelt, zeigen Ihnen den aktuellen Zustand des Gerätes und helfen Ihnen bei der Fehlersuche.

Sie können mit *ELSA LANmonitor* auch den Datenverkehr auf den verschiedenen Schnittstellen der Router beobachten und erhalten so wichtige Hinweise darüber, mit welchen Einstellungen Sie den Datenverkehr optimieren können.

Neben den Statistiken des Geräts, die Sie zum Beispiel auch in einer Telnet- oder Terminalsitzung oder mit *ELSA WEBconfig* auslesen können, stehen Ihnen im *ELSA LANmonitor* noch weitere, nützliche Funktionen zur Verfügung.

4.8.1

ELSA LANmonitor installieren

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

Falls *ELSA LANmonitor* noch nicht auf Ihrem Rechner installiert ist, legen Sie die *ELSA LANCOM Business*-CD ein. Wenn das Setup-Programm beim Einlegen der CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' auf der *ELSA LANCOM Business*-CD. Ansonsten klicken Sie auf das Symbol **Arbeitsplatz** und doppelklicken Sie dann das Symbol Ihres CD-ROM-Laufwerks. Starten Sie die Datei 'Autorun.exe' durch Doppelklick. Das Installationsprogramm startet.

Aktivieren Sie bei der Installation die Option für *LANmonitor*.

Sie können mit ELSA LANmonitor nur solche Geräte überwachen, die Sie inband im lokalen Netzwerk über IP erreichen. Über die serielle Schnittstelle können Sie einen Router mit diesem Programm nicht ansprechen. Auch auf Geräte in entfernten Netzwerken, die nur über zwischengeschaltete Router zu erreichen sind, kann mit ELSA LANmonitor nicht zugegriffen werden.



4.8.2

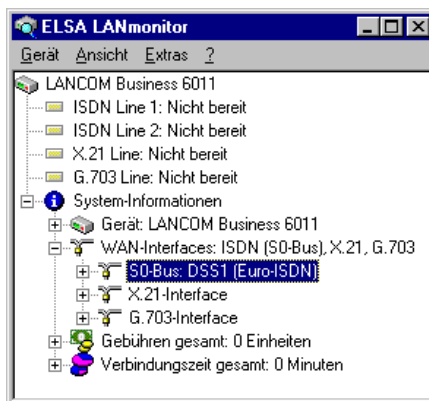
Internet-Verbindung kontrollieren

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

- ① Richten Sie den Router für die Verbindung zu Ihrem Provider ein, z.B. mit dem Setup-Assistenten von *ELSA LANconfig*.
- ② Starten Sie *ELSA LANmonitor* mit **Start ► Programm ► ELSA LAN ► LANmonitor**. Legen Sie mit **Gerät ► Neu** ein neues Gerät an und geben im folgenden Fenster die IP-Adresse für den Router an, den Sie überwachen wollen. Falls die Konfiguration des Gerätes mit einem Passwort gesichert ist, geben Sie dieses gleich mit ein.

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

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



In diesem Beispiel können Sie aus den Protokoll-Informationen zum PPP ablesen, welche IP-Adresse der Provider Ihrem Router für die Dauer der

Verbindung zugewiesen hat und welche Adressen für DNS- und NBNS-Server übermittelt wurden.

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

- ④ Durch einen Klick mit der rechten Maustaste auf den aktiven Kanal können Sie die Verbindung manuell trennen. Dazu benötigen Sie ggf. das Konfigurationspasswort.
- ⑤ Wenn Sie ein Protokoll der *ELSA LANmonitor*-Ausgaben in Form einer Datei wünschen, wählen Sie in Menü 'Ansicht' die 'Optionen' und wechseln zur Registerkarte 'Protokoll'. Aktivieren Sie die Protokollierung und stellen Sie ein, ob *ELSA LANmonitor* täglich, monatlich oder fortlaufend eine Protokolldatei erstellt.

4.9

Die Fernkonfiguration über DFÜ-Netzwerk

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

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

4.9.1

Das brauchen Sie für die Fernkonfiguration

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

4.9.2

Die erste Fernverbindung mit DFÜ-Netzwerk

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



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

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

4.9.3

Die erste Fernverbindung mit PPP-Client und Telnet

- ① Stellen Sie mit Ihrem PPP-Client eine Verbindung zum *ELSA LANCOM Business* her, verwenden Sie dabei folgende Angaben:
 - Benutzername 'ADMIN'
 - Passwort wie beim *ELSA LANCOM Business* eingestellt, im Auslieferungszustand kein Passwort
 - eine IP-Adresse für die Verbindung, nur wenn erforderlich
- ② Starten Sie eine Telnet-Verbindung zum *ELSA LANCOM Business*. Verwenden Sie dazu die folgende IP-Adresse:
 - '172.17.17.18', wenn Sie keine IP-Adresse für den PPP-Client festgelegt haben. Diese Adresse verwendet der *ELSA LANCOM Business* automatisch, falls nichts anderes vereinbart ist. Der anrufende PC reagiert dann auf die IP '172.17.17.17'.
 - Erhöhen Sie die IP-Adresse des PCs um eins, wenn Sie eine Adresse festgelegt haben. Beispiel: Sie haben für den PPP-Client die IP

'10.0.200.123' festgelegt, dann hört der *ELSA LANCOM Business* auf die '10.0.200.124'. Ausnahme: Bei einer '254' am Ende der IP reagiert der Router auf die 'x.x.x.1'.

- ③ Sie können den *ELSA LANCOM Business* über die Fernverbindung nun genauso einstellen wie alle anderen Geräte.

4.9.4

Fernkonfiguration einschränken

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

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

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

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

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

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

- ③ Geben Sie als Rufnummer im Bereich 'Konfigurationszugriff' eine Rufnummer Ihres Anschlusses ein, die nicht für andere Zwecke verwendet wird.

Geben Sie alternativ den folgenden Befehl ein:

```
set /setup/config-modul/Fernconfig 123456
```



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

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

```
passwd
```

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

4.10

Trace-Ausgaben – Infos für Profis

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

tation der Anzeigen nicht, sollte aber bei genaueren Analysen berücksichtigt werden.

4.10.1

So starten Sie einen Trace

Trace-Ausgaben starten Sie z.B. in einer Telnet-Sitzung. 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-Router	IPX-Routing
RIP	IPX Routing Information Protocol
SAP	IPX Service Advertising Protocol
IPX-Watchdog	IPX-Watchdog-Spoofing
SPX-Watchdog	SPX-Watchdog-Spoofing
NetBIOS	NetBIOS-Verwaltung
IP-Router	IP-Routing
IP-RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol

Dieser Parameter ruft beim Trace die folgende Anzeige hervor:
SCRPT	Script-Verhandlung
IP-Masquerading	Vorgänge im Masquerading-Modul
DHCP	Dynamic Host Configuration Protocol
D-Kanal	Trace des D-Kanals des angeschlossenen ISDN-Busses

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

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

Beispiele

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

Dieser Schlüssel ruft in Verbindung mit Trace die folgende Reaktion hervor:
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

4.11

Neue Firmware mit ELSA FirmSafe

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

4.11.1

So funktioniert ELSA FirmSafe

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

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

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

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

4.11.2

So spielen Sie eine neue Software ein

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

- *ELSA LANconfig*
- *ELSA WEBconfig*
- Terminal-Programme
- TFTP



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

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

ELSA LANconfig



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

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

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

ELSA WEBconfig

Starten Sie Ihren Browser, und geben Sie in das Adressfeld die IP-Adresse des Gerätes ein: Hört Ihr *ELSA LANCOM Business* beispielsweise auf die IP-Adresse 194.162.200.17, dann geben Sie ein: 'http://194.162.200.17'.

Auf der Startseite finden Sie den Link 'Eine neue Firmware hochladen'. Im nächsten Fenster können Sie die Firmware-Datei im Verzeichnissystem suchen und anschließend auf die Schaltfläche **Upload** klicken.

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

Stellen Sie bei Terminalprogrammen im Menü 'Firmware' mit dem Befehl 'set Modus-Firmsafe' zunächst ein, in welchem Modus Sie die neue Firmware laden wollen (unmittelbar, login oder manuell). Stellen Sie ggf. zusätzlich mit 'set Timeout-Firmsafe' die Zeit für den Firmwaretest ein.

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

- Bei 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

TFTP steht standardmäßig unter den Betriebssystemen Windows 2000 und Windows NT zu Verfügung. Es ermöglicht den einfachen Dateitransfer von Dateien mit anderen Geräten über das Netzwerk.

Auf *ELSA LANCOM Business* kann mit TFTP eine neue Firmware aufgespielt werden. Dazu wird der Befehl (bzw. das Ziel) **writeflash** angegeben. Um eine neue Firmware in einen *ELSA LANCOM Business* mit der IP-Adresse 194.162.200.17 zu übertragen, geben Sie z.B. unter Windows 2000 oder Windows NT folgenden Befehl ein:

```
tftp -i 194.162.200.17 put Lc_60xxu.220 writeflash
```

*Durch diesen Befehl wird die entsprechende Datei mit dem Befehl (bzw. Ziel) **writeflash** an die angegebene IP-Adresse gesendet. Dabei muss für TFTP die binäre Dateiübertragung eingestellt werden. Auf vielen Systemen ist jedoch das ASCII-Format voreingestellt. In diesem Beispiel für Windows 2000 und Windows NT erreichen Sie das durch den Parameter '-i'.*



Nach einem erfolgreichen Firmware-Upload bootet das Gerät und aktiviert so direkt die neue Firmware. Tritt während des Uploads ein Fehler auf (Schreibfehler im Flash-ROM, TFTP-Übertragungsfehler o.ä.), aktiviert ELSA FirmSafe die vorherige Firmware. Die Konfiguration bleibt dabei erhalten.

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

- `tftp 10.0.0.1 get readconfig file1`: Liest die Konfiguration aus dem Gerät mit der Adresse 10.0.0.1 und speichert diese unter `file1` im aktuellen Verzeichnis ab.
- `tftp 10.0.0.1 put file1 writeconfig`: Schreibt die Konfiguration aus `file1` in das Gerät mit der Adresse 10.0.0.1.
- `tftp 10.0.0.1 get dir/status/verb file2`: Speichert die aktuellen Verbindungsinformationen in `file2`.

5

Anschluss über 2-Mbit-Schnittstelle



In diesem Kapitel finden Sie technische Details zum wichtigsten Merkmal Ihres *ELSA LANCOM Business 6000*: Der Verbindung über die 2-Mbit-Schnittstelle(n). Dabei konzentriert sich die Darstellung hier auf die Konfiguration der Anschlüsse, also die Softwareeinstellungen.

5.1

Einsatzgebiete

Wofür möchten Sie den 2-Mbit-Anschluss benutzen? Zunächst ein Blick auf die wichtigsten Einsatzgebiete:

- **Schnelle Internet-Anbindung eines Netzwerks**

Viele Internet Service Provider bieten 2-Mbit-Anschlüsse ins Internet an. Über die im *ELSA LANCOM Business 6000* eingebaute IP-Router-Funktion steht der Internet-Zugriff jedem Rechner im Netz offen.

- **Kopplung zweier Netzwerke**

Für die ständige Verbindung zweier entfernter Netzwerke wird meistens eine Standleitung eingesetzt. Beim *ELSA LANCOM Business 6000* findet die Kopplung durch ein Routing der Pakete ins jeweils andere Netzwerk statt. Die beiden Netzwerke erscheinen, anders als beim Bridging von Netzen, weiterhin als zwei getrennte Netzwerke. Dabei können Sie allen Stationen in beiden Netzwerken den Zugriff auf Ressourcen des jeweils entfernten Netzwerks ermöglichen. Über mehrere Router lassen sich auch weitreichende Netze von Netzwerken aufbauen.

- **Einwahlpunkte für Fernzugriff**

Viele Telekommunikationsgesellschaften bieten den sogenannten „Primärmultiplexanschluss“ (PMxA, oder PRI für **P**rietary **R**ate **I**nterface) an. Über den PMxA können bis zu 30 parallele ISDN-D-Kanal-Verbindungen hergestellt werden. Die einzelnen Kanäle sind dabei unabhängig voneinander und können Verbindungen zu verschiedenen ISDN-Gegenstellen aufbauen. Beispielsweise können sich in dieser Konstellation bis zu 30 Rechner parallel über ISDN in ein Firmennetzwerk einwählen.

ELSA LANCOM Business sind für den Betrieb an Festverbindungen ausgelegt. Der Betrieb an einem PMxA ist nicht möglich. Die weiteren Ausführungen beschränken sich daher auf Festverbindungen.

Für die Konfiguration eines Internet-Anschlusses oder einer Netzwerkkopplung stehen Ihnen unter *LANconfig* und *WEBconfig* Assistenten zur Verfügung. Dazu finden Sie im weiteren Verlauf dieses Kapitels weitere

Informationen. Zunächst ein knapper Überblick über die Technik, die hinter den 2-Mbit-Anschlüssen steckt.

5.2 Technische Grundlagen

In diesem Abschnitt finden Sie die wichtigsten Informationen über die Technik und die Normen, die im Zusammenhang mit 2-Mbit-Verbindungen im *ELSA LANCOM Business* eingesetzt werden.

5.2.1 Die 2-Mbit-Schnittstellen Ihres Gerätes

Werfen wir einen kurzen Blick auf die 2-Mbit-Schnittstellen Ihres Gerätes und auf die technischen Eigenschaften, die sich dahinter verbergen.

Ihr *ELSA LANCOM Business 6000* verfügt je nach Ausführung über bis zu drei 2-Mbit-Anschlüsse:

- *ELSA LANCOM Business 6001*
 - ein X.21-Anschluss
- *ELSA LANCOM Business 6011*
 - ein X.21-Anschluss
 - ein G.703-Anschluss
- *ELSA LANCOM Business 6021*
 - ein X.21-Anschluss
 - zwei G.703-Anschlüsse

X.21 – Terminaladapter notwendig

Bei X.21 handelt es sich um einen seriellen Übertragungsstandard, nach dem Geschwindigkeiten von 2 Mbit/Sekunde und Entfernungen bis zu 10 Meter möglich sind.

An die X.21-Schnittstelle des *ELSA LANCOM Business* können Sie einen sogenannten Terminaladapter anschließen. Dieser Terminaladapter ist das Verbindungsglied zwischen dem Endgeräteanschluss Ihres Telekommunikationsanbieters und einem oder mehreren Routern.

G.703 – direkt an das Endgerät

Zusätzlich zur X.21-Schnittstelle verfügen die *ELSA LANCOM Business*-Modelle *6011* und *6021* über einen bzw. zwei G.703-Anschlüsse. Diese Modellen verbinden Sie direkt mit dem Endgeräteanschluss Ihres Telekom-

munikationsanbieters. Sie benötigen daher keinen zusätzlichen Terminaladapter mehr.

5.2.2

G.703 – einfache Basis für 2-Mbit-Verbindungen

G.703 bezeichnet eine Empfehlung der ITU (International Telecommunication Union) für digitale Fernverbindungen mit Übertragungsgeschwindigkeiten ab 64 kbit/Sekunde. In Europa werden 2-Mbit-Verbindungen nach G.703 als E1-Verbindungen bezeichnet. Der in Amerika übliche Standard T1 funktioniert wie E1, hat aber eine geringere Bandbreite von nur 1544 kbit/Sekunde.

Es handelt sich bei G.703 um einen Standard auf Ebene 1 des OSI-Modells, also auf der physikalischen Ebene. G.703 definiert die elektrischen und funktionalen Eigenschaften der Verbindungen.

Verbindungen nach G.703 arbeiten bitorientiert und synchron. Zwischen den beiden Endpunkten wird ein kontinuierlicher Datenstrom transferiert, unabhängig von der Tatsache, ob tatsächlich Nutzdaten zu übertragen sind, oder nicht.

Für die Umwandlung der transferierten Bits in Inhalte sind übergeordnete Protokolle notwendig, wie beispielsweise G.704.

5.2.3

G.704 bringt Struktur in den Datenstrom

Um den kontinuierlichen aber unstrukturierten Datenstrom für die Übermittlung von Inhalten verwenden zu können, bedarf es eines zusätzlichen Protokolls, das den Datenstrom mit zusätzlichen Informationen über die Struktur der übertragenen Bits versieht.

Die ITU hat deshalb gleich ein ergänzendes Protokoll zu G.703 definiert: G.704. Es ist nicht das zwingend erforderlich, G.704 als Protokoll zur Strukturierung des Datenflusses zu verwenden. Durch den Einsatz von G.704 ergeben sich jedoch eine Reihe von Vorteilen, die im weiteren Verlauf dieses Kapitels deutlich werden.

Die Kombination von G.703 und G.704 wird auch als „G.703 strukturiert“ bezeichnet, im Unterschied zum unstrukturierten „G.703“.

Aufteilung der Bandbreite in Zeitschlitze

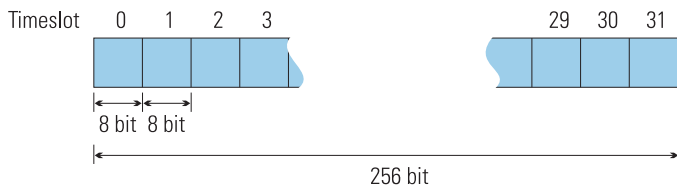
Aber von welcher Struktur ist die Rede? G.704 teilt die komplette G.703-Bandbreite in Zeitschlitze (Timeslots) ein. Für die Festlegung der Bandbreite eines einzelnen Zeitschlitzes orientiert sich der Standard an der seinerzeit minimal notwendigen Bandbreite für Sprachübermittlung. Nach dem damali-

gen Stand der Technik waren 64 kbit/Sekunde für eine saubere Sprachübermittlung notwendig. Die Zeitschlitzte sollten die kleinste unabhängige Einheit für eine einzelne Verbindung sein, deshalb wurden sie auf diese Bandbreite von 64 kbit/Sekunde fixiert.

Jeder Zeitschlitz erhielt eine definierte Datenbreite von 8 bit, es werden 8000 Datenpakete (Frames) pro Sekunde und Zeitschlitz übertragen. Daraus ergibt sich die geforderte Bandbreite eines jeden Zeitschlitzes von

$$8 \text{ bit/Frame} \times 8000 \text{ Frames/Sekunde} = 64 \text{ kbit/Sekunde}$$

Die 2-Mbit-Bandbreite von G.703 teilt sich somit in 32 Timeslots zu je 64 kbit/Sekunde. Die Timeslots sind von 0–31 durchnummeriert.



Reservierung von Zeitschlitzten für Steuerdaten

Für die Übermittlung von Framing-Daten belegt G.704 den ersten dieser 32 Zeitschlitzte (Timeslot 0) fest. Einige Endgeräte, beispielsweise bestimmte Terminaladapter, belegen auch Timeslot 16 für die Übermittlung von Steuerdaten fest. Diese festbelegten Zeitschlitzte erfüllen damit sehr ähnliche Aufgaben, für die im ISDN der D-Kanal zuständig ist. Alle nicht belegten Zeitschlitzte bleiben der Übermittlung von Nutzdaten erhalten. Sie entsprechen in Funktion und Bandbreite den bekannten B-Kanälen im ISDN.

Grundsätzlich können beliebige Kombinationen von Zeitschlitzten für die Nutz- und für die Steuerdaten verteilt werden, nur Timeslot 0 ist für die G.704-Framing-Informationen reserviert. Die zwischengeschalteten Vermittlungsstellen betrachten die Zeitschlitzte 1–31 immer als Nutzdaten. Die Verteilung dieser 31 Zeitschlitzte auf Nutzdaten und ergänzende Steuerdaten wird alleine durch die Konfiguration der beiden Endgeräte festgelegt. Für feststehende Punkt-zu-Punkt-Verbindungen gibt es normalerweise keinen Grund, einen der 31 Zeitschlitzte für die Übertragung zusätzlicher Steuerdaten zu reservieren.

Freie Kopplung von Zeitschlitzten

Nach G.704 ist optional auch eine Kopplung dieser Zeitschlitzte zu einer größeren Bandbreite möglich. Die Kopplung wird in den Endgeräten eingestellt. Die gekoppelten Zeitschlitzte ergeben Verbindungskanäle mit entsprechender Bandbreite. Diese Verbindungskanäle können auch für Festverbindungen zu unterschiedlichen Gegenstellen verwendet werden.

Die Geräte der Serie ELSA LANCOM Business 6000 sind für den Betrieb nur eines Verbindungskanals ausgelegt und unterstützen die freie Zuordnung von Zeitschlitzten zu Verbindungskanälen nicht.

G.704 gibt nur diese zusammengefassten Blöcke von Zeitschlitzten zur Nutzdatenübertragung an übergeordnete Protokolle weiter. Der ehemals unstrukturierte G.703-Datenstrom bleibt ihnen verborgen.

Integritätsprüfung von G.704

Neben der Strukturierung der G.703-Gesamtbandbreite in Zeitschlitzte sorgt G.704 auch für eine einfache Integritätsprüfung der übermittelten Daten mittels eines 4-bit-CRC-Algorithmus und verhindert auf diese Weise Übertragungsfehler.

5.2.4

Welche Methode für Ihren Zweck?

Halten wir fest: Unter G.703/704 sind drei Methoden üblich. Alle drei ergeben unterschiedliche Nutzdaten-Bandbreiten:

Modus	Verwendete Protokolle	Reservierte Zeitschlitzte für Steuerdaten	Anzahl Zeitschlitzte für Nutzdaten	Bandbreite für Nutzdaten
E1 unstrukturiert	G.703	–	32	2.048 kbit/Sek.
E1 strukturiert	G.703 + G.704	TS0	31	1.984 kbit/Sek.
E1 strukturiert (TS16 reserviert)	G.703 + G.704	TS0, TS16	30	1.920 kbit/Sek.

Die meisten Telekommunikationsunternehmen bieten sowohl unstrukturierte G.703-Verbindungen als auch strukturierte Verbindungen nach G.703/704 an. In Europa ist für 2-Mbit-Verbindungen die Bezeichnung E1 geläufig.

In verschiedenen Ländern haben sich für die europäischen Standards abweichende Bezeichnungen durchgesetzt. Folgender Überblick für Deutschland macht das beispielhaft deutlich:

	E1	E1 strukturiert	E1 strukturiert (TS16 reserviert)
Deutschland	D2MU	D2MS	D2MS ¹⁾

¹⁾ D2MS mit zusätzlicher Belegung des TS16 für Steuerdaten.

Die Wahl des verwendeten E1-Modus hängt zunächst vom Angebot Ihres Telekommunikationsanbieters ab. Für Anbieter mit einer stark auf Multiplexern basierenden Infrastruktur ist unstrukturiertes G.703 die bevorzugte, wenn nicht sogar einzige Verbindungsart. Anbieter mit einer stark auf Vermittlungsstationen basierenden Infrastruktur bieten auch G.704-Verbindungen an.

Auch bei unstrukturiertem G.703 – Struktur dank HDLC

Da die unstrukturierte Verbindung in keinem Fall zur Übertragung von Daten ausreicht, wird in jedem Fall ein Framing-Protokoll über den Datentransfer gelegt. Im Fall unstrukturierter G.703 über die komplette Bandbreite, bei G.704 über die sich ergebenden Zeitschlitzblöcke.

Daher ist die Datenintegrität in jedem Fall gewährleistet, wenn auch mit unterschiedlichen Fehlerraten. Dazu einige weitere Betrachtungen:

Betriebssicherheit und Fehlerrate

Ein wichtiger Vorteil von Verbindungen nach G.704 gegenüber einer Kombination aus G.703 und einem selbstkontrollierten Layer-2-Protokoll ist die hohe garantierte Betriebssicherheit. Für unstrukturierte G.703-Verbindungen sind nur wenige Leitungsanbieter bereit, über 95% Betriebssicherheit zu garantieren.

Da Fehler bei G.704-Leitung von den Leitungsanbietern überwacht und bemerkt werden, können diese die Fehlerquelle leicht lokalisieren und korrigierend eingreifen. Bei unstrukturierten G.703-Verbindungen lassen sich Fehler nur an den Endgeräten erkennen und entsprechend schwieriger korrigieren.

Mehrere Festverbindungen

Ein wichtiger Vorteil von G.704 ist die flexible Gestaltung mehrerer Festverbindungen. Einzelne Zeitslitze können für verschiedene Festverbindungen in den Vermittlungsstellen hardwaremäßig gebündelt werden. Ohne G.704 ist die Festverbindung zu mehreren Gegenstellen nicht möglich.

Datendurchsatz

Beim Datendurchsatz schneiden G.704-Verbindungen naturgemäß schlechter ab, da Timeslots für Protokoll Daten belegt werden und damit nicht für die Übertragung von Nutzdaten zur Verfügung stehen. Bei einer G.704-Verbindung, die nur TS0 belegt, verringert sich die für Nutzdaten zur Verfügung stehende Bandbreite um über 3%. Wird zusätzlich auch TS16 belegt, so ergibt sich ein Verlust von über 6% gegenüber unstrukturiertem G.703.

Fazit

Einfacher, sicherer und zugleich flexibler ist die Verwendung des Framing-Protokolls G.704. Mit einer unstrukturierten G.703-Verbindung ist eine höhere Bandbreite möglich. Bei besonders günstigen Leitungseigenschaften (nur geringe Entfernung, wenige zwischengeschaltete Vermittlungsstellen, nur eine Gegenstelle) kann es sein, dass der erhöhte Protokoll-Overhead von G.704 nicht lohnt.

5.2.5

Einstellung der Basisprotokolle

So komplex die Welt der 2-Mbit-Standards auch ist, so einfach ist die Konfiguration Ihres *ELSA LANCOM Business*.

Für die Einrichtung einer Internet-Anbindung oder die Kopplung zweier Netze über eine 2-Mbit-Verbindung rufen Sie den entsprechenden Assistenten über *LANconfig* oder *WEBconfig* auf.

X.21-Schnittstelle

Bei der Verwendung der X.21-Schnittstelle und eines Terminaladapters sind keine weiteren Eingaben notwendig. Hier wird die Konfiguration aller Verbindungsparameter am Terminaladapter vorgenommen, sofern dieser nicht sogar fest eingestellt ist.

G.703-Schnittstelle

Falls Sie eine G.703-Schnittstelle für die Verbindung auswählen, werden Sie nach den zu verwendenden Basisprotokollen gefragt.

Dabei gibt es drei Möglichkeiten:

- **'E1-U'** – unstrukturiertes E1
- **'E1-S (mit TS16)'** – strukturiertes E1, nur TS0 reserviert
- **'E1-S'** – strukturiertes E1, TS0 und TS16 reserviert

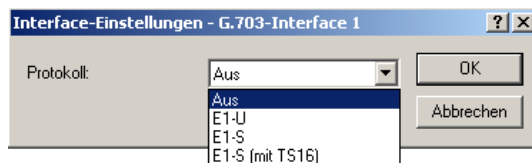
Die Wahl zwischen **E1-U** und **E1-S (mit TS16)** hängt davon ab, wie Ihr Leistungsanbieter die Leitung konfiguriert hat, ob er die Leitung auf unstrukturisiertes G.703 eingestellt hat, oder ob er zusätzlich Framing nach G.704 verwendet. **E1-S** wählen Sie nur in dem einen Fall, wenn das Gerät auf der Gegenseite zwingend TS16 für Steuerdaten reserviert. Bei einigen Terminaladaptoren ist das der Fall.

Manueller Zugriff auf die Einstellung

Die Interface-Einstellungen können Sie jederzeit manuell ändern. Sie finden das Menü unter:

- **LANconfig**

Management ► Interfaces ► Interface-Einstellungen



- **WEBconfig**

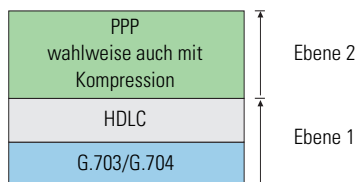
Experten-Konfiguration ► Setup ► Interface ► G.703-Interface

- **Telnet**

/Setup/Interfaces/G703-Interfaces

Weitere Einstellungen durch die Assistenten

Die Assistenten nehmen automatisch eine Reihe weiterer Einstellungen vor. Folgender Protokoll-Aufbau wird für die Verbindung standardmäßig eingestellt:



Für den Aufbau einer Verbindung zwischen zwei ELSA-Routern sind diese Einstellungen nahezu ideal. Nur bei Endgeräten, die andere Einstellungen erfordern, müssen Sie die Konfiguration von Hand anpassen. Die entsprechenden Einstellungstabellen finden Sie unter *LANconfig* im Bereich 'Kommunikation':

- Allgemein ► Kommunikations-Layer
- Gegenstellen ► Namenliste
- Gegenstellen ► Kanal-Liste
- Protokolle ► PPP-Liste

Unter *WEBconfig* befinden sich die Änderungen im Untermenü **Experten-Konfiguration ► Setup ► WAN-Modul** in den Tabellen:

- Namen-Liste
- Layer-Liste
- PPP-Liste
- Kanal-Liste

5.3

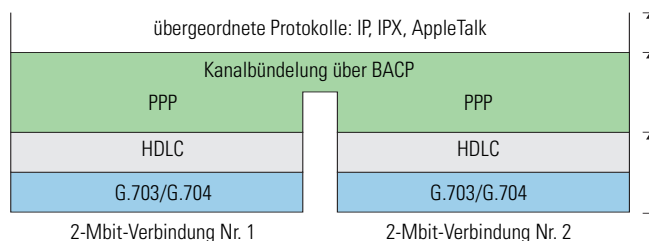
Bündelung von 2-Mbit-Verbindungen

Beim *ELSA LANCOM Business 6021* besteht die Möglichkeit, eine 4-Mbit-Verbindung durch Bündelung zweier 2-Mbit-Verbindungen aufzubauen. Dazu muss auch das Gerät auf der Gegenseite die Bündelung von zwei 2-Mbit-Verbindungen unterstützen.

Beim *ELSA LANCOM Business 6021* können nur zwei der drei 2-Mbit-Schnittstellen (eine X.21- und zwei G.703-Schnittstellen) gleichzeitig betrieben werden. Sie haben also die Möglichkeit, entweder die beiden G.703-Schnittstellen parallel zu benutzen, oder eine G.703-Schnittstelle mit einer Verbindung über den X.21-Anschluss zu kombinieren.

Die Bündelung findet im Datalink-Layer des OSI-Modells, also auf Ebene 2, statt. Sie erfolgt über das BACP-Protokoll (**B**andwidth **A**llocation **C**ontrol **P**rotocol) in Verbindung mit PPP (**P**oint-to-**P**oint **P**rotocol). Diese Protokoll-Kombination wird häufig auch als MLPPP (**M**ulti**L**ink **P**PP) bezeichnet.

Die Protokoll-Anordnung der gemeinsamen Verbindung sieht bei zwei 2-Mbit-Verbindungen wie folgt aus:



Die Kanalbündelung wird in der Kanal-Liste eingetragen:

● **LANconfig**

Kommunikation ► Kanal-Liste

The screenshot shows a dialog box titled 'Kanal-Liste - Eintrag bearbeiten'. It has the following fields and values:

- Gegenstelle: ZENTRALE (dropdown menu)
- Mindestens: 1 (text input)
- Höchstens: 1 (text input)
- Reihenfolge: 3-1 (text input)
- Backup-Kanäle: 0 (text input)

Buttons: OK, Abbrechen.

● **WEBconfig**

Experten-Konfiguration ► Setup ► WAN-Modul ► Kanal-Liste

● **Telnet**

/Setup/WAN-Modul/Kanal-Liste

In den Felder 'Mindestens' und 'Höchstens' wird die entsprechende Anzahl der Kanäle eingetragen. Der höchste sinnvolle Wert für eine 4-Mbit-Verbindung ist '2'.

Unter 'Reihenfolge' wird festgelegt, über welchen Kanal die Verbindung zunächst aufgebaut und welcher Kanal später hinzugebündelt wird. Die zuerst aufgebaute Verbindung wird innerhalb der BACP-Konventionen als 'Master', die hinzugebündelte als 'Slave' bezeichnet.

Die im Feld 'Reihenfolge' zu verwendende Kanalbezeichnung setzt sich aus zwei Ziffern zusammen, die mittels eines Bindestriches getrennt werden – beispielsweise '1-1'. Die erste Ziffer bezeichnet die Schnittstelle des Gerätes (im Beispiel die ISDN-Schnittstelle), die zweite den innerhalb der Schnittstelle verwendeten Kanal (im Beispiels erster B-Kanal). Beim *ELSA LANCOM Business 6021* stehen folgende Kanäle zur Verfügung:

Bezeichnung	Schnittstelle und Kanalnummer
1-1	ISDN-S ₀ -Bus, erster B-Kanal
1-2	ISDN-S ₀ -Bus, zweiter B-Kanal
2-1	X.21-Schnittstelle (hat nur einen Kanal)
3-1	erste G.703-Schnittstelle (neben der ISDN-Schnittstelle)
4-1	zweite G.703-Schnittstelle (ganz links)



Die ISDN-Kanäle sind in dieser Tabelle nur aus Gründen der Vollständigkeit erwähnt. Es hat in der Praxis keinen Sinn, ISDN-Kanäle mit 2-Mbit-Verbindungen zu bündeln. Dazu im weiteren Verlauf des Abschnittes mehr.

Im Feld 'Reihenfolge' werden die eingegebenen Kanäle mit einem Semikolon getrennt. Ein typischer Eintrag ist '3-1;4-1'. Mit diesem Eintrag wird die Verbindung zunächst über die erste G.703-Schnittstelle aufgebaut (diese Verbindung wird Master), später kommt dann die Verbindung über die zweite G.703-Schnittstelle hinzu (als Slave).

Die langsamste Verbindung entscheidet

Vorsicht bei Verbindungen mit unterschiedlichen Nutzdaten-Bandbreiten: Bei der Bündelung entscheidet die langsamste Verbindung über die Geschwindigkeit der gesamten Verbindung. Die überschüssige Bandbreite der schnelleren Verbindung wird nicht verwendet!

Wenn beispielsweise eine Verbindung über Kanal 4-1 mit einer Nutzdaten-Bandbreite von 1.920 kbit/Sekunde zu einer Verbindung über Kanal 3-1 mit 2.048 kbit/Sekunde gebündelt wird, so werden auch von dem schnelleren Kanal lediglich 1.920 kbit/Sekunde verwendet. Die Gesamtbandbreite beträgt anstelle der erwarteten 3.968 kbit/Sekunde nur 3.840 kbit/Sekunde.

Besonders auffällig wird der Geschwindigkeitsverlust bei der Bündelung einer 2-Mbit-Verbindung mit einem ISDN-Kanal: Hier beschränkt die langsame ISDN-Verbindung auch den Datendurchsatz der 2-Mbit-Verbindung auf nur noch 64 kbit/Sekunde.

6

Funktionen und Betriebsarten



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

- Sicherheitseinstellungen
 - Sicherheit für die Konfiguration
 - Sicherheit für das LAN
- IP-Adressmanagement für das LAN
 - Automatische Adressverwaltung mit DHCP
 - DNS-Server
- NetBIOS-Proxy zur Kopplung von Windows-Netzwerken
- SYSLOG-Funktion
- ISDN
 - Aufbau von ISDN-Wählverbindungen
 - Bürokommunikation mit *ELSA LANCAPi*
 - Reservierung von B-Kanälen
 - Modem-Einwahl (bis V.90)
 - Gebührenmanagement
 - Accounting
 - Least-Cost-Router

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

6.1

Sicherheit für Ihre Konfiguration

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

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

6.1.1

Passwortschutz

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

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

6.1.2

Die Login-Sperre

Die Konfiguration im *ELSA LANCOM Business* ist durch eine Login-Sperre gegen „Brute-Force-Angriffe“ geschützt. Bei einem Brute-Force-Angriff versucht ein unberechtigter Benutzer, ein Passwort zu knacken, und so Zugang zu einem Netzwerk, einem Rechner oder einem anderen Gerät zu erlangen. Dazu spielt z.B. ein Rechner automatisch alle möglichen Kombinationen aus Buchstaben und Zahlen durch, bis das richtige Passwort gefunden wurde.

Zum Schutz gegen solche Versuche kann die maximal zulässige Anzahl von fehlerhaften Login-Versuchen eingegeben werden. Wird diese Grenze erreicht, wird der Zugang für eine bestimmte Zeit gesperrt.

Tritt auf einem Zugang die Sperre in Kraft, so sind auch alle anderen Zugänge automatisch gesperrt.

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

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

6.1.3

Zugangskontrolle über TCP/IP

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

Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP ein Zugriff auf den Rou-

ter gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen.

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

6.2 Sicherheit für Ihr LAN

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

- Identifikationskontrolle
 - Zugangsschutz mit Name und Passwort
 - Zugangsschutz über die Anruferkennung
- Rückruf an festgelegte Rufnummern
- Filterung von Datenpaketen – Firewall
- IP-Masquerading (auch NAT/PAT genannt)

6.2.1 Die Identifikationskontrolle

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

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

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

Überprüfung des Namens

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

Beim PPP-Protokoll wird überprüft, ob der von der Gegenstelle verwendete Benutzername (häufig identisch mit dem Gerätenamen) in der eigenen PPP-Liste angegeben ist.

Nur der Name, kein geheimes Passwort? Doch, auch diese Möglichkeit bietet PPP: Hier kann zusätzlich ein speziell für dieses Protokoll gültiger Schutz nach PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) oder MS-CHAP (Microsoft-Variante des CHAP) verlangt werden.

Bei PPP wird zunächst ein Benutzername (und in Verbindung mit PAP, CHAP oder MS-CHAP auch ein Passwort) beim Verbindungsaufbau an die Gegenstelle übertragen. Wählt sich ein Computer in den *ELSA LANCOM Business* ein, so fragt die verwendete Verbindungssoftware, beispielsweise das DFÜ-Netzwerk unter Windows, den zu übermittelnden Benutzernamen und das Passwort in einem Eingabefenster ab.

Baut der Router selber eine Verbindung auf, etwa zu einem Internet Service Provider, so verwendet er seinerseits Benutzername und Passwort aus der PPP-Liste. Ist dort kein Benutzername eingetragen, wird stattdessen der Gerätename verwendet.

Die PPP-Liste finden Sie in *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Protokolle' bzw. im Menü /Setup/WAN-Modul/PPP-Liste.

Außerdem kann beim PPP-Protokoll auch der Anrufer von der Gegenstelle eine Authentifizierung verlangen. Er fordert dann die Gegenstelle zur Übermittlung eines Benutzer- bzw. Gerätenamens und eines Passwortes auf.



Die Sicherungsverfahren PAP, CHAP oder MS-CHAP wenden Sie natürlich nicht an, wenn Sie selber mit dem ELSA LANCOM Business 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 ...

Überprüfung der Nummer

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

Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen. Ist ein Schutz im *ELSA LANCOM Business* 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 (Layern) verwendet werden.

6.2.2

Der Rückruf

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

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

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

Und ganz nebenbei steuern Sie über die Einstellungen die Verteilung der Kosten für die Verbindung. Ist in der Namenliste ein Rückruf 'Nach Name' vereinbart, übernimmt der rückrufende Router alle Gebühren bis auf eine, die für die Namensübermittlung benötigt wird. Ebenfalls eine Einheit fällt für den Anrufer an, wenn der Anrufer nicht über CLIP (**C**alling **L**ine **I**dentifier **P**rotocol) identifiziert wird. Ist dagegen eine Identifizierung über die Rufnummer des Anrufers erlaubt und möglich, kommt der Anrufer sogar ganz ohne Kosten weg (Rückruf über den D-Kanal).

Eine besonders effektive Methode des Rückrufs ist das Fast-Call-Back-Verfahren (zum Patent angemeldet). Dieses Verfahren beschleunigt die Rückrufprozedur beträchtlich. Das Verfahren funktioniert nur dann, wenn es von beiden Gegenstellen unterstützt wird. Alle aktuellen ELSA-Router beherrschen das Fast-Call-Back-Verfahren.

6.2.3

Filterung von Datenpaketen – Firewall

Die Firewall-Filter des *ELSA LANCOM Business* bieten Filterfunktionen für einzelne Rechner und auch ganze Netze. Sie ermöglichen einen effektiven Schutz gegen ungewünschte Eindringlinge in Ihr Netzwerk.

Einrichten der Filter

Sie haben mehrere Möglichkeiten, die Firewall-Filter einzurichten:

- **LANconfig**

IP-Router ► Filter

*Auf die Filter-Funktion können Sie in LANconfig nur zugreifen, wenn unter **Ansicht** ► **Optionen** die 'Vollständige Ansicht der Konfiguration' eingestellt ist.*

- **WEBconfig**

Experten-Konfiguration ► Setup ► IP-Router-Modul ► Firewall

- **Telnet**

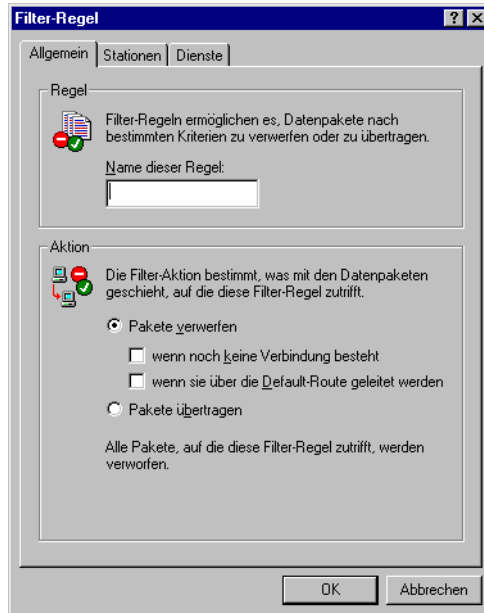
/Setup/IP-Router-Modul/Firewall

Bitte beachten Sie, dass alle Verfahren auf dieselben Konfigurationsdaten zugreifen. Wenn Sie die Filtereinstellungen beispielsweise in LANconfig ändern, hat dies auch direkte Auswirkungen auf die Werte unter WEBconfig und Telnet.



Einrichten der Filter unter *ELSA LANconfig*

Die Einrichtung der Filter mit Hilfe von *ELSA LANconfig* ist besonders komfortabel. Unter 'Filter' finden Sie die folgenden Karteikarten, mit deren Hilfe Filterregeln definiert werden können.



- 'Allgemein'
Hier wird der Name des Filterdienstes festgelegt und was mit den Datenpaketen geschehen soll (Aktion).
- 'Stationen'
Hier werden die Stationen – als Absender oder Adressat der Pakete – festgelegt, für die die Filterregel gelten soll.
- 'Dienste'
Hier wird festgelegt, für welche IP-Protokolle, Quell- und Zielports die Filterregel gelten soll.

Einrichten der Filter mit *ELSA WEBconfig* oder Telnet

Etwas schwieriger als in *LANconfig* ist die Konfiguration über *WEBconfig* oder Telnet.

Hier wird die Filterfunktion in der Filter-Liste eingestellt, die ihrerseits auf den Einträgen zweier anderer Tabellen basiert. Zum einen gibt es eine Objekt-Tabelle, in der Rechner, Netze, Protokolle etc. als Objekte definiert werden. Als zweites existiert eine Regel-Tabelle, in der Quelle, Ziel und Aktion mit Hilfe der einzelnen Objekte beschrieben werden. Aus diesen beiden Listen wird die eigentliche Filter-Liste erzeugt.

Die Filter-Liste kann zwar auch direkt erstellt werden, das ist jedoch nicht notwendig. Es reicht aus, in der Objekt-Tabelle und der Regel-Tabelle die gewünschten Eintragungen vorzunehmen, aus diesen Werten wird dann die Filter-Liste erzeugt. Auf diese Weise können keine inkonsistenten Einträge in der Filter-Liste auftauchen.

Was kann gefiltert werden? Es ist möglich, Quell- und Zielfilter für einzelne Ports oder auch Portbereiche aufzusetzen. Zudem können einzelne Protokolle oder beliebige Protokollkombinationen (TCP/UDP/ICMP) gefiltert werden.

Sobald eine Filterbedingung zutrifft, wird eine vorher bestimmte Aktion ausgeführt.

Objekt-Tabelle

In der Objekt-Tabelle werden diejenigen Elemente bzw. Objekte definiert, die in der Regel-Tabelle verwendet werden sollen. Objekte können sein:

- Protokolle
- einzelne Rechner
- ganze Netze
- Dienste

Diese Elemente lassen sich auch beliebig kombinieren. Zudem können Objekte hierarchisch definiert werden. So könnten zunächst Objekte für die Protokolle TCP und UDP definiert werden. Später kämen dann Objekte z.B. für FTP (= TCP + Ports 20 und 21), HTTP (= TCP + Port 80) und DNS (= TCP, UDP + Port 53) hinzu. Diese könnten dann wiederum zu einem Objekt zusammengefasst werden, das alle Definitionen der Einzelobjekte enthält.

Auf die direkten Beschreibungen, die Sie hier mit angeben können, wird im folgenden Abschnitt zum Thema Regel-Tabelle näher eingegangen.

Die Regel-Tabelle

In der Regel-Tabelle werden die Objekte zu Filterregeln verknüpft. Die Regel-Tabelle enthält das zu filternde Protokoll (das sie in der Objekt-Tabelle defi-

niert haben), die Quell-Objekte, die Ziel-Objekte sowie die auszuführende Filteraktion.

Das Protokoll sowie die Quell- bzw. Ziel-Objekte können sowohl aus zusammengestellten Objekten bestehen, als auch direkte Beschreibungen (z.B. %P6 für TCP) beinhalten, die durch '+' oder Leerzeichen getrennt werden. Eine direkte Beschreibung wird durch '%' gekennzeichnet. Mögliche Beschreibungen sind:

Beschreibung	Funktion
%A	IP-Adresse
%M	Netzmaske
%S	Dienst (Port)
%L	lokales Netz
%H	Hostname
%P	Protokoll (TCP/UDP/ICMP etc.)

Gleichartige Beschreibungen können durch Komma getrennte Listen, wie z.B. Host-Listen/Adresslisten (%A10.0.0.1, 10.0.0.2) oder durch Bindestrich getrennte Bereiche wie z.B. Portlisten (%S20-25) erzeugen. Die Angabe einer '0' oder eines Leerstrings bezeichnet das Any-Objekt:

alle Rechner: %A0.0.0.0

alle Dienste: %S0

alle Protokolle: %P0

Hostnamen können nur dann verwendet werden, wenn der *ELSA LANCOM Business* die Namen in IP-Adressen auflösen kann. Dafür muss der *ELSA LANCOM Business* die Namen über DHCP oder NetBIOS gelernt haben, oder die Zuordnung muss statisch in der DNS- oder IP-Routing-Tabelle eingetragen sein. Ein Eintrag in der IP-Routing-Tabelle kann dabei einem Hostnamen ein ganzes Netz zuordnen.

Die Filter-Liste

Aus Objekt-Tabelle und Regel-Tabelle wird schließlich die Filter-Liste aufgebaut. Dabei wird die Vereinigungsmenge aller durch die Regeln und Objekte definierten Filter gebildet.

Beachten Sie bitte, dass Filter bei einer Fehlangabe nicht erzeugt und auch keine Fehlermeldungen ausgegeben werden. Wenn Sie die Filter manuell



konfigurieren, sollten Sie in jedem Fall überprüfen, ob die gewünschten Filter erzeugt wurden.

6.2.4

Das Versteck – IP-Masquerading (NAT, PAT)

Eine der häufigsten Aufgaben für Router ist heute die Anbindung vieler Arbeitsplätze in einem LAN an das Netz der Netze, das Internet. Jeder soll nach Möglichkeit direkt von seinem Arbeitsplatz aus z.B. 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 Internet? Da kann doch dann auch jeder von außen dran! – Kann er nicht!

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

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

6.3

Automatische IP-Adressverwaltung mit DHCP

Für einen reibungslosen Betrieb in einem TCP/IP-Netzwerk benötigen alle Geräte in einem lokalen Netzwerk eindeutige IP-Adressen.

Zusätzlich brauchen sie noch die Adressen von DNS- und NBNS-Servern sowie eines Standard-Gateways, über das Datenpakete von lokal nicht erreichbaren Adressen geroutet werden sollen.

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

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

6.3.1

Der DHCP-Server

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

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

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

Ein völlig unkonfiguriertes Gerät kann sogar im DHCP-Automodus die IP-Adressen für sich selbst und für die Rechner im Netz selbständig festlegen.

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

6.3.2

DHCP – 'Ein', 'Aus' oder 'Auto'?

Der DHCP-Server kann drei verschiedene Zustände annehmen:

- 'Ein': Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adress-Pools) überprüft.
 - Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an.

- Bei einer fehlerhaften Konfiguration (z.B. ungültige Pool-Grenzen) wird der DHCP-Server wieder abgeschaltet und wechselt in den Zustand 'Aus'.
- 'Aus': Der DHCP-Server ist dauerhaft abgeschaltet.
- 'Auto': Der Server befindet sich im Automodus. In diesem Zustand sucht das Gerät nach dem Einschalten im lokalen Netz nach anderen DHCP-Servern. Diese Suche ist erkennbar durch das kurze Aufleuchten der Tx-LED nach dem Einschalten.
- Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Damit wird u.a. verhindert, dass ein unkonfiguriertes Gerät nach dem Einschalten im Netz Adressen vergibt, die nicht im lokalen Netz liegen.
- Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein.

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

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

6.3.3

So werden die Adressen zugewiesen

Zuweisung von IP-Adressen

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

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

- Sind beide angegeben, so hat die Intranet-Adresse den Vorrang bei der Bestimmung des Pools.

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

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

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

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

Zuweisung der Netzmaske

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

Zuweisung der Broadcast-Adresse

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



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

Zuweisung von DNS- und NBNS-Server

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

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

Zuweisung des Default-Gateways

Das Gerät weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse als Gateway-Adresse zu.

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

Gültigkeitsdauer einer Zuweisung

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

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

- **Maximale Gültigkeit in Minuten**
Hier kann die maximale Gültigkeitsdauer eingetragen werden, die der DHCP-Server einem Host zuweist.
Fordert ein Host eine Gültigkeit an, die die maximale Dauer überschreitet, so wird ihm nur diese maximale Gültigkeit zugewiesen!
Der Defaultwert von 6000 Minuten entspricht ca. 4 Tagen.
- **Default-Gültigkeit in Minuten**
Hier kann die Gültigkeitsdauer eingetragen werden, die zugewiesen wird, wenn der Host überhaupt keine Gültigkeitsdauer anfordert. Der Defaultwert von 500 Minuten entspricht ca. 8 Stunden.

Vorfahrt für den DHCP-Server – Zuweisung anfordern

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

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

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

Vorfahrt für den Rechner – Zuweisung überschreiben

Sollte ein Rechner andere Parameter verwenden als die ihm zugewiesenen (z.B. ein anderes Standard-Gateway), so müssen diese Parameter direkt am Arbeitsplatzrechner eingestellt werden. Der Rechner ignoriert dann die entsprechenden Parameter in der Zuweisung durch den DHCP-Server.

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

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

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

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

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

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

6.3.4

Konfiguration des DHCP-Servers

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

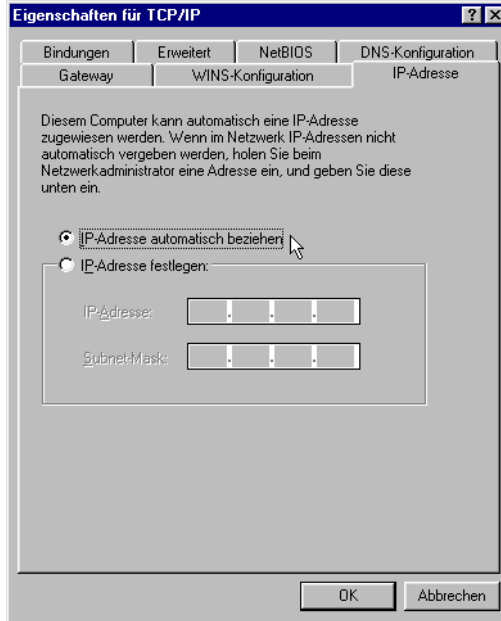
- Sie haben bisher noch kein Netzwerk eingerichtet, oder Ihr vorhandenes lokales Netz verwendet kein TCP/IP. Mit dem DHCP-Server in Ihrem neuen ELSA-Gerät können Sie auf einen Streich allen Rechnern im Netz und dem Gerät selbst IP-Adressen zuweisen.
- Sie haben auch bisher schon ein Netz mit TCP/IP,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

Konfiguration mit *ELSA LANconfig* und den Assistenten

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

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

Aktivieren Sie die Option 'IP-Adresse automatisch beziehen'. Wechseln Sie auf die Registerkarte 'DNS-Konfiguration', und löschen Sie alle vorhandenen DNS-Adressen. Löschen Sie dann auf der Registerkarte 'Gateway' alle evtl. vorhandenen Einträge und schließen alle Fenster mit **OK**. Nach einem Neustart, der mit dieser Einstellung verbunden ist, fordern die Rechner automatisch eine IP-Adresse aus dem Adress-Pool des DHCP-Servers an.



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

der zugehörigen Netzmaske zu. Aus der IP-Adresse ermittelt das Gerät dann den gültigen Adress-Pool für die DHCP-Zuweisung.

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

Manuelle Konfiguration

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

6.4

DNS

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

6.4.1

Was macht ein DNS-Server?

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

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

- Ein *ELSA LANCOM Business* kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbstständig verteilen. Der

DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-Server hätte bei der dynamischen Adressvergabe des DHCP-Servers möglicherweise Schwierigkeiten, die Zuordnung zwischen IP-Adresse und Namen aktuell zu halten.

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

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

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

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

6.4.2

So stellen Sie den DNS-Server ein

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

- ① Schalten Sie den DNS-Server ein.

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

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

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

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

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

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

- ④ Der DNS-Server dient hauptsächlich dazu, Anfragen nach Namen im Internet von den Anfragen nach Namen bei anderen Gegenstellen zu trennen. Tragen Sie daher alle Rechner in die DNS-Tabelle ein,

- ☐ deren Name und IP-Adresse Sie kennen,
- ☐ die nicht im eigenen LAN liegen,
- ☐ die nicht im Internet liegen und
- ☐ die über den Router erreichbar sind.

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

```
cd setup/dns-modul/dns-tabelle
set mail.ihredomain.de 10.0.0.99
```

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

Wenn Sie nun das Mailprogramm starten, wird es vermutlich automatisch den Server 'mail.ihredomain.de' suchen. Der DNS-Server gibt daraufhin die IP-Adresse '10.0.0.99' zurück. Das Mailprogramm sucht dann nach dieser IP-Adresse. Mit entsprechenden Einträgen in IP-Routing-Tabelle und Namenliste etc. wird dann automatisch die Verbindung zum Netz in der Zentrale hergestellt, wo der Mailserver schließlich gefunden wird.

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

```
cd setup/dns-modul/filter-liste
set 001 www.gespernte-domain.de 0.0.0.0 0.0.0.0
```

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

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



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

Durch die geeignete Wahl von IP-Adressen und Netzmasken können bei der Verwendung von Subnetting in Ihrem LAN auch einzelne Abteilungen

gefiltert werden. Dabei steht die IP-Adresse '0.0.0.0' jeweils für alle Rechner in einem Netz, die Netzmaske '0.0.0.0' für alle Netze.

6.5

NetBIOS-Proxy

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

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

6.5.1

Kurz und bündig: Was ist NetBIOS?

NetBIOS dient dazu, mehrere Rechner einfach und unkompliziert zu vernetzen. Ein wichtiger Vertreter eines NetBIOS-Netzes ist das Windows-Netz, über das sich mehrere Windows-Rechner einfach vernetzen lassen, und in dem die Ressourcen der jeweiligen Rechner (Laufwerke oder Drucker) für alle anderen freigegeben werden können.

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

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

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

IP-Adresse hinterlassen. Dabei sind die Rechner selbst für die Konsistenz der Namen im Netz verantwortlich.

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

6.5.2

Behandlung von NetBIOS-Paketen

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

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

- Zum Routen der wirklich benötigten Pakete kann im NetBIOS-Modul festgelegt werden, an welche Gegenstellen die Namensinformationen über NetBIOS übertragen werden sollen. Beim Einschalten des NetBIOS-Moduls wird nach einer zufälligen Wartezeit eine Verbindung zu den NetBIOS-Gegenstellen aufgebaut (sofern es sich nicht um einzelne Remote-Access-Rechner handelt). Gelingt der Aufbau nicht, so wird die Spanne der Wartezeit vergrößert. Mit dem anschließenden Austausch der NetBIOS-Informationen wird so erstmalig das schwarze Brett gefüllt.
- In der Funktion als Proxy beantwortet das Gerät Anfragen an die Rechner, die im NetBIOS-Modul (am schwarzen Brett) schon bekannt sind, selbst als Stellvertreter des entsprechenden Rechners. Sowohl bei Nachfragen nach Rechnern im eigenen LAN als auch nach bekannten Rechnern im Netz auf der Gegenseite werden also nach dem ersten Informationsaustausch keine neuen Verbindungen aufgebaut.

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

6.5.3

Welche Voraussetzungen müssen erfüllt sein?

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

Installierte Komponenten

Die Installation der benötigten Komponenten wird hier am Beispiel von Windows 95 bzw. Windows 98 beschrieben, läuft aber unter Windows 2000 und Windows NT 4.0 ähnlich ab. Installieren Sie die folgenden Komponenten auf allen Rechnern in den zu verbindenden Windows-Netzen:

- Netzwerkprotokoll

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



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

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

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

- Client

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

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

- Dienst

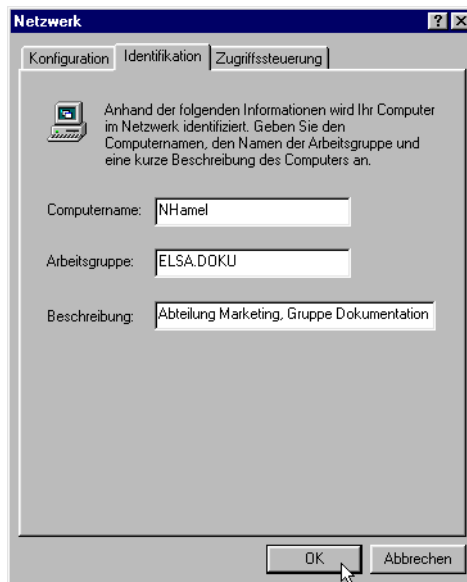
Die Datei- und Druckerfreigabe ermöglicht das Freigeben von Laufwerken oder Druckern für andere Benutzer im Windows-Netz.

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

Einstellungen im Windows-Netzwerk

- Namen und Gruppenbezeichnung

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



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

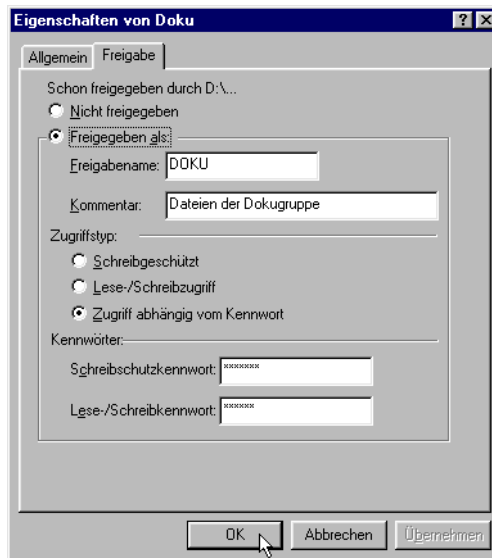
- Datei- und Druckerfreigabe

Prüfen Sie nach der Installation, ob die Datei- und Druckerfreigabe aktiviert ist. Klicken Sie dazu auf **Start ► Einstellungen ► Systemsteuerung ► Netzwerk ► Datei- und Druckerfreigabe**. Wählen Sie aus,

ob die anderen Benutzer im Windows-Netz den Drucker und/oder die Dateien von diesem Rechner nutzen können.



Alle Benutzer, die auf die freigegebenen Ressourcen zugreifen wollen, müssen sich beim Start von Windows mit Name und Passwort anmelden. Klicken Sie dann im Explorer mit der rechten Maustaste die Laufwerke, Ordner oder Drucker an, die Sie für die Benutzung durch andere Netzteilnehmer freigeben wollen, und wählen Sie den Punkt **Freigabe** aus dem Kontextmenü.



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



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

6.5.4

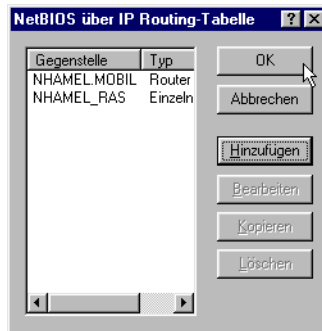
So verbinden Sie zwei Windows-Netze

Nachdem alle Vorbereitungen abgeschlossen sind, können Sie nun zwei Windows-Netze verbinden. Die Einstellungen für Arbeitsgruppennetze und Domänennetze (Windows NT und Windows 2000) sind dabei ähnlich. Die folgenden Schritte sind für beide Seiten der Verbindung auszuführen.

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

Filter für lokales Netz								
Von Ziel	Bis Ziel	Von Quell	Bis Quell	IP-Adresse	Netzmaske	Protokoll	Filtertyp	
0	0	137	139	255.255.255.255	0.0.0.0	alle	Default-R	

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



Bei der Konfiguration über Telnet geben Sie alternativ ein:

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

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



Der Parameter 'NT-Domain' kann bei Windows-95- oder Windows-98-Netzen i.d.R. frei gelassen werden. Beim Zugriff auf Windows-NT und Windows-2000-Rechner muss die entsprechende Domäne bzw. Arbeitsgruppe manuell eingetragen werden.

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

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

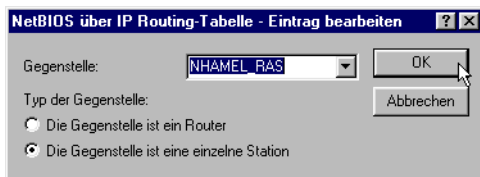
Nach dem Einschalten wird (nach einer zufälligen Wartezeit) eine Verbindung zu allen Gegenstellen aufgebaut, die nicht als Einwahl-Knoten gekennzeichnet sind. Bei dieser ersten Verbindung werden dann die notwendigen Informationen über die Rechner in den Netzen ausgetauscht. Erst danach kann auf die Rechner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

6.5.5

So wählt sich ein Remote-Access-Rechner ein

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

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



```
cd /Setup/NetBIOS-Modul/Gegenstellen-Tab.
```

```
set nhameL.ras workstation
```



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

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

6.5.6

Gesucht – Gefunden: Die Netzwerkumgebung

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

NetBIOS-Routing über LAN-LAN-Kopplung

Nachdem die Netze nach dem Einschalten der NetBIOS-Module gegenseitig die Informationen über die verfügbaren Rechner ausgetauscht haben, ist im

ELSA LANCOM Business nun eine Liste mit diesen Rechnernamen verfügbar. Über Telnet kann mit

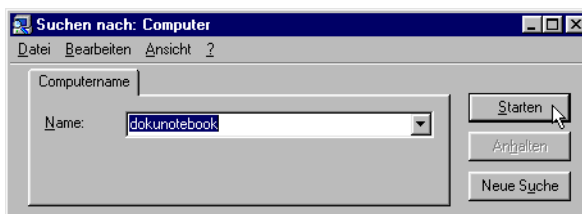
```
dir /Setup/NetBIOS-Modul/host-liste
```

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

Name	Typ	IP-Adresse	Gegenstelle	Timeout	Flags
DOKUNOTEBOOK	00	10.10.0.53	NHAMEL.MOBIL	4939	0020
DOKUNOTEBOOK	20	10.10.0.53	NHAMEL.MOBIL	4939	0020
ELSA	1d	10.10.0.53	NHAMEL.MOBIL	4939	0020
ELSA.DOKU	1d	10.1.253.246	4935	0000	
ELSA.DOKU	1d	192.168.100.162	4997	0000	
NHAMEL.MOBIL	00	10.10.0.1	NHAMEL.MOBIL	0	0020

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

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



Die Arbeitsgruppen und Rechner des entfernten Netzes können aus technischen Gründen nicht über die Funktion 'gesamtes Netzwerk durchsuchen' in der Windows-Netzwerkumgebung gefunden werden. Stattdessen kann nach entfernten Computern wie oben beschrieben gesucht werden, bzw. es können Verknüpfungen und Laufwerksverbindungen eingerichtet werden.

NetBIOS-Routing über RAS-Zugang

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

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

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

6.6

Das SYSLOG-Modul

Mit dem SYSLOG-Modul besteht die Möglichkeit, Zugriffe auf den *ELSA LANCOM Business* protokollieren zu lassen. Diese Funktion ist insbesondere für Systemadministratoren interessant, da sie die Möglichkeit bietet, eine lückenlose Historie aller Aktivitäten aufzeichnen zu lassen.

Um die SYSLOG-Nachrichten empfangen zu können, benötigen Sie einen entsprechenden Dämon bzw. Client. Unter UNIX/Linux erfolgt die Protokollierung durch den in der Regel standardmäßig eingerichteten SYSLOG-Dämon. Dieser meldet sich entweder direkt über die Konsole oder schreibt das Protokoll in eine entsprechende SYSLOG-Datei.

Unter Linux wird in der Datei `/etc/syslog.conf` angegeben, welche Facilitys (zu diesem Begriff später mehr) in welche Logdatei geschrieben werden sollen. Überprüfen Sie in der Konfiguration des Dämons, ob auf Netzwerkverbindungen explizit gehört wird.

Windows stellt keine entsprechende Systemfunktion bereit. Sie benötigen spezielle Software, die die Funktion eines SYSLOG-Dämons erfüllt.

6.6.1

Einrichten des SYSLOG-Moduls

Sie haben mehrere Möglichkeiten, das SYSLOG-Modul einzurichten:

- **LANconfig**
Management ► Meldungen

- **WEBconfig**

Vollkonfiguration ► Setup ► SYSLOG-Modul bzw.
Log und Trace ► SYSLOG-Modul konfigurieren

- **Telnet**

/Setup/SYSLOG-Modul

6.6.2

Beispielkonfiguration mit *ELSA LANconfig*

SYSLOG-Client anlegen

- ① Starten Sie *ELSA LANconfig*. Unter 'Management' wählen Sie die Karte 'Meldungen'.
- ② Schalten Sie das Modul ein, und klicken Sie auf **SYSLOG-Clients**.
- ③ Im nächsten Fenster klicken Sie auf **Hinzufügen...**
- ④ Geben Sie zunächst die IP-Adresse des SYSLOG-Clients ein, und legen Sie im weiteren die Quellen und Prioritäten fest.

SYSLOG-Clients - Neuer Eintrag

IP-Adresse:

Quelle:

<input checked="" type="checkbox"/> System	<input checked="" type="checkbox"/> Logins
<input checked="" type="checkbox"/> Systemzeit	<input type="checkbox"/> Konsolen-Logins
<input checked="" type="checkbox"/> Verbindungen	<input type="checkbox"/> Accounting
<input type="checkbox"/> Verwaltung	<input type="checkbox"/> Router

Priorität:

<input checked="" type="checkbox"/> Alarm	<input checked="" type="checkbox"/> Fehler
<input checked="" type="checkbox"/> Warning	<input checked="" type="checkbox"/> Information
<input type="checkbox"/> Debug	

SYSLOG kommt aus der UNIX-Welt, in der bestimmte Quellen vordefiniert sind. *ELSA LANCOM Business* ordnet seine eigenen internen Quellen diesen vordefinierten SYSLOG-Quellen, den sogenannten „Facilitys“, zu.

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller Nachrichtenquellen, die Sie im *ELSA LANCOM Business* einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die Zuordnung zwischen den internen Quellen des *ELSA LANCOM Business* und den SYSLOG-Facilitys an.

Quelle	Bedeutung	Facility
System	Systemmeldungen (Bootvorgänge, Timersystem etc.)	KERNEL
Logins	Meldungen über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler	AUTH
Systemzeit	Meldungen über Änderungen der Systemzeit	CRON
Konsolen-Logins	Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler	AUTHPRIV
Verbindungen	Meldungen über den Verbindungsauf- und -abbau sowie dabei auftretende Fehler (Display-Trace)	LOCAL0
Accounting	Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)	LOCAL1
Verwaltung	Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.	LOCAL2
Router	Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.	LOCAL3

Die im SYSLOG ursprünglich definierten acht Prioritätsstufen sind im *ELSA LANCOM Business* auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen Alarmlevel, Bedeutung und SYSLOG-Prioritäten.

Priorität	Bedeutung	SYSLOG-Priorität
Alarm	Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne dass ein Eingriff des Administrators notwendig wird (z.B. Verbindungsfehler).	ERROR
Warning	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z.B. Accounting-Informationen).	NOTICE, INFORM

Priorität	Bedeutung	SYSLOG-Priorität
Debug	Übertragung aller Debug-Meldungen. Debug-Meldungen erzeugen ein erhebliches Datenvolumen und beeinträchtigen den ordnungsgemäßen Betrieb des Geräts. Sie sollten daher im Regelbetrieb ausgeschaltet sein und ausschließlich zur Fehlersuche verwendet werden.	DEBUG

- ⑤ Wenn Sie alle Parameter definiert haben, bestätigen Sie die Eingaben mit **OK**. In der SYSLOG-Tabelle wird der SYSLOG-Client mit seinen Parametern eingetragen.

Facilitys

Über die Schaltfläche **Facility-Zuordnung** können alle Meldungen vom *ELSA LANCOM Business* einer Facility zugeordnet und dadurch vom SYSLOG-Dämon ohne zusätzlichen Aufwand in eine spezielle Log-Datei geschrieben werden.

Beispiel

Alle Facilitys werden auf 'local7' gesetzt. Unter Linux werden nun in der Datei '/etc/syslog.conf' durch den Eintrag

```
local7.* /var/log/lancom.log
```

alle Ausgaben des *ELSA LANCOM Business* in die Datei '/var/log/lancom.log' geschrieben.

6.7

ISDN-Verbindungen

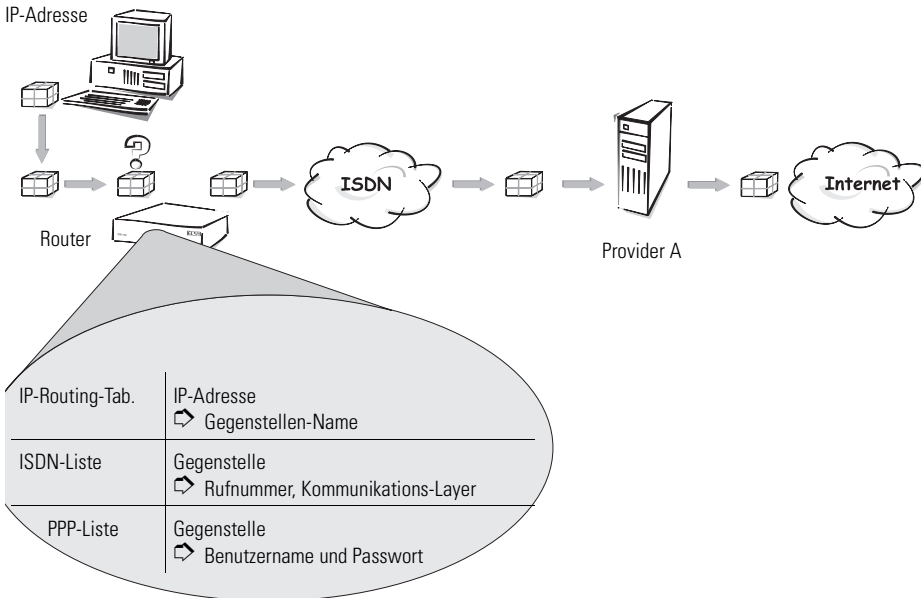
Die Datenkommunikation zwischen zwei ISDN-Endgeräten läuft über ISDN-Verbindungen ab. Bei diesen Verbindungen kann es sich prinzipiell um Wahlverbindungen oder Festverbindungen handeln.

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

Wir wollen diesen Ablauf an einem vereinfachten Beispiel verdeutlichen.

Datenpaket mit
IP-Adresse

PC des Internet-Nutzers



Ein Datenpaket aus einem Rechner findet den Weg ins Internet in erster Linie über die IP-Adresse des Empfängers. Mit dieser Adresse schickt der Rechner das Paket los über das LAN zum Router. Der Router schaut mit der IP-Adresse zunächst in der IP-Routing-Tabelle nach und findet die Gegenstelle, die zu dieser Adresse gehört, z.B. 'Provider_A'. Mit diesem Namen prüft der Router dann die ISDN-Namenliste und findet die Rufnummer der zugehörigen Gegenstelle, die über ISDN erreicht werden kann, inkl. des Kommunikations-Layers, der verwendet werden soll. Außerdem erhält der Router aus der PPP-Liste Benutzernamen und Passwort, die für die Anmeldung beim Provider A notwendig sind.

Der Router kann dann eine Verbindung auf der ISDN-Leitung zum Router des Providers aufbauen. Sobald die Verbindung hergestellt ist, kann der Router das Datenpaket über die ISDN-Leitung ins Internet weitergeben.

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

Die PPP-Liste wird in einem eigenen Kapitel beschrieben (siehe 'PPP-Liste').

Informationen zur IP-Routing-Tabelle finden Sie im Abschnitt 'IP-Routing'.

6.7.1

ISDN-Namenliste

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

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

- **Name**

Mit diesem Namen wird die Gegenstelle in den Routermodulen identifiziert.
- **Rufnummer**

Diese Rufnummer soll angerufen werden, wenn der Router selbst aktiv eine Verbindung zur Gegenstelle aufbauen soll.

Wenn die Gegenstelle unter verschiedenen Rufnummern erreicht werden kann, tragen Sie die weiteren Rufnummern in der Round-Robin-Liste ein.

Wird diese Gegenstelle über eine Festverbindung erreicht, kann hier die Rufnummer für eine Backup-Leitung über Wählverbindung angegeben werden.
- **Haltezeiten**

Diese Zeiten geben an, wie lange die B-Kanäle aktiv bleiben, nachdem

 - bei statisch aufgebauten Kanälen für die Haltezeit B1 keine Daten mehr übertragen wurden.
 - bei dynamisch aufgebauten Kanälen für die Haltezeit B2 der Datendurchsatz unter einem fest definierten Schwellwert liegt.
- **Layername**

Der Layer steht für eine Sammlung von Protokollen, die für diese Verbindung verwendet werden sollen. Der Layer muss auf beiden Seiten der Verbindung gleich eingestellt sein.
- **Rückruf**

Wenn der Router einen Anruf von dieser Gegenstelle erhält, können Sie hier optional einstellen, dass der Anruf nicht angenommen wird. Stattdessen wird die Gegenstelle zurückgerufen mit den folgenden Optionen:

 - normaler Rückruf
 - Rückruf nach dem schnellen ELSA-Verfahren
 - Rückruf nach Überprüfung des Namens

- selbst den Rückruf der Gegenstelle nach dem schnellen ELSA-Verfahren erwarten

6.7.2

Interface-Einstellungen

Sie finden die Interface-Einstellungen in *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Interfaces', in *WEBconfig* unter **Experten-Konfiguration ► Setup ► Interface** und bei Telnet- oder Terminalsitzungen unter `/Setup/Interface`.

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

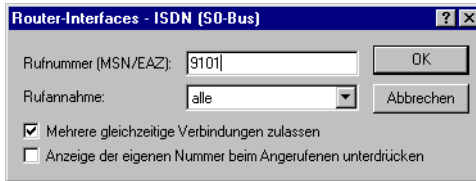
- Das D-Kanal-Protokoll, das an diesem S₀-Anschluss verwendet wird.
Automatische Erkennung: DSS1 (Euro-ISDN), DSS1 Punkt-zu-Punkt, 1TR6, Festverbindung Gruppe 0
- Festverbindungsoption
B-Kanal, der ggf. für die Festverbindung verwendet werden soll
- Anwahlpräfix
Nummer, die bei abgehenden Rufen der Rufnummer vorangestellt wird, z.B. die Amtskennziffer beim Betrieb an TK-Anlagen

6.7.3

Einstellungen für Wählverbindungs-Interfaces

Für die Interfaces mit Wählverbindung gibt es noch einige erweiterte Router-Einstellungen. Unter 'Router-Interface-Einstellungen' in *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Allgemein'. In *WEBconfig* finden sich diese Einstellungen unter **Experten-Konfiguration ► Setup ► WAN-Modul ► Router-Interface-Liste** und bei Telnet- oder Terminalsitzungen unter `/Setup/WAN-Modul/Router-Interface-Liste`.

In den Router-Interface-Einstellungen legen Sie für jedes Wählverbindungs-Interface die Parameter fest, die in der Betriebsart als Router verwendet werden. Diese Parameter gelten nicht für die anderen Betriebsarten der Geräte.



Es sind im Einzelnen:

- Rufnummern (MSN/EAZ)

Auf diese Rufnummern reagiert der Router bei eingehenden Anrufen. Mehrere Rufnummern werden durch Semikolon getrennt. Ohne Eingabe der Rufnummer reagiert der Router auf alle anliegenden Rufnummern.

Die erste der eingetragenen Rufnummern wird bei aktivem Verbindungsaufbau an die Gegenstelle übertragen. Ohne Eingabe der Rufnummer wird die Haupt-MSN des Anschlusses übertragen.

- Rufannahme

Hier können Sie Rufannahme auf digitale oder analoge Einwahlen beschränken.

- Mehrere gleichzeitige Verbindungen zulassen

Hier können Sie auswählen, ob auf diesem Anschluss gleichzeitig mehrere Verbindungen zu verschiedenen Gegenstellen bestehen dürfen. Durch Abschalten dieser Option können Sie gewährleisten, dass immer Kanäle für die Verbindung zu bestimmten Gegenstellen zur Verfügung steht.

- Unterdrückung der eigenen Rufnummer

Schalten Sie diese Option ein, wenn die eigene Rufnummer bei aktivem Verbindungsaufbau des Routers nicht bei der Gegenstelle angezeigt werden soll.

Diese Funktion muss vom Netzbetreiber unterstützt werden.

6.7.4

Interface-Einstellungen für *LANCPI*

Sie finden die Interface-Einstellungen für *LANCPI* in *ELSA LANconfig* im Konfigurationsbereich 'LANCPI' auf der Registerkarte 'Allgemein' oder bei

Telnet- oder Terminalsitzungen unter `/Setup/LANCAPI-Modul/Interface-Liste`.

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

- Rufnummern (MSN/EAZ)

Auf diese Rufnummern reagiert die *LANCAPI* bei eingehenden Anrufen. Mehrere Rufnummern werden durch Semikolon getrennt. Ohne Eingabe der Rufnummer reagiert der Router auf alle anliegenden Rufnummern.

- Zugriff auf die *LANCAPI*

Hier können Sie die Funktion der *LANCAPI* für das Interface ganz ausschalten, nur für ausgehende Rufe oder für ein- und ausgehende Rufe zulassen.

- Übertragung der eigenen Rufnummer

Normalerweise wird beim aktiven Verbindungsaufbau über die *LANCAPI* die Rufnummer übermittelt, die in der CAPI-Applikation eingestellt wurde. Falls diese Rufnummer fehlt oder nicht gültig ist, überträgt die *LANCAPI* keine Rufnummer. Mit dieser Option können Sie festlegen, dass bei fehlender Rufnummer der CAPI-Applikation stattdessen die erste im Feld 'Rufnummer' eingetragene Nummer übertragen wird.

6.7.5

Layer-Liste

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

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

- Layername

Unter diesem Namen werden die Protokoll-Einstellungen gespeichert. In der Namenliste wählen Sie die Einstellungen mit dem Layernamen für die entsprechende Verbindung aus.

- Encapsulation

Stellen Sie hier ein, ob den Datenpaketen ein Ethernet-Header hinzugefügt werden soll. Normalerweise reicht die Einstellung 'Transparent', nur bei HDLC-Verbindungen zu Fremdgeräten kann diese Einstellung notwendig sein.

- Layer-3

Layer-3-Protokoll für die Verbindung. Wird bei ankommenden Rufen teilweise automatisch erkannt.

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

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

- Layer-2

Layer-2-Protokoll für die Verbindung

- Optionen

Aktiviert optional die Kompression der Daten und die Kanalbündelung. Diese Optionen werden nur wirksam, wenn sie von den Protokollen auf Layer 2 und Layer 3 unterstützt werden.

- Layer-1

Layer-1-Protokoll für die Verbindung. Wird bei ankommenden Rufen teilweise automatisch erkannt.

6.7.6

Round-Robin-Liste

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

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

- Gegenstelle

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

- Round-Robin

Weitere Rufnummern für diese Gegenstelle. Mehrere Nummern werden durch Bindestriche getrennt.

- Anfangen mit:
Geben Sie an, ob ein neuer Verbindungsaufbau mit der zuletzt erfolgreichen Nummer gestartet werden soll oder immer mit der ersten Nummer der Liste.

6.7.7

Kanal-Liste

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

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

- Gegenstelle
Name der Gegenstelle, wie sie vorher in der Namenliste definiert wurde.
- Mindestens
Minimale Anzahl von Kanälen, die für die Verbindung aufgebaut werden sollen.

Wird mehr als ein Kanal angegeben, entsteht für diese Verbindung eine statische Kanalbündelung. Der verwendete Layer muss in den Layer-2-Optionen auf Bündelung eingestellt sein.
- Höchstens
Maximale Anzahl von Kanälen, die für die Verbindung aufgebaut werden sollen.

Werden mehr maximale als minimale Kanäle angegeben, entsteht für diese Verbindung eine dynamische Kanalbündelung. Der verwendete Layer muss in den Layer-2-Optionen auf Bündelung eingestellt sein.
- Reihenfolge
Die Reihenfolge, in der die Kanäle aufgebaut werden sollen, wird in der Syntax `[Interface]-[Kanal];[Interface]-[Kanal]` usw. angegeben.
- Backup
Anzahl der Kanäle, die bei einer Festverbindung über Wählleitungen aufgebaut werden sollen, wenn die Festverbindung gestört ist.

6.7.8

Script

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

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

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

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

6.7.9

Rufannahme

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

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

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

- Name oder Nummer

Der Anruf wird angenommen, wenn eine der beiden Überprüfungen erfolgreich ist.

6.7.10

Nummernliste

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

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

- Rufnummer

Rufnummer, die von der anrufenden Gegenstelle übermittelt wird (ggf. inkl. Landes- und Orts-Kennzahlen).

- Gegenstelle

Name der Gegenstelle, wie sie in der Namenliste definiert wurde. Ist in der Namenliste ein Rückruf definiert, wird diese Gegenstelle zurückgerufen.

6.8

Bürokommunikation und *ELSA LANCAP*

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

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

6.8.1

Die *ELSA LANCAP*

Welche Vorteile bietet die *LANCAP*?

Der Einsatz der *LANCAP* bringt vor allem wirtschaftliche Vorteile. Alle Arbeitsplätze, die im LAN (Local Area Network) integriert sind, erhalten über die *LANCAP* uneingeschränkten Zugriff auf Bürokommunikations-Funktionen wie Fax, Anrufbeantworter, Onlinebanking und EuroFile-Transfer. Ohne

zusätzliche Hardware an jedem einzelnen Arbeitsplatz werden alle Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsplätzen installiert.

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

Faxen über die Hardware

Beim Faxen über die *LANCAPi* wird die benötigte Rechenleistung vom Prozessor im *ELSA LANCOM Business* bereitgestellt. Das Gerät bietet damit über die *LANCAPi* eine echte Hardwarefax-Funktion an, die den faxenden Arbeitsplatzrechner deutlich entlastet.

Die *LANCAPi* wird bei der Installation der meisten Faxprogramme, die den CAPI-Betrieb unterstützen, automatisch als Hardwarefax Class II erkannt und automatisch verwendet.

Installation des *LANCAPi*-Clients

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

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

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

Einstellen des *LANCAPi*-Clients

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

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



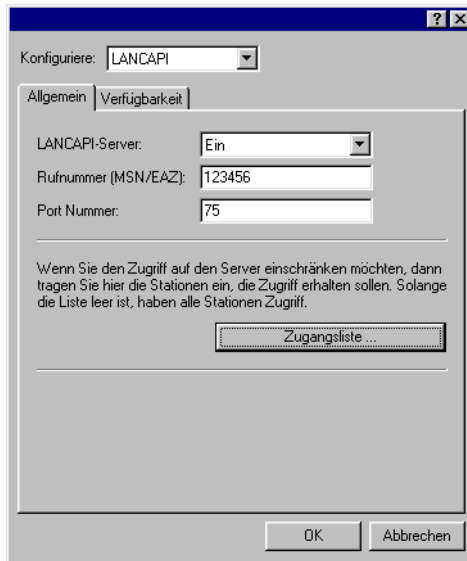
Einstellen des *LANCAPI*-Servers

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

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

So stellen Sie die entsprechenden Parameter ein:

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



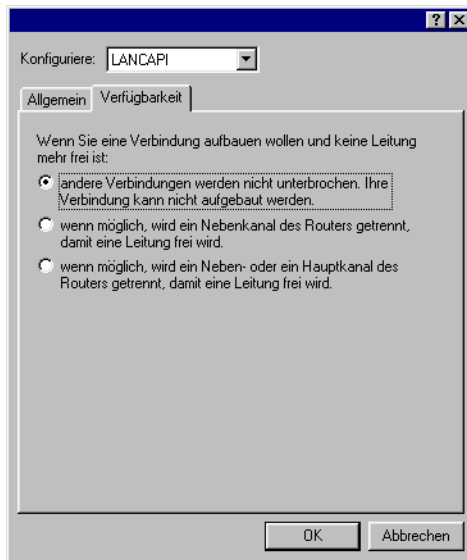
- ② Schalten Sie den *LANCAPI*-Server ein, oder lassen Sie nur abgehende Anrufe zu. In diesem Fall reagiert die *LANCAPI* nicht auf ankommende Rufe und kann z.B. nicht zum Empfangen von Faxmitteilungen eingesetzt werden. Lassen Sie z.B. dann nur abgehende Rufe zu, wenn Sie für die *ELSA LANCAP* keine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



Wenn Sie mehrere Rufnummern für die LANCAP eingeben, können Sie den einzelnen Arbeitsplätzen z.B. ein persönliches Fax oder einen persönlichen

Anrufbeantworter bereitstellen. Dazu geben Sie bei der Installation der Kommunikationsprogramme wie z.B. *ELSA-RVS-COM* an verschiedenen Arbeitsplätzen jeweils verschiedene Rufnummern an, auf die das Programm reagieren soll.

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



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

So verwenden Sie die *LANCAPI*

Zur Verwendung der *LANCAPI* gibt es zwei Möglichkeiten:

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

6.9

ELSA CAPI Faxmodem

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

Installation

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

Faxen über *ELSA CAPI Faxmodem*

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



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

6.10

Gebührenmanagement

Die Eigenschaft des Routers, Verbindungen selbstständig zu allen gewünschten Gegenstellen aufzubauen und sie mit dem Ende der Übertragung wieder zu beenden, ermöglicht dem Benutzer sehr komfortablen Zugriff z.B. auf das Internet. Bei der Datenübertragung über kostenpflichtige Leitungen können jedoch durch Fehlkonfiguration des Routers (z.B. bei der Filterkonfiguration) oder durch übermäßigen Gebrauch des Angebots (z.B. andauerndes Surfen im Internet) recht hohe Kosten entstehen.

Um diese Kosten zu begrenzen, bietet die Software verschiedene Möglichkeiten:

- Die verfügbaren ISDN-Verbindungsgebühren können für eine bestimmte Periode eingeschränkt werden.
- Die verfügbaren ISDN-Verbindungsminuten können für eine bestimmte Periode eingeschränkt werden.

6.10.1

Gebührenabhängige ISDN-Verbindungsbegrenzung

Werden an einem ISDN-Anschluss Gebühreninformationen übermittelt, können die anfallenden Verbindungsgebühren recht einfach eingeschränkt werden. Im Default-Zustand dürfen z.B. maximal 830 Gebühreneinheiten in sechs Tagen verbraucht werden. Ist diese Grenze erreicht, erlaubt der Router keinen weiteren aktiven Verbindungsaufbau.



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



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

6.10.2

Zeitabhängige ISDN-Verbindungsbegrenzung

Der Mechanismus der ISDN-Gebührenüberwachung greift nicht, wenn am ISDN-Anschluss keine Gebühreninformationen übertragen werden. Das ist z.B. dann der Fall, wenn die Übermittlung der Gebühreninformationen entwe-

der nicht beantragt wurde oder die Telefongesellschaft diese Informationen grundsätzlich nicht übermittelt.

Um die Kosten für ISDN-Verbindungen auch ohne Gebühreninformationen begrenzen zu können, kann die maximale Verbindungsdauer mit Hilfe der Zeit gesteuert werden. Dazu wird ein Zeitbudget für eine Periode vereinbart. Im Default-Zustand dürfen z.B. für maximal 210 Minuten innerhalb von sechs Tagen Verbindungen aktiv aufgebaut werden.



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

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

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



6.10.3

Einstellungen im Gebührenmodul

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

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

- **Tage/Periode**
Dauer einer Überwachungsperiode in Tagen angegeben
- **Budget-Einheiten, ISDN-Minuten-Budget**
Maximale ISDN-Einheiten bzw. ISDN-Online-Minuten in einer Überwachungsperiode
- **Rest-Budget, Rest-ISDN-Minuten**
Verfügbare ISDN-Einheiten bzw. ISDN-Online-Minuten in der gegenwärtigen Periode
- **Router-Einheiten, Router-ISDN-Minuten**
ISDN-Einheiten bzw. ISDN-Online-Minuten über alle Perioden
- **Gesamteinheiten**
Alle im Gerät anfallenden Gebühren

- Tabelle-Budget, Zeit-Tabelle

Tabellen mit Gebühren bzw. Zeiten für die jeweiligen Module



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

6.11

Accounting

Beim Accounting werden die Online-Zeiten und die übertragenen Datenvolumen ermittelt und nach den verursachenden Rechnern aufgeschlüsselt. Die Accounting-Daten werden in einer Liste für die aktuellen Verbindungen und in einer akkumulierten Liste abgelegt.

Dabei werden die folgenden Daten erfasst:

- User (Name, IP-Adresse, MAC-Adresse)

Die Online-Zeiten und die übertragenen Datenvolumen werden zunächst den MAC-Adressen der Rechner-Netzwerk-Interfaces im LAN zugeordnet. Aus DHCP- oder DNS-Server-Modulen kann der Router ggf. zusätzliche Informationen über die Zuordnung von MAC-Adressen und Rechnernamen verfügen. In diesem Fall kann die Online-Zeit auch direkt den Rechnernamen zugeordnet werden. Ist eine Zuordnung von MAC-Adresse zu Rechnernamen nicht möglich, wird eine andere verfügbare Information zur Kennzeichnung der Nutzer eingetragen, z.B. die IP-Adresse.

Bei Netzwerk-Teilnehmern, die über eine Dial-In-Verbindung Zugriff auf das LAN haben, ist i.d.R. die MAC-Adresse nicht bekannt. In diesem Fall erzeugt der Router eine Pseudo-Adresse, mit der die Dial-In-Gegenstellen beim Accounting identifiziert werden.

- Gegenstelle, zu der die Verbindung aufgebaut wurde
- Art der Verbindung
- Datenvolumen in Sende- und Empfangsrichtung
- Online-Zeit

Bei Wählverbindungen, die von mehreren Usern gemeinsam verwendet werden, kann die gesamte Dauer einer Verbindung länger sein als ein Teilnehmer sie wirklich benutzt. Daher wird in diesen Fällen die Dauer der Verbindung anhand der ersten und der letzten Aktion eines Users berechnet, zuzüglich der für die Verbindung gültigen Haltezeit.

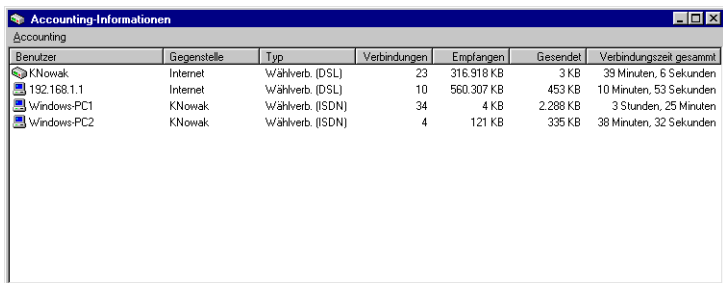
- Anzahl der Verbindungen
In diesem Feld wird angezeigt, wie oft die Aktion eines Users zu einem Verbindungsaufbau geführt hat.

6.11.1 Konfiguration des Accountings

Die Einstellungen für das Accounting sind unter `/Setup/Accounting` zu finden. Dort können das Accounting ein- oder ausgeschaltet und die Speicherung im Flash-ROM aktiviert werden. Außerdem kann hier die Sortierung der akkumulierten Tabelle nach Online-Zeit oder Transfervolumen beeinflusst werden.

6.11.2 Ablesen der Accounting-Informationen

Eine Anzeige der aufgezeichneten Daten ist möglich über *ELSA LANmonitor*. Dabei können die Daten auch als Datei auf einem Datenträger gesichert werden.



Benutzer	Gegenstelle	Typ	Verbindungen	Empfangen	Gesendet	Verbindungszeit gesamt
KNowak	Internet	Wählverb. (DSL)	23	316.918 KB	3 KB	39 Minuten, 6 Sekunden
192.168.1.1	Internet	Wählverb. (DSL)	10	560.307 KB	453 KB	10 Minuten, 53 Sekunden
Windows-PC1	KNowak	Wählverb. (ISDN)	34	4 KB	2.288 KB	3 Stunden, 25 Minuten
Windows-PC2	KNowak	Wählverb. (ISDN)	4	121 KB	335 KB	38 Minuten, 32 Sekunden

Beim Zugriff über Telnet können die jeweils aufgezeichneten Daten ebenfalls unter `/Setup/Accounting` abgefragt werden.

Aufgeschlüsselt nach Benutzername und Gegenstelle werden jeweils die folgenden Informationen aufgelistet:

- Username
Name des Users oder seine Layer-3-Adresse (IP-Adresse, IPX-Adresse oder im Bridge-Betrieb nochmal die MAC-Adresse)
- Gegenstelle
Gegenstelle, mit der der Nutzer Daten ausgetauscht hat
- Verbindungs-Typ
Art der Verbindung

- Rx-Bytes, Tx-Bytes
Datenvolumen auf dem Interface
- Gesamtzeit
Gesamte Online-Zeit für genau diesen User zu genau dieser Gegenstelle
- Verbindungen
Anzahl der für den User zu dieser Gegenstelle gezählten Verbindungen



Wenn ein User eine Verbindung zu einer anderen Gegenstelle aufbaut, wird ein neuer Eintrag in der Tabelle erzeugt. Alle Transfervolumen und Online-Zeiten von einem User zu einer Gegenstelle werden in einem Eintrag erfasst.

*Je nach Sortierung der Liste werden 512 Einträge mit dem größten Transfer-
volumen oder mit der größten Online-Zeit in der Tabelle erfasst.*

6.12

Der Least-Cost-Router

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

Für Telefonate zu bestimmten Tageszeiten und in verschiedenen Regionen ist der jeweils günstigste Tarif jedoch leider nicht bei immer demselben Provider, sondern oft bei verschiedenen Anbietern zu finden: morgens Provider 1, nachmittags Provider 2 und für Auslandsgespräche evtl. Provider 3. Um immer besonders günstig zu telefonieren, im Internet zu surfen oder Daten zu anderen Netzen zu übertragen, müssten Sie nun eigentlich vor jeder Verbindung überlegen, welcher Tarif nun gerade der günstigste ist. Ein *ELSA LANCOM Business* nimmt Ihnen diese Arbeit ab. Least-Cost-Routing (LCR) heißt die Funktion, die hier hilft. Sie definieren dabei einmal, welche Provider für Ihre Bedürfnisse die günstigsten Tarife haben, und das Gerät wählt bei jeder Verbindung (egal ob über Router, *LANCAP*/etc.) automatisch den Anbieter mit dem günstigsten Tarif.

6.12.1

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

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

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

Der LCR benötigt also folgende Eingaben:

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

Die ersten Versuche

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

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

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

Diese Einträge bedeuten, dass alle Verbindungen am Wochenende nach München (oder andere Nummern, die mit '089' beginnen) über den Provider

mit der Netzkennzahl '01097' geführt werden. Wochentags wird für diese Rufe in der Zeit zwischen 8:00 Uhr und 18:00 Uhr der Provider mit der Netzkennzahl '01098' verwendet. Auslandsgespräche am Sonntag gehen über den Provider mit der Netzkennzahl '01097'.

Für Fortgeschrittene: LCR mit System

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

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

- Einige Ortsnetze erreichen Sie zwar über eine Vorwahl, trotzdem aber zum normalen Ortstarif. Falls Sie diese Bereiche mit einem allgemeinen Eintrag umgeleitet haben, können Sie die Vorwahlen mit Ortstarif über die Vorwahl Ihrer Telefongesellschaft umleiten. Ein leerer Eintrag für die Netzkennzahl bedeutet ebenfalls „keine Umleitung“.
- Vielleicht geht der größte Teil Ihrer ISDN-Verbindungen in die gleichen Ortsnetze. Wenn die meisten Ihrer Gegenstellen in München liegen, können Sie diese Gegenstellen über einen bestimmten Anbieter erreichen.

- Untersuchen Sie die verschiedenen Tarifzonen. Welche Vorwahlen in welche Zone gehören, können Sie z.B. unter www.billiger-telefonieren.de im Internet nachsehen.

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

6.12.2

So stellen Sie den Least-Cost-Router ein

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

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

Um diese Fragen zu beantworten, gehen Sie so vor:

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

- ☐ Router
- ☐ LANCAPI



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

- ③ Wechseln Sie auf die Registerkarte 'Zeiten und Feiertage'. Öffnen Sie die **Least-Cost-Tabelle**, fügen Sie einen neuen Eintrag hinzu, und geben Sie die benötigten Daten ein:

- Welche Vorwahl soll umgeleitet werden?
- Über welche Provider soll diese Vorwahl umgeleitet werden? Wenn Sie hier mehrere Netzkennzahlen durch Semikola getrennt eintragen, wechselt der LCR automatisch zur nächsten Vorwahl, wenn eine vorherige besetzt ist.
- An welchen Tagen und zu welchen Uhrzeiten soll die Umleitung aktiv sein? Beachten Sie bitte, dass keine tagesübergreifenden Uhrzeiten (18:00 Uhr bis 6:00 Uhr) möglich sind!
- Soll der Anruf über die normale Telefongesellschaft geführt werden, wenn alle Call-by-Call-Leitungen besetzt sind? Wenn der 'automatische Rückfall' ausgeschaltet ist, beginnt der LCR ggf. nach der letzten Netzkennzahl wieder mit der ersten ...

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

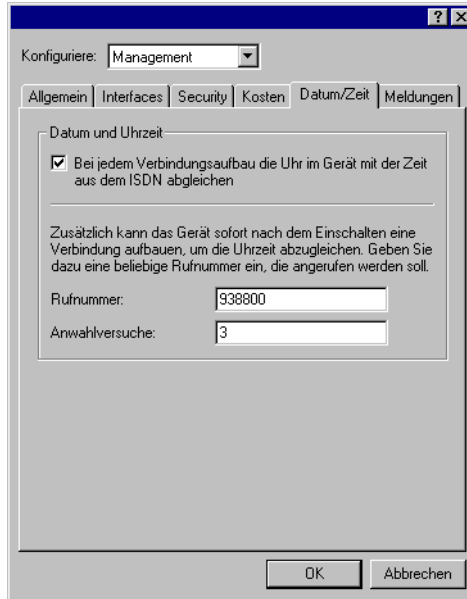


*Bauen Sie Ihre LCR-Tabelle schrittweise auf, und überprüfen Sie jeweils das Ergebnis. Öffnen Sie dazu z.B. den ELSA LANmonitor und starten Sie über die ELSA LANCAPI Verbindungen zu Gegenstellen, die der Tabelle nach umgeleitet werden sollten. Anhand der gewählten Rufnummer können Sie leicht ablesen,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

Die Uhrzeit für die Auswahl

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

- ① Wechseln Sie im *ELSA LANconfig* im Konfigurationsbereich 'Management' auf die Registerkarte 'Datum/Zeit'.
- ② Aktivieren Sie ggf. die Option für den automatischen Zeitabgleich bei jedem Verbindungsaufbau. Falls Sie die Zeit lieber manuell eintragen möchten, schalten Sie diese Option aus.
- ③ Beim Ausschalten verliert das Gerät die aktuelle Zeit. Geben Sie die Rufnummer einer beliebigen Gegenstelle und die max. Anzahl der Anwahlversuche ein, wenn das Gerät direkt nach dem Einschalten eine Verbindung aufbauen und so die Zeit mit dem ISDN-Netz abgleichen soll. Ihr *ELSA LANCOM Business* erkennt selbständig, ob es sich um eine digitale Gegenstelle (z.B. Mailboxen oder Internet-Provider) handelt oder um eine analoge Gegenstelle (Telefonansage oder Sprachdienst).



Konfiguriere: Management

Allgemein Interfaces Security Kosten Datum/Zeit Meldungen

Datum und Uhrzeit

☒ Bei jedem Verbindungsaufbau die Uhr im Gerät mit der Zeit aus dem ISDN abgleichen

Zusätzlich kann das Gerät sofort nach dem Einschalten eine Verbindung aufbauen, um die Uhrzeit abzugleichen. Geben Sie dazu eine beliebige Rufnummer ein, die angerufen werden soll.

Rufnummer: 938800

Anwahlversuche: 3

OK Abbrechen



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

7

Technische Grundlagen



Dieses Kapitel gibt eine kurze Einführung in die Technik, die Ihr neues Gerät nutzt. Profis in Sachen Netzwerktechnik können sicher schnell über diese Abhandlungen hinweggehen, für Einsteiger bietet dieser Teil der Dokumentation jedoch eine nützliche Hilfe beim Verstehen der Fachbegriffe und Prozesse.

7.1

Netzwerktechnik



*Dieser Abschnitt stellt in kurzen Worten einige Grundlagen der Netzwerktechnik vor. Diese Erläuterungen erklären **nicht alle** möglichen Techniken, Verfahren und Begriffe, die im Zusammenhang mit der Netzwerktechnik verwendet werden, sondern nur soweit sie für das Verständnis der anderen Produktinformationen notwendig oder hilfreich sind.*

7.1.1

Das Netzwerk und seine Komponenten

Netzwerk,
Übertragungsme-
dium,
Schnittstellen

Wenn mehrere Rechner miteinander kommunizieren, wird dieser Verbund als Netzwerk bezeichnet. Damit Rechner untereinander kommunizieren können, benötigen sie ein physikalisches Medium, über das die Informationen übertragen werden. Das können z.B. Kabel- oder Funkverbindungen sein, die über spezielle Schnittstellen (z.B. Netzwerkkarten) mit den Rechnern verbunden werden.



Wenn im Folgenden der Begriff Netzwerkkabel (oder nur Kabel) verwendet wird, ist damit auch jedes andere physikalische Medium gemeint, das die Funktion der Kabel übernehmen kann, wie z.B. Funkstrecken.

Pakete
Zellen

Die einzelnen elektronischen Informationen, die über ein Medium von einem Rechner zum anderen geschickt werden, bezeichnet man je nach Verfahren als Pakete oder als Zellen.



Für die meisten der folgenden Erläuterungen ist der Unterschied zwischen Paketen und Zellen nicht relevant. Wir verwenden also allgemein den Begriff Pakete oder Datenpakete, und gehen nur an den entsprechenden Stellen näher auf die speziellen Eigenschaften von Zellen ein.

Host

Die Rechner und andere Endgeräte (z.B. Drucker) in einem Netzwerk, die Informationen erzeugen oder verarbeiten, heißen Hosts. Idealerweise ist ein Host von der Aufgabe befreit, Informationen weiterzuleiten. Ein Host hat in

der Regel genau eine Schnittstelle, mit der er am Netzwerk angeschlossen ist.

Router

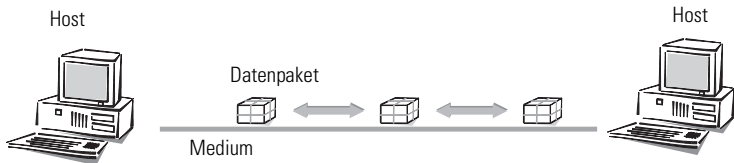
Der Transport von Paketen zwischen zwei Hosts erfolgt indirekt über Vermittlungsstellen, die ein Paket zum Zielrechner weiterreichen. Diese Vermittlungsstellen heißen Router. Ein Router hat mindestens zwei Schnittstellen, damit er die Daten von einem Sender in Empfang nehmen und an einen Empfänger weiterleiten kann. Ein Router hat neben der Vermittlungsfunktion auch immer die Eigenschaften eines Hosts, damit er selbst das Ziel von Datenpaketen sein kann, z.B. zum Zweck der Konfiguration.

7.1.2

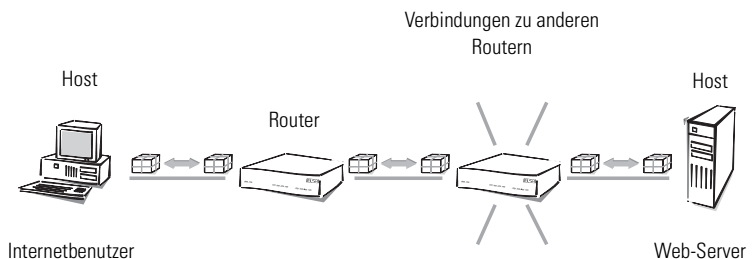
Verbindungsarten

Punkt-zu-Punkt-Verbindung

Werden genau zwei Hosts über ein Medium verbunden, spricht man von Punkt-zu-Punkt-Verbindungen. Dabei schickt ein Host Pakete ab, die nur bei genau **einem** Empfänger ankommen können (eindeutige Verbindung).



Auch bei einem Zugriff auf das Internet handelt es sich um eine Punkt-zu-Punkt-Verbindung. Die Datenpakete werden zwar vom Host beim Internetbenutzer über mehrere Router zum Host (Server) beim Internet-Provider gesendet, jedes Datenpaket hat jedoch ein ganz bestimmtes Ziel. Die Router geben die Datenpakete auch nur an genau einen Empfänger weiter. Daher bezeichnen wir auch diese Verbindung als eindeutig.

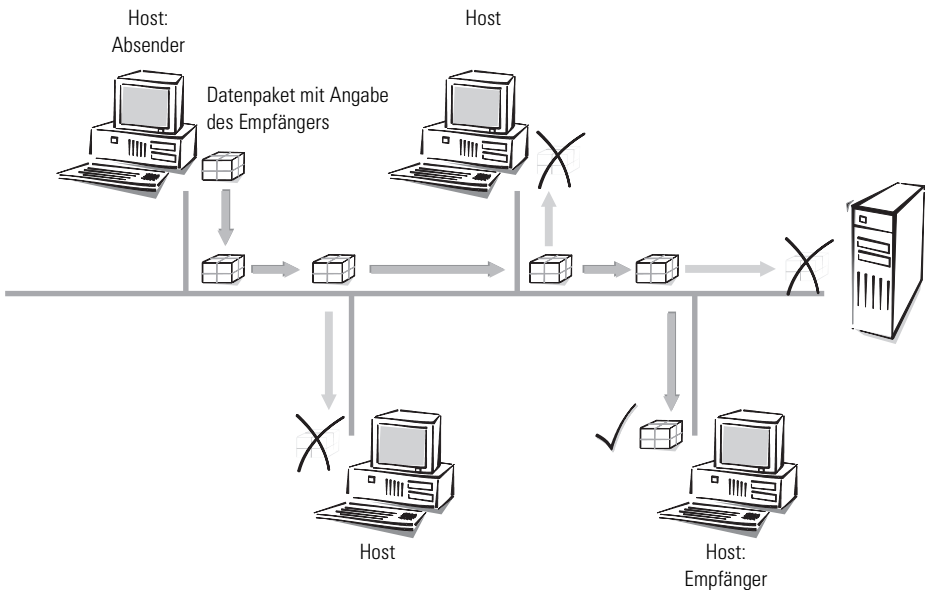




Punkt-zu-Mehr- punkt-Verbindung

Der Begriff der Punkt-zu-Punkt-Verbindung ist streng genommen nicht ganz korrekt. Für unsere Betrachtungen reicht es jedoch aus, diese Art der Verbindung gegen die folgenden Punkt-zu-Mehrpunkt-Verbindungen abzugrenzen.

In der Regel ist es unwirtschaftlich, alle Rechner eines Netzes durch Punkt-zu-Punkt-Kabel direkt miteinander zu verbinden, da dann jeder Rechner eine Vielzahl von Schnittstellen besitzen müsste. Daher schließt man die Rechner in dem Netzwerk an ein gemeinsames Medium an, das sich alle Hosts teilen. Der Absender schickt sein Paket mit der Angabe des Empfängers einfach los auf das Medium, an das mehrere Hosts angeschlossen sind. Das Datenpaket kommt bei **jedem** Host im Netzwerk an, der dann entscheidet, ob er selbst der Empfänger des Paketes ist oder nicht. Ist das Paket an den entsprechenden Host gerichtet, nimmt er es an, ansonsten beachtet er es nicht (er verwirft es). Dabei handelt es sich um eine nicht eindeutige Verbindung, man spricht von Punkt-zu-Mehrpunkt-Verbindungen.



7.1.3

Netzwerk-Arten

Protokoll

Eine wichtige Voraussetzung für die Rechnerkommunikation ist eine gemeinsame Sprache der Hosts untereinander. Diese Sprachen nennt man in der Netzwerktechnik „Netzwerkprotokoll“ oder kurz „Protokoll“.

TCP/IP

Das am weitesten verbreitete Netzwerkprotokoll ist das TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol). Es wird vorrangig im Internet benutzt, ist heute aber auch oft in Firmennetzwerken zu finden. Andere Netzwerkprotokolle sind z.B. IPX oder Apple Talk. Wegen der großen Verbreitung wird in diesem Kapitel hauptsächlich das TCP/IP betrachtet.

IP-Netz

Alle Hosts, die über das TCP/IP-Protokoll kommunizieren wollen, müssen zu einem gemeinsamen Netzwerk zusammengeschlossen sein und das TCP/IP-Protokoll (auch TCP/IP-Stack genannt) installiert haben. Ein solches Netz wird als IP-Netz bezeichnet.

*Internetwork
Internet*

Der Verbund mehrerer Netzwerke, die auf dem IP-Protokoll basieren, wird als Internetwork bezeichnet. Der größte Zusammenschluss von vielen kleinen, öffentlichen IP-Netzwerken ist das Internet.

*Lokales Netzwerk
(LAN)*

Ein Netzwerk von begrenzter räumlicher Ausdehnung, bei dem die Hosts gleichberechtigt ein gemeinsames Medium nutzen (Shared Medium), ist ein lokales Netzwerk (engl. **L**ocal **A**rea **N**etwork, LAN).

7.2

IP-Adressierung

*Paketorientierte
Übertragung*

In IP-Netzen erfolgt die Kommunikation zwischen Rechnern paketorientiert. Dabei werden Daten oder Nachrichten in Pakete variabler Länge verpackt und als Ganzes von einem Quellrechner zu einem Zielrechner transportiert. Ein Datenpaket enthält neben den eigentlich zu übertragenden Informationen (Nutzdaten) auch Kontroll- und Adressierungsinformationen.

IP-Adresse

In IP-Netzen werden IP-Adressen zur Kommunikation zwischen verschiedenen Geräten verwendet. Jeder Host hat dabei seine eigene Adresse, mit der er eindeutig identifiziert werden kann. 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.



Exakt betrachtet bezeichnet eine IP-Adresse nicht den Host, sondern seine Schnittstelle. Hat ein Endgerät im Netzwerk mehrere Schnittstellen (wie z.B. Router), so muss er für jede Schnittstelle eine eigene IP-Adresse besitzen. Deshalb haben ISDN-Router von ELSA z.B. sowohl eine IP-Adresse zur Kommunikation mit den Hosts im eigenen Netzwerk als auch eine zweite IP-Adresse zur Kommunikation mit der „Außenwelt“ über das ISDN-Netz. Kabelmodems von ELSA haben vergleichbar eine IP-Adresse für das eigene Netzwerk und eine weitere IP-Adresse für den Datenaustausch mit dem Kabelnetz.

Netzwerk-Adresse

In einer IP-Adresse ist sowohl die Adresse des Netzwerks enthalten als auch die des Hosts. Die Netzwerk-Adresse ist für alle Hosts in einem Netzwerk gleich, die Adresse eines Hosts ist einmalig und eindeutig in einem Netzwerk. Ein Router z.B. kann mehrere verschiedene, im Netzwerk eindeutige IP-Adressen haben.

Netzmaske

Wie unterscheidet man nun den Teil, der das Netzwerk bestimmt, und den Teil, der den Host 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 Netzwerk-Adresse 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

Die gleiche IP-Adresse, jetzt mit anderer Netzmaske:

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 ausreichend. Nur im Zusammenspiel mit der Netzmaske kann ein Host eindeutig bezeichnet werden.

Und Sie sehen weiter: Je weniger Bits in der Netzmaske eine Eins enthalten, um so mehr Bits bleiben übrig zur Identifizierung der einzelnen Hosts in einem zusammenhängenden Netzwerk. Während im ersten Beispiel mit der Netzmaske 255.255.255.0 nur 254 verschiedene Adressen vergeben werden kön-

nen sind es im zweiten Beispiel schon $254 \times 254 = 64.516$ verschiedene Adressen! Die erste und die letzte Ziffer eines Adressraums sind jeweils reserviert für die Netzwerk-Adresse und die Broadcast-Adresse (Adresse für Pakete an alle Hosts in einem IP-Netz). Bei der Netzmaske 255.255.255.0 sind das die '0' für die Netzwerk-Adresse und die '255' als Broadcast-Adresse.

Eine neuere Schreibweise der Netzmaske hängt einfach die Anzahl der Bits, die für die Netzwerk-Adresse stehen, an die IP-Adresse an: 137.226.4.101/24. Die Zahl hinter dem Schrägstrich zeigt an, dass die ersten 24 Bits die Netzwerk-Adresse angeben. Mit dieser Schreibweise wird die Länge der Einträge in den Routingtabellen reduziert.

Verwaltung der IP-Adressen

Um Irrtümer zu vermeiden, müssen die IP-Adressen innerhalb eines zusammenhängenden Netzes eindeutig sein. Da auch das Internet mit 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 und verteilen. Da die Anzahl der theoretisch verfügbaren IP-Adressen begrenzt ist, lassen sich die vergabeberechtigten Stellen die IP-Adressen teuer bezahlen.

Private Address Spaces

Damit eine Firma mit einem eigenen IP-Netzwerk aber nicht für jeden Arbeitsplatz eine IP-Adresse kaufen muss, sind bestimmte Bereiche der IP-Adressen für die kostenlose Verwendung reserviert (Private Address Spaces). Diese Adressen können in einem abgeschlossenen Netz beliebig benutzt werden, z.B. in einem privaten Netz oder im Netz einer Firma. Innerhalb dieses Netzes müssen die IP-Adressen zwar eindeutig sein, aber in einem anderen abgeschlossenen Netzwerk (z.B. in einer anderen Firma) können die gleichen IP-Adressen zum Einsatz kommen.

Diese reservierten IP-Adressen dürfen jedoch **nicht** nach außen (ins Internet) bekannt gemacht werden. Nur **die** Geräte in einem Netzwerk, die Verbindung mit öffentlichen Netzwerken haben (z.B. Router an der Schnittstelle zum Internet), müssen eine registrierte IP-Adresse haben.

Bei der Vergabe von IP-Adressen, kontrolliert durch die IANA (**I**nternet-**A**ssigned-**N**umbers-**A**uthority), wurden die folgenden vier Adressbereiche für nicht öffentliche IP-Netzwerke reserviert:

IP-Adressen	Netzmaske	Bemerkung
10.0.0.0	255.0.0.0	„10er“ Netze: Alle IP-Adressen, die mit einer 10. beginnen und deren Netzmaske mit 255. beginnt, fallen in den für private Netzwerke reservierten Adressbereich.
172.16.0.0	255.240.0.0	Alle IP-Adressen, die mit 172.16.–172.31. beginnen und deren Netzmaske größer oder gleich 255.240.0.0 ist, fallen in den für private Netzwerke reservierten Adressbereich.
192.168.0.0	255.255.0.0	Alle IP-Adressen, die mit 192.168. beginnen und deren Netzmaske mit 255.255. beginnt, fallen in den für private Netzwerke reservierten Adressbereich.
224.0.0.0	224.0.0.0	Alle IP-Adressen, die mit 224. beginnen und deren Netzmaske ebenfalls mit 224. beginnt, fallen in den reservierten Adressbereich. Dieser Bereich ist reserviert für Broadcasts und sollte nicht für private Netze verwendet werden.

Bei der Verwendung von IP-Adressen aus einem Private Address Space sind zwei Dinge zu beachten:

- Die im privaten Netzwerk verwendeten IP-Adressen (aus dem Private Address Space) dürfen dieses IP-Netzwerk nicht verlassen; das heißt, ein Anschluss an das Internet ist nur mit zusätzlichen Hilfsmitteln (z.B. IP-Masquerading) möglich.
- Im Internet werden Pakete für diese IP-Adressen nicht geroutet – das heißt, jeder Backbone-Router im Internet verwirft solche IP-Pakete stillschweigend. Evtl. kann die Einschleusung solcher IP-Pakete ins Internet sogar schwerwiegende Konsequenzen nach sich ziehen (abhängig vom Vorgehen des jeweiligen Providers).

7.2.1

Routing

IP-Routing und hierarchische IP-Adressierung

Jedes IP-Paket enthält die IP-Adressen von Quelle und Ziel. Ein Router nimmt an seinen Schnittstellen IP-Pakete entgegen, interpretiert die Zieladresse und leitet die Pakete an diejenige seiner Schnittstellen weiter, die dem Ziel am nächsten ist. Das Finden des geeigneten Weges wird als Routing bezeichnet.

Routingtabelle

Für das Routen verwaltet jeder Router eine Tabelle (Routingtabelle). Sie bezeichnet für jeden Host im Netz die Router-Schnittstelle, über die der Host

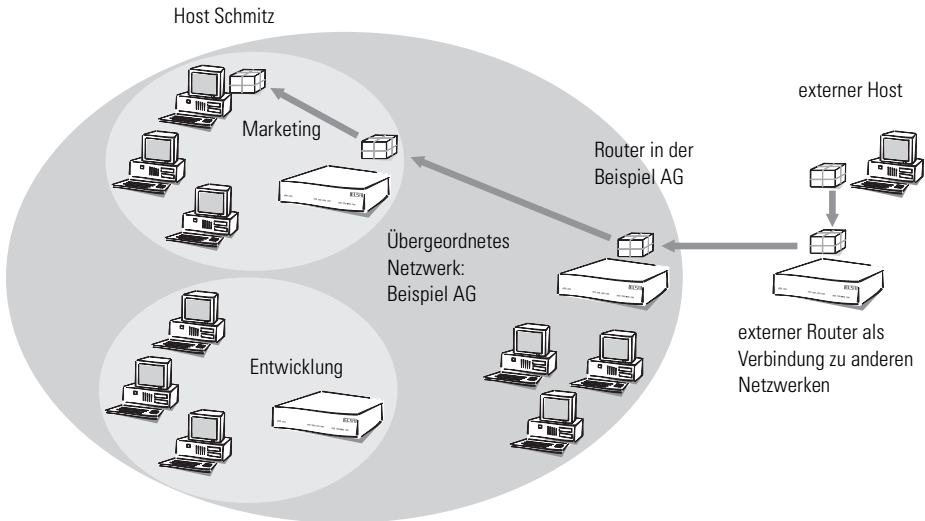
hierarchische IP-Adressen

am schnellsten zu erreichen ist. Es ist leicht vorstellbar, dass mit wachsender Netzgröße diese Tabellen die Kapazität der Router sprengen (das Internet als weltweiter Verbund von öffentlich erreichbaren IP-Rechnern enthält mehrere Millionen Hosts).

Aus diesem Grunde wurden hierarchische IP-Adressen eingeführt. Dazu wird das IP-Netz in Teilnetze unterteilt, in denen IP-Adressen aus einem zusammenhängenden Nummernraum vergeben werden. Es sind mehrere Hierarchie-Ebenen möglich, so dass mehrere Teilnetze zu größeren Teilnetzen zusammengefasst werden können. Dies ist vergleichbar mit der hierarchischen Adresse bei der Briefpost, die aus Land, Stadt, Straße und Hausnummer besteht.

Die Konsequenzen dieser hierarchischen IP-Adressierung:

- Da die Netzwerk-Adresse innerhalb eines Netzwerks für alle Hosts gleich ist, reicht für die Kommunikation der Hosts untereinander in einem Netzwerk die Hostadresse aus.
- Ein Router muss zum einen die Adressen der Hosts kennen, die direkt an ihn angeschlossen sind, zum anderen muss der Router die Adressen aller Netze und Teilnetze kennen, die über benachbarte Router zu erreichen sind.
- Ein Router muss **nicht alle** möglichen weiteren IP-Adressen kennen.



So kann z.B. eine Firma ein großes Netzwerk haben, in das die einzelnen Abteilungen als kleinere Teilnetze eingebunden sind. Die Adresse des Netzwerks für die Abteilung Marketing würde sich hierarchisch zusammensetzen aus der Adresse der Firma und der Abteilung.

Wenn ein Host außerhalb des Firmennetzes nun ein Paket an einen Host in der Beispiel AG senden möchte, passiert Folgendes:

- ① Der Absender gibt dem Paket die Zieladresse „Host Schmitz – Marketing – Beispiel AG“.
- ② Ein externer Router, der die Verbindung zu anderen Netzen herstellt, muss nur wissen, wie er die Beispiel AG erreicht. Sobald er ein Paket mit der Adresse für die Beispiel AG empfängt, leitet er das Paket an den Router weiter, der für die Beispiel AG zuständig ist.
- ③ Der Router in der Beispiel AG empfängt das Paket und entnimmt der Adresse die Information, dass es für die Beispiel AG gedacht ist. Weil er selber Teil der Beispiel AG ist, betrachtet er die Adresse genauer und sucht nach dem Namen der Abteilung. Dann leitet er das Paket weiter an den Router im Marketing.
- ④ Der Router im Marketing empfängt das Paket und entnimmt der Adresse die Information, dass es für das Marketing in der Beispiel AG gedacht ist. Weil er selber Teil dieser Abteilung ist, betrachtet er die Adresse genauer und sucht nach dem Namen des Hosts. Dann leitet er das Paket weiter an den Host von Mitarbeiter Schmitz.

Nun wollen wir das Beispiel einmal mit richtigen IP-Adressen betrachten und nicht mit den symbolischen Namen. Das Netzwerk der Beispiel AG verfügt über den Nummernraum '192.168.100.0' bis '192.168.100.255', mit der '0' als Netzwerk-Adresse und der '255' als Broadcast-Adresse.

Ein Router muss sich nur merken, dass alle Adressen, die mit '192.168.100' beginnen, im Netzwerk der Beispiel AG liegen.

Stellen wir uns jetzt einen Router vor, der mit einer Schnittstelle an das Netz der Beispiel AG angeschlossen ist. Empfängt er ein Paket mit Zieladresse '192.168.100.4' und Netzmaske '255.255.255.0', vergleicht er diese mit jeder ihm bekannten Netzwerk-Adresse. Dabei führt er ein logisches UND mit der Netzmaske aus und vergleicht das Ergebnis mit der Netzwerk-Adresse: '192.168.100.4' UND '255.255.255.0' ergibt '192.168.100.0'. Dies ist die Netzwerk-Adresse vom Netzwerk der Beispiel AG. Der Router erkennt, dass sich das Ziel in der Beispiel AG befindet und reicht das Paket an die Schnittstelle

weiter, über die die Beispiel AG erreichbar ist. Innerhalb der Beispiel AG wird das Paket dann in das entsprechende Teilnetz weitergeleitet.

Bei der Übertragung von IP-Paketen innerhalb eines Netzwerks funktioniert das Verfahren auch:

- ① Wenn ein Host im Teilnetz der Entwicklung ein Datenpaket an Herrn Schmitz senden möchte, gibt der Absender dem Paket die Zieladresse „Host Schmitz – Marketing – Beispiel AG“.
- ② Der Router in der Entwicklung empfängt das Paket und entnimmt der Adresse die Information, dass es für das Marketing in der Beispiel AG gedacht ist. Weil er selber Teil der Beispiel AG, nicht jedoch der Abteilung Marketing ist, leitet er das Paket weiter an den Router im übergeordneten Netzwerk.
- ③ Der Router in der Beispiel AG empfängt das Paket und entnimmt der Adresse die Information, dass es für die Beispiel AG gedacht ist. Weil er selber Teil der Beispiel AG ist, betrachtet er die Adresse genauer und sucht nach dem Namen der Abteilung. Dann leitet er das Paket weiter an den Router im Marketing, wo das Paket an den Empfänger weitergeleitet wird.

7.2.2

Erweiterung durch lokale Netze

Medium Access Control

Bisher haben wir nur Punkt-zu-Punkt-Verbindungen betrachtet. Viele Rechnernetze basieren jedoch auf Mehrpunkt-Verkabelungen wie dem Ethernet. Dabei können alle an ein gemeinsames Medium angeschlossenen Rechner die Signale aller anderen Rechner empfangen (sogenannte Broadcast-Übertragung auf einem Shared-Medium). Wenn mehrere Rechner gleichzeitig senden, überlagern und zerstören sich die einzelnen Signale. Auf der MAC-Ebene (engl. **M**edium **A**ccess **C**ontrol) sind zur Vermeidung und Auflösung derartiger Kollisionen Zugriffsverfahren wie CSMA/CD, Token Ring usw. implementiert.

LAN und IP-Netz

Der Verbund aller Rechner, die mittels eines MAC-Protokolls über ein Shared-Medium kommunizieren, wird als LAN bezeichnet. Ein LAN bildet ein eigenständiges Netz und ist dem IP-Netz logisch untergeordnet, das heißt, IP-Netze können die physikalischen Verbindungen eines LANs verwenden, um Verbindungen zwischen Hosts und Routern herzustellen. Ein LAN – Local Area Network – ist, wie der Name schon verrät, räumlich begrenzt.

MAC-Adresse

Zur Organisation der Übertragung im LAN werden spezifische LAN-Adressen verwendet, die vom Hersteller der Schnittstellenhardware fest einprogram-

miert werden. Da die LAN-Adressen für die Kommunikation über das MAC-Protokoll verwendet werden, heißen sie auch MAC-Adressen. Man kann sie sich wie einen Fingerabdruck der Schnittstellenhardware vorstellen. MAC-Adressen sehen z.B. so aus: 00-80-C7-6D-A4-6E.

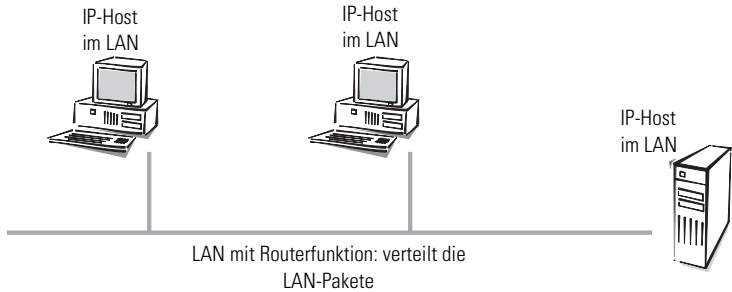
MAC-Adressen sind unabhängig von IP-Adressen. Ein IP-Host, dessen Schnittstelle über ein LAN arbeitet, hat eine IP- und eine MAC-Adresse. Während IP-Adressen durch ihre Postadressen-ähnliche Struktur dafür ausgelegt wurden, das Routen in riesigen IP-Netzen zu vereinfachen, wurden Fingerabdruck-ähnliche MAC-Adressen darauf ausgelegt, den Anschluss eines neuen Rechners an ein LAN so einfach wie möglich zu gestalten.

Auch in LANs wird paketorientiert übertragen. Jedes Paket enthält die MAC-Adresse von Quelle und Ziel. Zwar wird jedes Paket von allen Rechnern empfangen, jedoch nur von dem Zielrechner weiterverarbeitet. Zusätzlich gibt es eine spezielle MAC-Broadcast-Adresse, die von allen Rechnern im LAN weiterverarbeitet wird.

IP im LAN

Jedes LAN-Paket enthält einen Eintrag mit dem Typ des Netzwerkprotokolls. Ein IP-Paket kann z.B. über ein LAN übertragen werden, indem es in ein LAN-Paket verpackt und mit dem Protokoll-Typ 'IP' versehen wird. Die LAN-Schnittstelle im empfangenden Host erkennt anhand des IP-Eintrags, dass in dem LAN-Paket ein IP-Paket steckt, extrahiert es und verarbeitet es wie ein normales IP-Paket weiter. Auf diese Weise können über dasselbe LAN gleichzeitig IP-Pakete und Pakete anderer Netzprotokolle wie IPX übertragen werden, ohne dass es zu Konflikten kommt (man sagt daher, dass ein LAN multiprotokollfähig ist).

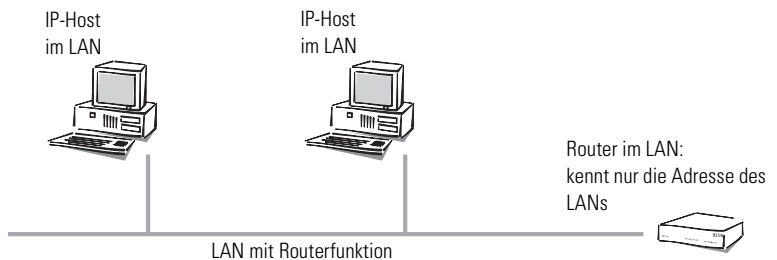
Für einen IP-Host verhält sich ein LAN so, als ob es ein eigenes Netzwerk mit einem Router wäre. Die Hosts geben die Pakete an das LAN ab, das die weitere Verteilung der Datenpakete übernimmt. Für die Kommunikation der Hosts untereinander über das IP-Protokoll dürfen in einem LAN somit nur IP-Adressen aus dem Nummernraum dieses Netzes verwendet werden.



Für einen Router im LAN erscheint ein Host im eigenen LAN, als wenn er sich hinter einem weiteren Router befände. Der Router steht also vor einer einfachen Aufgabe: Da er für den Betrieb im IP-Netz nur die IP-Adressen

- der direkt angeschlossenen Hosts und
- die der erreichbaren Netze und Teilnetze

kennen muss, muss er sich also nur die Netzwerk-Adresse und die Netzmaske des Teilnetzes im LAN merken.



Der Host steht dagegen vor einer schwierigeren Aufgabe als der Router. Bei einer Schnittstelle mit Punkt-zu-Punkt-Kabel weiss ein Host, dass alle Pakete, die er über die Schnittstelle verschickt, automatisch z.B. bei seinem Router ankommen. Bei den Punkt-zu-Mehrpunkt-Verbindungen zum LAN muss er nun aber zwei Fälle unterscheiden.

- Ein Paket mit einer Zieladresse außerhalb des eigenen LANs gibt der sendende Host an einen Router im LAN weiter, der sich um die weitere Verarbeitung des Pakets kümmert.
- Ein Paket mit einer Zieladresse im eigenen LAN muss der sendende Host direkt an den Ziel-Host senden, denn ein Router im Netz kennt nicht die Adressen der einzelnen Hosts.

Datenübertragung im eigenen LAN

Veranschaulichen wir uns das an einem Beispiel. Stellen wir uns vor, dass die Hosts des Teilnetzes im Marketing über ein LAN verkabelt sind. Die Hosts haben IP-Adressen aus dem Nummernraum '137.226.4.1' bis '137.226.4.254' (die Adressen '137.226.4.0' und '137.226.4.255' sind reserviert), die Netzwerk-Adresse ist '137.226.4.0' und die Netzmaske '255.255.255.0'. An das LAN ist ein Router angeschlossen, der den Übergang in die weite Welt des Internet bildet. Seine LAN-Schnittstelle hat die IP-Adresse '137.226.4.1' und die MAC-Adresse '00-80-C7-6D-A4-6E'.

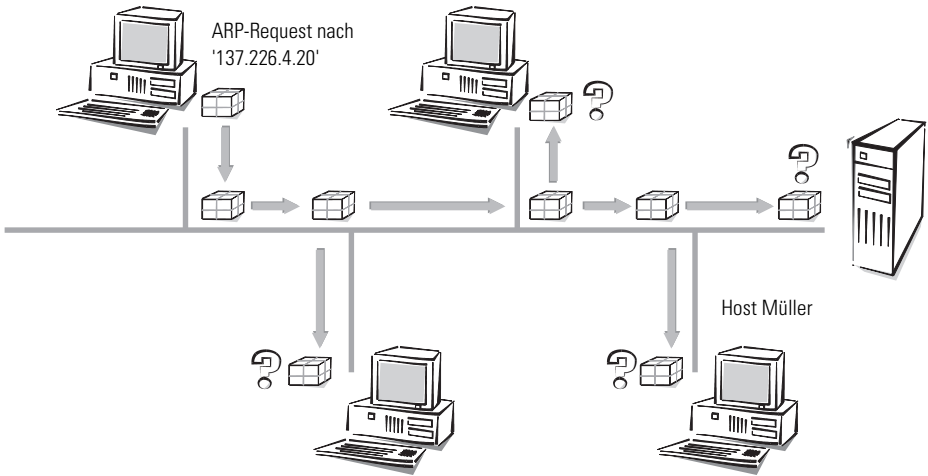
Stellen wir uns jetzt der Aufgabe, ein IP-Paket von Host Schmitz (mit IP-Adresse '137.226.4.10' und MAC-Adresse '00-10-5A-31-20-DF') an Host Müller (mit IP-Adresse '137.226.4.20' und MAC-Adresse '00-10-5A-31-20-EB') zu übertragen. Host Schmitz erkennt anhand der Netzwerk-Adresse und Netzmaske, dass Host Müller im Teilnetz des eigenen LANs ist. Er muss das Paket somit direkt über das LAN an Host Müller schicken. Leider kann er der LAN-Schnittstelle nicht sagen: „Schicke das IP-Paket an IP-Adresse 137.226.4.20“, denn die LAN-Schnittstelle versteht nur MAC-Adressen.

Jeder Host muss daher eine Tabelle verwalten, die IP-Adressen in MAC-Adressen übersetzt. Aber wie kommen die Einträge in die Tabelle? Sie könnten zwar von Hand eingetragen werden, aber das widerspricht der Vorgabe, den Anschluss eines neuen Rechners an ein LAN so einfach wie möglich zu gestalten.

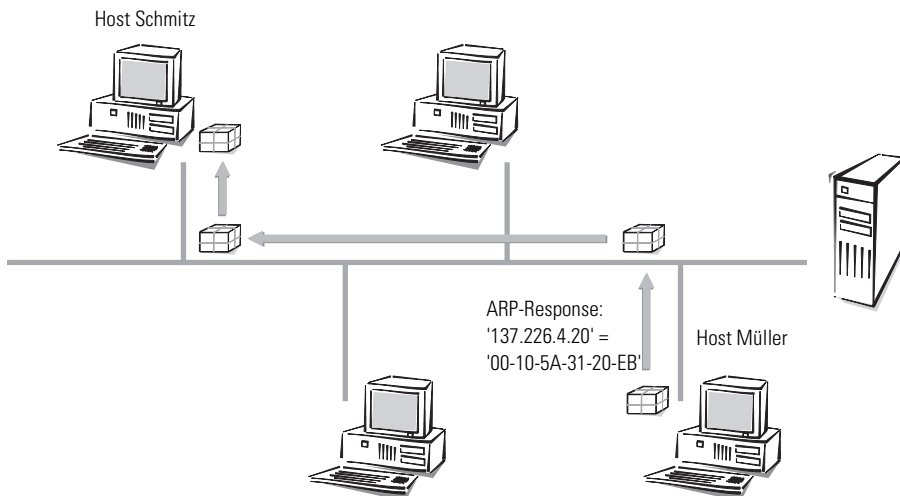
ARP

Daher gibt es im LAN einen speziellen Mechanismus, der dies automatisiert: das **A**dress-**R**esolution-**P**rotokoll, ARP. Die Tabelle selbst wird ARP-Tabelle genannt. Immer wenn ein Host für eine IP-Adresse (in unserem Beispiel '137.226.4.20') keinen Eintrag in der ARP-Tabelle findet, verschickt er ein ARP-Request-Paket an alle Hosts im LAN (mit der LAN-Broadcast-Adresse als Zieladresse).

Host Schmitz

ARP-Request nach
'137.226.4.20'

Dieses ARP-Request-Paket ist nichts anderes als die Frage an alle, wer denn auf die IP-Adresse '137.226.4.20' hört. Host Müller empfängt das Paket, fühlt sich angesprochen und antwortet mit einem ARP-Response-Paket, das er direkt an Host Schmitz verschickt. Die MAC-Adresse '00-10-5A-31-20-DF' von Host Schmitz entnimmt er dem Absenderfeld im ARP-Request-Paket. Host Schmitz erkennt dies als Antwort auf seine Anfrage, entnimmt dem Absenderfeld des ARP-Response-Paketes die MAC-Adresse '00-10-5A-31-20-EB' von Host Müller und trägt sie in seine ARP-Tabelle ein.



Anschließend kann er sich endlich seiner ursprünglichen Aufgabe zuwenden, das IP-Paket an Host Müller zu verschicken. Er findet jetzt in der ARP-Tabelle den Eintrag „IP-Adresse 137.226.4.20 entspricht MAC-Adresse '00-10-5A-31-20-EB'“ und sagt seiner LAN-Schnittstelle: „Verschicke dieses IP-Paket an den Rechner mit der MAC-Adresse '00-10-5A-31-20-EB'“.

Datenübertragung aus dem eigenen LAN ins Internet

Stellen wir uns jetzt der zweiten Aufgabe, ein IP-Paket von Host Schmitz an einen weit entfernten Host Extern mit der IP-Adresse 151.189.12.43 zu übertragen. Host Schmitz vergleicht die IP-Adresse mit seiner Netzwerk-Adresse und erkennt, dass Host Extern sich nicht im eigenen LAN befindet. Somit ist Host Extern nur über den Router zu erreichen. Die MAC-Adresse des Routers '00-80-C7-6D-A4-6E' erfährt er über dessen IP-Adresse durch Nachschauen in der ARP-Tabelle (ggf. vorher noch ein ARP-Request). Somit sagt Host Schmitz zu seiner LAN-Schnittstelle: „Verschicke dieses IP-Paket an den Rechner mit der LAN-Adresse '00-80-C7-6D-A4-6E'“. Der Router entnimmt dem LAN-Paket das IP-Paket und liest daraus die IP-Adresse von Host Extern. In der Routing-Tabelle sucht der Router dann nach der Netzwerk-Adresse von diesem Host und findet so die Schnittstelle, über die er das IP-Paket weiterleiten muss.

LAN-Kopplung auf MAC-Basis

Sie wissen, dass LANs das Anschließen von Rechnern an ein lokales Netz stark vereinfachen. Daher basieren fast alle Hausnetze auf LANs. Es gibt Situationen, wo einzelne LANs räumlich so weit ausgedehnt sind, dass die physikalischen Eigenschaften des Kabels den Anschluss weiterer Rechner behindern. Daraus ergibt sich der Bedarf, mehrere LANs so miteinander zu koppeln, dass sie elektrisch und bezüglich des MAC-Protokolls wie getrennte LANs agieren, aber gegenüber dem IP-Protokoll wie ein einziges großes LAN erscheinen.

Diese Kopplung von LANs erfolgt durch Bridges. Eine Bridge arbeitet ähnlich wie ein Router, verwendet zur Wegefindung jedoch keine IP-Adressen, sondern ausschließlich MAC-Adressen. Da die MAC-Adressen im Gegensatz zu IP-Adressen nichts über die Struktur des Netzes verraten, muss jede Bridge die MAC-Adressen aller Rechner im gesamten LAN kennen.

Somit hat man wieder das Problem, das man bei Routern vor der Einführung von Teilnetzen hatte: Mit wachsender LAN-Größe werden die Adresstabellen der Bridges irgendwann gesprengt. Man kann also nicht beliebig viele LANs durch Bridges verbinden. Andererseits ermöglichen die unstrukturierten MAC-Adressen, dass die Bridges die Positionen von Rechnern im LAN automatisch anhand der empfangenen Pakete erlernen. Man nennt dies „selbstlernende Bridge“.

7.3

Point-to-Point Protocol

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

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

7.3.1

Das Protokoll

Was ist PPP?

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

- Passwortschutz nach PAP, CHAP oder MS-CHAP
- Rückruf-Funktionen
- Aushandlung der über die aufgebaute Verbindung zu benutzenden Netzwerkprotokolle (z.B. IP). Dazu gehören auch für diese Protokolle notwendige Parameter wie z.B. IP-Adressen. Diese Verhandlung läuft über das Protokoll IPCP (IP Control Protocol) ab.
- Überprüfung der Verbindung mit dem LCP (Link Control Protocol)
- Bündelung von mehreren Kanälen (Multilink PPP)

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

Wozu wird PPP verwendet?

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

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

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

Die Phasen einer PPP-Verhandlung

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

- Establish-Phase

Nach einem Verbindungsaufbau über den Datenkommunikationsteil startet die Aushandlung der Verbindungsparameter über das LCP.

Es wird festgestellt, ob die Gegenstelle auch bereit ist, PPP zu benutzen, die Paketgrößen und das Authentifizierungsprotokoll (PAP, CHAP, MS-CHAP oder keines) werden festgelegt. Danach wechselt das LCP in den Opened-Zustand.

- Authenticate-Phase

Falls notwendig, werden danach die Passworte ausgetauscht. Bei Authentifizierung nach PAP wird das Passwort nur einmalig übertragen. Bei Benutzung von CHAP oder MS-CHAP wird ein verschlüsseltes Passwort periodisch in einstellbaren Abständen gesendet.

Evtl. wird in dieser Phase auch ein Rückruf über CBCP (Callback Control Protocol) ausgehandelt.

- Network-Phase

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

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

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

- Terminate-Phase

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

Die PPP-Verhandlung im *ELSA LANCOM Business*

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

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

```
trace + ppp
```

kann die Ausgabe der ausgetauschten PPP-Protokoll-Frames innerhalb einer Terminal-Sitzung gestartet werden. Wird diese Terminal-Sitzung in einem

Log-File protokolliert, kann nach Abbruch der Verbindung eine detaillierte Analyse erfolgen.

7.3.2

Die PPP-Liste

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

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

In dieser Spalte der PPP-Liste tragen Sie folgende Werte ein:
Gerätename	Name der Gegenstelle, mit dem sich diese bei Ihrem Router anmeldet
Username	Name, mit dem sich Ihr Router bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Geräteiname Ihres Routers verwendet.
Sicherung	Verfahren zur Sicherung der PPP-Verbindung ('PAP', 'CHAP', 'MS-CHAP' oder 'keine'). Ihr eigener Router verlangt von der Gegenstelle die Einhaltung dieses Verfahrens! Nicht etwa umgekehrt. Daher bietet sich die Sicherung nach 'PAP', 'CHAP' oder 'MS-CHAP' nicht an bei Verbindungen zu Internet Service Providern, die uns vielleicht kein Passwort übermitteln wollen. Für solche Verbindungen wählen Sie 'keine' Sicherung.
Passwort	Passwort, das von Ihrem Router an die Gegenstelle übertragen wird (falls gefordert). * in der Liste zeigt an, dass ein Eintrag vorhanden ist.
Zeit	Zeit zwischen zwei Überprüfungen der Verbindung mit LCP. Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z.B. 2 für 20 Sek.). Gleichzeitig die Zeit zwischen zwei Überprüfungen der Verbindung nach CHAP. Diese Zeit geben Sie in Minuten ein. Für Gegenstellen mit Windows-Betriebssystem muss die Zeit auf '0' gesetzt werden!

In dieser Spalte der PPP-Liste tragen Sie folgende Werte ein:
Wdh	Anzahl der Wiederholungen für den Überprüfungsversuch. Mit mehreren Wiederholungen schalten Sie den Einfluss kurzfristiger Leitungsstörungen aus. Erst wenn alle Versuche erfolglos bleiben, wird die Verbindung abgebaut. Der zeitliche Abstand zwischen zwei Wiederholungen beträgt 1/10 der Zeit zwischen zwei Überprüfungen. Gleichzeitig die Anzahl der „Configure Requests“, die der Router maximal aussendet, bevor es von einer Leitungsstörung ausgeht und selber die Verbindung abbaut.
Conf, Fail, Term	Mit diesen Parametern wird die Arbeitsweise des PPPs beeinflusst. Die Parameter sind in der RFC 1661 definiert und werden hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in dieser RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im allgemeinen sind die Default-Einstellungen ausreichend. Diese Parameter können nur über SNMP oder TFTP (mit <i>ELSA LAN-config</i>) verändert werden!
Rechte	Netzwerkprotokolle, die über diese Verbindung geroutet werden sollen: IP, IPX, NTB (NetBIOS). NetBIOS erfordert immer eines der beiden anderen Protokolle. Netzwerkprotokoll, das über diese Verbindung geroutet werden soll: IP

7.3.3

Alles o.k.? Leitungsüberprüfung mit LCP

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

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

Was passiert nun, wenn der Reply ausbleibt? Zuerst werden einige Wiederholungen der Anfrage gestartet, um kurzfristige Störungen der Leitung auszuschließen. Wenn alle diese Wiederholungen unbeantwortet bleiben, wird die Leitung abgebaut und ein Ersatzweg gesucht. Der kann z.B. in Form einer Backup-Leitung gefunden werden.



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

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

7.3.4

Zuweisung von IP-Adressen über PPP

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

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



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

● Beispiel: Remote-Access

Die Zuweisung der Adresse wird durch einen speziellen Eintrag in der IP-Routing-Tabelle ermöglicht. Neben dem Eintrag der IP-Adresse, die der Gegenstelle aus dem Feld 'Router-Name' zugewiesen werden soll, wird als Netzmaske die 255.255.255.255 angegeben. Der Routername ist in

diesem Fall der Name, mit dem sich die Gegenstelle beim *ELSA LANCOM Business* anmelden muss.

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

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

● Beispiel: Internet-Access

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

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

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

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



7.3.5

Rückruf-Funktionen

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

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

Mit diesem Eintrag stellen Sie den Rückruf so ein:
Aus	Es wird nicht zurückgerufen.
Auto (nicht Windows 95, Windows 98 oder Windows NT, s.u.)	Wenn die Gegenstelle in der Nummernliste gefunden wird, so wird diese zurückgerufen. Hierzu wird der Ruf zunächst abgelehnt und, sobald der Kanal wieder frei ist, zurückgerufen (Dauer ca. 8 Sekunden). Wird die Gegenstelle nicht in der Nummernliste gefunden, so wird sie zunächst als DEFAULT-Gegenstelle angenommen, und der Rückruf wird während der Protokollverhandlung ausgehandelt. Dabei fällt eine Gebühr von einer Einheit an.
Name	Bevor ein Rückruf erfolgt, wird immer eine Protokollverhandlung durchgeführt, auch wenn die Gegenstelle in der Nummernliste gefunden wurde (z.B. für Rechner mit Windows, die sich auf dem Gerät einwählen). Dabei fällt eine Gebühr von einer Einheit an.
ELSA	Wenn die Gegenstelle in der Nummernliste gefunden wird, wird der schnelle Rückruf durchgeführt, d.h., der <i>ELSA LANCOM Business</i> sendet ein spezielles Signal zur Gegenstelle und ruft sofort zurück, wenn der Kanal wieder frei ist. Nach ca. 2 Sekunden steht die Verbindung. Nimmt die Gegenstelle den Ruf nicht unmittelbar nach dem Signal zurück, so erfolgt zwei Sekunden später ein Rückfall auf das normale Rückrufverfahren (Dauer wieder ca. 8 Sekunden). Dieses Verfahren steht nur an DSS1-Anschlüssen zur Verfügung.
Looser	Benutzen Sie die Option 'Looser', wenn von der Gegenstelle ein Rückruf erwartet wird. Diese Einstellung erfüllt zwei Aufgaben gleichzeitig. Zum einen sorgt sie dafür, dass ein eigener Verbindungsaufbau zurückgenommen wird, wenn ein Ruf von der gerade angerufenen Gegenstelle hereinkommt, zum anderen wird mit dieser Einstellung die Funktion aktiviert, auf das schnelle Rückruf-Verfahren reagieren zu können. D.h., um den schnellen Rückruf nutzen zu können, muss sich der Anrufer im 'Looser'-Modus befinden, während beim Angerufenen der Rückruf auf 'ELSA' eingestellt sein muss.



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

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

Rückruf nach Microsoft CBCP

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

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

Über das CBCP ist es möglich, von einem Rechner mit einem Windows-Betriebssystem eine Verbindung zum *ELSA LANCOM Business* 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.

Namenliste (ISDN) - Eintrag bearbeiten

Name:

Rufnummer:

Haltezeit: Sekunden

Haltezeit für Bündelung: Sekunden

Layername:

Verkehrs-Kontrakt:

Automatischer Rückruf:

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

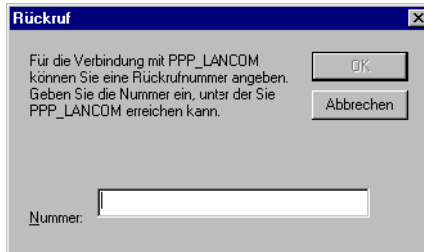
Keinen Rückruf durchführen

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

Rückrufnummer selbst wählen

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

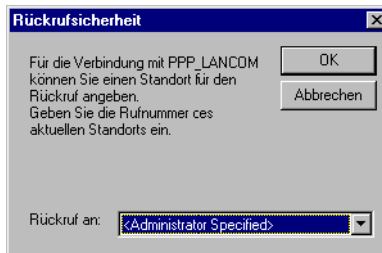
Nach der Authentifizierung erscheint bei Windows 95 die folgende Dialogbox, in der der Anwender seine Rufnummer angeben kann:



Rückrufnummer vom *ELSA LANCOM Business* bestimmt

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

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



Der Rückruf an einen Windows-Rechner erfolgt ca. 15 Sekunden, nachdem die Verbindung abgebaut wurde. Diese Zeit kann nicht verkürzt werden, da sie vom Windows vorgegeben ist.

Schneller Rückruf nach ELSA

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

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

Rückruf nach RFC 1570 (PPP LCP Extensions)

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

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

7.3.6

Kanalbündelung mit MLPPP

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

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

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

- Statische Kanalbündelung

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

- Dynamische Kanalbündelung

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

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

So stellen Sie die Kanalbündelung ein

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

- ① Erstellen Sie in der Namenliste einen Eintrag für die Verbindung, die die Kanalbündelung verwenden soll. Wählen Sie dabei einen Layer aus, der in den Layer-2-Optionen die Bündelung eingestellt hat.
 - **compr.** nach dem LZS-Datenkompressionsverfahren (Stac) reduziert das Datenvolumen, wenn die Daten nicht schon vorher komprimiert waren. Dieses Verfahren wird auch von Routern anderer Hersteller und von ISDN-Adaptern unter Windows-Betriebssystemen unterstützt.
 - **Buendeln** verwendet mehrere B-Kanäle für eine Verbindung. Die Art der Kanalbündelung wird über die Konfiguration der Layer-2-Optionen in der Layerliste, der Haltezeiten in der Namenliste, des Eintrags für die Y-Verbindung in der Interface-Tabelle und des Eintrags in der Kanaltabelle eingestellt.
 - **bnd+compr** nutzt beides (Komprimierung und Kanalbündelung) und stellt damit die maximal mögliche Übertragungsleistung zur Verfügung.

- ② Stellen Sie ebenfalls in der Namenliste die Haltezeiten für diese Verbindung ein. Beachten Sie folgende Regeln:
- Die B1-Haltezeit sollte je nach Anwendungsfall so groß gewählt werden, dass die Verbindung nicht durch das kurzzeitige Ausbleiben von Paketen zu früh abgebaut wird. Erfahrungsgemäß sind Werte zwischen 60 und 180 Sekunden für den Beginn eine gute Basis, die man im Betrieb dann weiter anpassen kann.
 - Die B2-Haltezeit entscheidet darüber, nach welcher Zeit die dynamischen Kanäle wieder abgebaut werden, wenn der Datendurchsatz unter dem Schwellwert liegt.
- ③ Legen Sie in der Kanalliste fest, wie viele Kanäle für die Verbindung verwendet werden sollen. Außerdem können Sie hier bestimmen, welche Kanäle in Anspruch genommen werden dürfen und so z.B. bestimmte Kanäle für die Einwahl über RAS freihalten.

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

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

7.4 IPX-Routing

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

7.4.1 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 eingegraben. 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.

7.4.2 Informationen über das LAN

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

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

7.4.3

IPX-Routing-Tabelle

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

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

- Gegenstelle

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

- Netzwerk

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

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

- Binding

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

- Propagate

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

erster Linie für den Datenaustausch zwischen Stationen in einem lokalen Netz (LAN) verwendet.

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

- **Backoff**

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

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

Die Default-Einstellung ist 'Ein'.

7.4.4

Was passiert bei der Datenübertragung im IPX-Netz?

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

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

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

7.4.5

RIP- und SAP-Tabellen

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

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

RIP-Tabellen können 64, SAP-Tabellen 128 Einträge aufnehmen. Wenn jedes neue Paket die Tabellen aktualisiert, müssen natürlich irgendwann auch die alten Einträge verschwinden. Dazu bekommen die Einträge ein künstliche Alterung. Für alle Einträge in den RIP/SAP-Tabellen, die durch lokalen Datenaustausch gelernt wurden, wird das Alter alle 60 Sekunden um eins erhöht. Ein neues RIP- bzw. SAP-Paket für einen Eintrag setzt das Alter auf Null zurück. Nach einem einstellbaren Alter von 1 bis 60 wird die Route oder der Service als unerreichbar (Down) bezeichnet. Ist das Doppelte dieser Zeit abgelaufen, wird der Eintrag entfernt. Außerdem werden bei einem Verbindungsaufbau alle RIP- und SAP-Informationen, die diese Gegenstelle betreffen, aus den Tabellen gelöscht und durch neue Informationen ersetzt.

7.4.6

So viele Router hier ...

Ist in einem Netz der Aufbau zu mehr Gegenstellen gleichzeitig erwünscht, als ein Router realisieren kann, dann wird es Zeit für einen zweiten (oder weitere) Router. Damit das Zusammenspiel der Brüder reibungslos funktioniert und das Netz wirklich immer einen Ansprechpartner findet, werden in allen Routern die gleichen Einträge in der Routing-Tabelle vorgenommen. Durch die RIP-Pakete werden jedem Router dann auch die gleichen Routing-Informationen übermittelt, allerdings mit höherem Tic- und Hopcount (Setup/IPX-Modul/LAN-Einstellung/RIP-SAP-Skal. einschalten).

Dadurch werden diese Routen quasi als Reserve markiert, wenn auf dem angesprochenen Gerät alle Kanäle besetzt sind.

7.4.7

Redundante Routen

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

Sollte es trotzdem einmal nötig sein, redundante Routen im lokalen Netz bekannt zu geben, 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'.

7.4.8

Exponential-Backoff

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

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

- Die erste Anwahl erfolgt nach $10 + x$ Sekunden. x ist dabei 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 der Router schließlich auf. Durch das ständige Anwachsen der Wartezeit ist nach 16 Versuchen maximal ein Tag vergangen.



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

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

7.4.9

Filter für die IPX-Pakete

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

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

- **Propagated Frames**

Diese speziellen Datenpakete verwenden Protokolle, die eigentlich nicht geroutet werden können. Um trotzdem am gemeinsamen Routing teilnehmen zu können, werden diese Daten in normale IPX-Pakete gekapselt und als Broadcast verschickt.

Manchmal sind diese Pakete beim Routing nicht erwünscht. Daher können Sie für diesen Paket-Typ explizit einstellen, ob er geroutet oder gefiltert werden soll.

- **Socket-Filter**

Jedes Datenpaket in einem IPX-Netz enthält neben Ziel- und Quelladressen auch Ziel- und Quell-Sockets. Sockets bezeichnen die Prozesse, für die die Daten in dem Paket bestimmt sind.

Für die Sockets aus dem lokalen sowie aus den entfernten Netzen gibt es jeweils eine entsprechende Filtertabelle, die die Filter beinhaltet, mit denen einzelne Ziel-Sockets oder ganze Gruppen von der Übertragung ausgeschlossen werden können. Einige Sockets, die bekanntermaßen häufig für unerwünschte Verbindungen sorgen, sind als Voreinstellung schon in der Socket-Filtertabelle eingetragen.

● RIP- und SAP-Informationen

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

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



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

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

- Mit einer LAN- und einer WAN-Filtertabelle kann der Router angewiesen werden, Informationen über Routen zu bestimmten Netzen bzw. über bestimmte verfügbare Dienste nicht in die interne RIP- oder SAP-Tabelle zu übernehmen. Die betroffenen Routen werden also nicht verwendet und auch nicht weiter bekannt gegeben, 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 Verbindungsleistung.
- Die RIP- und SAP-Pakete werden nur dann versendet, wenn sich Änderungen in der Information ergeben haben.
- RIPs und SAPs können in regelmäßigen, einstellbaren Zeiten übertragen werden. Normalerweise werden die Informationen im Abstand von einer Minute verschickt. Mit der Zeiteinstellung kann dieser Abstand auf bis zu 60 Minuten ausgedehnt werden.

- Die gebührenschonendste Behandlung der RIP- und SAP-Pakete überträgt die Informationen einmalig nur dann, wenn eine Verbindung aufgebaut ist.
- IPX- und SPX-Watchdogs:
Mit diesen Datenpaketen erkundigen sich die Server z.B. bei den Arbeitsplatzrechnern, ob sie noch aktiv sind oder ob sie ggf. abgemeldet werden können. Damit diese „Hallo, bist du noch wach?“-Pakete für Rechner in einem entfernten Netz nicht ständig zum Verbindungsaufbau führen, können Sie die Beantwortung dieser Anfragen folgendermaßen einstellen:
 - IPX-Watchdogs bleiben völlig unbeantwortet. Nach der beim Server eingestellten Zeit werden die Rechner abgemeldet.
 - IPX- und SPX-Watchdogs können lokal beantworten werden. Dieses Verfahren nennt man Spoofing. Der Router antwortet dann anstelle der angesprochenen Rechner, die dann natürlich nie abgemeldet werden. Die Einstellung einer Zeit beim Server, nach der die entsprechenden Geräte auf jeden Fall abgemeldet werden, ist also sinnvoll.
 - IPX- und SPX-Watchdogs können natürlich auch ganz normal geroutet werden, führen dann aber recht häufig zum Aufbau einer Verbindung.

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



7.5

IP-Routing

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

7.5.1

Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem Router, an welche Gegenstelle (also welchen anderen Router oder Rechner) er die Daten für bestimmte IP-Adressen oder IP-Adress-Bereiche schicken soll. So ein Eintrag heißt auch „Route“, weil der Weg der Datenpakete damit beschrieben wird. Da Sie diese Einträge selbst vornehmen und sie solange unverändert bleiben, bis Sie selbst sie wieder ändern oder löschen, heißt dieses Verfahren auch „statisches Routing“. Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing“. Dabei tauschen die Router selbstständig untereinander Informationen über die Rou-

ten aus und erneuern diese fortlaufend. Die statische Routing-Tabelle kann bis zu 64 Einträge aufnehmen, die dynamische Tabelle 128. Bei aktiviertem IP-RIP beachtet der IP-Router beide Tabellen.

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

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

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

Was bedeuten die einzelnen Einträge in der Liste?

- IP-Adresse und IP-Netzmaske

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

Die Route mit der IP-Adresse „255.255.255.255“ mit Netzmaske „0.0.0.0“ ist die Default-Route. Alle Datenpakete, die nicht durch andere Routing-Einträge geroutet werden können, werden über diese Route übertragen.

- Router-Name

An diese Gegenstelle überträgt der Router die zur IP-Adresse und Netzmaske passenden Datenpakete. Ist die Gegenstelle ein Router in einem anderen Netz oder ein einzelner Arbeitsplatzrechner, dann steht hier ein

Name. Kann der eigene Router die Gegenstelle nicht selbst erreichen, steht hier die IP-Adresse eines anderen Routers, der den Weg ins Zielnetz kennt.

Der Router-Name gibt an, was mit den zur IP-Adresse und Netzmaske passenden Datenpaketen geschehen soll.

Routen mit dem Router-Namen „0.0.0.0“ bezeichnen Ausschluss-Routen. Datenpakete für diese „Null-Routen“ werden 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.

Wird als Router-Name eine IP-Adresse eingetragen, handelt es sich dabei um einen lokal erreichbaren Router, der für die Übertragung der entsprechenden Datenpakete zuständig ist.

● Distanz

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

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

● Maskierung

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

- 'aus': Es wird keine Maskierung durchgeführt.
- 'ein': Mit diesem Eintrag fordern Sie von Ihrem Provider die Zuweisung einer beliebigen, im Internet gültigen IP-Adresse an, die Sie im weiteren für die Verbindung und die Maskierung verwenden wollen.

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

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

Beispiele mit Erläuterungen:

IP-Adresse	IP-Netzmaske	Router-Name	Dist.	Und das passiert:
192.168.1.9	255.255.255.255	AUSSENDIENST	2	Die Gegenstelle AUSSENDIENST ist unter der IP-Adresse 192.168.1.9 zu erreichen.
192.168.120.0	255.255.255.0	ROUTER01	2	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.120.x werden an ROUTER01 übertragen.
192.168.125.0	255.255.255.0	ROUTER02	3	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.125.x werden an ROUTER02 übertragen.
192.168.130.0	255.255.255.0	192.168.140.123	0	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.130.x werden an den lokal erreichbaren Router mit der IP-Adresse 192.168.140.123 übertragen.
192.168.0.0	255.255.0.0	0.0.0.0	0	Schließt die Übertragung aller Datenpakete in 10er-Netze aus.
172.16.0.0	255.255.0.0	0.0.0.0	0	
10.0.0.0	255.0.0.0	0.0.0.0	0	
224.0.0.0	224.0.0.0	0.0.0.0	0	
255.255.255.255	0.0.0.0	ZENTRALE	2	Alle Datenpakete, die nicht den zuvorstehenden Einträgen zugeordnet werden können, werden an die Gegenstelle ZENTRALE übertragen.



Wichtig ist dabei auch die Reihenfolge der Einträge: Sie werden von oben nach unten abgearbeitet! Der Router sortiert die Einträge dabei selbstständig: Zuerst nach den Netzmasken, davon die größte nach oben. Dann nach den IP-Adressen, davon die kleinsten nach oben. Dadurch landet der 'ZENTRALE'-Eintrag ganz am Ende der Liste. Mit diesem Eintrag ganz oben in der

Liste würde der Router alle (!) Datenpakete, die nicht ins eigene Netz gehören, ins Netz der Zentrale senden.

7.5.2 Filter für die TCP/IP-Pakete

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

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

Der Router kann sich die Ziel- und Quell-Ports von solchen Datenpaketen ansehen, die TCP oder UDP als Protokoll verwenden. Aus diesen Ports kann dann abgeleitet werden, für welchen Zweck die Daten gedacht sind. So können z.B. FTP-Zugriffe oder Telnet-Sitzungen erkannt werden.

Mit Hilfe der entsprechenden Filter-Tabelle können Sie festlegen, dass bestimmte Daten nicht aus dem LAN an das WAN übertragen werden sollen. Genauso können natürlich auch Daten für bestimmte Ports aus dem WAN in Richtung des LANs gesperrt werden.

Neben der Definition der Portbereiche und der zugehörigen Protokolle kann in den Filter-Tabellen mit dem Filter-Typ auch festgelegt werden, ob die betroffenen Datenpakete nie übertragen werden oder ob sie nur nicht zu einem Verbindungsaufbau führen sollen (also nur bei bestehender Verbindung übertragen werden).

Im Router befinden sich zwei separate Filtertabellen für Pakete, die aus dem LAN kommen und Pakete, die von WAN kommen.

Diese Filtertabellen finden Sie in *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Filter' bzw. im Menü */Setup/IP-Router*.

7.5.3

Proxy-ARP

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

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

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

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

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

7.5.4

Lokales Routing

Sie kennen das folgende Verhalten der Arbeitsplatzrechner in einem lokalen Netz: Möchte der Rechner ein Datenpaket an eine IP-Adresse senden, die nicht in seinem eigenen LAN 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 nicht selbst das Zielnetz erreichen, er kennt aber einen anderen Router, der zu diesem Ziel findet.

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

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

Manche Rechner können mit den ICMP-Redirects leider nichts anfangen. Um die Datenpakete trotzdem zustellen zu können, verwenden Sie das lokale Routing (im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' oder im Menü `/Setup/IP-Router-Modul/Lok. - Routing Ein`). Dadurch weisen Sie den Router in Ihrem Gerät an, das Datenpaket selbst zum anderen, zuständigen Router zu senden. Außerdem werden dann keinen ICMP-Redirects mehr geschickt.

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

7.5.5

Dynamisches Routing mit IP-RIP

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

Welche Informationen werden über IP-RIP propagiert?

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

- Routen, die mit der Router-Einstellung '0.0.0.0' verworfen werden.

- Routen, die auf andere Router im lokalen Netz lauten.
- Routen, die einzelne Rechner über Proxy-ARP an das LAN anbinden.

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

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



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

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

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

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

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

Was bedeuten die Einträge?

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

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

- Die Route ist in der Tabelle noch gar nicht vorhanden, dann wird sie aufgenommen (sofern Platz in der Tabelle ist).
- Die Route ist in der Tabelle vorhanden mit der Zeit von '5' oder '6'. Die neue Route wird dann verwendet, wenn sie die gleiche oder eine bessere Distanz aufweist.
- Die Route ist in der Tabelle vorhanden mit der Zeit von '7' bis '10', hat also die Distanz '16'. Die neue Route wird auf jeden Fall verwendet.
- Die Route ist in der Tabelle vorhanden. Die neue Route kommt von dem gleichen Router, der auch diese Route bekannt gegeben hat, hat aber eine schlechtere Distanz als der bisherige Eintrag. Wenn ein Gerät so die Verschlechterung seiner eigenen statischen Routing-Tabelle bekannt



macht (z.B. durch den Abbau einer Verbindung steigt die Distanz von '1' auf '2', siehe unten), dann glaubt der Router ihm das und nimmt den schlechteren Eintrag in seine dynamische Tabelle auf.

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

Zusammenspiel: statische und dynamische Tabelle

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

Router ohne IP-RIP-Unterstützung

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

Skalierung durch IP-RIP

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

7.6

IP-Masquerading (NAT, PAT)

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

Die Lösung heißt hier IP-Masquerading. Bei diesem Verfahren tritt nur ein Router des LANs mit einer IP-Adresse im Internet in Erscheinung. Diese IP-Adresse wird dem Router z.B. fest vom NIC oder temporär von einem Internet-Provider zugewiesen. Alle anderen Rechner im Netz „verstecken“ sich dann

hinter dieser einen IP-Adresse. Neben dem angenehmen Spareffekt bildet das IP-Masquerading auch einen sehr effektiven Schutz gegen Zugriffe aus dem Internet auf das lokale Netz.

Zwei Adressen für den Router

Bei Masquerading treffen zwei gegensätzliche Forderungen an den Router aufeinander: Zum einen soll er eine im lokalen Netz gültige IP-Adresse haben, damit er aus dem LAN erreichbar ist, zum anderen soll er eine im Internet gültige Adresse haben. Da diese beiden Adressen prinzipiell nicht in einem logischen Netz liegen dürfen, hilft hier nur eins: Zwei IP-Adressen müssen her.

Der Router bekommt also nun eine **Internet**-Adresse und eine **Intranet**-Adresse, jeweils natürlich mit passender Netzmaske. Mit der Option 'Maskierung' in der Routing-Tabelle informieren Sie den Router darüber, welche der beiden Adressen er bei der Weitergabe der Pakete verwenden soll.

- 'aus': Es wird keine Maskierung durchgeführt.
- 'dyn.': Mit diesem Eintrag fordern Sie von Ihrem Provider die Zuweisung einer beliebigen, im Internet gültigen IP-Adresse an, die Sie im weiteren für die Verbindung und die Maskierung verwenden wollen.
- 'stat.': Mit diesem Eintrag fordern Sie von Ihrem Provider die Zuweisung einer bestimmten, unter /setup/TCP als IP-Adresse eingetragenen Adresse an, die Sie im weiteren für die Verbindung und die Maskierung verwenden wollen.

Wird dabei vom Provider eine bestimmte Adresse angefordert, gibt es zwei Möglichkeiten der tatsächlichen Adresszuweisung:

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

- Der Provider weist dem Router eine andere Adresse zu. Dann werden **alle** Rechner im lokalen Netz hinter der zugewiesenen Adresse maskiert.

Wie funktioniert IP-Masquerading?

Das Masquerading nutzt die Eigenschaft der Datenübertragung über TCP/IP aus, dass neben der Quell- und Ziel-Adresse auch Portnummer für Quelle und Ziel verwendet werden. Bekommt der Router nun ein Datenpaket zur Übertragung, merkt er sich die IP-Adresse und den Port des Absenders in einer internen Tabelle. Dann gibt er dem Paket seine eigene IP-Adresse und eine beliebige neue Portnummer. Diesen neuen Port trägt er 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 Routers mit der neuen Absender-Portnummer. Mit dem Eintrag in der internen Tabelle kann der Router diese Antwort nun wieder dem ursprünglichen Absender zuordnen.

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

Einfaches und inverses Masquerading

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

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

Der kleine Unterschied:

- Der Zugriff von außen auf einen Dienst (Port) im Intranet muss vorher durch Angabe einer Portnummer 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 LAN auf das Internet hingegen wird der Eintrag in der Tabelle mit Port- und IP-Adress-Informationen durch den Router selbst vorgenommen.

Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also **gleichzeitig** 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

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

Welche Protokolle werden mit IP-Masquerading übertragen?

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

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

- TCP (und alle darauf aufbauenden Protokolle wie FTP, HTTP etc.)
- UDP
- ICMP

7.7

DNS-Forwarding

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

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

Wenn nun ein Rechner aus dem Intranet eine Homepage aufrufen möchte, sendet er zunächst einen DNS-Request aus: „Welche IP-Adresse gehört zu www.domain.com?“

Wenn der Router bei den Arbeitsplatzrechnern als DNS-Server eingetragen ist, wird diese Anfrage folgendermaßen behandelt:

- Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist (in *ELSA LANconfig* im Konfigurationsbereich

'TCP/IP' auf der Registerkarte 'Adressen' oder im Menü /Setup/TCP-IP-Modul). Wird er dort fündig, holt er die gewünschte Information von diesem Server.

- Gibt es keinen eingetragenen DNS-Server im Router, versucht er auf einer evtl. bestehenden PPP-Verbindung (z.B. zum Internet-Provider) einen DNS-Server zu erreichen, und holt die Zuordnung der IP-Adresse zum Namen von dort. Das gelingt natürlich nur dann, wenn während der PPP-Verhandlung die Adresse eines DNS-Servers an den Router übermittelt worden ist.
- Besteht keine Verbindung, wird die Default-Route aufgebaut und dort nach dem DNS-Server gesucht.

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

7.7.1

Policy Based Routing

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

8

Technische Daten

8.1

Leistungs- und Kenndaten

Funktionsarten	IP-Router, IPX-Router, CAPI-Server, DHCP-Server; Least-Cost-Router für Router- und CAPI-Verbindungen, gleichzeitiger Betrieb aller Funktionsarten möglich
2-Mbit-WAN-Anschlüsse	alle Geräte: X.21 (elektrisch konform X.24/V.11), max. 2 Mbit/s, Vollduplex, externer Takt
	ELSA LANCOM Business 6011: 1 x G.703/G.704, max. 2 Mbit/s, Vollduplex
	ELSA LANCOM Business 6021: 2 x G.703/G.704, max. 2 Mbit/s, Vollduplex
ISDN-Schnittstelle	Anschluss: ISDN-S ₀ -Bus, Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-Konfiguration, I.430 D-Kanal: 1TR6, Euro-ISDN (DSS1), Autosensing, Festverbindungen Gruppe 0 (D64S, D64S2, D64SY) B-Kanal: PPP (asynch./synch.), MLPPP, X.75, HDLC, V.110, CAPI 2.0 über ELSA LANCAPI, Stac-Datenkompression
LAN-Anschluss	Ethernet IEEE 802.3, 10/100Base-TX (RJ45, Node/Hub, Switch), Autosensing, Vollduplex
Netzwerk-Protokolle	IP-Router: ARP, Proxy ARP, DHCP-Server, IP, ICMP, UDP, TCP, RIP-1, RIP-2, Proxy DNS, Proxy NetBIOS/IP IPX-Router: IPX, SPX, RIP, SAP, Novell NetBIOS, Novell-Burst-Mode
Security-Funktionen	Auswertung der Rufnummer der Gegenstelle (CLIP); PAP, CHAP und MS-CHAP zur Beglaubigung unter PPP; automatischer Rückruf über ISDN; Filtermöglichkeiten im IP-, IPX- und Bridge-Betrieb, Schutz der Konfiguration über Zugangslisten und Passwort, Aufzeichnung der letzten Verbindungsinformationen, IP-Masquerading
Filter-Möglichkeiten (Firewall)	IP-Router: Quell- und Zielfilter für Netzwerke, Protokolle und Ports IPX-Router: RIP, SAP, IPX- und SPX-Watchdog, Sockets, Routen, Propagated Packets
IP-Masquerading	Übersetzung von internen IP-Adressen und Ports auf eine externe IP-Adresse; statische/dynamische Zuweisung der IP-Adresse via PPP; Maskierung von TCP, UDP, ICMP und FTP; DNS-Forwarding; inverse Maskierung für Dienste im Intranet wie z.B. Web-Server (DMZ)
Spoofing	IPX-Router: RIP- und SAP-Packets; IPX- und SPX-Watchdogs, Novell NetBIOS, Keep-alive-Packets

CAPI-Server	virtuelle CAPI 2.0 für Windows-Betriebssysteme, NDIS-WAN-Treiber, Fax-Class 1
Leistungssteuerung	automatischer Rückruf mit oder ohne Verbindungsaufbau; Line-on-Demand (dynamische Kanalbündelung), Short-Hold-Modus, Round-Robin-Auswahl, Fast Call Back, Dial-Backup für Festverbindungen
Gebührenschatz	Maximale Onlinezeit oder Gebühren pro Periode (AOC-D, AOC-E)
Management	via LAN, ISDN (Fernwartung) oder V.24, Managementsoftware <i>ELSA LANconfig</i> und <i>ELSA LANmonitor</i> für Windows, <i>ELSA xLANconfig</i> für LINUX, Konfiguration über SNMP v.1, TFTP, Telnet oder Terminal möglich
Betriebssicherheit	Hardware-Watchdogs, regelmäßige Selbsttests, <i>ELSA FirmSafe</i> -Konzept für Remote-Software-Upgrade
Statistiken	Zähler für LAN/WAN getrennt, Pakete, Fehler, Verbindungen und Online-Zeit; Logging der Leistungssteuerung und Online-Zeit mit <i>ELSA LANmonitor</i> und SYSLOG; Accounting der Verbindungen, Online-Zeit, Volumen pro IP mit <i>ELSA LANmonitor</i> ; Trace von Protokollen zur Diagnose
Anzeigen/Bedienung	LCD-Display und Tastatur, LEDs für LAN- und WAN-Status
Stromversorgung	12 V AC mit Steckernetzteil für 230 V, 12 VA
Umgebungsbedingungen	Temperatur: 5–40°C, Luftfeuchtigkeit: 0–80%, nicht kondensierend
Ausführung und Maße	stabiles Metallgehäuse, Anschlüsse auf der Rückseite; Abmessungen 230 x 38 x 228 mm (B x H x T)
Lieferumfang	Gerät inkl. Netzkabel, ISDN- und X.21-Anschlusskabel, ein (nur <i>ELSA LANCOM Business 6011</i>) bzw. zwei (nur <i>ELSA LANCOM Business 6021</i>) G.703-Anschlusskabel, Anschlusskabel für serielle Konfigurations-Schnittstelle (Twisted-Pair-Kabel CAT-5), ausführliche Dokumentation und <i>ELSA LANCOM Business</i> -CD Software: Konfigurationsprogramme <i>ELSA WEBconfig</i> (in der Firmware des Gerätes) und <i>ELSA LANconfig</i> und <i>ELSA xLANconfig</i> (beta), Überwachungsprogramm <i>ELSA LANmonitor</i> , Terminalprogramm <i>ELSA-ZOC</i>
Zulassungen	für Deutschland, Schweiz und alle Länder der EU
Service und Garantie	6 Jahre Garantie
Support	über Hotline und Internet

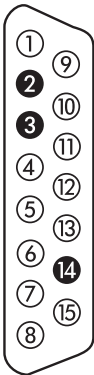
8.2

Anschlussbelegung

8.2.1

X.21-Schnittstelle

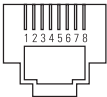
Die elektrische Übertragung erfolgt konform den Spezifikationen X.24/V.11.
15-poliger D-Sub-Stecker, entsprechend ISO 4903

Stecker	Pin-Nr.	X.21	Richtung	Funktion
	1	–	–	–
	2	Txd(+)	►	transmit data
	3	Ctrl(+)	►	control
	4	Rxd(+)	◄	receive data
	5	Ind(+)	◄	indicate
	6	Set(+)	◄	signal element timing
	7	–	–	–
	8	GND		signal ground
	9	Txd(-)	►	transmit data
	10	Ctrl(-)	►	control
	11	Rxd(-)	◄	receive data
	12	Ind(-)	◄	indicate
	13	Set(-)	◄	signal element timing
	14	–	–	–
	15	–	–	–

8.2.2

G.703-Schnittstelle

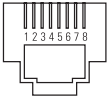
Über diese Schnittstelle verfügen nur die Geräte *ELSA LANCOM Business 6011* und *ELSA LANCOM Business 6021*.
8-polige RJ45-Buchse, entsprechend ISO 8877, EN 60603-7

Steckverbindung	RJ45-Pin	Bezeichnung	Funktion
	1	Ra	receive input
	2	Rb	receive ground
	3	–	–
	4	Ta	transmit output
	5	Tb	transmit ground
	6	–	–
	7	–	–
	8	–	–

8.2.3

ISDN-S₀-Schnittstelle

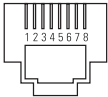
8-polige RJ45-Buchse, entsprechend ISO 8877, EN 60603-7

Steckverbindung	RJ45-Pin	Leitung	IAE
	1	–	–
	2	–	–
	3	T+	2a
	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	–	–
	8	–	–

8.2.4

Ethernet-Schnittstelle 10/100Base-T

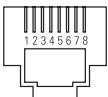
8-polige RJ45-Buchse, entsprechend ISO 8877, EN 60603-7

Steckverbindung	RJ45-Pin	Leitung
	1	–
	2	–
	3	T+
	4	R+
	5	R-
	6	T-
	7	–
	8	–

8.2.5

Konfigurationsschnittstelle (Outband)

8-polige RJ45-Buchse, entsprechend ISO 8877, EN 60603-7; Belegung kompatibel zu Cisco

Steckverbindung	RJ45-Pin	Funktion
	1	CTS
	2	DSR
	3	RXD
	4	Ground
	5	Ground
	6	TXD
	7	DTR
	8	RTS

8.2.6

Wichtiger Hinweis zum Recycling



Bitte beachten Sie: Dieses Gerät enthält eine fest eingebaute Lithium-Batterie. Sie sind gesetzlich verpflichtet, schadstoffhaltige Batterien umweltgerecht zu entsorgen!

Bitte schicken Sie ELSA-Geräte mit eingebauter Batterie im Falle eines Defekts oder zur vollständigen Entsorgung daher grundsätzlich nur an uns zurück.

9

Anhang

9.1

Konformitätserklärung

**KONFORMITÄTSERKLÄRUNG**

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen
(FTEG) und der Richtlinie 1999/5/EG (R&TTE)

EC- DECLARATION OF CONFORMITY appropriate to the law of radio and telecom terminalequipment and
Directive 1999/5/EC (R&TTE)

Die Firma:
The Company: **ELSA AG**
Sonnenweg 11
52070 Aachen

erklärt, daß das Produkt:
declares that the product: **ELSA LANCOM Business 6001**
ELSA LANCOM Business 6011
ELSA LANCOM Business 6021

Telekommunikations (TK-) Endeinrichtung
telecommunications terminal equipment

Verwendungszweck:
intended purpose: **2Mbit-ISDN Router**

den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG
(Artikel 3 der R&TTE) entspricht.
complies with the appropriate essential requirements of the FTEG (Article 3 of R&TTE) and the other relevant provisions.

Harmonisierte Normen: **Gesundheit und Sicherheit gemäß §3 (1) 1. (Artikel 3 (1) a))**
Harmonised Standards: **Health and Safety requirements contained in §3 (1) 1. (Article 3 (1) a))**

EN 60 950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1996 +A11: 1998

Harmonisierte Normen: **Schutzanforderungen in Bezug auf die EMV §3 (1) 2, Artikel 3 (1) b))**
Harmonised Standards: **Protection requirements with respect to EMC §3 (1) 2, (Article 3 (1) b))**

EN 50 082-2: 1995 Teile / parts: EN 61 000-4-2, 3, 4, 5, 6, 11
EN 50 081-1: 1992 Teile / parts: EN 55 022: 1998 class B

Schnittstellenspezifikation: **Netzabschluß eines öffentlichen digitalen Tk-Netzes**
Interface specification: **Termination point of a digital public telecom. network**

Spezifikation **TBR 3, TBR 4 (Modell 6011, 6021)**
specification:

Diese Erklärung wird verantwortlich abgegeben durch:
This declaration is submitted by:

Aachen, 21. September 2000
Aachen, 21st September 2000

i.V. Stefan Kriebel
Bereichsleiter Entwicklung
VP Engineering

9.2

Allgemeine Garantiebedingungen

Diese Garantie vom 01.06.1998 gewährt die ELSA AG den Erwerbern von ELSA-Produkten nach ihrer Wahl zusätzlich zu den ihnen zustehenden gesetzlichen Gewährleistungsansprüchen nach Maßgabe der folgenden Bedingungen:

1 Garantieumfang

- a) Die Garantie erstreckt sich auf das gelieferte Gerät mit allen Teilen. Sie wird in der Form geleistet, daß Teile, die nachweislich trotz sachgemäßer Behandlung und Beachtung der Gebrauchsanweisung aufgrund von Fabrikations- und/oder Materialfehlern defekt geworden sind, nach unserer Wahl kostenlos ausgetauscht oder repariert werden. Alternativ hierzu behalten wir uns vor, das defekte Gerät gegen ein Nachfolgeprodukt auszutauschen oder dem Käufer den Original-Kaufpreis gegen Rückgabe des defekten Geräts zu erstatten. Handbücher und evtl. mitgelieferte Software sind von der Garantie ausgeschlossen.
- b) Die Kosten für Material und Arbeitszeit werden von uns getragen, nicht aber die Kosten für den Versand vom Erwerber zur Service-Werkstätte und/oder zu uns.
- c) Ersetzte Teile gehen in unser Eigentum über.
- d) Wir sind berechtigt, über die Instandsetzung und den Austausch hinaus technische Änderungen (z.B. Firmware-Updates) vorzunehmen, um das Gerät dem aktuellen Stand der Technik anzupassen. Hierfür entstehen dem Erwerber keine zusätzlichen Kosten. Ein Rechtsanspruch hierauf besteht nicht.

2 Garantiezeit

Die Garantiezeit beträgt für dieses ELSA-Produkt sechs Jahre. Die Garantiezeit beginnt mit dem Tag der Lieferung des Gerätes durch den ELSA-Fachhändler. Garantieleistungen bewirken weder eine Verlängerung der Garantiefrist, noch setzen sie eine neue Garantiefrist in Lauf. Die Garantiefrist für eingebaute Ersatzteile endet mit der Garantiefrist für das ganze Gerät.

3 Abwicklung

- a) Zeigen sich innerhalb der Garantiezeit Fehler des Gerätes, so sind Garantieansprüche unverzüglich, spätestens jedoch innerhalb von sieben Tagen geltend zu machen.
- b) Transportschäden, die äußerlich erkennbar sind (z.B. Gehäuse beschädigt), sind unverzüglich gegenüber der Transportperson und uns geltend zu machen. Äußerlich nicht erkennbare Schäden sind unverzüglich nach Entdeckung, spätestens jedoch innerhalb von sieben Tagen nach Anlieferung, schriftlich gegenüber der Transportperson und uns zu reklamieren.
- c) Der Transport zu und von der Stelle, welche die Garantieansprüche entgegennimmt und/oder das instandgesetzte Gerät austauscht, geschieht auf eigene Gefahr und Kosten des Erwerbers.
- d) Garantieansprüche werden nur berücksichtigt, wenn mit dem Gerät das Rechnungsoriginal vorgelegt wird.

4 Ausschluß der Garantie

Jegliche Garantieansprüche sind insbesondere ausgeschlossen,

- a) wenn das Gerät durch den Einfluss höherer Gewalt oder durch Umwelteinflüsse (Feuchtigkeit, Stromschlag, Staub u.ä.) beschädigt oder zerstört wurde;
- b) wenn das Gerät unter Bedingungen gelagert oder betrieben wurde, die außerhalb der technischen Spezifikationen liegen;

- c) wenn die Schäden durch unsachgemäße Behandlung – insbesondere durch Nichtbeachtung der Systembeschreibung und der Betriebsanleitung – aufgetreten sind;
- d) wenn das Gerät durch hierfür nicht von uns ermächtigte Personen geöffnet, repariert oder modifiziert wurde;
- e) wenn das Gerät mechanische Beschädigungen irgendwelcher Art aufweist;
- f) wenn Schäden an der Bildröhre eines ELSA-Monitors festgestellt werden, die insbesondere durch mechanische Belastungen (Verschiebung der Bildröhrenmaske durch Schockeinwirkung oder Beschädigungen des Glaskörpers), starke Magnetfelder in unmittelbarer Nähe (bunte Flecken auf dem Bildschirm), permanente Darstellung des gleichen Bildes (Einbrennen des Phosphors) hervorgerufen wurden;
- g) wenn und soweit sich die Luminanz der Hintergrundbeleuchtung bei TFT-Panels im Laufe der Zeit allmählich reduziert;
- h) wenn der Garantieanspruch nicht gemäß Ziffer 3a) oder 3b) gemeldet worden ist.

5 Bedienungsfehler

Stellt sich heraus, dass die gemeldete Fehlfunktion des Gerätes durch fehlerhafte Fremd-Hardware, -Software, Installation oder Bedienung verursacht wurde, behalten wir uns vor, den entstandenen Prüfaufwand dem Erwerber zu berechnen.

6 Ergänzende Regelungen

- a) Die vorstehenden Bestimmungen regeln das Rechtsverhältnis zu uns abschließend.
- b) Durch diese Garantie werden weitergehende Ansprüche, insbesondere solche auf Wandlung oder Minderung, nicht begründet. Schadensersatzansprüche, gleich aus welchem Rechtsgrund, sind ausgeschlossen. Dies gilt nicht, soweit z.B. bei Personenschäden oder Schäden an privat genutzten Sachen nach dem Produkthaftungsgesetz oder in Fällen des Vorsatzes oder der groben Fahrlässigkeit zwingend gehaftet wird.
- c) Ausgeschlossen sind insbesondere Ansprüche auf Ersatz von entgangenem Gewinn, mittelbaren oder Folgeschäden.
- d) Für Datenverlust und/oder die Wiederbeschaffung von Daten haften wir in Fällen von leichter und mittlerer Fahrlässigkeit nicht.
- e) In Fällen, in denen wir die Vernichtung von Daten vorsätzlich oder grob fahrlässig verursacht haben, haften wir für den typischen Wiederherstellungsaufwand, der bei regelmäßiger und gefahrensprechender Anfertigung von Sicherheitskopien eingetreten wäre.
- f) Die Garantie bezieht sich lediglich auf den Erstkäufer und ist nicht übertragbar.
- g) Gerichtsstand ist Aachen, falls der Erwerber Vollkaufmann ist. Hat der Erwerber keinen allgemeinen Gerichtsstand in der Bundesrepublik Deutschland oder verlegt er nach Vertragsabschluß seinen Wohnsitz oder gewöhnlichen Aufenthaltsort aus dem Geltungsbereich der Bundesrepublik Deutschland, ist unser Geschäftssitz Gerichtsstand. Dies gilt auch, falls Wohnsitz oder gewöhnlicher Aufenthalt des Käufers im Zeitpunkt der Klageerhebung nicht bekannt ist.
- h) Es findet das Recht der Bundesrepublik Deutschland Anwendung. Das UN-Kaufrecht gilt im Verhältnis zwischen uns und dem Erwerber nicht.

10 Index

● Ziffern

10/100Base-TX	13
10/100Base-TX-Anschluss	16
100Mbit-Netz	13
2-Mbit	
Basisprotokolle	47
Bündelung	49
Master	51
Slave	51
Kanalbezeichnung	50
2-Mbit-Verbindung	41

● A

Adress-Pool	64, 70
Adressverwaltung	62
Anruferkennung	55
Anschlußbelegung	
Ethernet-Schnittstelle	168
G.703-Schnittstelle	167
ISDN-S ₀ -Schnittstelle	168
Konfigurationsschnittstelle	168
X.21-Schnittstelle	167
Anschlussbelegung	167
Outband	168
AOCD	103
Apple Talk	118
Assistenten	25
Auslandsgespräche	107
Ausschluss-Routen	152
Authentifizierung	139
automatischer Zeitabgleich	112
Automodus	63

● B

BACP	49
Basiskonfiguration	25
Benutzername	33, 56

Betriebsarten	53
Betriebssicherheit	46
Betriebszustände	11
B-Kanal	30, 44
B-Kanal-Protokoll	57
BRI	17
Broadcastadresse	120
Broadcast-Übertragung	124
Brute-Force	54
Bürokommunikation	96

● C

Call-by-Call	107, 108
CAPI Faxmodem	102
CAPI-Schnittstelle	96
CBCP	138
CBCP (Callback Control Protocol)	132
CD	15
Challenge Handshake	
Authentication Protocol	56
CHAP	56, 131, 132
CLI	57
Client für Windows-Netzwerke	77
Common ISDN Application	
Programming Interface	96

● D

D2MS	16, 46
D2MU	16, 46
Datei- und Druckerfreigabe	78
Datenkompressionsverfahren	
LZS	141
Datenpakete	115
Datenübertragung	141
Datenübertragung im IPX-Netz	145
DFÜ-Netzwerk	31, 56
DHCP	62

DHCP für WINS-Auflösung	67
DHCP-Automodus	63
DHCP-Server	63, 71
Konfiguration	68
Dienst	71
Distanz einer Route	152
D-Kanal	44, 57
DNS	71, 162
DNS-Forwarding	162
DNS-Forwarding-Mechanismus	72
DNS-Server	62, 66, 71
Filterliste	74
Filtermechanismus	72
verfügbare Informationen	72
Dokumentation	15
Domain Name Service	71, 162
Domains	71
Domains sperren	74
Durchsatz	141
Dynamic Host Configuration Protocol	63
Dynamische Kanalbündelung	141
dynamisches Routing	150

E

E1	43
strukturiert	45
unstrukturiert	45
E1-S	47
E1-S (mit TS16)	47
E1-U	47
Ein/Aus-Schalter	13, 16
elektronische Dokumentation	15
End-Adresse	64
erreichbare Rechner	83

F

Fast Call Back	57
Fax	102
Fax Class 1	102
Faxmodem	

LANCAPI	102
Faxtreiber	102
Faxübertragung	102
Fehlerrate	46
Fehlersuche	29
Feiertage	108
Ferngespräche	108
Fernkonfiguration	21, 22
Fernverbindung	32
Fernzugang	31
Festverbindung	17
Filter	55
Filter-Liste	61
Firewall	55
Firewall-Funktion	62
FirmSafe, ELSA FirmSafe	37
Firmware-Upload	38
mit LANconfig	38
mit Terminal-Programm	39
mit TFTP	39
Flash-ROM-Speicher	37
Frames	44
Framing	44
Freigabe	79
freigegebene Ressourcen	79
Funkstrecke	115

G

G.703	16, 17, 43
G.703 strukturiert	43
RAI	13
G.703-Schnittstelle	12, 42
G.704	43
Integritätsprüfung	45
Garantiebedingungen	172
Gateway	62, 66
Gebühren	76
Gebührenbegrenzung	103
Gebühreneinheiten	103, 141
Gebühreninformation	103

Gebühreninformationen	141
Gebührenmanagement	103
Gruppen	75
Gültigkeitsdauer	63, 66

H

Haltezeit	141
Hardwarefax	97
HDLC	46, 48
hierarchische IP-Adressen	122
Hohe Telefonkosten	103
Host	71, 115

I

IANA	121
Identifikation	78
Identifikationskontrolle	55
Identifizierung des Anrufers	56
Inband	21, 22
mit Telnet	24
Inband-Konfiguration	22
interne Uhr	111
Internet	62, 118
Internet-Access	136
Internet-Adresse	160
Internet-Anbindung	41
Internetwork	118
Internet-Zugang	131
Intranet-Adresse	160
IP Control Protocol	131
IP Masquerading	62
IP-Adresse	30, 62, 135
IP-Adressen	118
IP-Adressverwaltung	62
IPCP	131, 132
IP-Filter	76
IP-Masquerading	55, 159
einfaches Masquerading	161
unterstützte Protokolle	162
IP-Netz	118

IP-Routing	
Filter	154
FTP	154
Telnet	154
IP-Routing-Tabelle	150
IPX	118
IPX Watchdogs	150
IPX-Adressierung	143
IPXCP	131, 132
IPX-Routing	
Backoff	145
Binding	143, 144
Exponential Backoff	147
Filter	148
Gegenstelle	144
Hops	146
Loop-Propagieren	147
Netzwerk	144
Propagate	144
RIP- und SAP-Tabellen	146
Tics	146
IPX-Routing-Tabelle	144
ISDN	44
TEI	14
ISDN-Netz	118
ISDN-S ₀ -Anschluss	12
ISDN-Schnittstelle	17
ISDN-Verbindungsgebühren	103
ITU	43

K

Kabel	115
Kabelnetz	118
Kanalbündelung	140
Dynamisch	141
Statisch	140
keine Gebühreninformationen	103
Kennwörter	79
Kompatibilität	131
Konfiguration	

SNMP	25
Verfahren	21
Konfigurations-Schnittstelle	21
Kopplung zweier Netzwerke	41
Kosten begrenzen	103

L

LAN	118, 124
LAN-Anschlusskabel	15
LANCAPI	31, 96
Client	97
Server	99
LANconfig	23, 29, 31, 38
Assistenten	25
LANmonitor	29, 111
LCP	131
LCP-Echo-Reply	134
LCP-Echo-Request	134
LCR	103, 107
LCR-Tabelle	108
Least-Cost-Router	107, 110
automatischer Rückfall	111
Betriebsarten	110
Gebührenüberwachung	110
Least-Cost-Routing	103
LED	11
Lieferumfang	15
Line-LED	13
Link Control Protocol	131
Local Area Network	118
Login	37
Login-Sperre	54
Login-Versuche	54
lokales Netzwerk	118
LZS-Datenkompression	141

M

MAC-Adresse	125
MAC-Protokoll	125
Mailserver	74

Medium Access Control	124
Mehrpunkt-Verkabelungen	124
Meldungen	11
MLPPP	49, 140
MS-CHAP	131, 132
Multilink PPP	49, 131, 140
Multiprotokollfähigkeit	125

N

Namen	75
Namen und Gruppenbezeichnung	78
Namenräume	75
Namensinformationen	76
NAT	55, 62, 159
NBNS	75
NBNS-Server	62, 66, 67
NetBIOS	72
Gegenstelle	80
Gegenstellen	76
IP-Filter	80
LAN-LAN-Kopplung	80
Nameserver	75
Netzwerkprotokoll	77
Ports	76
Proxy	75
Remote Access	82
TCP/IP	77
NetBIOS-Netze	72
Network Information Center	159
Netzbetreiber	107
Netzkennziffer	107
Netzmaske	119
Netzteil	15
Netzteilanschluss	13
Netzwerk	115
Netzwerkadresse	119
Netzwerk-kabel	115
Netzwerk-karte	115
Netzwerk-kopplung	41
Netzwerknamen	71

Netzwerkprotokoll	117
Netzwerkumgebung	82
NIC	159
Node/Hub-Umschalter	13
NTPMKU	17

● O

Objekt-Tabelle	60
Ortsgespräch	109
Ortsnetz	109
Ortstarif	109
Outband	21
Outband-Konfiguration	22

● P

Pakete	115
PAP	56, 131
Password Authentication Protocol	56
Passwort	30, 34, 55, 56, 133
Passwortschutz	54
PAT	55, 62, 159
Periode	103
physikalisches Medium	115
Point-to-Point Protocol	131
Port	100
Portnummer	161
Power	11
PPP	30, 48, 56, 131, 140
Aushandlung	131
Authenticate-Phase	132
Establish-Phase	132
LCP Extensions	140
Leitungsüberprüfung mit LCP	134
Network-Phase	132
Passwortschutz	131
Phasen einer PPP-Verhandlung	131
Rückruf-Funktionen	131, 137
Terminate-Phase	132
Überprüfung der Verbindung	131
Verhandlungsphase	33

Zuweisung von IP-Adressen	135
PPP-Client	22, 31
PPP-Liste	56
PPP-Verbindung	33
Preselection	107
PRI	41
Primärmultiplexanschluss	41
Prioritätensteuerung	101
Private Address Spaces	120
Propagated Frames	148
Protokoll	117
Provider	107
Punkt-zu-Mehrpunkt-Verbindung	117
Punkt-zu-Punkt-Verbindung	116

● R

RAS	76, 131
Rechner-Namen	71
Rechnernamen	75
Regel-Tabelle	60
registrierte IP-Adresse	120
Remote Access	76
Remote-Access	131, 135
reservierte Adressbereiche	121
Reset	13
RIP	145
RIP-Tabellen	146
Router	116
Router-Name	151
Routing	76, 121
Routing Information Protocol	145
Routingabelle	121
Rückruf	55, 57
Fast Call Back	57

● S

SAP	145
SAP-Tabellen	146
Schnittstelle	115
Schutz der Konfiguration	54

Scopes	75
serielle Schnittstelle	22
Service Advertising Protocol	145
Shared Medium	118, 124
Sicherheit	53, 55, 62
Sicherung	133
Sicherungsverfahren	56
Single User Access	62
SNMP	25
Socket-Filter	148
Software einspielen	37
Sonderrufnummern	109
Sparmöglichkeiten beim	
Telefonieren	109
Sperre	54
Split Horizon	147
SPX Watchdogs	150
Stac	141
Standard-Faxprogramme	102
Start-Adresse	64
Statische Kanalbündelung	140
statisches Routing	150
Statusanzeigen	13
G.703-Schnittstelle	13
ISDN-S ₀ -Schnittstelle	14
X.21-Schnittstelle	13
Status-LED	13
Steuerdaten	44

T

T1	43
Tageszeit	108
Tarife	107
Tarifstruktur	109
Tarifzone	109
Tasten	11
TCP/IP	118, 150
TCP/IP-Netze	71
TCP/IP-Stack	118
Technische Daten	165, 171

Teilnetz	122
Telefongesellschaft	110
Telnet	31
Terminaladapter	42
Timeout	141
Timeslots	43
Trace	
Beispiele	36
Schlüssel und Parameter	35
starten	35
Trace-Ausgaben	34
TS0	47
TS16	47
Type-of-Service	163

U

Übertragungsmedium	115
Übertragungsraten	31
Überwachung	29
Uhrzeit	108, 111
Umleitung	108
Upload	37
Username	133

V

V.24-Konfigurationsschnittstelle	13
Verbindungsaufbau	76
Verbindungsbegrenzung	103
Verfügbarkeit	101
Vorwahl	107

W

Wählpräfix	108
WAN-Schnittstellen	13, 165
Watchdogs	150
<i>WEBconfig</i>	38, 39
Wildcards	74
Windows Internet Name Service	
Server	75
Windows-Networking	82

Windows-Netz	67, 75
Windows-Netze routen	75
WINS-Konfiguration	67
WINS-Server	75
Wochentage	108

● **X**

X.21-Anschluss	12, 42
----------------------	--------

● **Y**

Y-Verbindung	141
--------------------	-----

● **Z**

Zeit im ISDN-Netz	112
Zeitabhängige Verbindungs- begrenzung	103
Zeitbudget	104
Zeitschlitz	43
Kopplung	45
Zellen	115
Zugangskontrolle	54
Zugangsschutz	55
Name	55
Name oder Nummer	55
Nummer	55
Zugriffstyp	79

