ELSA LANCOM™ DSL/25 Office

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.

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

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.com

Aachen, Mai 2000

20659/0500

Ein Wort vorab

DE

Vielen Dank für Ihr Vertrauen!

Mit dem *ELSA LANCOM DSL/25 Office* haben Sie sich für einen Router entschieden, mit dem Sie lokale Netzwerke oder einzelne Arbeitsplatzrechner mit anderen Netzwerken über eine ATM-Verbindung koppeln können. Der Anschluß an das ATM-Netz wird dabei über eine ADSL-Verbindung realisiert.

Dokumentation

Die beiliegende Dokumentation besteht aus:

- Handbuch

  Hardware-Installation, Beschreibung der Funktionen und Betriebsarten und Konfigurationsbeispiele

- elektronischer Dokumentation auf CD

  Technische Grundlagen (z.B. zu ATM, allgemeiner Netzwerktechnik, TCP/IP etc.), Workshop mit ausführlichen Anwendungsbeispielen, Referenzteil zum Nachschlagen mit vollständiger Beschreibung der Menüs

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

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

editorial@elsa.de

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

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

Inhalt

DE

DE

1 Einleitung

Die rasante Entwicklung der Computertechnik hat in den letzten Jahren zu einem sprunghaften Anstieg des elektronisch übertragenen Datenvolumens geführt. Immer mehr Anwender wollen immer mehr Daten senden und empfangen. Eine Forderung, der die bisherigen Übertragungstechnologien (über Modem oder ISDN-Geräte) nicht mehr gewachsen sind.

Neue Technologien heben diese Beschränkungen auf und bieten dem Anwender echte Breitbandkommunikation mit deutlich höheren Übertragungsraten als bisher. Als wichtiges Kriterium für die Verbreitung dieser neuen Zugangstechnologien steht die Verfügbarkeit in möglichst vielen Büros oder Firmen im Vordergrund. Eine der neuen Technolgien ist die Übertragung mittels xDSL, die über einfache Kupferleitungen die „letzte Meile" überbrückt. Damit wird z.B. der Anschluß an ATM-Hochgeschwindigkeitsnetze möglich.

Mit *ELSA LANCOM DSL/25 Office* steht Ihnen ein Router zur Verfügung, der speziell für die ATM-Schnittstelle der xDSL-Anschlüsse entwickelt wurde. *ELSA LANCOM DSL/25 Office* erlaubt den Anschluß von einzelnen Arbeitsplätzen oder ganzen lokalen Netzwerken und bietet dabei deutlich größere Übertragungsraten, als sie bisher über ISDN möglich waren.

Die besonderen Highlights:

- Superschnelle Internet-Anbindung. *ELSA LANCOM DSL/25 Office* erlaubt im ATM-Netz Übertragungsraten bis zu 6 Mbit/s downstream und 0,6 Mbit/s upstream.
- LAN-Kopplung über ATM oder ISDN. *ELSA LANCOM DSL/25 Office* unterstützt neben den Festverbindungen auch Wählverbindungen zu Gegenstellen im ATM- und im ISDN-Netz (in Vorbereitung bei einigen Netzbetreibern) und ermöglicht so die Kopplung einzelner lokaler Netzwerke zu einem gemeinsamen WAN (Wide Area Network).
- Bürokommunikation über Breitband-CAPI. Mit der integrierten Breitband-CAPI können auch normale ISDN-CAPI-Anwendungen wie Remote Access oder Fax von der verfügbaren Übertragungsbandbreite profitieren.

Dieses Kapitel stellt Ihnen das Gerät und seine Funktionen kurz vor. Eine ausführliche Beschreibung der Funktionen, der Software und ihre Bedienung sowie eine Einführung in die technischen Grundlagen finden Sie in den nachfolgenden Kapiteln.

DE

1.1 Was macht ein Router überhaupt?

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

Dieser Weg steht z.B. in Form einer ATM-Verbindung bereit, die mit Hilfe der Übertragungstechologie xDSL über normale Kupfer-Telefonleitungen realisiert wird.

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

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

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

Wann setzen Sie Router nun ganz konkret ein?

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

- Internet im LAN

  In vielen Unternehmen wächst die Forderung nach dem Zugriff auf das Internet von allen Arbeitsplätzen im LAN. Online-Recherchen, Filetrans-

fer und E-Mail sind nur einige der Anwendungen, die den Anwendern am PC die Arbeit erleichtern sollen.

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

- LAN-LAN-Kopplung

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

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

- Teleworking mit Remote-Access

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

  Remote-Access heißt hier das Zauberwort. Teleworking für die Kollegen im Home-Office oder Kontakt zur Zentrale für Außendienst-Mitarbeiter von unterwegs werden über den Router im lokalen Netz der Zentrale ermöglicht. Auch beim Remote-Access tut ein *ELSA LANCOM DSL/25 Office* natürlich alles für den Schutz der firmeneigenen Datenbestände: Die Rückruffunktion über eingetragene Namen und Rufnummern gibt nur bestimmten Personen den Sesam-öffne-dich-Schlüssel. Und für die leichtere Abrechnung werden damit die Telefonkosten in der Firma zentral erfaßt.

- Bürokommunikation über *LANCAPI*

  Faxen direkt aus den Anwendungen heraus, Anrufbeantworter mit unterschiedlichen Ansagetexten je nach Tageszeit und Bankgeschäfte erledi-

DE

gen, ohne das Büro zu verlassen: Diese Funktionen werden ermöglicht durch den Einsatz der *LANCAPI*.

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

1.2 Was bietet ein *ELSA LANCOM DSL/25 Office*?

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

Einfache Installation

- *ELSA LANCOM DSL/25 Office* mit Spannung versorgen
- Verbindung zum LAN herstellen
- ATM-Kabel einstecken
- Einschalten
- Loslegen

LAN-Anschluß

DSL-Router von ELSA werden über den 10/100Base-T-Anschluß an ein (Fast-)Ethernet angeschlossen. Der Anschluß ermittelt dabei automatisch, mit welcher Geschwindigkeit das lokale Netz betrieben wird.

WAN-Anschluß

ELSA LANCOM DSL/25 Office wird an die ATM-Schnittstelle eines xDSL-Anschlusses angeschlossen. Damit stehen Ihnen prinzipiell alle Funktionen einer direkten Verbindung ins ATM-Netz zur Verfügung.

ELSA LANCOM DSL/25 Office unterstützt sowohl dauernd bereitgestellte Verbindungen (Festverbindungen, auch PVC, Permanent Virtual Connection) als auch Wählverbindungen (SVC, Switched Virtual Connection).

IP über ATM, Classical IP

ELSA LANCOM DSL/25 Office überträgt Daten verschiedener Netzwerkprotokolle wie IP und IPX über die ATM-Strecke. Damit können z.B. Netzwerke von verschiedenen Standorten über ATM verbunden werden oder mit hohen Bandbreiten an das Internet angebunden werden.

PPP über ATM

ELSA LANCOM DSL/25 Office überträgt auch PPP über die ATM-Strecke. Damit stehen alle Vorteile der PPP-Verbindungen für die Datenübertragung über ATM zur Verfügung, u.a.:

- Datenkompression über Stac
- Aushandlung und Zuweisung von IP-Adressen über die WAN-Strecke
- Rückruffunktionen
- Paßwortschutz

Subadressing

ELSA LANCOM DSL/25 Office unterstützt Subadressing bei der Übermittlung und Auswertung der Rufnummern. Dadurch können auch an Anschlüssen mit nur einer Rufnummer verschiedene Geräte direkt angesprochen werden.

Konfiguration

Die Einstellung und Anpassung der Geräte an Ihre spezielle Aufgabe erfolgt schnell und komfortabel über das mitgelieferte Konfigurationstool *ELSA LANconfig* für Windows-Betriebssysteme.

Benutzer anderer Betriebssysteme verwenden die HTML-basierte Konfiguration Telnet oder ein beliebiges Terminalprogramm.

Der Zugriff auf das Gerät ist dabei möglich aus dem WAN, aus dem LAN oder direkt über die eigene Konfigurationsschnittstelle. Bei Konfigurationen aus dem LAN oder WAN wird neben TFTP auch SNMP unterstützt.

Die integrierten Installations-Assistenten von *ELSA LANconfig* und der HTML-Konfiguration helfen Ihnen, die Geräte in wenigen Schritten in Betrieb zu nehmen.

Software-Update

Damit Sie immer auf dem neuesten Stand der Technik in Sachen Software bleiben, haben die Geräte einen Flash-ROM-Speicher. Eine neue Firmware kann so komfortabel eingespielt werden, ohne daß man das Gerät öffnen muß.

Die aktuelle Version steht immer in unseren Online-Medien für Sie bereit und kann über das LAN, das WAN oder über die Konfigurationsschnittstelle eingespielt werden.

DE

FirmSafe

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

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

Zugriffschutz

Zum Schutz vor unberechtigtem Zugriff auf das Firmen-Netz bietet der Router neben dem einfachen Paßwortschutz mit Authentifizierungsmechanismen im PPP, Firewall-Filtern und IP-Masquerading ein geschlossenes Sicherheitskonzept. Zusätzlich verhindert die Login-Sperre „Brute-Force-Angriffe" und sperrt den Zugang zum Router nach einer einstellbaren Anzahl von Login-Versuchen mit falschem Paßwort.

Gebührenschutz

Die Gebühren für die ATM-Verbindungen werden je nach Provider zeitabhängig berechnet. Um nicht am Ende des Monats von einer unerwünscht hohen Rechnung überrascht zu werden, können Sie vorher festlegen, wie viele Online-Minuten für den WAN-Anschluß in einem bestimmten Zeitraum (z.B. 600 Minuten in 6 Tagen) über ein *ELSA LANCOM DSL/25 Office* erlaubt sind. Je nach Netzbetreiber werden auch Gebühreninformationen übertragen, die zum Gebührenschutz verwendet werden können.

ELSA LANmonitor

Unter Windows-Betriebssystemen haben Sie mit diesem Tool die Statusinformationen der Router immer auf dem Bildschirm. Für jedes Gerät im lokalen Netz werden die wichtigsten Informationen angezeigt, z.B.:

- Name der verbundenen Gegenstelle
- Verbindungsdauer und Übertragungsraten
- Auszüge aus der Statistik des Geräts (z.B. Informationen aus der PPP-Verhandlung)

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

Statusanzeigen

LED-Anzeigen an der Frontseite Ihres Geräts ermöglichen die Überprüfung von ATM- und Ethernet-Anschlüssen und erleichtern somit die Diagnose bei möglichen Systemstörungen.

Statistiken

Mit den umfangreichen Statistiken haben Sie *ELSA LANCOM DSL/25 Office* im Griff. Hier finden Sie z.B. alle Informationen über die übertragenen Datenpakete und optimieren so die Konfiguration Ihres Geräts.

DHCP

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

Im Automatik-Modus kann der Router auch alle Adressen im Netz selbst festlegen und den Geräten im Netz zuweisen.

DNS-Server

Über den DNS-Serverfunktionsumfang des Routers können Sie Verknüpfungen zwischen IP-Adressen und Namen von Rechnern oder Netzen herstellen. Bei Anfragen nach bekannten Rechnernamen kann so direkt die richtige Route zugeordnet werden.

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

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

ELSA LANCAPI und *ELSA CAPI Faxmodem*

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

Alle Workstations, die im LAN (Local Area Network) integriert sind, erhalten über die *LANCAPI* uneingeschränkten Zugriff auf Bürokommunikations-Funktionen wie Fax und EuroFileTransfer. Ohne zusätzliche Hardware an den

DE

Arbeitsstationen, werden alle Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ATM-Adaptern. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsstationen installiert.

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

Leitungsaufbau und -verwaltung

Der Router überprüft alle Daten in einem Netzwerk daraufhin, ob sie in ein anderes Netz oder zu einem anderen Rechner übertragen werden müssen. Ist eine Übertragung notwendig, baut der Router selbständig die Verbindung auf und beendet diese nach der Übertragung. Dabei werden angefangene Gebühreneinheiten bis zum Schluß ausgenutzt, wenn die Gebühreninformationen während der Übertragung übermittelt werden.

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

NetBIOS-Proxy

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

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

Kompatibilität durch PPP

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

Fernkonfiguration über PPP

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

DE

2 Installation

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

Die folgenden Informationen wenden sich an erfahrene Anwender mit Kenntnissen der Hardware- und Netzwerkkonfiguration.

2.1 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 DSL/25 Office*
- Netzteil
- LAN-Anschlußkabel
- ATM-Anschlußkabel
- Kabel für die Konfigurationsschnittstelle
- Adapter für Konfigurationskabel
- Dokumentation
- CD mit *ELSA LANconfig* und weiterer Software und elektronischer Dokumentation

Falls etwas fehlen sollte, wenden Sie sich bitte direkt an Ihren Händler.

2.2 Systemvoraussetzungen

Die Rechner, die Sie mit Hilfe des Geräts an das Internet anschließen möchten, müssen folgende Voraussetzung erfüllen:

- beliebiges Betriebssystem, auf dem das Netzwerkprotokoll TCP/IP läuft, z.B. Windows 95, Windows 98, Windows 2000, Windows NT 4.0, OS/2, Linux oder BeOS
- Windows 95, Windows 98, Windows 2000 oder Windows NT 4.0 und ein CD-ROM-Laufwerk für die Rechner, auf denen Sie die Konfigurationsoftware *ELSA LANconfig* installieren möchten.
- Ethernet-Netzwerkkarte

DE

- Netzwerkprotokoll TCP/IP installiert und auf die Netzwerkkarte gebunden

2.3 Arbeitsplatzrechner einrichten

Router von ELSA machen die Verwaltung von Adressen in einem lokalen Netzwerk zum Kinderspiel. Einige Einstellungen sind evtl. bei den Arbeitsplatzrechnern erforderlich, um die Zusammenarbeit zwischen Routern und Arbeitsplatzrechnern zu ermöglichen.

2.3.1 Windows 95 und Windows 98

Am Beispiel von Windows 95 und Windows 98 zeigen wir hier kurz, was Sie zur einwandfreien Kommunikation der Rechner im TCP/IP-Netz mit dem Router auf den Arbeitsplatzrechnern einrichten müssen, falls es nicht schon erledigt ist.

- TCP/IP installieren

  Installieren Sie TCP/IP mit **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ Hinzufügen ▶ Protokoll**. Wählen Sie als Hersteller 'Microsoft' und als Netzwerkprotokoll 'TCP/IP'.

- IP-Adressen zuweisen lassen (DHCP verwenden)

  Wenn Sie den Router als DHCP-Server betreiben, stellen Sie die Arbeitsplatzrechner auf das automatische Beziehen der IP-Adressen ein: **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ TCP/IP ▶ Eigenschaften ▶ IP-Adresse ▶ IP-Adresse automatisch beziehen**. Löschen Sie außerdem evtl. vorhandene Einträge für DNS-Server und Gateways (auf den Registerkarten 'Gateway' und 'DNS-Konfiguration'. Der Rechner sucht dann nach dem Neustart einen DHCP-Server im Netz und läßt sich von diesem eine IP-Adresse zuweisen.

- Feste IP-Adressen einstellen (kein DHCP verwenden)

  Wenn Sie keinen DHCP-Server in Ihrem Netz verwenden möchten, stellen Sie an den Arbeitsplatzrechnern feste IP-Adressen ein: **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ TCP/IP ▶ Eigenschaften ▶ IP-Adresse ▶ IP-Adresse festlegen**.

  Vergeben Sie eindeutige IP-Adressen, z.B. aus einem reservierten Adreßbereich. Die Arbeitsplatzrechner können z.B. die Adressen '10.1.1.2' bis '10.1.1.253' bekommen, der Router die '10.1.1.1', alle mit der Netzmaske '255.255.255.0'. Ob die für den Router vorgesehene IP-Adresse frei ist, z.B. die '10.1.1.1', testen Sie in der DOS-Box mit `ping 10.1.1.1` .

Wenn Sie auf diese Anfrage keine Antwort erhalten, ist die Adresse wahrscheinlich noch frei.

- Gateway und DNS-Server eintragen (nicht nötig bei Verwendung von DHCP)

  Tragen Sie die Adresse des Routers aus dem eigenen lokalen Netz als Gateway und als Domain Name Server (DNS-Server) bei den Arbeitsplatzrechnern ein: **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ TCP/IP ▶ Eigenschaften ▶ Gateway** und **DNS-Konfiguration**. Tragen Sie bei der DNS-Konfiguration auch einen Host-Namen ein. Verwenden Sie dazu aus Konsistenzgründen den Namen des PCs, der in Idealfall mit dem Namen des Benutzers übereinstimmt.

- Überprüfung der IP-Konfiguration

  Unter Windows 95 oder Windows 98 können Sie mit **Start ▶ Ausführen ▶ winipcfg** die aktuelle IP-Konfiguration des Rechners abfragen. Hier können Sie u.a. sehen, welche IP-Adresse der DHCP-Server dem Rechner zugewiesen hat und welche Adressen für DNS-Server und Gateway übermittelt wurden.

2.3.2 Windows NT 4.0

Am Beispiel von Windows NT 4.0 zeigen wir hier kurz, was Sie zur einwandfreien Kommunikation der Rechner im TCP/IP-Netz mit dem Router auf den Arbeitsplatzrechnern einrichten müssen, falls es nicht schon erledigt ist.

- TCP/IP installieren

  Installieren Sie TCP/IP mit **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ Protokolle ▶ Hinzufügen**. Wählen Sie als Netzwerkprotokoll 'TCP/IP-Protokoll'.

- IP-Adressen zuweisen lassen (DHCP verwenden)

  Wenn Sie den Router als DHCP-Server betreiben, stellen Sie die Arbeitsplatzrechner auf das automatische Beziehen der IP-Adressen ein. Wählen Sie dazu beim Abschluß der Netzwerkprotokoll-Installation die Schaltfläche **Ja**.

DE

Windows kopiert anschließend die erforderlichen Dateien und erwartet dann einen Neustart.

- Feste IP-Adressen einstellen (kein DHCP verwenden)

  Wenn Sie keinen DHCP-Server in Ihrem Netz verwenden möchten, stellen Sie an den Arbeitsplatzrechnern feste IP-Adressen ein: **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ Protokolle ▶ Eigenschaften**. Auf dieser Registerkarte können Sie außerdem das Standard-Gateway einstellen.

Vergeben Sie eindeutige IP-Adressen, z.B. aus einem reservierten Adreßbereich. Die Arbeitsplatzrechner können z.B. die Adressen '10.1.1.2' bis '10.1.1.253' bekommen, der Router die '10.1.1.1', alle mit der Netzmaske '255.255.255.0'. Ob die für den Router vorgesehene IP-Adresse frei ist, z.B. die '10.1.1.1', testen Sie in der DOS-Box mit `ping 10.1.1.1`. Wenn Sie auf diese Anfrage keine Antwort erhalten, ist die Adresse wahrscheinlich noch frei.

- DNS-Server eintragen (nicht nötig bei Verwendung von DHCP)

  Tragen Sie auf der Registerkarte 'DNS' die Adresse des Routers aus dem eigenen lokalen Netz und als Domain Name Server (DNS-Server) bei den

Arbeitsplatzrechnern ein. Tragen Sie bei der DNS-Konfiguration auch einen Host-Namen ein. Verwenden Sie dazu aus Konsistenzgründen den Namen des PCs, der in Idealfall mit dem Namen des Benutzers übereinstimmt.

- Überprüfung der IP-Konfiguration

  Unter Windows NT 4.0 können Sie mit **Start ▶ Ausführen ▶ ipconfig** die aktuelle IP-Konfiguration des Rechners abfragen. Hier können Sie sehen, welche IP-Adresse der DHCP-Server dem Rechner zugewiesen hat und welche Adresse für das Gateway übermittelt wurden (nicht für den DNS-Server).

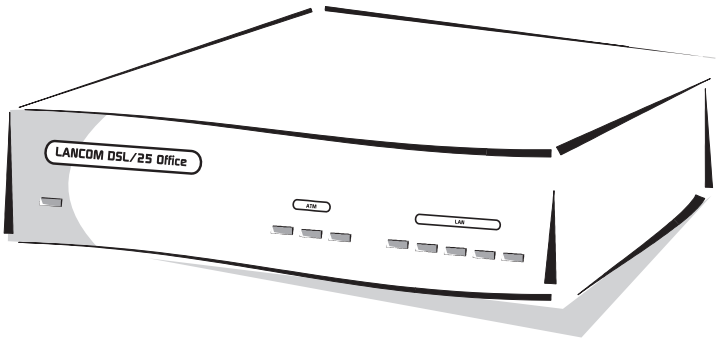
2.4 *ELSA LANCOM DSL/25 Office* stellt sich vor

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

2.4.1 Die Frontseite des Geräts

An der Vorderseite finden Sie als Anzeigeelemente einige Leuchtdioden (LEDs).

DE



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

ATM-Status

Diese LED zeigt den Zustand der ATM-Verbindung zur Vermittlungsstelle an:

aus	Kein Signal von der ATM-Vermittlungsstelle
blinkend	Signal der Vermittlungstelle liegt an, es ist aber noch keine gültige Verbindung zur Vermittlungsstelle aufgebaut
an	mindestens 1 gültige Verbindung ist aufgebaut

ATM-Rx
ATM-Tx

Diese LEDs zeigen die Datenbewegungen auf der ATM-Verbindung an:

ATM-Rx	grün	Datenpaket von der ATM-Vermittlungsstelle empfangen
ATM-Tx	gelb	Datenpaket vom Gerät an die ATM-Vermittlungsstelle gesendet

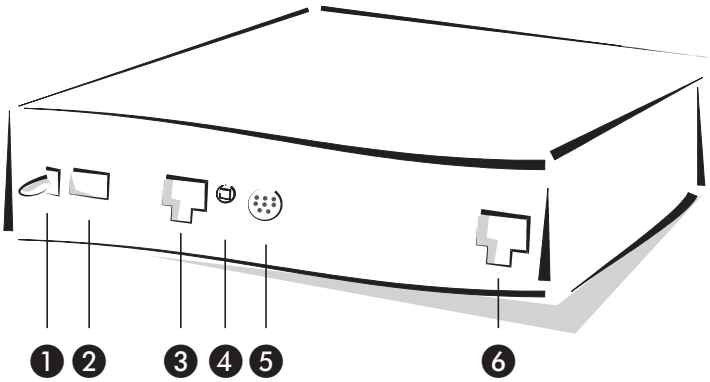
LAN-Tx, -Rx, LAN-Coll, -Link LAN-FDpx, -Fast

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

LAN-Rx/Tx	gelb	Datenpaket vom Gerät an das LAN oder vom LAN an das Gerät gesendet
LAN-Coll	rot	Sendekollision
LAN-Link	grün	Der Anschluß zum LAN ist hergestellt und bereit
LAN-FDpx	grün	Der Router sendet und empfängt Daten gleichzeitig
LAN-Fast	grün	*ELSA LANCOM DSL/25 Office* befindet sich im 100-Mbit-Betrieb

2.4.2 Die Rückseite des Geräts

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



1. Ein/Aus-Schalter
2. Anschluß für das Netzteil
3. 10/100Base-TX für 10-Mbit- oder 100-Mbit-Netze
4. Node/Hub-Umschalter
5. V.24-Konfigurationsschnittstelle
6. ATM-25.6-Anschluß

DE

2.5 So schließen Sie das Gerät an

① Verbinden Sie Ihr *ELSA LANCOM DSL/25 Office* mit dem LAN. Stecken Sie dazu das mitgelieferte Netzwerkkabel 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).

② Verbinden Sie Ihr *ELSA LANCOM DSL/25 Office* mit dem ATM-Netz. Stecken Sie dazu das mitgelieferte ATM-Anschlußkabel in den ATM-25.6-Anschluß des Geräts und in die Ethernet-Schnittstelle des NTBBA.

③ Versorgen Sie das Gerät über das Netzteil mit der benötigten Spannung und schalten Sie es ein. Nach einem kurzen Selbsttest des Geräts leuchtet die LED 'Power/Msg' permanent. Die LED 'LAN-Link' 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.

2.6 Software-Installation

Mit der Konfigurationssoftware *ELSA LANconfig* für Windows-Betriebssysteme können Sie Ihren Router einfach und komfortabel auf die gewünschte Anwendung einstellen.

Zum Betrieb von *ELSA LANconfig* benötigen Sie einen Windows-PC im LAN.

① Installieren Sie zuerst das Netzwerkprotokoll TCP/IP auf dem Rechner, von dem aus Sie Ihr Gerät einstellen möchten.

② Installieren Sie anschließend *ELSA LANconfig*. Wenn das Setup-Programm beim Einlegen der *ELSA LANCOM*-CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' auf der *ELSA LANCOM*-CD und folgen den weiteren Hinweisen der Installationsroutine.

2.7 Konfiguration

Die Konfiguration des Geräts gliedert sich in folgende Schritte:

- Grundeinstellungen
- ATM-Anschlußeinstellung

DE

- Routerkonfiguration

Für die einzelnen Teile der Konfiguration gibt es jeweils eine Info-Tabelle. Sie zeigt Ihnen an, welche Informationen Sie brauchen. Füllen Sie diese Tabelle aus, bevor Sie mit der Konfiguration beginnen.

2.7.1 Grundeinstellungen

In der Grundeinstellung geben Sie dem Gerät einen Namen und legen die IP-Adressen für den Betrieb im lokalen Netz fest. In diesem Beispiel übernimmt der DHCP-Server im Router automatisch die Verteilung der IP-Adressen im LAN.

ELSA LANconfig

Beim ersten Start von *ELSA LANconfig* wird ein neues Gerät im TCP/IP-Netz erkannt und kann sofort konfiguriert werden. Dabei startet automatisch ein Assistent, der Ihnen bei der Grundeinstellung des Geräts behilflich ist oder Ihnen die Arbeit ganz abnehmen kann.

① Starten Sie die neue Software mit **Start** ▶ **Programme** ▶ **ELSAlan** ▶ ***ELSA LANconfig***.

② Wählen Sie die Option 'Alle Einstellungen automatisch durchführen', wenn Sie **nicht** mit Netzwerken und IP-Adressen vertraut sind und eine der folgenden Annahmen zutrifft:

- Sie haben bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet, möchten das ab jetzt aber gerne tun. Welche IP-Adressen dabei

DE

verwendet werden, ist Ihnen egal. Der Router wird dann als DHCP-Server die IP-Adressen für alle Geräte im Netzwerk (LAN und WLAN) automatisch festlegen und zuweisen.

oder

○ Sie möchten überhaupt keine IP-Adressen verwenden, weil Sie z.B. ein reines Windows-Netzwerk betreiben.

*Wenn Sie nicht wissen, ob in Ihrem Netzwerk bisher IP-Adressen verwendet wurden, klicken Sie bitte zunächst auf **Start** ▶ **Ausführen**, geben in das sich öffnende Fenster das Kommando* `winipcfg` *ein und klicken **OK**. Wenn in dem folgenden Fenster im Feld 'IP-Adresse' der Wert '0.0.0.0' steht, hat der Rechner bisher noch keine IP-Adresse.*

③ Wählen Sie die Option 'Ich möchte Einstellungen selber vornehmen', wenn Sie mit Netzwerken und IP-Adressen vertraut sind und eine der folgenden Annahmen zutrifft:

○ Sie haben bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet, möchten das ab jetzt aber gerne tun. Sie möchten die IP-Adresse für den Router jedoch selbst festlegen und geben ihm eine beliebige Adresse aus einem der für private Zwecke reservierten Adreßbereiche, z.B. '10.0.0.1' mit der Netzmaske '255.255.255.0'. Damit legen Sie auch gleichzeitig den Adreßbereich fest, den der DHCP-Server anschließend für die anderen Geräte im Netz verwendet (sofern der DHCP-Server nicht ausgeschaltet wird).

○ Sie haben auch bisher schon IP-Adressen auf den Rechnern im LAN verwendet. Geben Sie dem Router eine freie Adresse aus dem bisher verwendeten Adreßbereich, und wählen Sie aus, ob der Router als DHCP-Server arbeiten soll oder nicht.

Weitere Informationen zum Aufbau von Netzwerken allgemein und zur IP-Adressierung finden Sie in der elektronischen Dokumentation auf der ELSA LANCOM-CD. Die Funktionsweise des DHCP-Servers ist weiter hinten in diesem Handbuch beschrieben.

Telnet

Starten Sie Telnet-Verbindung zur Adresse '10.0.0.254', wenn Sie bisher noch keine IP-Adressen in Ihrem Netz verwendet haben, oder zur Adresse 'x.x.x.254', wobei 'x.x.x' für den bisher im Netz verwendeten Adreßkreis steht.

Geben Sie die folgenden Befehle ein:

① Die Telnetverbindung starten Sie z.B. mit dem Befehl **Start ▶ Ausführen** und geben in das sich öffnende Fenster das Kommando `telnet 10.0.0.254` ein.

② Ändern Sie die Sprache für die Konfiguration mit dem Befehl:

```
set /Setup/config-module/language deutsch
```

③ Intranet-Adresse und Netzmaske:

```
set /Setup/TCP-IP-modul/Intranet-Adr. 10.0.0.1
set /Setup/TCP-IP-modul/Intranet-Maske
255.255.255.0
```

Mit dem Ändern der Intranet-Adresse wird die Telnet-Verbindung unterbrochen.

④ Evtl. DHCP-Funktion ausschalten:

```
set /Setup/DHCP-Modul/Zustand aus
```

Auch wenn die Einträge Ihnen an dieser Stelle ohne weitere Erklärungen noch nicht allzuviel sagen, erreichen Sie damit das gleiche Ziel wie bei der Einstellung über ELSA LANconfig!

Mit diesen Einstellungen haben Sie Ihren neuen Router im lokalen Netz bekannt gemacht. Er ist selber unter der IP-Adresse '10.0.0.1' ansprechbar. Nach einem Neustart beziehen alle Geräte im lokalen Netz ihre IP-Adresse vom DHCP-Server im Router. Dabei wird automatisch der Adreß-Pool von '10.0.0.2' bis '10.0.0.253' verwendet.

2.7.2 ATM-Anschlußeinstellung

Tragen Sie die Werte für Ihren ATM-Anschluß und die Verbindungen zu anderen Geräten ein. Einige dieser Werte haben Sie von Ihrer Telefongesellschaft erhalten.

DE

Welche Informationen brauchen Sie?

❶	Protokoll für den Signalisierungskanal	
❷	Anwahlpräfix (nur für ATM-TK-Anlagen und private Netze nötig)	
❸	Virtual Path Identifier (VPI)	
❹	Link Cell Rate (LCR) für den ATM-Anschluß (upstream)	
❺	Verkehrskontrakt für den Signalisierungskanal	
❻	Rufnummer(n) für das ATM-Interface	

Einstellung mit *ELSA LANconfig* oder Telnet

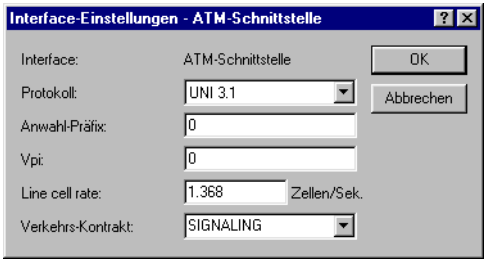
① Starten Sie *ELSA LANconfig* aus der Programmgruppe 'ELSAlan'. *ELSA LANconfig* sucht nun automatisch im lokalen Netz und an der Konfigurationsschnittstelle nach neuen Geräten.

Stellen Sie alternativ mit Telnet eine Verbindung zu ihrem neuen Gerät her. Geben Sie dazu z.B. an der Eingabeaufforderung den folgenden Befehl ein:

```
telnet 10.0.0.1
```

② Öffnen Sie den Konfigurationsdialog mit einem Klick auf den entsprechenden Eintrag in der Geräteliste.

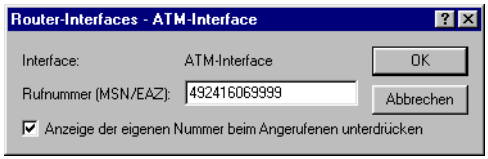
③ Wechseln Sie auf die Registerkarte 'Interfaces' und öffnen Sie die Liste der **Interface-Einstellungen**. Geben Sie für die ATM-Schnittstelle das Protokoll für den Signalisierungskanal ❶, ggf. ein Anwahl-Präfix ❷, die Nummer des virtuellen Verbindungspfades (VPI ❸), die physikalische Geschwindigkeit des Anschlusses (LCR ❹) und den Verkehrskontrakt für den Signalisierungskanal ❺ an.




```
set Setup/WAN-Modul/Interface-Liste ATM-1 UNI3.1
1368 0 0 SIGNALING
```

Der hier eingestellte Verkehrskontrakt bezieht sich ausschließlich auf den Signalisierungskanal bei Wählverbindungen. Diese Einstellung hat keine Auswirkung auf die Datenübertragungskanäle! Verkehrskontrakte können im Konfigurationsbereich 'Kommunikation' auf die Registerkarte 'Allgemein' oder per Telnet unter `/setup/wan-modul/verkehrskontrakte` *eingestellt werden.*

④ Wechseln Sie in den Konfigurationsbereich 'Kommunikation' auf die Registerkarte 'Allgemein' und öffnen Sie unter Router-Interfaces die Einstellungen für des ATM-Interface. Geben Sie die Rufnummer(n) ❻ ein, auf die der Router reagieren soll. Die erste der eingegebenen Rufnummern wird dabei für abgehende Rufe verwendet. Wählen Sie außerem aus, ob die eigene Rufnummer bei der Gegenstelle angezeigt werden soll oder nicht.



Die Rufnummern im ATM-Netz werden immer im vollständigen internationalen Format eingegeben, jedoch ohne die führenden Nullen!

```
set /Setup/WAN-Modul/Router-Interface-Liste ATM-
1 492416069999 Ein
```

Nachdem Sie die allgemeinen Einstellungen vorgenommen haben, können Sie die Verbindungen zu den gewünschten Gegenstellen einrichten.

DE

2.7.3 ATM-Festverbindung einstellen

Eine Festverbindung über das ATM-Netz wird einfach durch die Zuordnung eines Gegenstellennamens zu einem VCI konfiguriert.

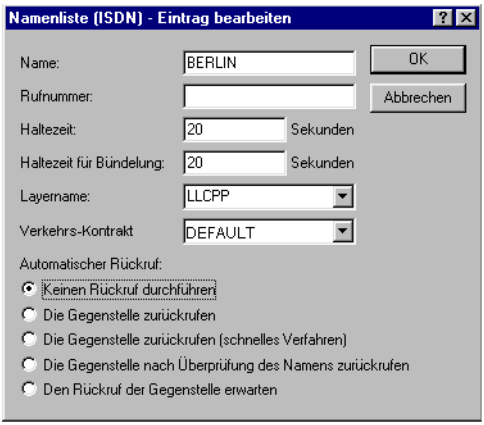
Welche Informationen brauchen Sie?

❶	Name der Gegenstelle	
❷	Layername	
❸	Verkehrskontrakt	
❹	Virtual Channel Identifier (VCI)	

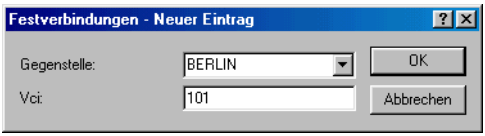
Einstellung mit *ELSA LANconfig* oder Telnet

① Öffnen Sie die Konfiguration, wechseln Sie auf die Registerkarte 'Gegenstellen' und öffnen Sie die **Namenliste**. Geben Sie den Namen der Gegenstelle ein ❶ und wählen Sie den Layernamen ❷ und den Verkehrskontrakt ❸ für diese Verbindung aus.

```
set /Setup/WAN-Modul/Namenliste BERLIN * * *
LLCPPP DEFAULT
```



② Wechseln Sie auf die Registerkarte 'Gegenstellen' und öffnen Sie die Liste der **Festverbindungen**. Wählen Sie die Gegenstelle aus, zu der Sie die Festverbindung definieren möchten ❶, und geben Sie die Nummer des virtuellen Verbindungskanals (VCI) an ❹.




```
set /Setup/WAN-Modul/Festverbindung BERLIN 101
```

Fertig! Alle Datenpakete, die durch die Einstellungen in der Routing-Tabelle der gegenstelle 'Berlin' zugeordnet werden, nutzen nun die Festverbindung über den virtuellen Verbindungskanal '101'.

2.7.4 ATM-Wählverbindung einstellen

Eine Wählverbindung über das ATM-Netz wird durch die Vereinbarung eines Verkehrskontraktes und die Zuordnung einer Rufnummer zu einem Gegenstellennamen konfiguriert.

Welche Informationen brauchen Sie?

❶	Name für den Verkehrskontrakt	
❷	Traffic Type	
❸	QoS	
❹	Sustainable Cell Rate (Tx/Rx)	
❺	Peak Cell Rate (Tx/Rx)	
❻	Maximum Burst Size (Tx/Rx)	
❼	Name der Gegenstelle	
❽	Rufnummer der Gegenstelle	
❾	Layername	

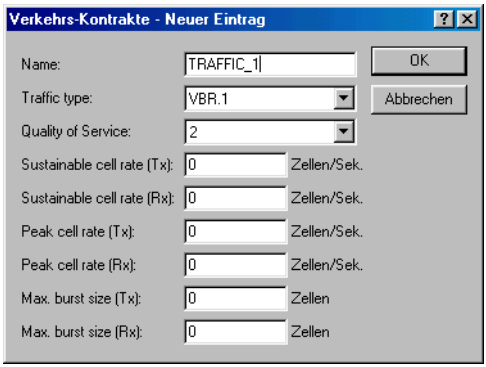
Einstellung mit *ELSA LANconfig* oder Telnet

① Öffnen Sie die Konfiguration, wechseln Sie auf die Registerkarte 'Kommunikation' und öffnen Sie die Liste der **Verkehrskontrakte**. Geben Sie einen Namen für den Verkehrkontrakt ein und wählen Sie den Typ des Verkehrskontraktes aus ❷ (variable, nicht festgelegte bzw. konstante Bitrate oder ISDN für Gegenstellen im ISDN-Netz). Stellen Sie den Wert für den Quality of Service ein ❸ und tragen Sie dann die Werte für die

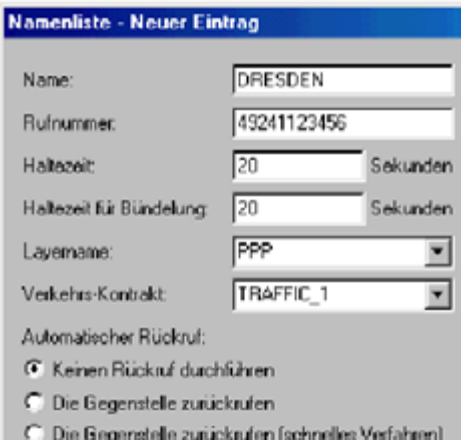
DE

mittlere ❹ und maximale Zellenrate ❺ sowie die maximale Burstlänge ❻ jeweils in Sende- und Empfangsrichtung ein.

```
set /Setup/WAN-Modul/Verkehrskontrakte Traffic_1
VBR.1 2 300 300 800 800 20 20
```



② Wechseln Sie auf die Registerkarte 'Gegenstellen' und öffnen Sie die **Namenliste**. Geben Sie den Namen der Gegenstelle ein ❼ und die Rufnummer ein ❽ wählen Sie den Layernamen ❾ und den Verkehrskontrakt ❶ für diese Verbindung aus.




```
set /Setup/WAN-Modul/Namenliste DRESDEN
49241123456 * * PPP TRAFFIC_1
```

Fertig! Alle Datenpakete, die durch die Einstellungen in der Routing-Tabelle der gegenstelle 'Dresden' zugeordnet werden, nutzen nun die Wählverbindung mit dem Verkehrskontrakt 'Traffic_1'.

DE

3 Konfigurationsmöglichkeiten

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

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

3.1 Viele Wege führen zum *ELSA LANCOM DSL/25 Office*

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

- Über die Konfigurations-Schnittstelle (Config-Schnittstelle) an der Rückseite der Router (auch Outband genannt)
- Über das angeschlossene Netzwerk, LAN oder WAN (Inband)

Was unterscheidet nun diese Möglichkeiten?

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

Zum anderen die Anforderungen an weitere Soft- oder Hardware. Die Inband-Konfiguration benötigt einen der ohnehin vorhandenen Rechner im LAN oder WAN und eine geeignete Software. Die Outband-Konfiguration braucht neben der Software auch einen der Rechner (mit serieller Schnittstelle) und das entsprechende Konfigurationskabel.

3.2 Der direkte Weg: Outband

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

DE

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

3.2.1 Voraussetzungen für die Outband-Konfiguration

Was brauchen Sie dazu?

- Einen Rechner mit Windows 95, Windows 98 oder Windows NT 4.0 und *ELSA LANconfig*

  oder

  einen Rechner mit beliebigem Betriebssystem und ein Terminalprogramm (z.B. *Telix* oder Hyperterminal).
- Das mitgelieferte Konfigurationskabel und ggf. den 9/25poligen Adapter zur Verbindung des Rechners mit dem Router (COM-Port des PC an Konfigurations-Schnittstelle des Routers).

3.2.2 Outband-Konfiguration mit *ELSA LANconfig*

Starten Sie *ELSA LANconfig* z.B. aus der Windows-Startleiste mit **Start** ▶ **Programme** ▶ **ELSAlan** ▶ ***ELSA LANconfig***. *ELSA LANconfig* sucht nun automatisch im lokalen Netz (nicht jedoch an der seriellen Schnittstelle) nach *ELSA LANCOM DSL/25 Office*-Geräten. Ein neues Gerät an der seriellen Schnittstelle finden Sie mit **Gerät** ▶ **Suchen** ▶ **An allen Schnittstellen suchen**. *ELSA LANconfig* zeigt neue Router in der Liste mit der Gerätebezeichnung an.

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

3.2.3 Outband-Konfiguration mit Terminalprogramm

Wenn das Terminalprogramm gestartet ist, drücken Sie nur einige Male die Return-Taste, um automatisch die Bitrate zu erkennen (bis zu 230 Kbit/s, 38,4 Kbit/s als Standard).

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

3.3 Der komfortable Weg: Inband

Mit der Inband-Konfiguration haben Sie von jedem Rechner aus dem WAN oder LAN aus Zugriff auf den Router. Der Zugang kann allerdings über die IP-

Zugangsliste eingeschränkt oder ganz gesperrt werden. Für diese Konfiguration verwenden Sie entweder Telnet (gehört zum Lieferumfang der meisten Betriebssysteme) oder *ELSA LANconfig* für Windows. *ELSA LANconfig* ist im Lieferumfang Ihres Geräts enthalten. Aktuelle Versionen stehen immer in unseren Online-Medien für Sie bereit.

3.3.1 Voraussetzungen

Die Konfiguration mit Telnet oder *ELSA LANconfig* läuft über TCP/IP bzw. TFTP ab. Dazu muß also auf dem verwendeten Rechner das TCP/IP installiert sein, und Ihr Router benötigt eine IP-Adresse, mit der Sie ihn ansprechen können.

Ein noch nicht konfiguriertes Gerät hört auf die IP-Adresse XXX.XXX.XXX.254. Die vielen X stehen dabei für die Netzwerkadresse in Ihrem LAN. Haben die Rechner in Ihrem Netz also z.B. Adressen wie 192.168.130.1, dann können Sie Ihr Gerät mit der Adresse 192.168.130.254 erreichen.

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

3.3.2 Alternativ: Adreßverwaltung mit dem DHCP-Server

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

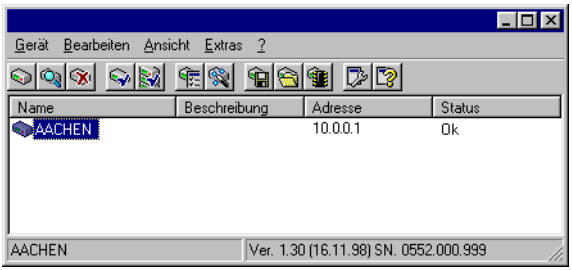
3.3.3 Konfiguration über *ELSA LANconfig*

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.

Um die Suche eines neuen Geräts manuell einzuleiten, klicken Sie nur 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.

DE

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

3.3.4 Konfiguration über Telnet

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

```
telnet 10.1.80.125
```

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

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

3.4 Der Fernzugang: Konfiguration über DFÜ-Netzwerk

Besonders einfach wird die Einstellung von Routern an entfernten Standorten mit der Fernkonfiguration über das DFÜ-Netzwerk. Das Gerät ist nach dem Einschalten und der Verbindung mit dem 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.

3.4.1 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 ATM-Karte oder ein *ELSA LANCOM DSL/25 Office* mit *ELSA LANCAPI*

3.4.2 So bereiten Sie die Fernkonfiguration vor

① Versorgen Sie den Router mit der nötigen Spannung.

② Verbinden Sie das Gerät mit einem WAN-Anschluß.

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

① Wählen Sie im *ELSA LANconfig* **Gerät** ▶ **Neu**, aktivieren Sie die 'DFÜ-Verbindung' als Anschlußtyp und geben Sie die Rufnummer des WAN-Anschlusses ein, an dem der *ELSA LANCOM DSL/25 Office* angeschlos-

sen ist. Stellen Sie dazu ggf. die Zeit ein, nach der eine Verbindung ohne Datentransfer automatisch getrennt werden soll.

② *ELSA LANconfig* legt nun automatisch einen neuen Eintrag im DFÜ-Netzwerk an. Wählen Sie ein PPP-fähiges Gerät (z.B. den NDIS-WAN-Treiber aus dem Lieferumfang der *LANCAPI*) für die Verbindung aus, und bestätigen Sie mit **OK**.

③ Anschließend zeigt *ELSA LANconfig* in der Geräteliste ein neues Gerät mit dem Namen 'Unbekannt' und der Rufnummer über DFÜ als Adresse an.

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

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

3.4.4 Die erste Fernverbindung mit PPP-Client und Telnet

① Stellen Sie mit Ihrem PPP-Client eine Verbindung zum *ELSA LANCOM DSL/25 Office* her, verwenden Sie dabei folgende Angaben:

- Benutzername 'ADMIN'
- Paßwort wie beim *ELSA LANCOM DSL/25 Office* eingestellt, im Auslieferungszustand kein Paßwort
- eine IP-Adresse für die Verbindung, nur wenn erforderlich

② Starten Sie eine Telnet-Verbindung zum *ELSA LANCOM DSL/25 Office*. 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 DSL/25 Office* 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 DSL/25 Office* 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 DSL/25 Office* über die Fernverbindung nun genauso einstellen wie alle anderen Geräte.

3.4.5 Fernkonfiguration einschränken

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

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

① Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Security'.

② Wählen Sie im Feld 'Konfigurationszugriff' aus, ob die Einstellung aus entfernten Netzen vollständig, nur zum Lesen oder nicht erlaubt ist.

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

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

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

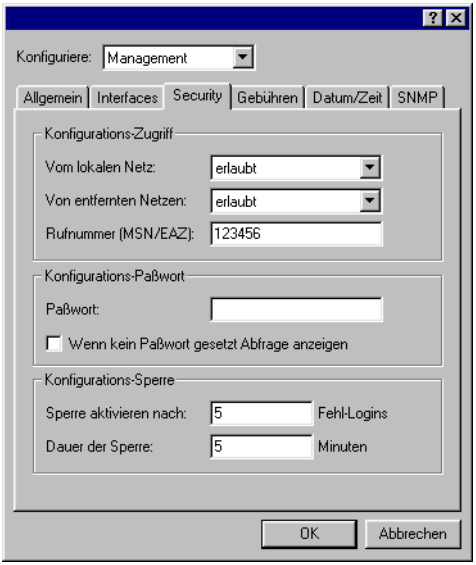
③ Geben Sie als Rufnummer im Bereich 'Konfigurationszugriff' eine Rufnummer Ihres Anschlusses ein, die nicht für andere Zwecke verwendet wird.

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.

DE



Geben Sie alternativ den folgenden Befehl ein:

```
passwd
```

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

3.5 Neue Firmware mit 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!

3.5.1 So funktioniert FirmSafe

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

Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firm-

ware 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 bestimmten, 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.

3.5.2 So spielen Sie eine neue Software ein

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

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

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

DE

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**.

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

Über TFTP kann eine neue Firmware mit dem Befehl **writeflash** eingespielt werden. Um eine neue Firmware in ein Gerät mit der IP-Adresse 194.162.200.17 zu übertragen, geben Sie z.B. unter Windows NT folgenden Befehl ein:

tftp -i 194.162.200.17 put lcdsl25u.160 writeflash

*Durch diesen Befehl wird die entsprechende Datei mit dem Kommando **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 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 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.

3.6 Was ist los auf der Leitung?

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

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

3.6.1 *ELSA LANmonitor*

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

DE

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

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

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

Verbindung mit *ELSA LANmonitor* kontrollieren

① Starten Sie *ELSA LANmonitor* mit **Start** ▶ **Programm** ▶ **ELSAlan** ▶ **LANmonitor**. Legen Sie ein neues Gerät an mit **Gerät** ▶ **Neu** und geben Sie im folgenden Fenster die IP-Adresse für den Router an, den Sie überwachen wollen. Falls die Konfiguration des Gerätes mit einem Paßwort gesichert ist, geben Sie dieses gleich mit ein.

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

② *ELSA LANmonitor* legt automatisch einen neuen Eintrag in der Geräteliste an und zeigt zunächst den Zustand der Kanäle. Sobald die Verbindung hergestellt ist, zeigt 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.

3.6.2 Trace-Ausgaben

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

können sowohl in der Konfiguration eigener 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 Interpretation der Anzeigen nicht, sollte aber bei genaueren Analysen berücksichtigt werden.

So starten Sie einen Trace

Der Trace-Aufruf folgt dieser Syntax:

```
trace [Schlüssel] [Parameter]
```

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

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

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
Status	Status-Meldungen der Verbindungen
Error	Fehler-Meldungen der Verbindungen
PPP	Verhandlung des PPP-Protokolls
IP-Router	IP-Routing
IP-RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
IP-Masquerading	Vorgänge im Masquerading-Modul
DHCP	Dynamic Host Configuration Protocol
ATM	Zeigt fehlerhafte Zellen und Zellen, die keiner logischen verbindung zugeordnet werden können.

DE

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
OAM-cells	Zeigt OAM-Zellen an.
AAL5-frames	Zeigt den Anfang und den trailer eines AAL5-Pakets an.
SSCOP	ATM-Sicherungsprotokoll
SAAL	Zeigt AAL5-Pakete der Signalisierungsschicht an.

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
Time	zeigt vor der eigentlichen Trace-Ausgabe auch die Systemzeit an
Source	zeigt vor der eigentlichen Trace-Ausgabe auch das Protokoll an, das die Ausgabe veranlaßt hat

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

Beispiele:

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

3.6.3 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.

Detaillierte Informationen über die Konfiguration von ELSA-Geräten mit SNMP finden Sie in der elektronischen Dokumentation auf der CD.

DE

4 Funktionen und Betriebsarten

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

- Sicherheit für die Konfiguration
- Sicherheit für das LAN
- ATM-Verbindungen
- PPP-Unterstützung
- IPX-Routing
- IP-Routing
- Automatische Adreßverwaltung mit DHCP
- DNS-Server
- NetBIOS-Proxy

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

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

4.1 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 DSL/25 Office* die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

4.1.1 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 /

DE

`Setup/Config-Modul/Passw.Zwang` ein. Das Paßwort selbst wird in diesem Fall mit dem Befehl `passwd` gesetzt.

4.1.2 Die Login-Sperre

Die Konfiguration im *ELSA LANCOM DSL/25 Office* 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 dieser Grenze erreicht, wird der Zugang für eine bestimmte Zeit gesperrt.

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

Zur Konfiguration der Login-Sperre stehen 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`)

4.1.3 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 Telnet oder TFTP (*ELSA LANconfig*) bezeichnet.

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

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

4.2 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 DSL/25 Office* bietet verschiedene Möglichkeiten, den Zugriff von außen einzuschränken:

- Zugangsschutz mit Name und Paßwort
- Filterung von Datenpaketen
- IP-Masquerading (auch NAT oder PAT genannt)

4.2.1 Die Kontrolle

Welcher „Identifier" 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

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

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

DE

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

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

Die Sicherungsverfahren PAP, CHAP oder MS-CHAP wenden Sie natürlich nicht an, wenn Sie selber mit dem ELSA LANCOM DSL/25 Office z.B. einen Internet-Service-Provider anwählen. Sie werden den ISP wahrscheinlich nicht dazu bewegen können, eine Anfrage an ihn nach einem Paßwort zu beantworten ...

Und woher kommen Name und Paßwort des Anrufers?

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

4.2.2 Überprüfung der Nummer

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 DSL/25 Office* über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekannten Rufnummern abgelehnt.

Der Rückruf

Eine besondere Variante des Zugriffschutzes 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 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 Router an, wenn der Anrufer nicht über CLI identifiziert wird. Ist dagegen eine Identifizierung über die Rufnummer des Anrufers erlaubt und möglich, kommt der Anrufer sogar ganz ohne Kosten weg.

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

4.2.3 Das Versteck – IP-Masquerading (NAT, PAT)

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

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

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

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

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

DE

4.3 Gebührenmanagement

Die Eigenschaft des Routers, Verbindungen selbständig zu allen gewünschten Gegenstellen aufzubauen und sie mit dem Ende der Übertragung wieder zu beenden, ermöglicht dem Benutzer sehr komfortablen Zugriff 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 Online-Minuten können für eine bestimmte Periode eingeschränkt werden.

4.3.1 Begrenzung der Online-Minuten

Je nach Provider werden die Kosten für den ATM-Anschluß zeitabhängig berechnet.

Um die Kosten begrenzen zu können, kann die maximale Verbindungsdauer mit Hilfe der Zeit gesteuert werden. Dazu wird ein Zeit-Limit in einer Periode vereinbart. Im Default-Zustand dürfen die ATM-Verbindungen z.B. für maximal 210 Minuten in sieben Tagen genutzt werden.

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

4.3.2 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

- Minuten-Budget

  Maximale Online-Minuten in einer Überwachungsperiode

DE

- Rest-Budget
  Verfügbare Online-Minuten in der gegenwärtigen Periode
- Router-Einheiten
  Von den Routermodulen verbrauchte 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.

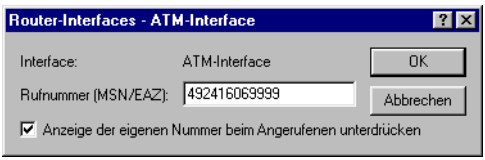
4.4 ATM-Verbindungen

Ein *ELSA LANCOM DSL/25 Office* verbindet Netzwerke über ATM-Festverbindungen (PVCs) oder ATM-Wählverbindungen (SVCs). Um die Datenübertragung über die ATM-Strecke zu ermöglichen, müssen die entsprechenden Parameter im Router eingetragen werden.

4.4.1 Anschlußeinstellungen

Einige der Parameter für die Datenübertragung im ATM-Netz sind für alle Verbindungen gleich und werden daher nur einmal für den Anschluß eingestellt.

- Im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Allgemein' wird die Rufnummer (ggf. mehrere) eingetragen, auf die der Router reagieren soll. Die erste der eingegebenen Rufnummern wird dabei für abgehende Rufe verwendet. Hier stellen Sie außerdem ein, ob die eigene Rufnummer bei der Gegenstelle angezeigt werden soll oder nicht.



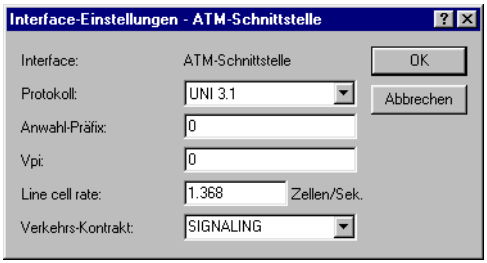
Die Rufnummern im ATM-Netz werden immer im vollständigen internationalen Format eingegeben, jedoch ohne die führenden Nullen!

DE

Subadressen können durch einen Punkt getrennt an die eigentlich Rufnummern angehängt werden.

Bei der Konfiguration über Telnet geben Sie diese Werte im menü `/Setup/WAN-Modul/Router-Interface-Liste` ein.

- Im Konfigurationsbereich 'Management' auf der Registerkarte 'Interfaces' finden Sie die **Interface-Einstellungen**. Hier können Sie für die ATM-Schnittstelle folgende Werte eintragen:
  - das Protokoll für den Signalisierungskanal
  - ggf. ein Anwahl-Präfix
  - die Nummer des virtuellen Verbindungspfades (VPI)
  - die physikalische Geschwindigkeit des Anschlusses (Line Cell Rate LCR)
  - den Verkehrskontrakt für den Signalisierungskanal



Bei der Konfiguration über Telnet geben Sie diese Werte im menü `/Setup/WAN-Modul/Interface-Liste` ein.

Der hier eingestellte Verkehrskontrakt bezieht sich ausschließlich auf den Signalisierungskanal bei Wählverbindungen. Diese Einstellung hat keine Auswirkung auf die Datenübertragungskanäle! Verkehrskontrakte können im Konfigurationsbereich 'Kommunikation' auf die Registerkarte 'Allgemein' oder per Telnet unter `/setup/wan-modul/verkehrskontrakte` *eingestellt werden.*

Die Werte für Ihren ATM-Anschluß haben Sie von Ihrem Provider erhalten.

4.4.2 Layer-Liste

Mit einem Layer definieren Sie eine Sammlung von Protokoll-Einstellungen, die für die Verbindung zu bestimmten Gegenstellen verwendet werden soll.

Die Liste der Kommunikation-Layer finden Sie im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Allgemein'.

Neben dem Namen, der den Layer bezeichnet, können Sie folgende Werte eingeben:

- Encapsulation, entweder LLC/SNAP oder Transparent
- Layer-3-Protokoll, entweder PPP oder Transparent
- Layer-2-Protokoll, entweder SSCOP oder Transparent
- Kompression der Daten als Option

Das Layer-1-Protokoll ist fest auf den Wert 'AAL-5' voreingestellt.

Bei der Konfiguration über Telnet geben Sie diese Werte im menü `/Setup/WAN-Modul/Layer-Liste` ein.

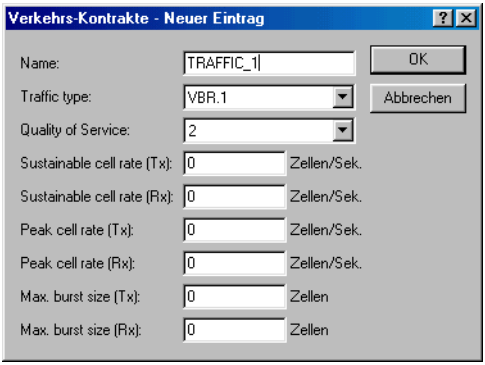
4.4.3 Verkehrskontrakte

In einem Verkehrskontrakt sind auf der Registerkarte 'Kommunikation' unter einem frei wählbaren Namen die Leistungsmerkmale einer ATM-Verbindung hinterlegt. Zu diesen Leistungsmerkmalen gehören:

- Typ des Verkehrskontraktes
  - variable Bitrate
  - nicht festgelegte Bitrate
  - konstante Bitrate
  - ISDN für Gegenstellen im ISDN-Netz
- Der Quality of Service (0 bis 5) ist die gewünschte QoS-Klasse. Der Eintrag 'Default' entspricht dem Typ, der normalerweise für den eingestellten Typ des Verkehrskontraktes verwendet wird.
- Der Grundanteil der übertragenen Bandbreite (Sustainable Cell Rate, SCR) in Sende- und Empfangsrichtung muß nur für VBR-Verkehrskontrakttypen eingetragen werden.
- Die maximal in einer Spitze übertragene Bandbreite (Peak Cell Rate, PCR) in Sende- und Empfangsrichtung muß für alle Verkehrskontrakttypen außer 'ISDN-HDLC-64kBit/s' eingetragen werden.
- Die Länge einer SCR-Überschreitung in ATM-Zellen (Maximum Burst Size, MBS) in Sende- und Empfangsrichtung muß nur für VBR-Verkehrskontrakttypen eingetragen werden.

Wird in den Rx-Feldern von SCR, PCR oder MBS der Wert '0' eingetragen, wird der entsprechende Tx-Wert verwendet.

DE

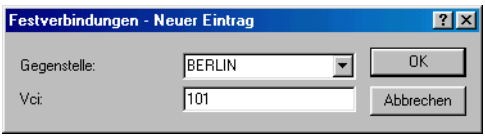


Die Werte für die Verkehrskontrakte haben Sie von Ihrem Provider erhalten.

Bei der Konfiguration über Telnet geben Sie diese Werte im menü `/Setup/WAN-Modul/Verkehrskontrakte` ein.

4.4.4 Liste der Festverbindungen

Mit dem Eintrag in der Liste der Festverbindungen auf der Registerkarte 'Gegenstellen' stellen Sie eine Verbindung her zwischen einer bestimtmen Gegenstelle und dem virtuellen Übertragungskanal im ATM-Netz.



Alle weiteren Parameter für die Festverbindungen werden über den Gegenstellennamen aus den entsprechenden Tabellen übernommen.

Bei der Konfiguration über Telnet geben Sie diese Werte im menü `/Setup/WAN-Modul/Festverbindung` ein.

4.4.5 Namenliste

Mit dem Eintrag in der Namenliste stellen Sie eine Verbindung her zwischen dem virtuellen Übertragungsweg im ATM-Netz und dem bei dieser Übertragung zu verwendenden Protokoll-Layer und Verkehrskontrakt. Dieser Zuordnung geben Sie einen Namen, den Sie in der Routingtabelle als Ziel für bestimmte Datenpakete aus Ihrem lokalen Netz angeben können. Die

Namenliste finden Sie im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Gegenstellen'.

Die Namenliste enthält Einträge mit folgenden Parametern:

- Name

  Geben Sie hier einen aussagekräftigen Namen für die Verbindung an. Diesen Namen könne Sie anschließend in der Routingtabelle als 'Router' auswählen.

- Rufnummer

  Die Rufnummern im ATM-Netz werden immer im vollständigen internationalen Format eingegeben, jedoch ohne die führenden Nullen!

  Bei Festverbindungen entfällt die Angabe der Rufnummer.

- Layername

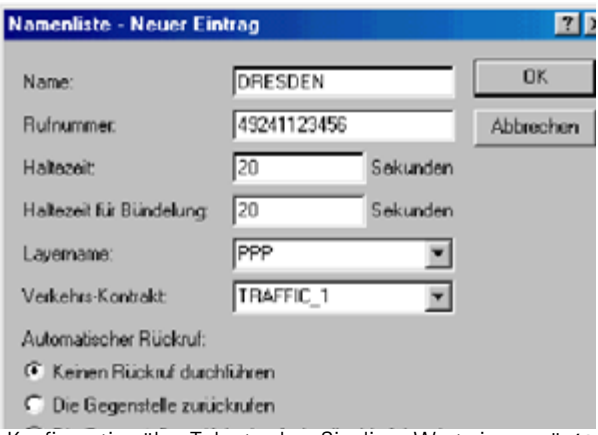
  Wählen Sie den Kommunikationslayer aus, die für diese Verbindung verwendet werden sollen.

- Verkehrs-Kontrakt

  Wählen Sie den Verkehrs-Kontrakt aus, die für diese Verbindung verwendet werden sollen.

- Automatischer Rückruf

  Hier stellen Sie für Wählverbindungen ein, ob und nach welchem Verfahren die anrufende Gegenstelle zurückgerufen werden soll.



Bei der Konfiguration über Telnet geben Sie diese Werte im menü `/Setup/WAN-Modul/Namenliste` ein.

DE

4.5 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.

4.5.1 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
- 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)

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
- Internet-Access (mit der Übermittlung von Adressen)

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.

- Network-Phase

  Im *ELSA LANCOM DSL/25 Office* 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 DSL/25 Office*

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

DE

```
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.

4.5.2 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 sie sich bei Ihrem Router anmeldet
Username	Name, mit dem sich Ihr Router bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Gerätename 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 zeigen an, daß ein Eintrag vorhanden ist.

In dieser Spalte der PPP-Liste ...	... tragen Sie folgende Werte ein:
Zeit	Zeit zwischen zwei Überprüfungen der Verbindung mit LCP. Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z.B. 2 für 20 Sek.). Gleichzeitig die Zeit zwischen zwei Überprüfungen der Verbindung nach CHAP. Diese Zeit geben Sie in Minuten ein. Für Gegenstellen mit Windows 95, Windows 98 oder Windows NT muß die Zeit auf '0' gesetzt werden!
Wdh	Anzahl der Wiederholungen für den Überprüfungsversuch. Mit mehreren Wiederholungen schalten Sie den Einfluß kurzfristiger Leitungsstörungen aus. Erst wenn alle Versuche erfolglos bleiben, wird die Verbindung abgebaut. Der zeitliche Abstand zwischen zwei Wiederholungen beträgt 1/10 der Zeit zwischen zwei Überprüfungen. Gleichzeitig die Anzahl der „Configure Requests", die der Router maximal aussendet, bevor es von einer Leitungsstörung ausgeht und selber die Verbindung abbaut.
Conf, Fail, Term	Mit diesen Parametern wird die Arbeitsweise des PPPs beeinflußt. Die Parameter sind in der RFC 1661 definiert und werden hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in dieser RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im allgemeinen sind die Default-Einstellungen ausreichend. Diese Parameter können nur über SNMP oder TFTP (mit *ELSA LANconfig*) verändert werden!

4.5.3 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.

DE

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.

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.

4.6 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.

4.6.1 IPX-Adressierung

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

4.6.2 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 verschiede-

nen 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.

4.6.3 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 ≠ WAN-Adresse 1 = WAN-Adresse 2 ≠ LAN-Adresse 2 ≠ 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'.

4.6.4 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.

4.6.5 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.

4.6.6 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, dritten und 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.

4.6.7 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 bekanntgeben. Er sendet diese Routen also nur an die Router, die die Route nicht propagiert haben. Dieses Verfahren nennt man Split Horizon.

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

4.6.8 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 ein Zahl zwischen 0 und 10.
- Der zweite Versuch wird um 10 + x Sekunden nach dem Scheitern des ersten Versuchs gestartet. x steht jetzt für eine Zahl zwischen 0 und 20 Sekunden.

- Der obere Wert für x wird nun bei jedem neuen Versuch verdoppelt. Nach dem 16. erfolglosen Versuch gibt der Router schließlich auf. Durch das ständige Anwachsen der Wartezeit ist nach 16 Versuchen maximal ein Tag vergangen.

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

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

4.6.9 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

DE

häufig für unerwünschte Verbindungen sorgen, sind als Voreinstellung schon in der Socket-Filtertabelle eingetragen.

- RIP- und SAP-Informationen

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

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

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

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

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

von einer Minute verschickt. Mit der Zeiteinstellung kann dieser Abstand auf bis zu 60 Minuten ausgedehnt werden.

- ○ Die gebührenschonendste Behandlung der RIP- und SAP-Pakete überträgt die Informationen einmalig nur dann, wenn eine Verbindung aufgebaut ist.

- IPX- und SPX-Watchdogs:

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

  - ○ IPX-Watchdogs bleiben völlig unbeantwortet. Nach der beim Server eingestellten Zeit werden die Rechner abgemeldet.
  - ○ IPX- und SPX-Watchdogs können lokal 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.

4.7 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.

4.7.1 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".

DE

Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing". Dabei tauschen die Router selbständig untereinander Informationen über die Routen aus und erneuern diese fortlaufend. Die statische Routing-Tabelle kann bis zu 64 Einträge aufnehmen, die dynamische Tabelle 128. Bei aktiviertem IP-RIP beachtet der IP-Router beide Tabellen.

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

Die Routingtabelle finden Sie 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 angeschlossen sind. Diese „Proxy-Hosts" werden gar nicht propagiert.

- Maskierung

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

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

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

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 selbständig:

Zuerst nach den Netzmasken, davon die größte nach oben. Dann nach den IP-Adressen, davon die kleinsten nach oben. Dadurch landet der 'ZENTRALE'-Eintrag ganz am Ende der Liste. Mit diesem Eintrag ganz oben in der Liste würde der Router alle (!) Datenpakete, die nicht ins eigene Netz gehören, ins Netz der Zentrale senden.

4.7.2 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).

Diese Filtertabellen finden Sie in *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Filter' bzw. im Menü `/Setup/IP-Router.`

DE

4.7.3 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.

4.7.4 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.

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

4.7.5 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.

DE

- 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:

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

DE

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

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

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

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 Infomation 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.

4.7.6 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 **Inter**net-Adresse und eine **Intra**net-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.

DE

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 können mit IP-Masquerading übertragen werden?

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

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

Wenn nun ein Rechner aus dem Intranet eine Homepage aufrufen möchte, sendet er zunächst einen DNS-Request aus: „Welche IP-Adresse gehört zu www.domain.com?"

Wenn der Router bei den Arbeitsplatzrechnern als DNS-Server eingetragen ist, wird diese Anfrage folgendermaßen behandelt:

- Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist (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

DE

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.

4.7.8 Policy Based Routing

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

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

4.8 Automatische Adreßverwaltung mit DHCP

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

Zusätzlich brauchen sie noch die Adressen von DNS- und NBNS-Servern sowie eines Standard-Gateways, über das 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.

4.8.1 Der DHCP-Server

ELSA LANCOM DSL/25 Office 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 Adreß-Zuweisungen im lokalen Netz selbst.

4.8.2 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'.

4.8.3 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 akti-

viertem 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-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 DCHP-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 Adreß-Zuweisung.

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

- neu

  Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.

- unbek.

  Bei der Überprüfung der Eindeutigkeit wurde festgestellt, daß die Adresse bereits an einen anderen Rechner vergeben wurde. Der DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.

DE

- 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.

4.8.4 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 Netzwerkkabel 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.

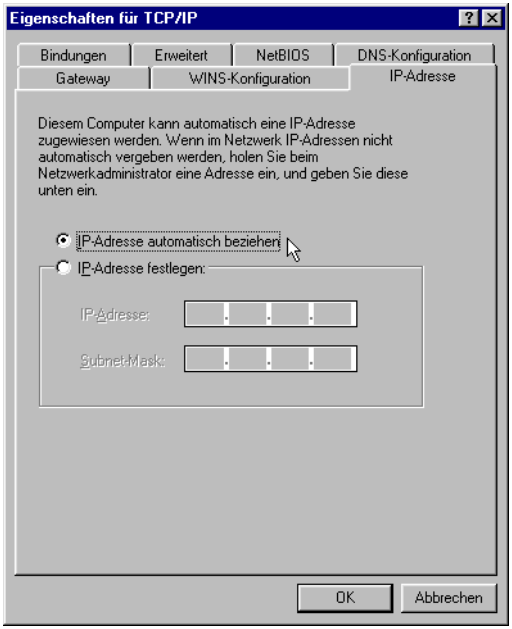
② Schalten Sie das Gerät ein. Es findet dann zunächst keinen anderen DHCP-Server im Netz und aktiviert seine eigenen DHCP-Funktionen.

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 'ELSAlan'. Beim Start bemerkt *ELSA LANconfig*, daß sich ein unkonfigurierter Router im Netz befindet, und startet den Assistenten für die Grundeinstellungen.

○ Wenn Sie bisher noch keine IP-Adressen in Ihrem Netz verwendet haben, wählen Sie in diesem Assistenten die Option 'Alle Einstellungen automatisch vornehmen', und betätigen Sie im nächsten Fenster

die Schaltfläche **Fertigstellen**.
Der Assistent weist dem Router nun die IP-Adresse '10.0.0.1' mit der Netzmaske '255.255.255.0' zu und schaltet den DHCP-Server ein. Aus der IP-Adresse ermittelt das Gerät dann den gültigen Adreß-Pool für die DHCP-Zuweisung.

- Wenn Sie auch vor der Umstellung auf DHCP-Betrieb IP-Adressen in Ihrem Netz verwendet haben, wählen Sie in diesem Assistenten die Option 'Ich möchte die Einstellungen selber vornehmen'. Geben Sie im nächsten Fenster eine freie IP-Adresse aus dem bisher verwendeten Adreßbereich ein, und schalten Sie den DHCP-Server ein.
  Der Assistent weist dem 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. ein 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`).

4.9 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 zuordnen zu können.

4.9.1 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 Dien-

stes, 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 DSL/25 Office* anzusiedeln:

- Ein *ELSA LANCOM DSL/25 Office* kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbständig verteilen. Der DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-Server hätte bei der 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 DSL/25 Office* 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 DSL/25 Office* kann gleichzeitig als sehr komfortabler Filtermechnismus 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.

4.9.2 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.

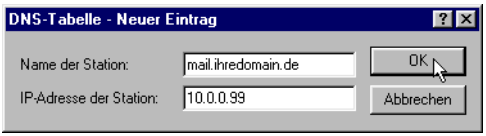
```
set setup/dns-modul/dhcp-verwenden ja
set setup/dns-modul/NetBIOS-verw. ja
```

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:

DE




```
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.gesperrte-domain.de 0.0.0.0 0.0.0.0
```

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

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

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

Durch die geeignete Wahl von IP-Adressen und Netzmasken können bei dei 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.

4.10 NetBIOS-Proxy

Mit der Funktion als NetBIOS-Proxy kann ein *ELSA LANCOM DSL/25 Office* 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.

4.10.1 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-3.11-, -9x- und -NT-Rechner einfach vernetzen lassen, und in dem die Ressourcen der jeweiligen Rechner (Laufwerke oder Drucker) für alle anderen freigegeben werden können.

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

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

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

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

Ein *ELSA LANCOM DSL/25 Office* 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.

4.10.2 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 Verbindungaufbau zu vermeiden, kann ein *ELSA LANCOM DSL/25 Office* 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 entprechenden 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.

DE

4.10.3 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 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-Protokol) 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 DSL/25 Office auf IP aufsetzen!

  Das Routing von NetBIOS-Paketen im *ELSA LANCOM DSL/25 Office* basiert aufgrund der besseren Filtermechnismen auf TCP/IP. Dieses Protokoll muß also auf allen Rechnern, die gekoppelt werden sollen, installiert sein.

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

- Client

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

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

- Dienst

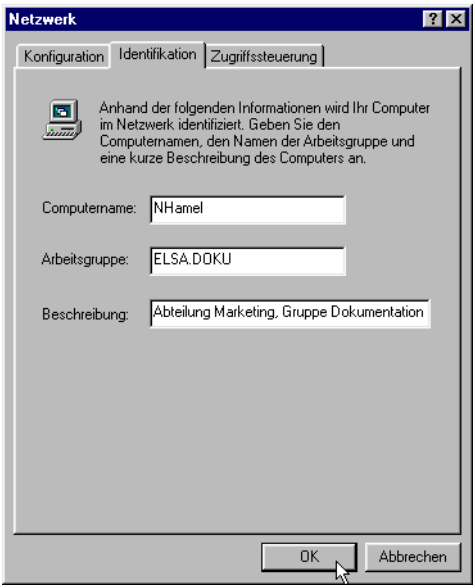
  Die Datei- und Druckerfreigabe ermöglicht das Freigeben von Laufwerken oder Druckern für andere Benutzer im Windows-Netz.

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

Einstellungen im Windows-Netzwerk

- Namen und Gruppenbezeichnung

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

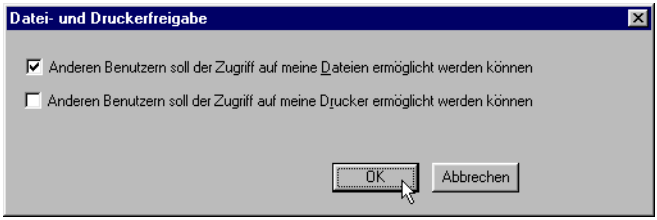


  Der Name des Rechners muß eindeutig sein. Das gilt für alle Windows-Netze und alle in diesen Netzen vorhandenen Gruppen, die Sie über NetBIOS verbinden wollen. Auch in verschiedenen Gruppen darf ein Name also nicht mehrfach auftauchen.

- Datei- und Druckerfreigabe

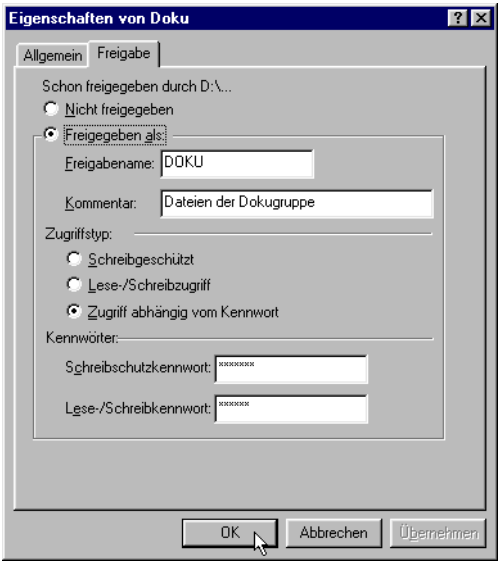
  Prüfen Sie nach der Installation, ob die Datei- und Druckerfreigabe aktiviert ist. Klikken Sie dazu **Start** ▶ **Einstellungen** ▶ **Systemsteuerung** ▶ **Netzwerk** ▶ **Datei- und Druckerfreigabe**. Wählen Sie aus, ob die

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, 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.

DE

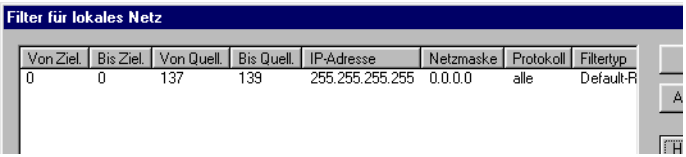
Ob die Einstellungen im Windows-Netzwerk korrekt erfolgt sind, können Sie leicht prüfen: Der eigene Rechner muß in der Netzwerkumgebung mit seinem Namen angezeigt werden.

4.10.4 So verbinden Sie zwei Windows-Netze

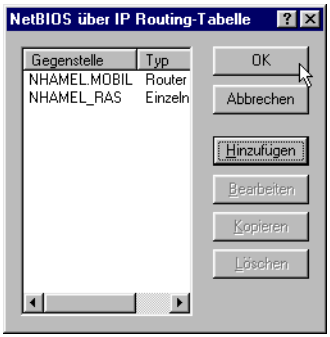
Nachdem alle Vorbereitungen abgeschlossen sind, können Sie nun zwei Windows-Netze verbinden. Die Einstellungen für Arbeitsgruppennetze und Domänen-Netze (Windows NT) sind dabei ähnlich. Die folgenden Schritte sind für beide Seiten der Verbindung auszuführen.

① Stellen Sie die beiden Netze für eine LAN-LAN-Kopplung über TCP/IP ein, wie im Workshop beschrieben. Verwenden Sie dazu nach Möglichkeit den komfortablen Assistenten von *ELSA LANconfig*.

② Prüfen Sie die Einstellung der IP-Filter. Dieser Filter muß alle NetBIOS-Pakete erfassen, die über die DEFAULT-Route geschickt werden sollen, damit NetBIOS-Pakete nicht zum Verbindungsaufbau über die DEFAULT-Route führen. Im Auslieferungszustand der Geräte ist dieser Filter so voreingestellt:



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



Bei der Konfiguration über Telnet geben Sie alternativ ein:

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

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

Der Parameter 'NT-Domain' kann bei Windows-95- oder Windows-98-Netzen i.d.R. frei gelassen werden. Beim Zugriff auf Windows-NT-Maschinen muß die entsprechende Domain 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.

4.10.5 So wählt sich ein Remote-Access-Rechner ein

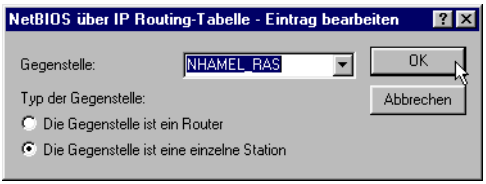
Der Zugriff von einzelnen, entfernten Rechner über Remote-Access auf ein Windows-Netz ist ebenfalls schnell erledigt.

DE

① *ELSA LANCOM DSL/25 Office* und Remote-Access-Rechner werden, wie im Workshop beschrieben, auf den Netz-Zugriff vorbereitet. Auch in diesem Fall sind die IP-Filter im *ELSA LANCOM DSL/25 Office* zu prüfen (siehe 'So verbinden Sie zwei Windows-Netze').

② Wenn die Zuweisung der IP-Adresse für die remote Gegenstelle aus dem IP-Pool realisiert wird, muß für diese Gegenstelle zusätzlich eine Route in der IP-Routing-Tabelle angelegt werden.

③ Erstellen Sie auch für die remoten Gegenstellen einen Eintrag in der NetBIOS-IP-Routing-Tabelle.




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

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

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

4.10.6 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 DSL/25 Office* nun eine Liste mit diesen Rechnernamen verfügbar. Über Telnet kann mit

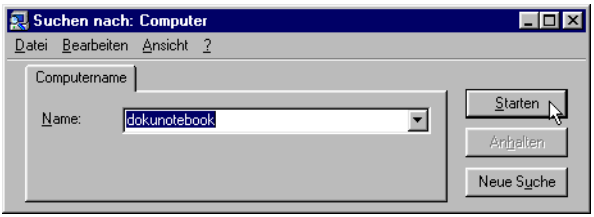
```
dir /Setup/NetBIOS-Modul/host-liste
```

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:

DE

- Auf der Seite des Einwahl-Knotens ist keine Host-Liste vorhanden, aus der die verfügbaren Rechner im Windows-Netz auf der Gegenseite abgelesen werden könnten. Der RAS-Benutzer muß also die Namen der Rechner kennen, auf die er zugreifen darf und will.
- Die Verbindung wird nicht automatisch aufgebaut. Der RAS-Benutzer muß also erst ein Verbindung über das DFÜ-Netzwerk zum *ELSA LANCOM DSL/25 Office* herstellen.

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

4.11 *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 DSL/25 Office* ermöglicht.

4.11.1 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**.

4.11.2 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.

DE

4.12 Bürokommunikation und *ELSA LANCAPI*

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

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

4.12.1 ELSA LANCAPI

Welche Vorteile bietet die *LANCAPI*?

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

Installation des *LANCAPI*-Clients

Die *LANCAPI* besteht aus zwei Komponenten, einem Server (im *ELSA LANCOM DSL/25 Office*) und einem Client (auf den PCs). Der *LANCAPI*-Client wird auf den Rechnern im lokalen Netz installiert, die die Funktionen der *LANCAPI* nutzen möchten.

① Legen sie die *ELSA LANCOM*-CD in Ihr CD-ROM-Laufwerk ein. Wenn das Setup-Programm beim Einlegen der CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' auf der *ELSA LANCOM*-CD.

② Wählen Sie den Eintrag 'LANCOM Software installieren'.

③ Markieren Sie die Option 'ELSA LANCAPI'. Klicken Sie auf **Weiter**, und folgen Sie den Hinweisen der Installationsroutine.

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

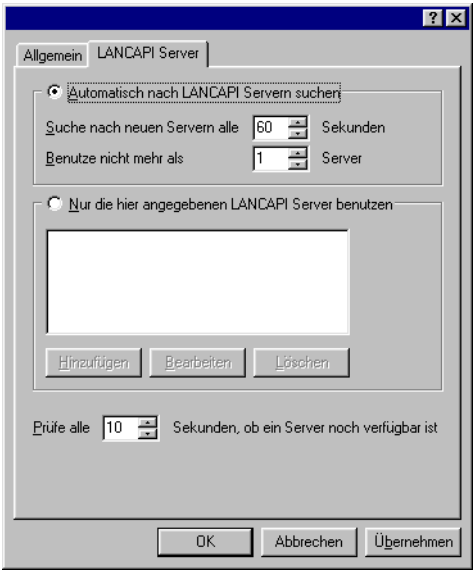
Einstellen des *LANCAPI*-Clients

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 ein *ELSA LANCOM DSL/25 Office* 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 'ELSAlan'. 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 solange, bis er die im nächsten Feld eingestellte Anzahl an Servern gefunden hat. Hat er die geforderte Zahl an Servern gefunden, hört er mit der Suche auf.
- Wenn der Client nicht automatisch nach Servern suchen soll, geben Sie in der Liste die IP-Adressen der Server an, die der Client verwenden soll. Diese Festlegung ist z.B. dann sinnvoll, wenn Sie mehrere *ELSA LANCOM DSL/25 Office* 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.



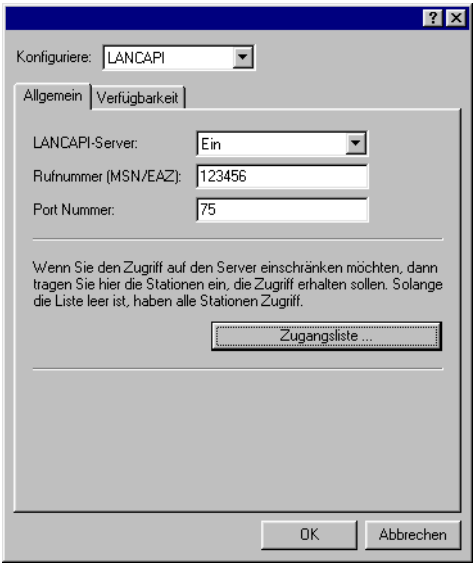
Einstellen des *LANCAPI*-Servers

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 LANCAPI* keine eigene Rufnummer frei haben.

③ Wenn der *LANCAPI*-Server eingeschaltet ist, geben Sie im Feld 'Rufnummern' die Telefonnummern ein, auf die *LANCAPI* reagieren soll. Mehrere Rufnummern können Sie durch Semikola getrennt eingeben. Wenn Sie hier keine Rufnummer eingeben, werden alle eingehenden Rufe an die *LANCAPI* gemeldet.

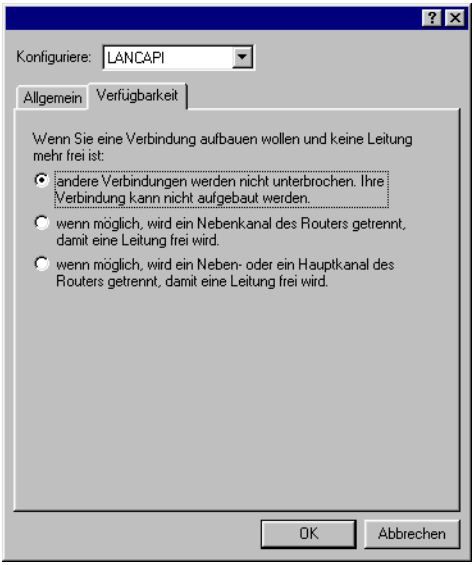
④ Der von der *LANCAPI* verwendete Port ist auf '75' (any private telephony service) voreingestellt. Verändern Sie diese Einstellung nur dann, wenn dieser Port in Ihrem lokalen Netz schon für andere Dienste verwendet wird.

⑤ Falls nicht alle Rechner aus dem lokalen Netz Zugriff auf die Funktionen der *LANCAPI* haben sollen, können Sie in der Zugangsliste die berechtigten Teilnehmer (über die IP-Adressen) genau festlegen.

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

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

Wechseln Sie auf die Registerkarte 'Verfügbarkeit'. Hier legen Sie fest, wie sich ein *ELSA LANCOM DSL/25 Office* 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. Nebenkanäle 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.

DE

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'.

DE

5 Anhang

5.1 Technische Daten

Funktionsarten:	IP-Router, DHCP-Server, DHCP-Client, DNS-Server, NetBIOS-Proxy, IPX-Router
LAN-Anschluß:	Ethernet IEEE 802.3, 10/100Base-T (RJ45, Node/Hub Switch), autosense, Full-Duplex-Betrieb
Netzwerk-Protokolle:	**IP:** ARP, PROXY ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, NetBIOS über IP, DNS, PPP over ATM, Classical-IP **IPX:** IPX, SPX, RIP, SAP, Propagate Packets
Filter-Möglichkeiten:	Quell- und Zielfilter für Netzwerke, Protokolle und Ports; WAN und LAN getrennt
WAN-Schnittstelle:	Ethernet IEEE 802.3, 10Base-T (RJ45) ATM 25.6F
Gebührenschutz:	Maximale Gebührenmenge (je nach Provider) oder Verbindungszeit in einem vorgegebenen Zeitraum festlegbar
Security- und Firewall-Funktionen:	PAP, CHAP und MS-CHAP, Authentifizierungsmechanismen im PPP; Filtermöglichkeiten im IP-Betrieb; Schutz der Konfiguration über Zugangslisten und Paßwort; IP-Masquerading; ATM-Schutzmechanismen (CLIP, Rückruf etc.)
IP-Masquerading: (NAT/PAT)	IP-Adreß- und -Port-Umsetzung über eine IP-Adresse; statische/dynamische Zuweisung der IP-Adresse über PPP oder DHCP; Maskierung von TCP, UDP, ICMP, FTP; DNS-Forwarding; inverses Masquerading für IP-Dienste aus dem Intranet wie z.B. Web-Server; NetBIOS-Masquerading
Management:	V.24/V.28-Outband-Schnittstelle (8poliger Mini-DIN), TFTP-Konfiguration und Firmware-Upload, SNMP-Management via SNMP v.1 oder v.2, WAN- oder LAN-Zugänge getrennt aktivierbar, Diagnose-Ausgaben für Protokolle und Schnittstellen, Diagnose-Tools, Status-Anzeige ELSA LANmonitor, Fernkonfiguration über PPP
Betriebssicherheit:	Hardware-Watchdogs, regelmäßige Selbsttests, FirmSafe-Konzept für Remote-Software-Upgrade
Statistiken:	LAN- und WAN-Paketzähler, Fehler-, Verbindungs-, Gebührenzähler
Anzeigen/Bedienung:	LEDs für LAN-, WAN- und Geräte-Status
Stromversorgung:	12 VA 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 158 x 40 x 125 mm (B x H x T)

DE

Lieferumfang	Netzteil, Kabel für Outband-Schnittstelle, LAN-Twisted-Pair-Kabel, ATM-Anschlußkabel, ausführliche Dokumentation
Zulassungen:	CE: EN 55022, EN 55024 und EN 60950; T-Nova: 1269510198 und E.000009.07.01
Service	Garantie: 6 Jahre Support: über Infoline und Internet

DE

5.2 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 ELSA-Produkte sechs Jahre. Ausgenommen hiervon sind ELSA-Monitore und ELSA-Videokonferenzsysteme; hierfür beträgt die Garantiezeit drei Jahre. Die Garantiezeit beginnt mit dem Tag der Lieferung des Gerätes durch den ELSA-Fachhändler. Garantieleistungen bewirken weder eine Verlängerung der Garantiefrist, noch setzen sie eine neue Garantiefrist in Lauf. Die Garantiefrist für eingebaute Ersatzteile endet mit der Garantiefrist für das ganze Gerät.

3 Abwicklung

a) Zeigen sich innerhalb der Garantiezeit Fehler des Gerätes, so sind Garantieansprüche unverzüglich, spätestens jedoch innerhalb von sieben Tagen geltend zu machen.

b) Transportschäden, die äußerlich erkennbar sind (z.B. Gehäuse beschädigt), sind unverzüglich gegenüber der Transportperson und uns geltend zu machen. Äußerlich nicht erkennbare Schäden sind unverzüglich nach Entdeckung, spätestens jedoch innerhalb von sieben Tagen nach Anlieferung, schriftlich gegenüber der Transportperson und uns zu reklamieren.

c) Der Transport zu und von der Stelle, welche die Garantieansprüche entgegennimmt und/oder das instandgesetzte Gerät austauscht, geschieht auf eigene Gefahr und Kosten des Erwerbers.

d) Garantieansprüche werden nur berücksichtigt, wenn mit dem Gerät das Rechnungsoriginal vorgelegt wird.

4 Ausschluß der Garantie

Jegliche Garantieansprüche sind insbesondere ausgeschlossen,

a) wenn das Gerät durch den Einfluß höherer Gewalt oder durch Umwelteinflüsse (Feuchtigkeit, Stromschlag, Staub u.ä.) beschädigt oder zerstört wurde;

b) wenn das Gerät unter Bedingungen gelagert oder betrieben wurde, die außerhalb der technischen Spezifikationen liegen;

c) wenn die Schäden durch unsachgemäße Behandlung – insbesondere durch Nichtbeachtung der Systembeschreibung und der Betriebsanleitung – aufgetreten sind;

d) wenn das Gerät durch hierfür nicht von uns ermächtigte Personen geöffnet, repariert oder modifiziert wurde;

e) wenn das Gerät mechanische Beschädigungen irgendwelcher Art aufweist;

f) wenn Schäden an der Bildröhre eines ELSA-Monitors festgestellt werden, die insbesondere durch mechanische Belastungen (Verschiebung der Bildröhrenmaske durch Schockeinwirkung oder Beschädigungen des Glaskörpers), starke Magnetfelder in unmittelbarer Nähe (bunte Flecken auf dem Bildschirm), permanente Darstellung des gleichen Bildes (Einbrennen des Phosphors) hervorgerufen wurden;

g) wenn und soweit sich die Luminanz der Hintergrundbeleuchtung bei TFT-Panels im Laufe der Zeit allmählich reduziert;

h) wenn der Garantieanspruch nicht gemäß Ziffer 3a) oder 3b) gemeldet worden ist.

5 Bedienungsfehler

Stellt sich heraus, daß die gemeldete Fehlfunktion des Gerätes durch fehlerhafte Fremd-Hardware, -Software, Installation oder Bedienung verursacht wurde, behalten wir uns vor, den entstandenen Prüfaufwand dem Erwerber zu berechnen.

6 Ergänzende Regelungen

a) Die vorstehenden Bestimmungen regeln das Rechtsverhältnis zu uns abschließend.

b) Durch diese Garantie werden weitergehende Ansprüche, insbesondere solche auf Wandlung oder Minderung, nicht begründet. Schadensersatzansprüche, gleich aus welchem Rechtsgrund, sind ausgeschlossen. Dies gilt nicht, soweit z.B. bei Personenschäden oder Schäden an privat genutzten Sachen nach dem Produkthaftungsgesetz oder in Fällen des Vorsatzes oder der groben Fahrlässigkeit zwingend gehaftet wird.

c) Ausgeschlossen sind insbesondere Ansprüche auf Ersatz von entgangenem Gewinn, mittelbaren oder Folgeschäden.

d) Für Datenverlust und/oder die Wiederbeschaffung von Daten haften wir in Fällen von leichter und mittlerer Fahrlässigkeit nicht.

e) In Fällen, in denen wir die Vernichtung von Daten vorsätzlich oder grob fahrlässig verursacht haben, haften wir für den typischen Wiederherstellungsaufwand, der bei regelmäßiger und gefahrentsprechender 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.

DE

5.3 Konformitätserklärung

CE

KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:
This declaration is valid for the following product:

Geräteart: **ATM Router**
Type of Device:
Typenbezeichnung: ***LANCOM DSL/25 Office***
Product Name:

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:
This is to confirm that this product meets all essential protection requirements relating to the

Niederspannungs Richtlinie (73/23/EWG)
Low Voltage Directive (73/23/EEC)
EMV Richtlinie (89/336/EWG)
EMC Directive (89/336/EEC)

Zur Beurteilung der Konformität wurden folgende **Normen** herangezogen:
The assessment of this product has been based on the following **standards**

EN 50081-1: 1992 Teile/ parts**: EN 55022: 1994**
EN 50082-1: 1997 Teile/ parts**: EN55024: 1999**
EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1996

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:
On behalf of the manufacturer / importer:

ELSA AG
Sonnenweg 11
D-52070 Aachen

abgegeben durch: / this declaration is submitted by:

Aachen, 23. August 1999
Aachen, 23rd August 1999

i.V. Stefan Kriebel
Bereichsleiter Entwicklung
VP Engineering

DE

6 Index

DE

DE

DE

DE

DE