

ELSA LANCOM™ I600 Office-Serie

© 2001 ELSA AG, Aachen (Germany)

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

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

ELSA ist DIN-EN-ISO-9001-zertifiziert. Mit der Urkunde vom 15.06.1998 bescheinigt die akkreditierte Zertifizierungsstelle TÜV-CERT die Konformität mit der weltweit anerkannten Norm DIN EN ISO 9001. Die an ELSA vergebene Zertifikatsnummer lautet 09 100 5069.

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

Marken

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

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

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

ELSA AG

Sonnenweg 11

52070 Aachen

Deutschland

www.elsa.de

Aachen, Juni 2001

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Mit einem *ELSA LANCOM 1600 Office* haben Sie sich für einen Router entschieden, mit dem Sie lokale Netzwerke oder einzelne Arbeitsplatzrechner mit höchster Geschwindigkeit an das Internet anschließen können.

Modellvarianten

Diese Dokumentation beschreibt verschiedene Modellvarianten aus der Serie *ELSA LANCOM 1600 Office*, die in Hard- und Softwareausstattung unterschiedlich sind:

- *ELSA LANCOM DSL/1610 Office*
- *ELSA LANCOM DSL/I-1611 Office*

Modell-
Einschränkungen

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

Dokumentation

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

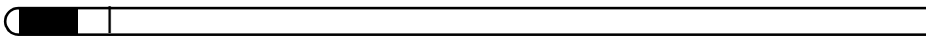
Sollten Sie dennoch einen Fehler finden, oder Sie möchten einfach eine Kritik oder Anregung zu dieser Dokumentation äußern, senden Sie bitte eine E-Mail direkt an:



editorial@elsa.de



*Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, stehen Ihnen unsere Online-Dienste (www.elsa.de) rund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' alle FAQs (**F**requently **A**squired **Q**uestions – häufig gestellte Fragen) zu Ihrem Produkt. Die Wissensdatenbank (KnowledgeBase) bietet einen zusätzlichen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Handbücher stehen Ihnen jederzeit zum Download bereit.*



Inhalt

1 Einleitung	9
1.1 Was macht ein Router überhaupt?	9
1.2 Typische Anwendungen	10
1.2.1 Internet im LAN	10
1.2.2 LAN-LAN-Kopplung	11
1.2.3 Heimarbeit mit Remote Access	11
1.2.4 Bürokommunikation	12
1.3 Was bietet ein <i>ELSA LANCOM 1600 Office</i> ?	12
1.3.1 Alle Geräte der <i>ELSA LANCOM 1600 Office</i> -Serie	12
1.3.2 Zusätzliche Funktionen <i>ELSA LANCOM DSL/I-1611 Office</i>	16
2 <i>ELSA LANCOM 1600 Office</i> stellt sich vor	19
2.1 Die Frontseite des Geräts	19
2.2 Die Rückseite des Geräts	21
3 Installation	23
3.1 Lieferumfang	23
3.2 Systemvoraussetzungen	23
3.3 Installation der Hardware	24
3.4 Installation der Software	25
3.4.1 ELSA-Setup starten	25
3.4.2 Welche Software installieren?	26
3.5 Im nächsten Kapitel	27
4 Grundeinstellungen	29
4.1 Start des Setup-Assistenten	29
4.1.1 Grundeinstellungen mit <i>ELSA LANconfig</i>	29
4.1.2 Grundeinstellungen mit <i>ELSA WEBconfig</i>	32
4.2 Den Zugang zum Internet einrichten	35
4.2.1 Aufruf des Assistenten unter <i>ELSA LANconfig</i>	35
4.2.2 Aufruf des Assistenten unter <i>ELSA WEBconfig</i>	35
4.2.3 Eingabe der Zugangsdaten	36
4.3 Einstellungen an den Arbeitsplatz-PCs	36
4.4 Fertig!	36

5 Konfiguration und Management	39
5.1 Mittel und Wege für die Konfiguration	39
5.2 Software zur Konfiguration	40
5.2.1 Konfiguration über <i>ELSA LANconfig</i>	40
5.2.2 Konfiguration mit <i>ELSA WEBconfig</i>	42
5.2.3 Konfiguration über Telnet	44
5.2.4 Konfiguration über SNMP	45
5.3 Die Fernkonfiguration über das DFÜ-Netzwerk	45
5.3.1 Das brauchen Sie für die Fernkonfiguration	46
5.3.2 Die erste Fernverbindung mit DFÜ-Netzwerk	46
5.3.3 Die erste Fernverbindung mit PPP-Client und Telnet	46
5.3.4 Fernkonfiguration einschränken	47
5.4 <i>ELSA LANmonitor</i> – wissen, was läuft	49
5.4.1 Erweiterte Anzeige-Optionen	49
5.4.2 Internet-Verbindung kontrollieren	50
5.5 Trace-Ausgaben – Infos für Profis	51
5.5.1 So starten Sie einen Trace	51
5.6 Abspeichern und Wiederherstellen der Konfiguration	54
5.7 Neue Firmware mit <i>ELSA FirmSafe</i>	54
5.7.1 So funktioniert <i>ELSA FirmSafe</i>	55
5.7.2 So spielen Sie eine neue Software ein	55
6 Sicherheit	59
6.1 Schutz für die Konfiguration	59
6.1.1 Passwortschutz	59
6.1.2 Die Login-Sperre	61
6.1.3 Zugangskontrolle über TCP/IP	62
6.2 Schutz für das LAN	62
6.2.1 Das Versteck – IP-Masquerading (NAT, PAT)	63
6.2.2 Filterung von Datenpaketen – Firewall	67
6.3 Den ISDN-Zugang absichern	70
6.3.1 Die Identifikationskontrolle	71
6.3.2 Der Rückruf	73
6.4 Die Sicherheits-Checkliste	74
7 Server-Dienste für das LAN	77
7.1 Automatische IP-Adressverwaltung mit DHCP	77
7.1.1 Der DHCP-Server	77
7.1.2 DHCP – 'Ein', 'Aus' oder 'Auto'?	78
7.1.3 So werden die Adressen zugewiesen	79

7.2	DNS	83
7.2.1	Was macht ein DNS-Server?	83
7.2.2	DNS-Forwarding	85
7.2.3	So stellen Sie den DNS-Server ein	86
7.3	Gebührenmanagement	90
7.3.1	Verbindungs-Begrenzung für DSL und Kabelmodem	90
7.3.2	Gebührenabhängige ISDN-Verbindungsbegrenzung	92
7.3.3	Zeitabhängige ISDN-Verbindungsbegrenzung	92
7.3.4	Einstellungen im Gebührenmodul	93
7.4	Das SYSLOG-Modul	93
7.4.1	Einrichten des SYSLOG-Moduls	94
7.4.2	Beispielkonfiguration mit <i>ELSA LANconfig</i>	94
7.5	Bürokommunikation mit <i>ELSA LANCAPi</i>	96
7.5.1	Welche Vorteile bietet die <i>ELSA LANCAPi</i> ?	97
7.5.2	Installation des <i>ELSA LANCAPi</i> -Clients	97
7.5.3	Konfiguration der <i>ELSA LANCAPi</i> -Clients	98
7.5.4	Konfiguration des <i>ELSA LANCAPi</i> -Servers	99
7.5.5	So setzen Sie die <i>ELSA LANCAPi</i> ein	102
7.5.6	Das <i>ELSA CAPI Faxmodem</i>	102

8 Routing und WAN-Verbindungen 105

8.1	Allgemeines über WAN-Verbindungen	105
8.1.1	Brücken für Standard-Protokolle	105
8.1.2	Was passiert bei einer Anfrage aus dem LAN?	106
8.2	IP-Routing	107
8.2.1	Die IP-Routing-Tabelle	107
8.2.2	Lokales Routing	110
8.2.3	Dynamisches Routing mit IP-RIP	111
8.2.4	Policy Based Routing	115
8.2.5	SYN/ACK-Speedup	115
8.3	Die Konfiguration von Gegenstellen	116
8.3.1	Namenliste	116
8.3.2	Layer-Liste	118
8.4	Verbindungsaufbau mit PPP	120
8.4.1	Das Protokoll	120
8.4.2	Alles o.k.? Leitungsüberprüfung mit LCP	122
8.4.3	Zuweisung von IP-Adressen über PPP	123
8.4.4	Einstellungen in der PPP-Liste	125
8.5	DSL-Verbindungsaufbau mit PPTP	126
8.6	Dauerverbindung für Flatrates – Keep-Alive	127

8.7	Rückruf-Funktionen	128
8.7.1	Rückruf nach Microsoft CBCP	128
8.7.2	Schneller Rückruf mit dem ELSA-Verfahren	130
8.7.3	Rückruf nach RFC 1570 (PPP LCP Extensions)	130
8.7.4	Konfiguration der Rückruf-Funktion im Überblick	131
8.8	Kanalbündelung mit MLPPP	132
9	Technische Daten	137
9.1	Leistungs- und Kenndaten	137
9.2	Anschlussbelegung	139
9.2.1	Ethernet-Schnittstellen 10/100Base-T (LAN) und 10Base-T (WAN)	139
9.2.2	ISDN-S ₀ -Schnittstelle	139
9.2.3	Konfigurationsschnittstelle (Outband)	140
10	Anhang	141
10.1	Allgemeine Garantiebedingungen	141
10.2	Konformitätserklärung Europäische Union (CE)	143
11	Index	145

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 Privatwohnungen im Vordergrund. Eine der neuen Technologien ist die Übertragung mittels DSL, die über einfache Kupferleitungen die „letzte Meile“ überbrückt. Auch über den heimischen Kabel-TV-Anschluss kann ein Breitbandanschluss ins Internet realisiert werden.

Ein *ELSA LANCOM 1600 Office* arbeitet mit nahezu jedem Highspeed-Internet-Anschluss auf DSL- oder Kabel-TV-Basis zusammen. Der eigentliche Zugang zum Internet erfolgt dabei immer über ein Modem, an das der Router angeschlossen wird.

Dieses Kapitel ...

... führt Sie kurz in die Funktionen und die Anwendungsgebiete von Routern ein. Anschließend erhalten Sie einen Überblick über die Fähigkeiten Ihres *ELSA LANCOM 1600 Office*. Eine ausführliche Beschreibung der Funktionen, der Software und ihrer Bedienung sowie eine Einführung in die technischen Grundlagen finden Sie in den nachfolgenden Kapiteln.

1.1

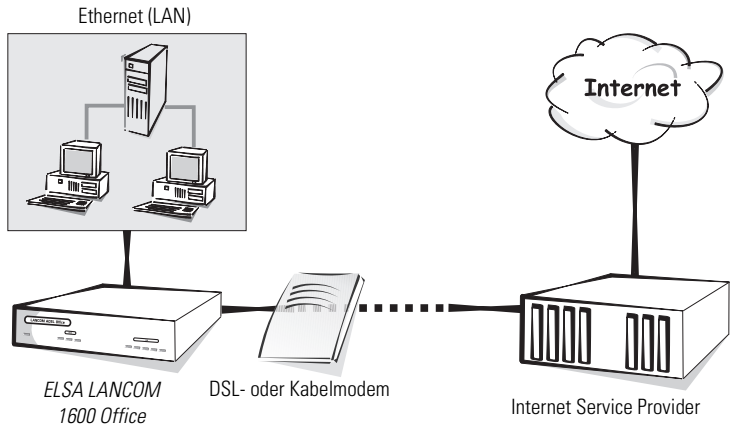
Was macht ein Router überhaupt?

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 DSL-Verbindung bereit, die z.B. über normale Kupfer-Telefonleitungen realisiert werden kann. Als weitere Möglichkeit steht bei einem *ELSA LANCOM DSL/I-1611 Office* eine ISDN-Verbindung

zur Verfügung mit einem vollwertigen ISDN-Router, den Funktionen der *ELSA LANCAPI* sowie als Backup für die Internet-Verbindung.

Mit diesen Leistungswerten empfiehlt sich ein *ELSA LANCOM 1600 Office* insbesondere für die Nutzung von Highspeed-Internet-Anbindungen. 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.



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 selbstständig, ob Daten in ein anderes Netzwerk übertragen werden müssen.

1.2 Typische Anwendungen

1.2.1 Internet im LAN

In vielen Unternehmen wächst die Forderung nach dem Zugriff auf das Internet von allen Arbeitsplätzen im LAN. Online-Recherchen, E-Mail und File-transfer 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 und Firewall-Filter schirmen Ihr Netz auch gegen Zugriff von außen ab.

1.2.2

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.

*Nur ELSA LANCOM
DSL/I-1611 Office*

Eine direkte LAN-LAN-Kopplung kann mit einem *ELSA LANCOM DSL/I-1611 Office* über ISDN aufgebaut werden. Schneller, kostengünstiger und flexibler ist die Netzwerkkopplung über das Internet. Hier kommt der Breitband-Zugang (über DSL oder das Kabel-TV-Netz) ins Internet zum Einsatz. LAN-LAN-Kopplungen über das Internet erfolgen als Virtuelle Private Netzwerke (VPN).

Alle *ELSA LANCOM 1600 Office* können mit der *ELSA LANCOM VPN Option* ausgerüstet werden und unterstützen dann den Aufbau von VPN.

1.2.3

Heimarbeit mit Remote Access

*Nur ELSA LANCOM
DSL/I-1611 Office*

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 ermöglicht ein *ELSA LANCOM 1600 Office* natürlich einen hohen Grad an Schutz für die 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 Verbindungsgebühren in der Firma zentral erfasst.

Remote Access ermöglicht der *ELSA LANCOM DSL/I-1611 Office* über die ISDN-Schnittstelle.

1.2.4

Nur *ELSA LANCOM DSL/I-1611 Office*

Bürokommunikation

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

Die *ELSA 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.

Bürokommunikations-Funktionen ermöglicht der *ELSA LANCOM DSL/I-1611 Office* über die ISDN-Schnittstelle.

1.3

Was bietet ein *ELSA LANCOM 1600 Office*?

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

1.3.1

Alle Geräte der *ELSA LANCOM 1600 Office*-Serie

Einfache Installation

- *ELSA LANCOM 1600 Office* mit Spannung versorgen
- Verbindung zum LAN herstellen
- Verbindung zum DSL- oder Kabelmodem herstellen
- ISDN-Kabel anschließen (nur *ELSA LANCOM DSL/I-1611 Office*)
- Einschalten
- Installation der *ELSA*-Software und Grundkonfiguration über die komfortablen Assistenten
- 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 1600 Office wird an die Ethernet-Schnittstelle eines DSL- oder Kabelmodems angeschlossen.

Ein *ELSA LANCOM DSL/I-1611 Office* verfügt außerdem über einen ISDN-Anschluss, der an die S_0 -Schnittstelle(n) eines ISDN-(Mehrgeräteanschlusses (Punkt-zu-Mehrpunkt-Konfiguration) oder eines Anlagenanschlusses (Punkt-zu-Punkt-Konfiguration) angeschlossen wird. Der Router erkennt den ISDN-Anschlusstyp und das verwendete D-Kanal-Protokoll automatisch.

IP-Routing: Leitungsaufbau und -verwaltung

Der Router überprüft alle IP-Pakete 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 selbstständig die Verbindung auf und beendet diese nach der Übertragung.

Sicherheitsfunktionen

Zum Schutz vor unberechtigtem Zugriff auf das Firmen-Netz von außerhalb verfügt ein *ELSA LANCOM 1600 Office* über leistungsfähige Sicherheitsfunktionen. IP-Masquerading versteckt alle Arbeitsstationen im LAN hinter einer einheitlichen öffentlichen IP-Adresse. Ihre wirkliche Identität bleibt verborgen. Firewall-Filter erlauben die gezielte Sperrung von IP-Adressen, Protokollen und Ports. Mit MAC-Adress-Filtern kann auch der Zugriff von Arbeitsstationen im LAN auf die IP-Routing-Funktion des Gerätes gezielt kontrolliert werden.

Die Login-Sperre verhindert „Brute-Force-Angriffe“ und sperrt den Zugang zum Router nach einer einstellbaren Anzahl von Login-Versuchen mit falschem Passwort. Diese Maßnahme schützt die Konfiguration des Routers wirksam gegen wiederholte Angriffsversuche.

DHCP

Ihr *ELSA LANCOM 1600 Office* verfügt über folgende DHCP-Modi:

- DHCP-Server, er verteilt IP-Adressen
- DHCP-Relay-Agent, er leitet DHCP-Anfragen weiter

In der Voreinstellung arbeitet das Gerät mit einem ausgeklügelten Automatik-Modus, der die Inbetriebnahme eines *ELSA LANCOM 1600 Office* sowohl in einem bestehenden als auch in einem neuen Netzwerk zum Kinderspiel macht.

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 und aus dem NetBIOS-Modul 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.

Virtual Private Network (VPN)

Ihr *ELSA LANCOM 1600 Office* kann mit der VPN-Option zu einem vollwertigen VPN-Gateway (nach dem IPSec-Standard) aufgerüstet werden. Damit wird er in die Lage versetzt, sichere Netzwerk-Kopplungen zu anderen VPN-Gateways über das Internet (oder andere IP-Netzwerke) aufzubauen. Der IPSec-Standard und modernste Verschlüsselungstechniken gewährleisten ein hohes Sicherheitsniveau der VPN-Verbindungen.

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.:

- Verbindungszustand für jeden Übertragungskanal (nur *ELSA LANCOM DSL/I-1611 Office*)
- Name der verbundenen Gegenstelle
- Welches Modul aus dem Gerät ist verbunden (Router, *ELSA LANCAPi*)
- 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 aller LAN- und WAN-Anschlüsse und erleichtern somit die Diagnose bei möglichen System-Störungen.

Konfiguration

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

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

Benutzer anderer Betriebssysteme verwenden die HTML-basierte Konfiguration mit *ELSA WEBconfig*, ein SNMP Managementsystem, Telnet oder ein beliebiges Terminalprogramm.

Der Zugriff auf das Gerät ist dabei möglich aus dem LAN, aus dem WAN, per Fernkonfiguration über ISDN (nur *ELSA LANCOM DSL/I-1611 Office*) oder direkt über die eingebaute Konfigurationsschnittstelle. Bei Konfigurationen aus dem LAN oder WAN wird neben SNMP auch das Übertragungsprotokoll TFTP unterstützt.

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

Firmware-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 auf der ELSA-Homepage für Sie bereit und kann über das LAN, das WAN (nur *ELSA LANCOM DSL/I-1611 Office*) oder über die Konfigurationsschnittstelle eingespielt werden.

ELSA FirmSafe

Beim Einspielen der neuen Firmware gehen Sie kein Risiko ein: Die ELSA-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.



Gebührenschutz

Die Gebühren für die Internetnutzung werden je nach Provider zeitabhängig berechnet. Um nicht am Ende des Monats von einer hohen Rechnung überrascht zu werden, können Sie vorher festlegen, wie viele Online-Minuten für den Internet-Anschluss in einem bestimmten Zeitraum (z.B. 600 Minuten in 6 Tagen) über ein *ELSA LANCOM 1600 Office* erlaubt sind.

Statistiken

Mit den umfangreichen Statistiken haben Sie *ELSA LANCOM 1600 Office* im Griff. Hier finden Sie z.B. alle Informationen über die übertragenen Datenpakete und optimieren so die Konfiguration Ihres Geräts.

1.3.2

Zusätzliche Funktionen *ELSA LANCOM DSL/I-1611 Office*

Der *ELSA LANCOM DSL/I-1611 Office* verfügt über einen ISDN-Anschluss und bietet daher einige zusätzliche Funktionen.

Multiprotokoll-Router

Über die ISDN-Schnittstelle können neben IP auch andere Protokolle geroutet werden. So ermöglicht das Protokoll IPX die Kopplung von Novell-Netzwerken.

Für die Kopplung von Microsoft-Peer-to-Peer-Netzwerken bieten Router von ELSA ein besonderes Feature. Durch integriertes Routing von IP-Net-BIOS-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. 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.

Sicherheitsfunktionen für die ISDN-Schnittstelle

Zur Absicherung der eingebauten ISDN-Schnittstelle verwendet ein *ELSA LANCOM DSL/I-1611 Office* neben dem Passwortschutz und der Rufnummernerkennung (CLIP) auch die Rückruf-Funktion, mit der der Verbindungsaufbau auf vorher festgelegte ISDN-Rufnummern beschränkt wird. Authentifizierungsmechanismen im PPP erweitern das Sicherheitskonzept.

Optionales *ELSA Dynamic VPN*

Auf einem *ELSA LANCOM DSL/I-1611 Office* können Sie mit der *ELSA LANCOM VPN Option* VPN-Tunnel auch zu einer Gegenstellen mit dynamischer IP-Adresse aufbauen. Dazu wird die von ELSA zum Patent angemeldete Technologie *ELSA Dynamic VPN* eingesetzt.

ELSA LANCAPI* und *ELSA CAPI Faxmodem

Der Einsatz der *ELSA LANCAPI* bringt vor allem wirtschaftliche Vorteile. Die *ELSA 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 *ELSA LANCAPI* uneingeschränkten Zugriff auf Bürokommunikations-Funktionen wie Fax und Eurofiletransfer. Ohne zusätzliche Hardware an den Arbeitsstationen werden alle Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsstationen installiert.

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

Automatische Zeitkontrolle

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

Kanalbündelung und Kompression

Auf der ISDN-Leitung unterstützt das Gerät statische und dynamische Kanalbündelung über MLPPP und BACP. Mit der Stac-Datenkompression (hi/fn) kann eine Steigerung der Datenübertragungsrate um bis zu 400% erreicht werden.

Least-Cost-Routing

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

Festverbindungsoption

Die Netzwerkkopplung über ISDN-Standleitungen ist mit der optionalen Festverbindungsoption möglich.

2

ELSA LANCOM 1600 Office stellt sich vor

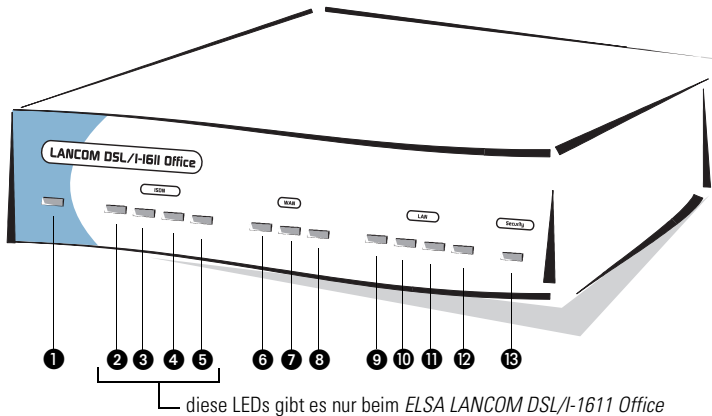
DE

In diesem Abschnitt stellen wir Ihnen Ihr Gerät vor. Sie erfahren etwas über die Bedeutung der Anzeigeelemente sowie die Anschlussmöglichkeiten.

2.1

Die Frontseite des Geräts

An der Vorderseite finden Sie als Anzeigeelemente eine Reihe von Leuchtdioden (LEDs).



Bedeutung der LEDs

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

aus		Gerät abgeschaltet
rot	1 x kurz	Bootvorgang (Test und Laden) begonnen
rot	blinkend	Anzeige eines Bootfehlers (im Blinkcode kodiert); Dauerblinken auch beim Erreichen des Zeit- oder Gebührenbudgets
rot		Gerät betriebsbereit

Nur ELSA LANCOM
DSL/I-1611 Office

2 ISDN-S₀-Status – zeigt den Zustand des ISDN-S₀-Anschlusses an:

aus		nicht angeschlossen oder keine S ₀ -Spannung (häufig wird an ISDN-Anschlüssen nach einer inaktiven Zeit die S ₀ -Spannung deaktiviert)
grün	blinkend	Initialisierung (Kontaktaufnahme mit Verbindungsstelle)
grün		betriebsbereit (S ₀ -Bus aktiviert, TEI vorhanden und D-Kanal-Protokoll geprüft)
grün	Power aus	LED ist an, wobei Power-LED aus ist: Gerät im Boot-Monitor

Nur ELSA LANCOM
DSL/I-1611 Office

3 ISDN-Chan1 – Zustand des ersten logischen ISDN-B-Kanals (sowohl im Router-Betrieb als auch im CAPI-Betrieb) an:

aus		Kanal in Ruhe
rot	blinkend	ankommender Ruf liegt an
grün	blinkend	abgehender Ruf wird durchgeführt
rot		Kanal ist physikalisch hergestellt/Protokollverhandlung läuft
grün		zugehörige Protokollverhandlung (X.75, PPP, etc.) ist abgeschlossen; Kanal ist logisch online
grün/rot	kurze rote Blitze (Dauer ca. 1/10 s)	zeigen ein empfangenes Daten-Paket an

Nur ELSA LANCOM
DSL/I-1611 Office

4 ISDN-Chan2 – Zustand des zweiten logischen ISDN-B-Kanals (Bedeutung wie ISDN-Chan1)

Nur ELSA LANCOM
DSL/I-1611 Office

5 ISDN-1+2 – zeigt an, ob die aktuelle ISDN-Verbindung eine statische bzw. dynamische Kanalbündelung ist.

aus	keine Verbindung bzw. keine Bündelverbindung aktiv
grün	statische bzw. dynamische Bündelverbindung aktiv

6 WAN-Rx/Tx – Diese gelbe LED zeigt die Datenbewegungen auf der WAN-Verbindung (über DSL- oder Kabelmodem) an.

7 WAN-Link – Diese grüne LED zeigt an, dass die Ethernet-Verbindung zwischen ELSA LANCOM 1600 Office und DSL- bzw. Kabelmodem in Ordnung ist.

8 WAN-Chan – Diese LED zeigt den Zustand der WAN-Verbindung (über DSL- oder Kabelmodem) zum Provider an. Die Verbindung zum Provider

erfordert normalerweise ein Login mit Benutzernamen und Kennwort. Bei zeitabhängigen Verbindungstarifen fallen während dieser Zeit Gebühren an. Die Bedeutung der LED im Detail:

aus	Es wurde kein Login bei der Vermittlungsstelle angefordert
rot	Es wurde ein Login bei der Vermittlungsstelle angefordert, das Login wird durchgeführt
grün	Das Login war erfolgreich, die Verbindung zum Provider ist hergestellt.

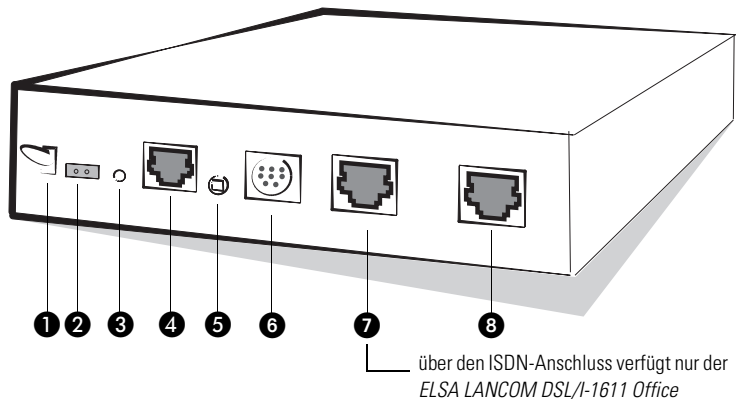
- 9 **LAN-Rx/Tx** – Datenpaket vom Gerät an das LAN oder vom LAN an das Gerät gesendet
- 10 **LAN-Coll** – Sendekollision
- 11 **LAN-Link** – Der Anschluss zum LAN ist hergestellt und bereit
- 12 **LAN-Fast** – Das Gerät arbeitet im LAN im 100-Mbit-Betrieb
- 13 **Security-VPN/Msg** – Im VPN-Gateway-Betrieb liefert das LED Statusinformationen über den gesamten VPN-Betrieb:

aus	keine aktive VPN-Verbindung aufgebaut
grün	bestehende aktive VPN-Verbindung(en)
rot	VPN-Tunnelaufbau

2.2

Die Rückseite des Geräts

Auf der Rückseite befinden sich die Anschlüsse und Schalter des Gerätes.





- ❶ Ein/Aus-Schalter
- ❷ Anschluss für das Netzteil

Verwenden Sie ausschließlich das mitgelieferte Netzteil! Die Verwendung eines ungeeigneten Netzteils kann zu Personen- oder Sachschäden führen.

- ❸ Reset-Schalter – um das Gerät in den Auslieferungszustand zu versetzen, drücken Sie den eingelassenen Reset-Knopf und halten ihn ca. 5 Sekunden lang gedrückt. Sobald der Reset ausgelöst wird, leuchten die LEDs auf der Vorderseite des Gerätes auf, und das Gerät startet neu in den Auslieferungszustand.
- ❹ 10/100Base-Tx für den Anschluss an das LAN. Unterstützt werden 10-Mbit- oder 100-Mbit-Anschlüsse. Der *ELSA LANCOM 1600 Office* erkennt die verwendete Netzwerkgeschwindigkeit automatisch (Auto-sensing).
- ❺ Node/Hub-Umschalter – die Sende- und Empfangsleitungen des LAN-Anschlusses (❹) können im Gerät für den direkten Anschluss eines PC gekreuzt werden (Hub-Einstellung). Bei Anschluss an einen Hub oder ein Switch sollte der Schalter auf 'Node'-Einstellung (Voreinstellung) geschaltet sein.
- ❻ V.24-Konfigurationsschnittstelle
- ❼ ISDN/S₀-Anschluss (nur *ELSA LANCOM DSL/I-1611 Office*)
- ❽ 10Base-T-Anschluss für DSL- oder Kabelmodem

3

Installation

Dieses Kapitel hilft Ihnen, möglichst schnell Hard- und Software zu installieren. Zunächst überprüfen Sie Lieferumfang und Systemvoraussetzungen. Sind alle Voraussetzungen erfüllt, gelingen Anschluss und Inbetriebnahme schnell und ohne Mühe.

3.1

Lieferumfang

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

- *ELSA LANCOM 1600 Office*
- Netzteil
- LAN-Anschlusskabel, grüne Stecker
- WAN-Anschlusskabel für DSL- oder Kabelmodem, dunkelblaue Stecker
- ISDN-Anschlusskabel, hellblaue Stecker (nur *ELSA LANCOM DSL/I-1611 Office*)
- Kabel für die serielle Konfigurationsschnittstelle
- *ELSA LANCOM Office*-CD mit *ELSA LANtools* und weiterer Software
- Lizenzaufkleber mit Software-Seriennummern
- Gedruckte Dokumentation

Falls etwas fehlen sollte, wenden Sie sich bitte an die Kontaktadresse, die auf dem Lieferschein zu Ihrem Gerät angegeben ist.

3.2

Systemvoraussetzungen

Die PCs, die mit einem *ELSA LANCOM 1600 Office* in Verbindung treten möchten, müssen mindestens die folgenden Voraussetzungen erfüllen:

- Beliebiges Betriebssystem mit TCP/IP-Unterstützung, z.B. Windows Millennium Edition (Me), Windows 2000, Windows 98, Windows 95, Windows NT, Linux, Apple Mac OS, OS/2, BeOS.
- Eine Ethernet-Karte muss installiert sein.
- Das TCP/IP-Protokoll muss eingerichtet sein.
- Ein Web-Browser sollte installiert sein.

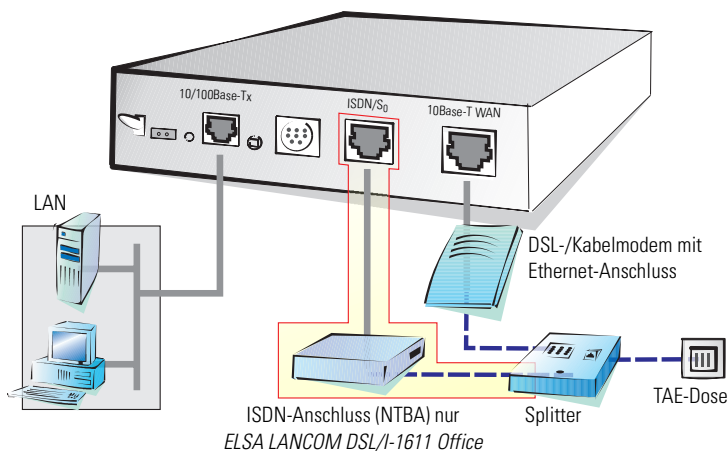


Die ELSA LANtools und die Funktionen der ELSA LANCAPAPI (nur ELSA LANCOM DSL/I-1611 Office) benötigen zudem ein Windows-Betriebssystem.

3.3

Installation der Hardware

- ① Verbinden Sie Ihr *ELSA LANCOM 1600 Office* mit dem LAN. Stecken Sie dazu das mitgelieferte Netzkabel (grüne Stecker) in den 10/100Base-Tx-Anschluss des Geräts (4) und in eine freie Netzwerkanschlussdose Ihres lokalen Netzes (bzw. in eine freie Buchse eines Hubs in Ihrem LAN). Alternativ können Sie auch einen einzelnen PC anschließen. In diesem Fall stellen Sie den Node/Hub-Umschalter (5) auf die Position 'Hub'.



- ② Verbinden Sie Ihr *ELSA LANCOM 1600 Office* mit dem DSL- oder Kabel-TV-Netz. Stecken Sie dazu das WAN-Anschlusskabel (dunkelblaue Stecker) in den 10Base-T-WAN-Anschluss (8) des Geräts. Das andere Ende verbinden Sie mit Ihrem DSL- oder Kabelmodem.
- ③ Verbinden Sie Ihr *ELSA LANCOM DSL/I-1611 Office* mit dem ISDN. Stecken Sie dazu das eine Ende des mitgelieferten ISDN-Anschlusskabels (hellblaue Stecker) in den ISDN/S₀-Anschluss (7) des Geräts und das andere Ende in einen ISDN/S₀-Anlagenanschluss oder Mehrgeräteanschluss (Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Konfiguration).

Nur ELSA LANCOM
DSL/I-1611 Office



Bitte beachten Sie, dass Ihr DSL- oder Kabelmodem über einen Ethernet-Anschluss (10Base-T) verfügen muss. Der Betrieb des ELSA LANCOM

1600 Office an einem Modem, das ausschließlich über eine USB- oder ATM-F-Schnittstelle verfügt, ist nicht möglich.

- ④ 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.



Sollte diese LED nicht leuchten, betätigen Sie auf der Rückseite des Gerätes den Node/Hub-Umschalter (⑤). Falls die LED dann noch immer nicht leuchtet, liegt evtl. ein Problem mit Netzwerkkarte oder der Verkabelung vor.

3.4

Installation der Software

In diesem Abschnitt beschreiben wir die Installation der mitgelieferten ELSA-Software, die unter Windows läuft. Sollten Sie Ihren *ELSA LANCOM 1600 Office* ausschließlich mit PCs verwenden, die unter anderen Betriebssystemen als Windows laufen, können Sie diesen Abschnitt überspringen. In diesem Fall ist eine Software-Installation nicht erforderlich.



Einige Funktionen Ihres Routers erfordern ein Windows-Betriebssystem. Zu diesen Funktionen gehört die Überwachung mit ELSA LANmonitor. Beim ELSA LANCOM DSL/I-1611 Office setzen die ELSA LANCAPI-Funktionen für die ISDN-Schnittstelle ebenfalls ein Windows-Betriebssystem auf den Arbeitsplatz-PCs voraus.

3.4.1

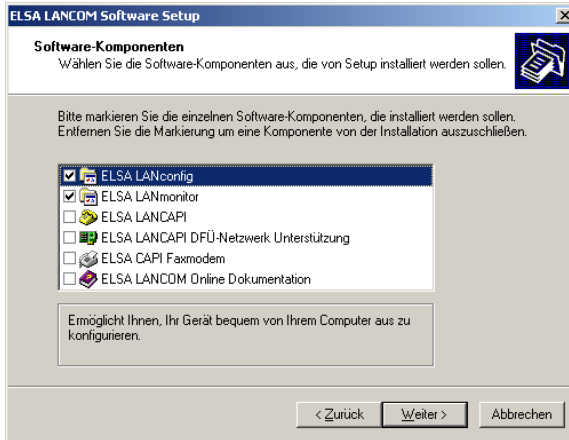
ELSA-Setup starten

Legen Sie die *ELSA LANCOM Office*-CD in Ihr Laufwerk ein. Daraufhin startet das ELSA-Setup-Programm automatisch. Der automatische Start funktioniert nicht unter Windows NT: Hier müssen Sie die Datei AUTORUN.EXE im Stammverzeichnis der CD manuell aufrufen.



Der manuelle Aufruf der AUTORUN.EXE ist auch erforderlich, wenn auf Ihrem PC die CD-Autostart-Funktion deaktiviert ist, oder das ELSA-Setup aus anderen Gründen nicht automatisch startet.

Klicken Sie im ELSA-Setup auf **LANCOM Software installieren**. Es erscheint folgendes Auswahlmenü auf dem Bildschirm:



3.4.2

Welche Software installieren?

Nicht jede Software, die das Auswahlmenü Ihnen anbietet, ist für Ihren *ELSA LANCOM 1600 Office* notwendig.

- **ELSA LANconfig** ist das Konfigurationsprogramm für alle *ELSA LANCOM*. Alternativ (oder ergänzend) kann über einen Web-Browser *ELSA WEBconfig* verwendet werden.
- Mit **ELSA LANmonitor** überwachen Sie alle *ELSA LANCOM* im LAN.



Für die drei folgenden Programme benötigen Sie einen ELSA LANCOM mit ISDN-Schnittstelle. Von den Geräten der ELSA LANCOM 1600 Office-Serie verfügt nur der ELSA LANCOM DSL/I-1611 Office über eine ISDN-Schnittstelle.

- Die **ELSA LANCAPI** ermöglicht jedem Windows-PC im LAN, beliebige ISDN-Software so einzusetzen, als wäre eine ISDN-Karte im PC eingebaut. Tatsächlich erfolgt die ISDN-Verbindung zentral über den *ELSA LANCOM* mit ISDN-Schnittstelle.
- Die **ELSA LANCAPI DFÜ-Netzwerk Unterstützung** ermöglicht Ihnen, die CAPI-Software-Schnittstelle auf Ihrem Windows-PC wie einen Netzwerkadapter zu benutzen, etwa für die Remote-Access-Einwahl in einen *ELSA LANCOM*.
- Das **ELSA CAPI Faxmodem** richtet auf Ihrem Windows-PC einen Faxmodemtreiber ein, mit dem Sie Faxe über die *ELSA LANCAPI* verschicken können.

Wählen Sie die gewünschten Software-Optionen aus und bestätigen Sie mit **Weiter**. Die Software wird automatisch installiert.

3.5

Im nächsten Kapitel ...

... führen wir die Grundkonfiguration des Gerätes durch. Mit nur wenigen Mausklicks richten Sie Ihren *ELSA LANCOM 1600 Office* so ein, dass alle PCs im LAN mit höchster Geschwindigkeit auf das Internet zugreifen können.

4

Grundeinstellungen

In diesem Kapitel nehmen wir die wichtigsten Grundeinstellungen an Ihrem *ELSA LANCOM 1600 Office* vor:

- Zuweisung einer IP-Adresse
- Aktivierung des eingebauten DHCP-Servers (auf Wunsch)
- Sichern des Konfigurationszugangs durch Kennwort
- Die Konfiguration der ISDN-Schnittstelle (nur beim *ELSA LANCOM DSL/I-1611 Office*)
- Einrichtung des Internet-Zugangs

4.1

Start des Setup-Assistenten

Einen unkonfigurierten *ELSA LANCOM 1600 Office* können Sie auf zwei komfortable Arten erreichen:

- *ELSA LANconfig* findet einen unkonfigurierten *ELSA LANCOM* automatisch und startet den Setup-Assistenten für die Grundeinstellungen.
- Mit *ELSA WEBconfig*: Geben Sie an einem PC im Netzwerk die IP-Adresse des unkonfigurierten *ELSA LANCOM 1600 Office* in die Adresszeile eines Web-Browsers ein. In bestimmten Netzwerkumgebungen erreichen Sie Ihren *ELSA LANCOM 1600 Office* auch mit der Eingabe eines beliebigen Namen in der Adresszeile. Dazu später mehr.



In einem Netzwerk sollten sich niemals mehrere unkonfigurierte ELSA LANCOM befinden. Da sich alle unkonfigurierten ELSA LANCOM unter derselben IP-Adresse (mit den Endziffern 254) melden, kommt es bei mehreren Geräten zu Adresskonflikten. Zur Vermeidung von Problemen sollten mehrere Geräte nur hintereinander konfiguriert und jeweils sofort mit einer eindeutigen IP-Adresse versehen werden.

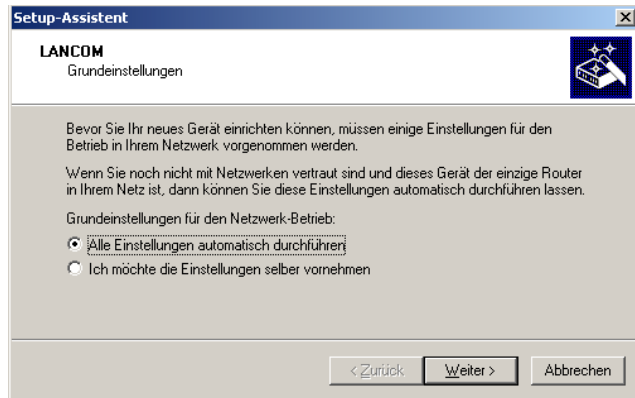
4.1.1

Grundeinstellungen mit *ELSA LANconfig*

- ① Starten Sie *ELSA LANconfig* mit **Start ► Programme ► ELSAan ► ELSA LANconfig**.

ELSA LANconfig erkennt den neuen *ELSA LANCOM 1600 Office* im TCP/IP-Netz selbstständig. Daraufhin startet der Setup-Assistent, der Ihnen bei der Grundeinstellung des Geräts behilflich ist oder Ihnen (die pas-

sende Netzwerkumgebung vorausgesetzt) sogar die gesamte Arbeit abnimmt.



Sollte der Setup-Assistent nicht automatisch starten, so suchen Sie manuell nach neuen Geräten im Netzwerk (**Gerät ► Suchen**).



Dieses Eingabefenster erscheint nur, wenn in Ihrem Netzwerk kein DHCP-Server aktiv ist und Ihrem PC auch manuell keine IP-Adresse zugewiesen wurde. Ansonsten läuft der Assistent genauso ab, wie das für die Eingabe 'Ich möchte die Einstellungen selber vornehmen' unter ② beschrieben ist.

Treffen Sie Ihre Wahl nach folgenden Überlegungen:

Wählen Sie 'Alle Einstellungen automatisch durchführen' ...

... wenn Sie mit Netzwerken und IP-Adressen **nicht** vertraut sind, und Sie bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet haben. Der Router wird dann als DHCP-Server die IP-Adressen für alle Geräte im LAN automatisch festlegen und zuweisen.

Wählen Sie '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 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 aktiviert wird).

- ☐ Sie haben auch bisher schon IP-Adressen auf den Rechnern im LAN verwendet.
- ② Wenn Sie die IP-Einstellungen selber vornehmen wollen, dann geben Sie dem *ELSA LANCOM 1600 Office* eine verfügbare Adresse aus dem bisher verwendeten IP-Adressbereich. Bestätigen Sie mit **Weiter**.
- ③ Zu den vorzunehmenden IP-Einstellungen gehört auch die Einstellung, ob der Router als DHCP-Server arbeiten soll oder nicht. Wählen Sie aus, und bestätigen Sie mit **Weiter**.
- ④ Im folgenden Fenster legen Sie das Passwort für den Konfigurationszugriff fest. Ferner bestimmen Sie, ob das Gerät nur aus dem LAN konfiguriert werden darf, oder ob auch die Fernkonfiguration über einen WAN-Anschluss (über DSL/Kabelmodem und beim *ELSA LANCOM DSL/I-1611 Office* auch über ISDN) erlaubt ist. Bestätigen Sie Ihre Wahl mit **Weiter**.



Bitte beachten Sie, dass mit Freischaltung der Fernkonfiguration auch die Fernkonfiguration aus dem Internet heraus ermöglicht wird. Sie sollten in jedem Fall darauf achten, dass der Konfigurationszugriff geeignet abgesichert ist, z. B. durch ein Passwort.

- ⑤ Bei einem *ELSA LANCOM DSL/I-1611 Office* ergibt sich die Möglichkeit, die ISDN-Schnittstelle jetzt zu konfigurieren. Bestätigen Sie Ihre Wahl mit **Weiter**.
- ⑥ Wenn Sie bei Ihrem *ELSA LANCOM DSL/I-1611 Office* die ISDN-Einstellungen einstellen wollen, geben Sie eine Rufnummer (in Form einer MSN) an, auf der das Gerät Rufe annehmen soll. Außerdem können Sie eine Amtsziffer für die Wahl ins ISDN eingeben. Schließlich sollten Sie angeben, ob an Ihrem ISDN-Anschluss die Gebühreninformationen übermittelt werden oder nicht. Bestätigen Sie mit **Weiter**.
- ⑦ Schließen Sie die Konfiguration mit **Fertig stellen** ab.

4.1.2

Grundeinstellungen mit *ELSA WEBconfig*

Wie Sie wissen, können Sie mit *ELSA WEBconfig* Ihren *ELSA LANCOM 1600 Office* mit jedem Web-Browser konfigurieren. Sie sind also nicht wie bei *ELSA LANconfig* auf das Betriebssystem Windows angewiesen.

Einzige Voraussetzung für den Zugriff: Sie müssen wissen, wie Sie den unkonfigurierten Router im LAN ansprechen. Ein unkonfigurierter *ELSA LANCOM* reagiert in jedem Fall auf eine bestimmte IP-Adresse, in einigen Netzwerk-Konfiguration sogar auf einen Namen.

Reagiert mein *ELSA LANCOM 1600 Office* auf einen Namen?

Wenn Sie in Ihrem LAN bisher weder einen DHCP- noch einen DNS-Server haben, reagiert der Router auf jeden Namen (z.B. 'LANCOM' oder 'Router'), den Sie im URL-Adressfeld eines Web-Browsers eingeben.



Wenn Sie nicht wissen, ob in Ihrem Netzwerk bisher IP-Adressen verwendet wurden, lassen Sie sich die IP-Adresse des eigenen PC anzeigen (siehe folgender Abschnitt). Wenn im Feld 'IP-Adresse' der Wert '0.0.0.0' steht, hat die Netzwerkkarte bisher noch keine IP-Adresse.

Welche IP-Adresse hat der *ELSA LANCOM 1600 Office*?

Die IP-Adresse eines unkonfigurierten *ELSA LANCOM* ergibt sich aus der IP-Adresse des aufrufenden PC, indem Sie die letzte Zahl dieser IP-Adresse (hinter dem dritten Punkt) durch 254 ersetzen.

Ist Ihrem PC beispielsweise die IP-Adresse 10.0.0.17 zugewiesen, dann finden Sie einen unkonfigurierten *ELSA LANCOM* unter der Adresse 10.0.0.254. Die IP-Adresse Ihres PC lassen Sie sich (je nach Betriebssystem) mit folgenden Kommandozeilen-Befehlen anzeigen (Eingabe unter Windows in der Eingabeaufforderung):

Betriebssystem	Befehl in der Kommandozeile
Windows 95, Windows 98, Windows Me	winiptcfg
Windows NT 4.0, Windows 2000	ipconfig
Linux, UNIX	ifconfig

Aufruf der Assistenten in *WEBconfig*

- ① Öffnen Sie also Ihren Web-Browser (Internet Explorer, Netscape Navigator) und rufen Sie dort den *ELSA LANCOM 1600 Office* auf:

http://<IP-Adresse des LANCOM> (bzw. über beliebigen Namen)
Es erscheint folgendes Hauptmenü:



Die Assistenten sind auf den jeweiligen ELSA LANCOM zugeschnitten und fallen daher unterschiedlich aus. Es kann daher sein, dass Ihr Gerät nicht alle abgebildeten Assistenten anbietet.

- ② Wählen Sie den Eintrag **Grundeinstellungen**. Im folgenden Fenster bietet sich Ihnen die Auswahl zwischen 'IP-Parameter automatisch festlegen' und 'IP-Parameter selber festlegen'.

Diese Auswahlmöglichkeit erscheint nur, wenn in Ihrem Netzwerk kein DHCP-Server aktiv ist und Ihrem PC keine IP-Adresse zugeordnet wurde. Ansonsten läuft der Assistent genauso ab, wie ab Schritt ④ beschrieben.

- ③ Treffen Sie Ihre Wahl nach folgenden Überlegungen:

Aktivieren Sie 'IP-Parameter automatisch festlegen' ...

... wenn Sie mit Netzwerken und IP-Adressen **nicht** vertraut sind und bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet haben. Der Router wird dann als DHCP-Server die IP-Adressen für alle Geräte im LAN automatisch festlegen und zuweisen.

Deaktivieren Sie 'IP-Parameter automatisch festlegen' ...

... 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 das neue Gerät jedoch selbst festlegen und ihm eine beliebige Adresse aus einem der für private Zwecke reservierten Adressbereiche, z.B. '10.0.0.x' mit der Netzmaske '255.255.255.0' zuweisen. Damit legen Sie auch gleichzeitig den Adressbereich fest, den der DHCP-Server anschließend für die anderen Geräte im Netz verwendet (sofern der DHCP-Server aktiviert wird).
 - Sie haben auch bisher schon IP-Adressen auf den Rechnern im LAN verwendet. Geben Sie dem neuen Gerät eine freie Adresse aus dem bisher verwendeten Adressbereich. Bestimmen Sie ferner, ob das Gerät als DHCP-Server im LAN arbeiten soll oder nicht.
- ④ Wenn Sie die IP-Einstellungen selber vornehmen wollten, dann geben Sie dem *ELSA LANCOM 1600 Office* eine verfügbare Adresse aus dem bisher verwendeten IP-Adressbereich. Stellen Sie außerdem ein, ob er als DHCP-Server arbeiten soll oder nicht. Bestätigen Sie Ihre Eingabe mit **Setzen**.
- ⑤ Im folgenden Fenster 'Sicherheitseinstellungen' legen Sie das Passwort für den Konfigurationszugriff fest. Ferner bestimmen Sie, ob das Gerät nur aus dem LAN konfiguriert werden darf, oder ob auch die Fernkonfiguration über einen WAN-Anschluss (über DSL/Kabelmodem und beim *ELSA LANCOM DSL/I-1611 Office* auch über ISDN) erlaubt ist. Bestätigen Sie Ihre Wahl mit **Setzen**.



Bitte beachten Sie, dass mit Freischaltung der Fernkonfiguration auch die Fernkonfiguration aus dem Internet heraus ermöglicht wird. Sie sollten in jedem Fall darauf achten, dass der Konfigurationszugriff geeignet abgesichert ist, z.B. durch ein Passwort.

- ⑥ Die Online-Hilfe für *ELSA WEBconfig* liegt auf der ELSA-Website im Internet zur direkten Verwendung bereit. Alternativ kann der Inhalt der Online-Hilfe in Form von HTML-Dateien auf einem Fileserver im LAN oder

lokal auf den Konfigurations-PCs abgelegt werden. Den Ort der Online-Hilfe legen Sie in Form eines URL-Pfads fest.

Wenn Sie den voreingestellten Pfad übernehmen, lädt der *ELSA LANCOM 1600 Office* bei Bedarf die Hilfetexte von der ELSA-Website. Möchten Sie aber auch ohne bestehende Internet-Verbindung auf die Hilfetexte zugreifen, dann ändern Sie den Pfad entsprechend ab. Weitere Informationen zu diesem Thema finden Sie im Abschnitt 'Die Hilfedateien für ELSA WEBconfig (HTTP-Modul)' auf Seite 42.

Bei einem *ELSA LANCOM DSL/I-1611 Office* ergibt sich die Möglichkeit, die ISDN-Schnittstelle jetzt zu konfigurieren. Bestätigen Sie Ihre Wahl mit **Setzen**.

- ⑦ Wenn Sie die Konfiguration des ISDN-Anschlusses gewünscht haben, werden Sie abschließend danach gefragt, ob auf Ihrem ISDN-Anschluss die Gebühreninformation übermittelt wird. Treffen Sie Ihre Wahl und bestätigen Sie mit **Setzen**.
- ⑧ Wenn *ELSA WEBconfig* die Annahme der Eingaben meldet, ist die Grundkonfiguration abgeschlossen.

4.2 Den Zugang zum Internet einrichten

Für die Einrichtung des Internet-Zugangs steht Ihnen ein eigener Assistent zur Verfügung. Diesen rufen Sie wie folgt auf:

4.2.1 Aufruf des Assistenten unter *ELSA LANconfig*

- ① Wählen Sie Ihr *ELSA LANCOM 1600 Office* aus dem Auswahlfenster aus.
- ② Mit dem Befehl **Extras ► Setup Assistent** erhalten Sie das Menü mit den verfügbaren Assistenten. Wählen Sie **Internet-Zugang einrichten**.

4.2.2 Aufruf des Assistenten unter *ELSA WEBconfig*

Den Internet-Zugangs-Assistent rufen Sie direkt im Hauptmenü von *ELSA WEBconfig* auf.

4.2.3

Eingabe der Zugangsdaten

Der Internet-Zugangs-Assistent fragt Sie schrittweise alle notwendigen Daten für den Zugang zum Internet ab. Diese Zugangsdaten hat Ihnen Ihr Internet Service Provider angegeben.

4.3

Einstellungen an den Arbeitsplatz-PCs

In Abhängigkeit von der Methode, mit der in Ihrem LAN die IP-Adressen vergeben werden, sind an den PCs im LAN folgende Einstellungen für den Internetzugang vorzunehmen:

- **DHCP-Vergabe über den *ELSA LANCOM 1600 Office* (Normalfall)**

Der *ELSA LANCOM 1600 Office* übermittelt über DHCP auch seine eigene IP-Adresse als Standard-Gateway und DNS-Server an die PCs. Die Arbeitsplatz-PCs sind so einzustellen, dass sie ihre eigene IP-Adresse, ebenso wie die IP-Adressen von Standard-Gateway und DNS-Server automatisch (über DHCP) beziehen.

- **DHCP-Vergabe über einen separaten DHCP-Server**

Die Arbeitsplatz-PCs sind so einzustellen, dass sie ihre eigene IP-Adresse, ebenso wie die IP-Adressen von Standard-Gateway und DNS-Server automatisch (über DHCP) beziehen. Auf dem DHCP-Server ist die IP-Adresse des *ELSA LANCOM 1600 Office* so zu hinterlegen, dass der DHCP-Server sie an die PCs im LAN als Standard-Gateway übermittelt. Außerdem sollte der DHCP-Server den *ELSA LANCOM 1600 Office* als DNS-Server angeben,

- **Manuelle Zuweisung der IP-Adressen**

Werden die IP-Adressen im Netzwerk statisch vergeben, so sind bei jedem PC im LAN die IP-Adresse des *ELSA LANCOM 1600 Office* als Standard-Gateway und als DNS-Server in der TCP/IP-Konfiguration einzustellen.



Weitere Informationen und Hilfe zu den TCP/IP-Einstellungen Ihres PC finden Sie in der Dokumentation Ihres Betriebssystems.

4.4

Fertig!

Mit diesen wenigen Mausklicks haben Sie Ihren *ELSA LANCOM 1600 Office* vollständig für den Internet-Zugang konfiguriert. Alle Rechner in Ihrem LAN können von nun an mit Höchstgeschwindigkeit durch das Internet surfen ...

Nach der Basis-Konfiguration sind in den meisten Fällen die notwendigen Einstellungen am *ELSA LANCOM 1600 Office* für den konkreten Einsatzbereich vorgenommen.

Sie können natürlich auch eine Vielzahl weitergehender Einstellungen vornehmen. Eine ausführliche Beschreibung dieser Optionen finden Sie in den folgenden Kapiteln.

5

Konfiguration und Management



In diesem Kapitel geben wir Ihnen einen Überblick, mit welchen Mitteln und über welche Wege Sie auf das Gerät zugreifen können, um erweiterte Einstellungen vorzunehmen. Sie finden Beschreibungen zu folgenden Themen:

- Konfigurationstools
- Kontroll- und Diagnosefunktionen von Gerät und Software
- Sicherung und Wiederherstellung kompletter Konfigurationen
- Installation neuer Firmware im Gerät

5.1

Mittel und Wege für die Konfiguration

ELSA LANCOM 1600 Office sind flexible Geräte, die verschiedene Mittel (sprich Software) und Wege (in Form von Kommunikationszugängen) für die Konfiguration unterstützen. Zunächst der Blick auf die möglichen Wege.

Einen *ELSA LANCOM 1600 Office* können Sie über bis zu drei verschiedene Zugänge erreichen:

- über die Konfigurations-Schnittstelle (Config-Schnittstelle) an der Rückseite des Routers (auch Outband genannt)
- über das angeschlossene Netzwerk (sowohl LAN als auch WAN – Inband)
- Fernkonfiguration über den ISDN-Anschluss (nur beim *ELSA LANCOM DSL/I-1611 Office*)

Was unterscheidet nun diese drei Wege?

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

Zum anderen die Anforderungen an zusätzliche Hard- und Software: Die Inband-Konfiguration benötigt einen der ohnehin vorhandenen Rechner im LAN oder WAN und nur noch eine geeignete Software, beispielsweise *ELSA LANconfig* (vgl. folgender Abschnitt). Die Outband-Konfiguration braucht zusätzlich zur Konfigurationssoftware noch einen Rechner mit serieller Schnittstelle. Für die Fernkonfiguration sind die Voraussetzungen am umfangreichsten: Neben dem ISDN-Anschluss am *ELSA LANCOM 1600 Office* (nur beim *ELSA LANCOM DSL/I-1611 Office* vorhanden) wird im

Konfigurations-PC eine ISDN-Karte, ein ISDN-Adapter oder Zugriff über *ELSA LANCAPI* auf einen weiteren *ELSA LANCOM* mit ISDN-Schnittstelle benötigt.

5.2

Software zur Konfiguration

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

Die Situationen, in denen konfiguriert wird, unterscheiden sich – aber auch die persönlichen Ansprüche und Vorlieben der Ausführenden. *ELSA LANCOM 1600 Office*-Router verfügen daher über ein breites Angebot von Konfigurationssoftware:

- **ELSA LANconfig** – menügeführt, übersichtlich und einfach lassen sich nahezu alle Parameter eines *ELSA LANCOM 1600 Office* einstellen. Unterstützt Outband-, Inband- und Fernkonfiguration.
- **ELSA WEBconfig** – diese Software ist fest eingebaut im Router. Auf dem Konfigurationsrechner wird nur ein Web-Browser vorausgesetzt. *ELSA WEBconfig* ist dadurch betriebssystemunabhängig. Unterstützt werden Inband- und Fernkonfiguration.
- **SNMP** – geräteunabhängige Programme zum Management von IP-Netzwerken basieren üblicherweise auf dem Protokoll SNMP. Über SNMP können Sie auf *ELSA LANCOM 1600 Office* inband und mittels Fernkonfiguration zugreifen.
- **Terminalprogramm, Telnet** – ein *ELSA LANCOM 1600 Office* kann mit einem Terminalprogramm über die Config-Schnittstelle (z.B. HyperTerminal) oder innerhalb eines IP-Netzwerks (z.B. Telnet) konfiguriert werden.
- **TFTP** – innerhalb von IP-Netzwerken (Inband- und Fernkonfiguration) kann begrenzt auch das Dateiübertragungs-Protokoll TFTP verwendet werden.



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

5.2.1

Konfiguration über *ELSA LANconfig*

Rufen Sie *ELSA LANconfig* z.B. aus der Windows-Startleiste auf mit **Start ► Programme ► ELSAalan ► ELSA LANconfig**. *ELSA LANconfig* sucht nun automatisch im lokalen Netz nach Geräten. Wird dabei ein noch nicht konfi-

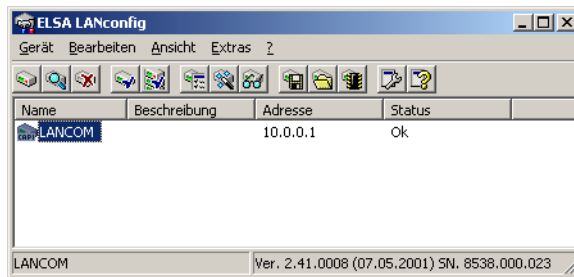
guriertes Gerät im lokalen Netz gefunden, startet *ELSA LANconfig* selbstständig den Setup-Assistenten. Die Beschreibung der Basiskonfiguration mit Hilfe des Setup-Assistenten finden Sie im Abschnitt 'Grundeinstellungen mit ELSA LANconfig' auf Seite 29.

Neue Geräte suchen



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

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



Der erweiterte Funktionsumfang für Profis

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 eingebaute Hilfe-Funktion

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

5.2.2

Konfiguration mit *ELSA WEBconfig*

Sie können die Einstellungen des Gerätes über einen beliebigen (auch text-basierten) Web-Browser vornehmen. Im *ELSA LANCOM 1600 Office* ist die Konfigurationssoftware *ELSA WEBconfig* integriert. Sie benötigen lediglich einen Web-Browser, um auf *ELSA WEBconfig* zuzugreifen.

Funktioniert mit beliebigem Web-Browser

ELSA WEBconfig bietet ähnliche Setup-Assistenten wie *ELSA LANconfig* an und bietet damit optimale Voraussetzungen für eine komfortable Konfiguration von *ELSA LANCOM 1600 Office* – im Unterschied zu *ELSA LANconfig*, aber unter allen Betriebssystemen, für die es einen Web-Browser gibt.

Für die Verwendung von *ELSA WEBconfig* muss ein LAN-Anschluss über TCP/IP (bei Fernkonfiguration über PPP) aufgebaut sein. Der Zugriff auf *ELSA WEBconfig* erfolgt über die IP-Adresse des *ELSA LANCOM 1600 Office* (oder in geeigneter Netzwerkumgebung auch über einen beliebigen Namen).

Im Abschnitt 'Grundeinstellungen mit *ELSA WEBconfig*' auf Seite 32 lesen Sie, wie Sie das erste Mal mit *ELSA WEBconfig* auf ein unkonfiguriertes Gerät zugreifen und die Basiskonfiguration vornehmen.

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

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

Hinter diesem Link befindet sich ein Verweis auf Hilfedateien im HTML-Format. In der Voreinstellung verweist der Hilfe-Link auf die ELSA-Webseiten.

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

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

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

Zur Syntax sind zwei wichtige Feststellungen zu machen:

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

Wenn Sie beispielsweise in einem lokalen Verzeichnis 'C:\ELSAHTMLRef' die Hilfedateien-Struktur '\500\2\1611\' angelegt haben, dann geben Sie als Dokumentenwurzel nur 'file://C:/ELSA/HTMLRef' an.

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

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

Statt des Platzhalters <IP-Adresse> wird entweder die gültige IP-Adresse des HTTP-Servers im Format 'x.x.x.x' erwartet, also beispielsweise '128.7.9.155' oder ein Servername, etwa 'www.elsa.com'.

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



5.2.3

Konfiguration über Telnet

Über Telnet starten Sie die Konfiguration z.B. aus der Windows-Kommandozeile mit dem Befehl:

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

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

Nach der Eingabe des Passworts (sofern Sie eines zum Schutz der Konfiguration vereinbart haben) stehen Ihnen alle Konfigurationsbefehle zur Verfügung.

Die Sprache der Konsole auf Deutsch ändern

Der Terminalmodus steht in den Sprachen Deutsch und Englisch zur Verfügung. *ELSA LANCOM 1600 Office* werden werkseitig auf Englisch als Konsolensprache eingestellt. Im weiteren Verlauf dieser Dokumentation werden alle Konfigurationsbefehle in ihrer deutschen Form angegeben. Zur Änderung der Konsolensprache auf Deutsch verwenden Sie folgende Befehle:

Konfigurationstool	Aufruf (bei Englisch als eingestellter Konsolensprache)
<i>ELSA WEBconfig</i>	Expertenkonfiguration ► Config-Module ► Language
Telnet	set /Setup/Config-Module/Language Deutsch

TFTP

Bestimmte Funktionen lassen sich über Telnet nicht oder nicht befriedigend ausführen. Dazu gehören alle Funktionen, bei denen komplette Dateien übertragen werden, etwa der Upload von Firmware oder die Speicherung und Wiederherstellung von Konfigurationsdaten. In diesen Fällen wird TFTP eingesetzt.

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

Die Syntax des TFTP-Aufrufs ist abhängig vom Betriebssystem. Bei Windows 2000 und Windows NT lautet die Syntax:

```
tftp -i <IP-Adresse Host> [get|put] Quelle [Ziel]
```

Bei zahlreichen TFTP-Clients ist das ASCII-Format voreingestellt. Für die Übertragung binärer Daten (z.B. Firmware) muss daher meist die binäre Über-



tragung explizit gewählt werden. In diesem Beispiel für Windows 2000 und Windows NT erreichen Sie das durch den Parameter '-i'.

5.2.4

Konfiguration über SNMP

Das Simple Network Management Protocol (SNMP V.1 nach RFC 1157) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netz von einer zentralen Instanz aus.

Es gibt eine ganze Reihe von Konfigurations- und Management-Programmen, die über SNMP laufen. Kommerzielle Beispiele sind Tivoli, OpenView von Hewlett-Packard, SunNet Manager und CiscoWorks. Daneben existieren auch zahlreiche Programme auf Freeware- und Shareware-Basis.

Ihr *ELSA LANCOM 1600 Office* kann für die Verwendung in SNMP-Programmen sogenannte Geräte-MIB-Datei (**M**anagement **I**nformation **B**ase) exportieren.

Konfigurationstool	Aufruf
<i>ELSA WEBconfig</i>	SNMP-Geräte-MIB abrufen (im Hauptmenü)
TFTP	tftp 10.0.0.1 get readmib file1

5.3

Die Fernkonfiguration über das DFÜ-Netzwerk



Der komplette Abschnitt zur Fernkonfiguration gilt nur für ELSA LANCOM mit ISDN-Schnittstelle. Aus der Geräteserie ELSA LANCOM 1600 Office erfüllt nur der ELSA LANCOM DSL/I-1611 Office diese Anforderung.

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

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

5.3.1

Das brauchen Sie für die Fernkonfiguration

- Einen *ELSA LANCOM 1600 Office* mit ISDN-Anschluss
- Einen Rechner mit PPP-Client, z.B. Windows DFÜ-Netzwerk
- Ein Programm für die Inband-Konfiguration, z.B. *ELSA LANconfig* oder Telnet
- Einen Konfigurations-PC mit ISDN-Karte, ISDN-Adapter oder einen *ELSA LANCOM* mit ISDN-Anschluss und *ELSA LANCAPi*.

5.3.2

Die erste Fernverbindung mit DFÜ-Netzwerk

- ① Wählen Sie im *ELSA LANconfig* **Gerät ► Neu**, aktivieren Sie die 'DFÜ-Verbindung' als Anschlusstyp und geben Sie die Rufnummer des WAN-Anschlusses ein, an dem der *ELSA LANCOM DSL/I-1611 Office* angeschlossen ist. Stellen Sie dazu ggf. die Zeit ein, nach der eine Verbindung ohne Datentransfer automatisch getrennt werden soll.
- ② *ELSA LANconfig* legt nun automatisch einen neuen Eintrag im DFÜ-Netzwerk an. Wählen Sie ein PPP-fähiges Gerät (z.B. den NDIS-WAN-Treiber aus dem Lieferumfang der *ELSA 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 Löschen eines Eintrags in der Geräteliste wird auch die zugehörige Verbindung im Windows-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.

5.3.3

Die erste Fernverbindung mit PPP-Client und Telnet

- ① Stellen Sie mit Ihrem PPP-Client eine Verbindung zum *ELSA LANCOM 1600 Office* her, verwenden Sie dabei folgende Angaben:
 - Benutzername 'ADMIN'
 - Passwort wie beim *ELSA LANCOM DSL/I-1611 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/I-1611 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/I-1611 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/I-1611 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/I-1611 Office* über die Fernverbindung nun genauso einstellen wie alle anderen Geräte.

5.3.4

Fernkonfiguration einschränken

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

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

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

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

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



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

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

Geben Sie alternativ den folgenden Befehl ein:

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

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

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

```
passwd
```

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

5.4

ELSA LANmonitor – wissen, was läuft

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

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

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

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



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

5.4.1

Erweiterte Anzeige-Optionen

Unter **Ansicht ► Anzeigen** können Sie folgende Anzeige-Optionen ein- und ausschalten:

- Fehlermeldungen
- Diagnosemeldungen
- System-Informationen



Viele wichtige Details zum Status des ELSA LANCOM 1600 Office werden erst angezeigt, wenn die Anzeige der System-Informationen aktiviert ist. Dazu gehören beispielsweise die Schnittstellen und das Gebührenmanagement. Wir empfehlen daher interessierten Benutzern, die Anzeige der System-Informationen einzuschalten.

5.4.2

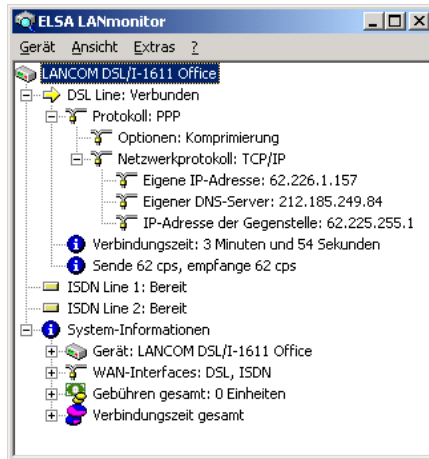
Internet-Verbindung kontrollieren

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

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

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

- ② *ELSA LANmonitor* legt automatisch einen neuen Eintrag in der Geräteliste an und zeigt zunächst den Zustand der Übertragungskanäle. Starten Sie Ihren Web-Browser, und geben Sie eine beliebige Webseite ein. *ELSA LANmonitor* zeigt nun an, wie auf einem Kanal eine Verbindung aufgebaut wird und welche Gegenstelle dabei gerufen wird. Sobald die Verbindung hergestellt ist, zeigt der Kommunikationskanal durch das Pluszeichen vor dem Eintrag an, dass zu diesem Kanal weitere Informationen vorliegen. Durch Klicken auf das Pluszeichen öffnen Sie eine baumartige Struktur, in der Sie verschiedene Informationen ablesen können.



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

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

- ③ Durch einen Klick mit der rechten Maustaste auf den aktiven Kanal können Sie die Verbindung manuell trennen. Dazu benötigen Sie ggf. das Konfigurationspasswort.
- ④ Wenn Sie ein Protokoll der *ELSA LANmonitor*-Ausgaben in Form einer Datei wünschen, wählen Sie in Menü 'Ansicht' die 'Optionen' und wechseln zur Registerkarte 'Protokoll'. Aktivieren Sie die Protokollierung und stellen Sie ein, ob *ELSA LANmonitor* täglich, monatlich oder fortlaufend eine Protokolldatei erstellt.

5.5

Trace-Ausgaben – Infos für Profis

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



können sowohl in der Konfiguration eigener Router als auch bei der Gegenseite zu finden sein.

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

5.5.1

So starten Sie einen Trace

Trace-Ausgaben starten Sie z.B. in einer Telnet-Sitzung. Der Trace-Aufruf folgt dieser Syntax:

```
trace [Schlüssel] [Parameter]
```

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

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

Dieser Parameter ruft beim Trace die folgende Anzeige hervor:
Status	Status-Meldungen der Verbindungen
Fehler	Fehler-Meldungen der Verbindungen
ELSA	Verhandlung des ELSA-Protokolls
IPX-Router	IPX-Routing
PPP	Verhandlung des PPP-Protokolls
SAP	IPX Service Advertising Protocol
IPX-Watchdog	IPX-Watchdog-Spoofing
SPX-Watchdog	SPX-Watchdog-Spoofing
LCR	Least-Cost-Router
Script	Script-Verhandlung

Dieser Parameter ruft beim Trace die folgende Anzeige hervor:
RIP	IPX Routing Information Protocol
IP-Router	IP-Routing
IP-RIP	IP Routing Information Protocol
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
IP-Masquerading	Vorgänge im Masquerading-Modul
DHCP	Dynamic Host Configuration Protocol
NetBIOS	NetBIOS-Verwaltung
DNS	Domain Name Service Protocol
Paket-Dump	Anzeige der ersten 64 Bytes eines Pakets in hexadezimaler Darstellung
D-Kanal-Dump	Trace des D-Kanals des angeschlossenen ISDN-Busses

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

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

Beispiele

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

5.6

Abspeichern und Wiederherstellen der Konfiguration

Die aktuelle Konfiguration eines *ELSA LANCOM 1600 Office* kann als Datei abgespeichert und bei Bedarf wieder in das Gerät (oder in ein anderes Gerät desselben Typs) geladen werden.

Sicherheitskopien der Konfiguration

Mit dieser Funktion können Sie Sicherungskopien der Konfiguration Ihres *ELSA LANCOM 1600 Office* zu erstellen. Sollte Ihr *ELSA LANCOM 1600 Office* (z.B. durch einen Defekt) seine Konfigurationsdaten verlieren, spielen Sie einfach die Sicherungskopie ein.

Komfortable Serienkonfiguration

Aber auch wenn Sie vor der Aufgabe stehen, mehrere gleichartige *ELSA LANCOM 1600 Office* konfigurieren zu müssen, werden Sie die Funktion des Abspeicherns und Wiederherstellens von Konfigurationen schätzen lernen. Sie können sich in diesem Fall einen großen Teil der Arbeit sparen, indem Sie in alle Geräte zunächst übereinstimmende Parameter als Grundkonfiguration

einspielen und nur noch die individuellen Einstellungen an den einzelnen Geräten vornehmen.

Funktionsaufruf

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	Bearbeiten ► Konfiguration als Datei sichern Bearbeiten ► Konfiguration aus Datei wiederherstellen
<i>ELSA WEBconfig</i>	Konfiguration speichern / Konfiguration laden (im Hauptmenü)
TFTP	tftp 10.0.0.1 get readconfig file1 tftp 10.0.0.1 put file1 writeconfig

5.7

Neue Firmware mit ELSA FirmSafe

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

5.7.1

So funktioniert ELSA FirmSafe

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

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

- 'Unmittelbar': Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:
 - Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.
 - Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit neu.

- 'Login': Um den Problemen eines fehlerhaften Uploads zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.
 - Im Unterschied zur ersten Variante wartet das Gerät anschließend fünf Minuten lang auf einen erfolgreichen Login. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.
 - Wenn das Gerät nicht mehr ansprechbar ist und ein Login somit unmöglich ist, aktiviert es automatisch wieder die bisherige Firmware und startet damit neu.
- 'Manuell': Bei der dritten Möglichkeit können Sie vorher selbst eine Zeit bestimmen, in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, dass die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird.

5.7.2

So spielen Sie eine neue Software ein

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

- *ELSA LANconfig*
- *ELSA WEBconfig*
- Terminalprogramm
- TFTP



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

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

ELSA LANconfig



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

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

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

ELSA WEBconfig

Starten Sie *ELSA WEBconfig* in Ihrem Web-Browser. Auf der Startseite finden Sie den Link **Eine neue Firmware hochladen**. Im nächsten Fenster können Sie die Firmware-Datei im Verzeichnissystem suchen und anschließend auf die Schaltfläche **Upload** klicken.

Terminalprogramm (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

Auf *ELSA LANCOM 1600 Office* kann mit TFTP eine neue Firmware aufgespielt werden. Dazu wird der Befehl (bzw. das Ziel) **writeflash** angegeben. Um eine neue Firmware in einen *ELSA LANCOM 1600 Office* mit der IP-Adresse 10.0.0.1 zu übertragen, geben Sie z.B. unter Windows 2000 oder Windows NT folgenden Befehl ein:

```
tftp -i 10.0.0.1 put Lc_16xxu.240 writeflash
```


6

Sicherheit



Dieses Kapitel widmet sich einem wichtigen Thema: der Sicherheit. Die Beschreibung der Sicherheitseinstellungen ist in folgende Abschnitte unterteilt:

- Schutz für die Konfiguration
 - Passwortschutz
 - Login-Sperre
 - Zugangskontrolle
- Schutz für das LAN
 - IP-Masquerading
 - Filterung von Datenpaketen
- Absichern des ISDN-Zugangs (nur *ELSA LANCOM DSL/I-1611 Office*)

Zum Ende des Kapitels finden Sie die wichtigsten Sicherheitseinstellungen in Form einer Checkliste. Damit Sie ganz sicher sein können, dass Ihr *ELSA LANCOM 1600 Office* bestens abgesichert ist.

6.1

Schutz für die 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 1600 Office* die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

6.1.1

Passwortschutz

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

Tipps für den richtigen Umgang mit Passwörtern

Für den Umgang mit Passwörtern möchten wir Ihnen an dieser Stelle einige Tipps ans Herz legen:

- **Halten Sie ein Passwort so geheim wie möglich.**

Notieren Sie niemals ein Passwort. Beliebte aber völlig ungeeignet sind beispielsweise: Notizbücher, Brieftaschen und Textdateien im Computer. Es klingt trivial, kann aber nicht häufig genug wiederholt werden: verraten Sie Ihr Passwort nicht weiter. Die sichersten Systeme kapitulieren vor der Geschwätzigkeit.

- **Passwörter nur sicher übertragen.**

Ein gewähltes Passwort muss der Gegenseite mitgeteilt werden. Wählen Sie dazu ein möglichst sicheres Verfahren. Meiden Sie: Ungeschütztes E-Mail, Brief, Fax. Besser ist die persönliche Übermittlung unter vier Augen. Die höchste Sicherheit erreichen Sie, wenn Sie das Passwort auf beiden Seiten persönlich eingeben.

- **Wählen Sie ein sicheres Passwort.**

Verwenden Sie zufällige Buchstaben- und Ziffernfolgen. Passwörter aus dem allgemeinen Sprachgebrauch sind unsicher. Auch Sonderzeichen wie '&“?#-*+_-.;!°' erschweren es Angreifern, Ihr Passwort zu erraten und erhöhen so die Sicherheit des Passworts.

- **Verwenden Sie ein Passwort niemals doppelt.**

Wenn Sie dasselbe Passwort für mehrere Zwecke verwenden, mindern Sie seine Sicherheitswirkung. Wenn eine Gegenseite unsicher wird, gefährden Sie mit einem Schlag auch alle anderen Verbindungen, für die Sie dieses Passwort verwenden.

- **Wechseln Sie das Passwort regelmäßig.**

Passwörter sollen möglichst häufig gewechselt werden. Das ist mit Mühe verbunden, erhöht aber die Sicherheit des Passwortes beträchtlich.

- **Wechseln Sie das Passwort sofort bei Verdacht.**

Wenn ein Mitarbeiter mit Zugriff auf ein Passwort Ihr Unternehmen verlässt, wird es höchste Zeit, dieses Passwort zu wechseln. Ein Passwort sollte auch immer dann gewechselt werden, wenn der geringste Verdacht einer undichten Stelle auftritt.

Wenn Sie diese einfachen Regeln einhalten, erreichen Sie ein hohes Maß an Sicherheit.

Eingabe des Passwortes

Das Feld zur Eingabe des Passworts finden Sie in *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Unter *ELSA WEBconfig* rufen Sie den Assistenten **Sicherheitseinstellungen** auf. In

einer Terminal- bzw. einer Telnet-Sitzung setzen oder ändern Sie das Passwort mit dem Befehl `passwd`.

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	Management ► Security ► Passwort
<i>ELSA WEBconfig</i>	Sicherheitseinstellungen
Terminal/Telnet	<code>passwd</code>

Den SNMP-Zugang schützen

Im gleichen Zug sollten Sie auch den SNMP-Lesezugriff mit Passwort schützen. Für SNMP wird das allgemeine Konfigurations-Passwort verwendet.

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	Management ► Security ► SNMP-Lesezugriff nur mit Passwort zulassen
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► SNMP-Modul ► Passw.Zwang-fuer-SNMP-Lesezugriff
Terminal/Telnet	<code>Setup/SNMP-Modul/Passw.Zwang</code>

6.1.2

Die Login-Sperre

Die Konfiguration im *ELSA LANCOM 1600 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 diese Grenze erreicht, wird der Zugang für eine bestimmte Zeit gesperrt.

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

Zur Konfiguration der Login-Sperre stehen in den Konfigurationstools folgende Einträge zur Verfügung:

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

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	Management ► Security
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► Config-Modul
Terminal/Telnet	Setup/Config-Modul

6.1.3

Zugangskontrolle über TCP/IP

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

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

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	TCP/IP ► Allgemein ► Zugangsliste
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► TCP-IP-Modul ► Zugangs-Liste
Terminal/Telnet	/Setup/TCP-IP-Modul/Zugangsliste

6.2

Schutz für das LAN

Sie mögen es sicher nicht, wenn jeder Außenstehende einfach die Daten auf Ihren Rechnern einsehen oder verändern kann. Ein *ELSA LANCOM 1600 Office* bietet verschiedene Möglichkeiten, den Zugriff von außen einzuschränken:

- IP-Masquerading (auch NAT/PAT genannt)
- Filterung von Datenpaketen – Firewall

6.2.1

Das Versteck – IP-Masquerading (NAT, PAT)

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

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

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

Wie funktioniert IP-Masquerading?

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

Die Antwort auf dieses Paket geht nun an die IP-Adresse 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.

Konfiguration von IP-Masquerading

Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle erreichen Sie wie folgt:

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	IP-Router ► Routing ► Routing-Tabelle
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► IP-Router-Modul ► IP-Routing-Tab
Terminal/Telnet	/Setup/IP-Router-Modul/IP-Routing-Tab

Zwei Adressen für den Router

Bei Masquerading treffen zwei gegensätzliche Forderungen an den Router aufeinander: Zum einen soll er eine im lokalen Netz gültige IP-Adresse haben, damit er aus dem LAN erreichbar ist, zum anderen soll er eine im Internet gültige Adresse haben. Da diese beiden Adressen prinzipiell nicht in einem logischen Netz liegen dürfen, hilft hier nur eins: Zwei IP-Adressen müssen her.

Der Router bekommt also nun eine **Internet**-Adresse und eine **Intranet**-Adresse, jeweils natürlich mit passender Netzmaske. Mit der Option **Maskierung** in der Routing-Tabelle informieren Sie den Router darüber, welche der beiden Adressen er bei der Weitergabe der Pakete verwenden soll:

- 'aus': Es wird keine Maskierung durchgeführt.
- 'dyn.': Mit diesem Eintrag fordern Sie von Ihrem Provider die Zuweisung einer beliebigen, im Internet gültigen IP-Adresse an, die Sie im weiteren für die Verbindung und die Maskierung verwenden wollen.
- 'stat.': Mit diesem Eintrag fordern Sie von Ihrem Provider die Zuweisung einer bestimmten IP-Adresse, die Sie im weiteren für die Verbindung und die Maskierung verwenden wollen. Die gewünschte IP-Adresse tragen Sie in folgendem Feld ein:

<i>ELSA LANconfig</i>	TCP/IP ► Allgemein ► Internet IP-Adresse
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► TCP/IP-Modul ► IP-Adresse
Terminal/Telnet	/Setup/TCP-IP-Modul/IP-Adresse

Unmaskierter Internetzugang für einzelne Geräte

Wird vom Provider eine bestimmte Adresse angefordert (Maskierungs-Option 'stat'), 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 (für 4 IP-Adressen): 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.

Ein Beispiel: Sie erhalten die IP-Netzadresse 123.45.67.0 mit der Netzmaske 255.255.255.248 vom Provider zugewiesen. Dann könnten Sie die IP-Adressen wie folgt verteilen:

IP-Adresse	Bedeutung/Verwendung
123.45.67.0	Netzadresse
123.45.67.1	<i>ELSA LANCOM 1600 Office</i> als Router für das LAN
123.45.67.2	Weiteres Gerät im LAN, das unmaskierten Zugang ins Internet erhalten soll, beispielsweise Web-Server
123.45.67.3	Broadcast-Adresse

Alle anderen Rechner und Geräte im LAN haben keine öffentliche IP-Adresse und treten daher mit der IP-Adresse des *ELSA LANCOM 1600 Office* (123.45.67.1) im Internet auf.

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. 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 Port-Nummer definiert werden. In einer Service-Tabelle wird dazu der Ziel-Port mit der Intranet-Adresse z.B. des FTP-Servers angegeben.
- Beim Zugriff aus dem 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.

Configuration des inversen Masqueradings

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	IP-Router ► Masq. ► Service-Tabelle
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► IP-Router-Modul ► Masquerading ► Service-Tabelle
Terminal/Telnet	/Setup/IP-Router-Modul/Masquerading/ Service-Tabelle

Welche Protokolle können mit IP-Masquerading übertragen werden?

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

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

- TCP (und alle darauf aufbauenden Protokolle wie FTP, HTTP etc.)
- UDP
- ICMP

6.2.2

Filterung von Datenpaketen – Firewall

Die Firewall-Filter des *ELSA LANCOM 1600 Office* bieten Filterfunktionen für einzelne Rechner und auch ganze Netze. Sie ermöglichen einen effektiven Schutz gegen unerwünschte Eindringlinge in Ihr Netzwerk.

Was kann gefiltert werden?

Wichtig sind die Quell- und Zielfilter für einzelne Ports oder auch Portbereiche. Zudem können einzelne Protokolle oder beliebige Protokollkombinationen (TCP/UDP/ICMP) gefiltert werden. Auch IP-Adressbereiche oder komplette IP-Netzwerke sind geeignete Objekte.

Neben diesen Objekten auf IP-Ebene können Stationen im LAN auch über ihre MAC-Adresse ausgewählt werden. „MAC“ steht für **M**edia **A**ccess **C**ontrol und ist Dreh- und Angelpunkt für die Kommunikation innerhalb eines LAN. Jedem Netzwerkadapter ist eine MAC-Adresse fest eingespeichert. MAC-Adressen sind weltweit eindeutig und unverwechselbar, ähnlich zu Seriennummern von Geräten. Über die MAC-Adressen lassen sich die PCs im LAN zuverlässig auswählen, um ihnen gezielt Rechte auf IP-Paketebene zu gewähren oder zu versagen. MAC-Adressen werden häufig außen auf den Netzwerkgeräten in hexadezimaler Darstellung (z.B. 00:A0:57:01:02:03) angebracht.

Die Filterung betrifft nur den IP-Router-Betrieb. Der Zugriff von PCs im LAN auf den ELSA LANCOM (z.B. auf die Konfigurationsdaten) kann mit den Firewall-Regeln nicht eingeschränkt werden.

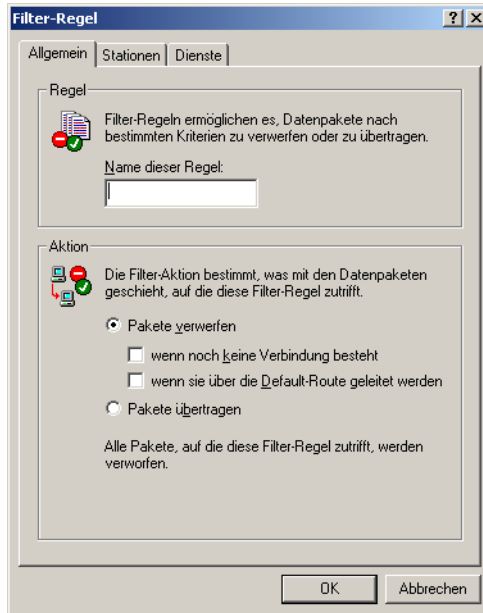
Einrichten der Filter

Die Firewall-Filter werden in folgenden Menüs und Listen konfiguriert:

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	IP-Router ► Filter ► Hinzufügen
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► IP-Router-Modul ► Firewall
Terminal/Telnet	/Setup/IP-Router-Modul/Firewall

Einrichten der Filter unter *ELSA LANconfig*

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



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

Einrichten der Filter mit **ELSA WEBconfig** oder über Terminal/Telnet

Etwas schwieriger als in *ELSA LANconfig* gestaltet sich die Konfiguration über *ELSA WEBconfig* oder über eine Terminal-/Telnet-Verbindung.

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



Die Filter-Liste kann nicht direkt erstellt werden. Sie wird aus den Einträgen in Objekt- und Regel-Tabelle automatisch erzeugt.

Die Objekt-Tabelle

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

- Protokolle
- einzelne Rechner
- ganze Netze
- Dienste

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

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

Die Regel-Tabelle

In der Regel-Tabelle werden die Objekte zu Filterregeln verknüpft. Die Regel-Tabelle enthält das zu filternde Protokoll (das sie in der Objekt-Tabelle definiert haben), die Quell-Objekte, die Ziel-Objekte sowie die auszuführende Filteraktion.

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

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

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

alle Rechner: %A0.0.0.0

alle Dienste: %S0

alle Protokolle: %P0

Hostnamen können nur dann verwendet werden, wenn der *ELSA LANCOM 1600 Office* die Namen in IP-Adressen auflösen kann. Dafür muss der *ELSA LANCOM 1600 Office* die Namen über DHCP oder NetBIOS gelernt haben, oder die Zuordnung muss statisch in der DNS- oder IP-Routing-Tabelle eingetragen sein. Ein Eintrag in der IP-Routing-Tabelle kann dabei einem Hostnamen ein ganzes Netz zuordnen.

Bei der Konfiguration über die Konsole (Telnet oder Terminalprogramm) müssen die kombinierten Parameter (Port, Destination, Source) jeweils in Anführungszeichen (Zollzeichen – ") eingeschlossen werden.

Die Filter-Liste

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



Beachten Sie bitte, dass Filter bei einer Fehlangabe nicht erzeugt und auch keine Fehlermeldungen ausgegeben werden. Wenn Sie die Filter manuell konfigurieren, sollten Sie in jedem Fall überprüfen, ob die gewünschten Filter erzeugt wurden.

6.3

Den ISDN-Zugang absichern

Bei einem Gerät mit ISDN-Anschluss kann sich prinzipiell jeder ISDN-Teilnehmer in Ihren *ELSA LANCOM* einwählen. Um unerwünschte Eindringlinge zu vermeiden, müssen Sie deshalb einen besonderen Augenmerk auf die Absicherung des ISDN-Zugangs legen.



Von den Geräten der Serie ELSA LANCOM 1600 Office verfügt nur der ELSA LANCOM DSL/I-1611 Office über einen ISDN-Anschluss. Die Ausführungen dieses Abschnittes beziehen sich daher nur auf dieses Gerät.

Die Absicherungsfunktionen des ISDN-Zugangs können in zwei Gruppen eingeteilt werden:

- Identifikationskontrolle
 - Zugangsschutz mit Name und Passwort
 - Zugangsschutz über die Anruferkennung
- Rückruf an festgelegte Rufnummern

6.3.1

Die Identifikationskontrolle

Zur Identifikationskontrolle kann entweder der Name der Gegenstelle oder die sogenannte Anruferkennung herangezogen werden. Die Anruferkennung ist die Telefonnummer des Anrufers, die bei ISDN normalerweise mit dem Anruf an die Gegenstelle übermittelt wird.

Welcher „Identifier“ zur Erkennung des Anrufers verwendet werden soll, wird im folgender Liste eingestellt:

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	Kommunikation ► Rufannahme
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► WAN-Modul ► Schutz
Terminal/Telnet	/Setup/WAN-Modul/Schutz

Zur Auswahl stehen die folgenden Möglichkeiten:

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

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

Überprüfung des Namens

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

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

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

Bei PPP wird zunächst ein Benutzername (und in Verbindung mit PAP, CHAP oder MS-CHAP auch ein Passwort) beim Verbindungsaufbau an die Gegenstelle übertragen. Wählt sich ein Computer in den *ELSA LANCOM 1600 Office* ein, so fragt die verwendete Verbindungssoftware, beispielsweise das DFÜ-Netzwerk unter Windows, den zu übermittelnden Benutzernamen und das Passwort in einem Eingabefenster ab.

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

Die PPP-Liste finden Sie wie folgt:

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	Kommunikation ► Protokolle ► PPP-Liste
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► WAN-Modul ► PPP-Liste
Terminal/Telnet	/Setup/WAN-Modul/PPP-Liste

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



Die Sicherungsverfahren PAP, CHAP oder MS-CHAP wenden Sie natürlich nicht an, wenn Sie selber mit dem ELSA LANCOM 1600 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 ...

Wenn das ELSA-Protokoll für den B-Kanal verwendet wird, läuft die Identifizierung ja nur über den Namen, ohne Passwort ab. Der Name ist dabei der Geräte name des anrufenden Routers.

Überprüfung der Nummer

Beim Anruf über eine ISDN-Leitung wird in den meisten Fällen über den D-Kanal die Rufnummer des Anrufers übertragen, schon bevor eine Verbindung zustande kommt (CLI – **C**alling **L**ine **I**dentifier).

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 1600 Office* über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekannten Rufnummern abgelehnt.

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

6.3.2

Der Rückruf

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

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	Kommunikation ► Gegenstellen ► Namenliste (ISDN)
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► WAN-Modul ► ISDN-Namenliste
Terminal/Telnet	/Setup/WAN-Modul/ISDN-Namenliste

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

- Der Router kann den Rückruf ablehnen.
- Es kann eine voreingestellte Rufnummer zurückrufen.
- Er kann zunächst den Namen überprüfen und dann eine voreingestellte Rufnummer zurückrufen.
- Die Rufnummer für den Rückruf kann vom Anrufer frei eingegeben werden.

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

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

Weitere Informationen zum Rückruf finden Sie im Abschnitt 'Rückruf-Funktionen' auf Seite 128.



6.4

Die Sicherheits-Checkliste

In der folgenden Checkliste finden Sie die wichtigsten Sicherheitsfunktionen im Überblick. Damit Sie ganz sicher sein können, nichts Wesentliches bei der Sicherheitskonfiguration Ihres *ELSA LANCOM 1600 Office* übersehen zu haben.

☐ **Haben Sie ein Passwort für die Konfiguration vergeben?**

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'. Es ist insbesondere dann ratsam ein Passwort zur Konfiguration zu vergeben, wenn Sie die Fernkonfiguration erlauben wollen!

☐ **Haben Sie die Fernkonfiguration zugelassen?**

Wenn Sie die Fernkonfiguration nicht benötigen, so schalten Sie sie ab. Wenn Sie die Fernkonfiguration benötigen, so vergeben Sie unbedingt einen Passwortschutz für die Konfiguration (siehe vorhergehender Abschnitt). Das Feld zur Abschaltung der Fernkonfiguration finden Sie ebenfalls in *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'.

○ **Haben Sie die SNMP-Konfiguration mit einem Passwort versehen?**

Schützen Sie auch die SNMP-Konfiguration mit einem Passwort. Das Feld zum Schutz der SNMP Konfiguration mit einem Passwort finden Sie ebenfalls in *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'.

Nur *ELSA LANCOM*
DSL/I-1611 Office

○ **Haben Sie den Remote Access erlaubt?**

Wenn Sie keinen Remote-Access benötigen, schalten Sie die Rufannahme aus, indem Sie in *ELSA LANconfig* im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Rufannahme' eine Rufannahme nach Nummer wählen und die Nummernliste leer lassen.

Nur *ELSA LANCOM*
DSL/I-1611 Office

○ **Haben Sie die Rückrufoptionen für den Remote Access aktiviert, und ist CLI eingeschaltet?**

Beim Anruf über eine ISDN-Leitung wird in den meisten Fällen über den D-Kanal die Rufnummer des Anrufers übertragen, schon bevor eine Verbindung zu Stande kommt (CLI – **C**alling **L**ine **I**dentifier). Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen (dieser Rückruf über den D-Kanal wird vom Windows-DFÜ-Netzwerk nicht unterstützt). Ist ein Schutz im *ELSA LANCOM 1600 Office* über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekannten Rufnummern abgelehnt.

○ **Haben Sie IP-Masquerading aktiviert?**

IP-Masquerading heisst das Versteck für alle lokalen Rechner beim Zugang ins Internet. Dabei wird nur das Router-Modul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet wie eine Wand. Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle finden Sie in *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router'.

○ **Haben Sie kritische Ports über Filter geschlossen?**

Die Firewall-Filter der *ELSA LANCOM 1600 Office* bieten Filterfunktionen für einzelne Rechner oder ganze Netze. Es ist möglich, Quell- und Ziel-Filter für einzelne Ports oder auch Portbereiche aufzusetzen. Zudem können einzelne Protokolle oder beliebige Protokollkombinationen (TCP/UDP/

ICMP) gefiltert werden. Besonders komfortabel ist die Einrichtung der Filter mit Hilfe von *ELSA LANconfig*. Unter 'IP-Router' finden Sie die Karteikarte 'Filter', mit deren Hilfe Filterregeln definiert werden können.

○ **Haben Sie bestimmte Stationen von dem Zugriff auf den Router ausgeschlossen?**

Mit einer speziellen Filter-Liste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfigurationssitzungen über *ELSA LANconfig*, *ELSA WEBconfig*, Telnet oder TFTP 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'.

○ **Lagern Ihre abgespeicherte LANCOM-Konfiguration an einem sicheren Ort, der vor unberechtigtem Zugriff geschützt ist?**

Schützen Sie abgespeicherte Konfigurationen an einem sicheren Ort vor unberechtigtem Zugriff. Eine abgespeicherte Konfiguration könnte sonst von einer unberechtigten Person in ein anderes Gerät geladen werden, wodurch z. B. Ihre Internet-Zugänge auf Ihre Kosten benutzt werden können.

7

Server-Dienste für das LAN

DE

Ein *ELSA LANCOM 1600 Office* bietet eine Reihe von Dienstleistungen für die PCs im LAN an. Es handelt sich dabei um zentrale Funktionen, die von den Arbeitsplatzrechnern genutzt werden können. Im einzelnen handelt es sich um:

- Automatische Adressverwaltung mit DHCP
- Namenverwaltung von Rechnern und Netzwerken mit DNS
- Protokollierung von Netzverkehr mit SYSLOG
- Gebührenerfassung
- Bürokommunikations-Funktionen mit *ELSA LANCAPI* (nur *ELSA LANCOM DSL/I-1611 Office*)

7.1

Automatische IP-Adressverwaltung mit DHCP

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

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

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

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

7.1.1

Der DHCP-Server

ELSA LANCOM 1600 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

- Standard-Gateway
- DNS-Server
- NBNS-Server
- Gültigkeitsdauer der zugewiesenen Parameter

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

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

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

7.1.2

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 LAN-Rx/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'.

7.1.3

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.

Wenn nun ein Rechner im Netz gestartet wird, der mit seinen Netzwerk-Einstellungen über DHCP eine IP-Adresse anfordert, wird ihm ein Gerät mit aktiviertem DHCP-Modul die Zuweisung einer Adresse anbieten. Als IP-Adresse wird dabei eine gültige Adresse aus dem Pool genommen. Wurde dem Rech-

ner 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 des Standard-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.

Zuweisung von DNS- und NBNS-Server

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

Ist bei den entsprechenden Feldern kein Server angegeben, so gibt der Router seine eigene IP-Adresse als DNS-Adresse weiter. Diese wird bestimmt, wie unter 'Zuweisung einer IP-Adresse' beschrieben. Der Router verwendet dann



DNS-Forwarding (siehe auch 'DNS-Forwarding'), um DNS- oder NBNS-Anfragen des Hosts aufzulösen.

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!

Die Voreinstellung 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. Die Voreinstellung 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 98 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.

IP-Adressen im LAN überprüfen

Konfigurationstool	Aufruf/Tabelle
ELSA WEBconfig	Experten-Konfiguration ► Setup ► DHCP-Modul ► Tabelle-DHCP
Terminal/Telnet	Setup/DHCP-Modul/Tabelle-DHCP

Eine Übersicht über die IP-Adressen im LAN gibt die DHCP-Tabelle. Sie zeigt die zugewiesene bzw. verwendete IP-Adresse, die MAC-Adresse, die Gültigkeitsdauer, den Namen des Rechners (falls vorhanden) sowie den Typ der Adresszuweisung.

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

- 'neu'
Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.
- 'unkb.'
Bei der Überprüfung der Eindeutigkeit wurde festgestellt, dass die Adresse bereits an einen anderen Rechner vergeben wurde. Der

DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.

- 'stat.'
Ein Rechner hat dem DHCP-Server mitgeteilt, dass er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr verwendet werden.
- 'dyn.'
Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

7.2

DNS

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

7.2.1

Was macht ein DNS-Server?

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

Ohne DNS-Server im lokalen Netz wird jeder lokal unbekannte Name über die Default-Route gesucht. Durch die Verwendung eines DNS-Servers können alle Namen, die mit ihrer IP-Adresse bekannt sind, direkt bei der richtigen Gegenstelle gesucht werden. Der DNS-Server kann dabei im Prinzip ein separater Rechner im Netz sein. Folgende Gründe sprechen jedoch dafür, den DNS-Server direkt im *ELSA LANCOM 1600 Office* anzusiedeln:

- Ein *ELSA LANCOM 1600 Office* kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbstständig verteilen. Der DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-Server hätte bei der dynamischen Adressvergabe des DHCP-Servers möglicherweise Schwierigkeiten, die Zuordnung zwischen IP-Adresse und Namen aktuell zu halten.

Nur *ELSA LANCOM
DSL/I-1611 Office*

- Beim Routing von Windows-Netzen über NetBIOS kennt ein *ELSA LANCOM 1600 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 1600 Office* kann gleichzeitig als sehr komfortabler Filtermechanismus eingesetzt werden. Anfragen nach bestimmten Domains, die nicht besucht werden dürfen, können durch die einfache Angabe des Domain-Namens für das ganze LAN, nur für Teilnetze (Subnetze) oder sogar für einzelne Rechner gesperrt werden.

Wie reagiert der DNS-Server auf eine Anfrage?

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.
- Schließlich prüft der DNS-Server, ob die Anfrage an einen anderen DNS-Server über ein WAN-Interface an einen anderen DNS-Server weitergeleitet werden soll (Spezielles DNS-Forwarding über die DNS-Destinationstabelle).

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

7.2.2

DNS-Forwarding

Wenn eine Anfrage nicht aus den eigenen DNS-Tabellen bedient werden kann, leitet der DNS-Server die Anfrage an andere DNS-Server weiter. Dieser Vorgang heisst DNS-Forwarding (DNS-Weiterleitung).

Dabei unterscheidet man zwischen

- **Speziellem DNS-Forwarding**
Anfragen nach bestimmten Namensbereichen werden an bestimmte DNS-Server weitergeleitet.
- **Generellem DNS-Forwarding**
Alle anderen nicht näher spezifizierten Namen werden an den „übergeordneten“ DNS-Server weitergeleitet.

Spezielles DNS-Forwarding

Beim Speziellen DNS-Forwarding können Namensbereiche definiert werden, für deren Auflösung festgelegte DNS-Server angesprochen werden.

Ein typischer Anwendungsfall für Spezielles DNS-Forwarding ergibt sich beim Heimarbeitsplatz: Der Benutzer möchte gleichzeitig sowohl auf das firmeneigene Intranet, als auch direkt auf das Internet zugreifen können. Die Anfragen ins Intranet müssen an den DNS-Server der Firma, alle anderen Anfragen an den DNS-Server des Providers geleitet werden.

Generelles DNS-Forwarding

Alle DNS-Anfragen, die nicht auf sonstige Weise aufgelöst werden können, werden an einen DNS-Server weitergeleitet. Dieser DNS-Server bestimmt sich nach folgenden Regeln:

- Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist. Wird er dort fündig, holt er die gewünschte Information von diesem Server. Bis zu zwei übergeordnete DNS-Server können angegeben werden.

<i>ELSA LANconfig</i>	TCP/IP ► Adressen ► Erster DNS-Server / Zweiter DNS-Server
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► TCP/IP-Modul ► DNS-Default / DNS-Backup
Terminal/Telnet	/Setup/TCP-IP-Modul/DNS-Default /Setup/TCP-IP-Modul/DNS-Backup

- Gibt es keinen eingetragenen DNS-Server im Router, versucht er auf einer evtl. bestehenden PPP-Verbindung (z.B. zum Internet-Provider) einen DNS-Server zu erreichen, und holt die Zuordnung der IP-Adresse zum Namen von dort. Das gelingt natürlich nur dann, wenn während der PPP-Verhandlung die Adresse eines DNS-Servers an den Router übermittelt worden ist.
- Besteht keine Verbindung, wird die Default-Route aufgebaut und dort nach dem DNS-Server gesucht.

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

7.2.3

So stellen Sie den DNS-Server ein

Die Einstellungen für den DNS-Server finden Sie im folgenden Menü bzw. in folgender Liste:

Konfigurationstool	Aufruf/Tabelle
<i>ELSA LANconfig</i>	TCP/IP ► DNS-Server
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► DNS-Modul
Terminal/Telnet	<code>cd /Setup/DNS-Modul</code>

Gehen Sie zur Einstellung des DNS-Servers wie folgt vor:

- ① Schalten Sie den DNS-Server ein.

<i>ELSA WEBconfig</i>	... ► Zustand
Terminal/Telnet	<code>set Zustand ein</code>

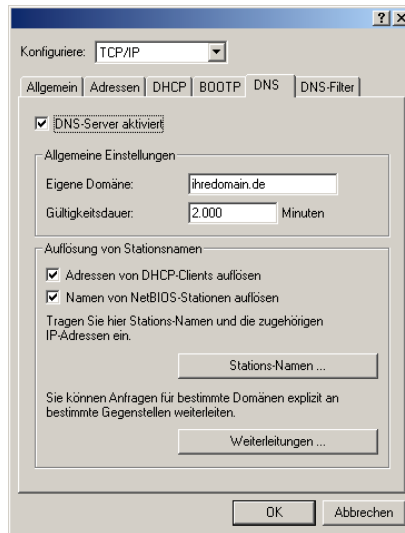
- ② Geben Sie die Domain ein, in der sich der DNS-Server befindet. Mit Hilfe dieser Domain erkennt der DNS-Server bei Anfrage, ob sich der gesuchte

Name im eigenen LAN befindet oder nicht. Die Angabe der Domain ist optional.

<i>ELSA WEBconfig</i>	... ► Domain
Terminal/Telnet	set Domain ihredomain.com

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

<i>ELSA WEBconfig</i>	... ► DHCP-verwenden ... ► NetBIOS-verw.
Terminal/Telnet	set DHCP-verwenden ja set NetBIOS-verw. ja



Aktivierter DNS-Server
in der TCP-IP-Konfiguration

- 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 Stations-Namen-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.

Mit folgenden Befehlen fügen Sie Stationen zur Stations-Namen-Tabelle hinzu:

<i>ELSA LANconfig</i>	TCP/IP ► DNS ► Stations-Namen ► Hinzufügen
<i>ELSA WEBconfig</i>	... ► DNS-Tabelle ► Hinzufügen
Terminal/Telnet	cd Setup/DNS-Modul/DNS-Tabelle set mail.ihredomain.de 10.0.0.99

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:

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 Um ganze Namensbereiche von einem anderen DNS-Server auflösen zu lassen, fügen Sie einen Weiterleitungseintrag bestehend aus Namensbereich und Gegenstelle hinzu:

<i>ELSA LANconfig</i>	TCP/IP ► DNS ► Weiterleitungen ► Hinzufügen
<i>ELSA WEBconfig</i>	... ► DNS-Destinationstabelle ► Hinzufügen
Terminal/Telnet	cd Setup/DNS-Modul/Destinationstabelle set *.intern FIRMA

Bei der Angabe der Namensbereiche dürfen die Wildcards '?' für einzelne Zeichen und '*' für mehrere Zeichen verwendet werden.

Um alle Domains mit der Endung '.intern' auf einen DNS-Server im LAN der Gegenstelle 'FIRMA' umzuleiten, erstellen Sie folgenden Eintrag:



Weiterleitungen - Neuer Eintrag [?] [X]

Domäne: OK

Gegenstelle: Abbrechen

Die IP-Adresse des DNS-Servers muss automatisch von der Gegenstelle per PPP übermittelt werden. Eine manuelle Angabe der IP-Adresse dieses DNS-Servers ist nicht möglich.

- ⑥ Mit der Filterliste können Sie schließlich ganz genau bestimmen, wer auf welche Namen oder Domain nicht zugreifen darf.

Um die Domain (in diesem Fall den Web-Server) 'www.gesperrt.de' für alle Rechner im LAN zu sperren, sind die folgenden Befehle und Eingaben notwendig:

ELSA LANconfig	TCP/IP ► DNS-Filter ► DNS-Filter ► Hinzufügen
ELSA WEBconfig	... ► Filter-Liste ► Hinzufügen
Terminal/Telnet	<pre>cd Setup/DNS-Modul/Filter-Liste set 001 www.gesperrt.de 0.0.0.0 0.0.0.0</pre>

DNS-Filter - Neuer Eintrag [?] [X]

Domäne: OK

IP-Adresse: Abbrechen

Netzmaske:

Der Index '001' im Konsolenbefehl ist frei gewählt und dient lediglich der Übersichtlichkeit. Bei der Eingabe der Domäne sind auch die Wildcards '?' (steht für genau ein Zeichen) und '*' (für beliebig viele Zeichen) erlaubt. Um nur einem bestimmten Rechner (z. B. mit IP 10.0.0.123) den Zugriff auf DE-Domains zu sperren, tragen Sie folgende Werte ein:

DNS-Filter - Neuer Eintrag [?] [X]

Domäne: OK

IP-Adresse: Abbrechen

Netzmaske:

Im Konsolenmodus lautet der Befehl:

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



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

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

7.3

Gebührenmanagement

Die Eigenschaft des Routers, Verbindungen selbständig zu allen gewünschten Gegenstellen aufzubauen und sie mit dem Ende der Übertragung automatisch 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.
- Für ISDN-Verbindungen kann für eine bestimmte Periode ein Gebührenlimit oder ein Zeitlimit festgelegt werden.

*Nur ELSA LANCOM
DSL/I-1611 Office*

7.3.1

Verbindungs-Begrenzung für DSL und Kabelmodem

Auch wenn sich eine DSL- oder eine Kabelmodem-Verbindung wie eine Festverbindung verhält, bei der kein Verbindungsaufbau notwendig ist (und damit auch eigentlich weder Anfang noch Ende der Verbindung erkennbar sind), werden die Kosten je nach Provider zeitabhängig berechnet.



Im weiteren Verlauf dieses Abschnitts wird nur noch von DSL-Verbindungen die Rede sein. Die Ausführungen gelten aber genauso für jede andere Verbindung, die über den 10Base-T-WAN-Anschluss des ELSA LANCOM 1600 Office erfolgt, beispielsweise für Kabelmodem-Verbindungen.

Um die Kosten begrenzen zu können, kann die maximale Verbindungsdauer mit Hilfe der Zeit gesteuert werden. Dazu wird ein Zeit-Limit für DSL-Verbindungen in einer Periode vereinbart. Im Auslieferungszustand dürfen die

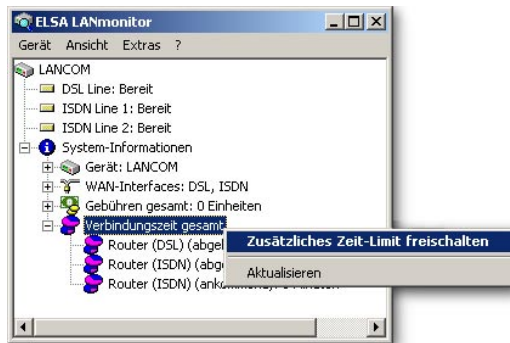
DSL-Verbindungen z.B. für maximal 600 Minuten in sechs Tagen genutzt werden.



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

Wenn Sie für einmalige Aktionen das Online-Budget verlängern wollen, z. B. um eine sehr große Datei aus dem Internet zu laden, müssen Sie nicht unbedingt das Zeit-Limit verändern. Sie können für solche Fälle ein zusätzliches Limit festlegen, das separat aktiviert werden kann.

In *ELSA LANmonitor* aktivieren Sie das zusätzliche Limit über das Kontext-Menü der Gesamtverbindungszeit (rechte Maustaste auf 'Verbindungszeit gesamt' drücken):



Sollten Sie in *ELSA LANmonitor* die System-Informationen nicht sehen, aktivieren Sie die entsprechende Anzeige mit **Ansicht ► Anzeigen ► System-Informationen**.

In *ELSA WEBconfig* und in der Konsole lauten die Befehle zur Freischaltung des zusätzlichen Zeit-Limits:

Konfigurationstool	Aufruf
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► Gebuehren-Modul ► Aktivieren-Reserve
Terminal/Telnet	cd /Setup/Gebuehren-Modul do Aktivieren-Reserve

Bei Aktivierung des zusätzlichen Zeit-Limit wird dieses für die aktuelle Periode freigeschaltet. In der nächsten Periode gilt wieder das normale Zeit-Limit.

7.3.2

Gebührenabhängige ISDN-Verbindungsbegrenzung

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



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



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

7.3.3

Zeitabhängige ISDN-Verbindungsbegrenzung

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

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



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



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

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

7.3.4

Einstellungen im Gebührenmodul

Konfigurationstool	Aufruf/Tabelle
<i>ELSA LANconfig</i>	Management ► Kosten
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► Gebuehren-Modul
Terminal/Telnet	<code>cd /Setup/Gebuehren-Modul</code>

Im Gebührenmodul können Sie die Onlinezeit überwachen und für den Aufbauschutz nutzen.

- Tage/Periode
Dauer einer Überwachungsperiode in Tagen angegeben
- Budget-Einheiten, DSL-/ISDN-Minuten-Budget
Maximale ISDN-Einheiten bzw. DSL-/ISDN-Online-Minuten in einer Überwachungsperiode



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.

7.4

Das SYSLOG-Modul

Mit dem SYSLOG-Modul besteht die Möglichkeit, Zugriffe auf den *ELSA LANCOM 1600 Office* protokollieren zu lassen. Diese Funktion ist insbesondere für Systemadministratoren interessant, da sie die Möglichkeit bietet, eine lückenlose Historie aller Aktivitäten aufzeichnen zu lassen.

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

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

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

7.4.1

Einrichten des SYSLOG-Moduls

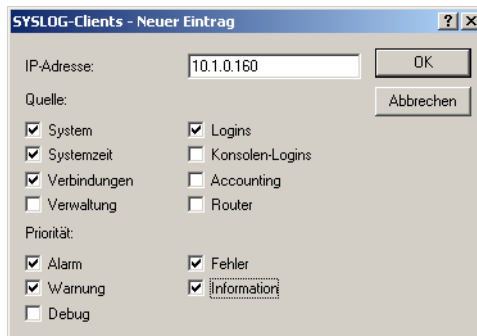
Konfigurationstool	Aufruf/Tabelle
ELSA LANconfig	Management ► Meldungen
ELSA WEBconfig	Experten-Konfiguration ► Setup ► SYSLOG-Modul
Terminal/Telnet	<code>cd /Setup/SYSLOG-Modul</code>

7.4.2

Beispielkonfiguration mit *ELSA LANconfig*

SYSLOG-Client anlegen

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



SYSLOG kommt aus der UNIX-Welt, in der bestimmte Quellen vordefiniert sind. *ELSA LANCOM 1600 Office* ordnet seine eigenen internen

Quellen diesen vordefinierten SYSLOG-Quellen, den sogenannten „Facilitys“, zu.

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller Nachrichtenquellen, die Sie im *ELSA LANCOM 1600 Office* einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die Zuordnung zwischen den internen Quellen des *ELSA LANCOM 1600 Office* und den SYSLOG-Facilitys an.

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

Die im SYSLOG ursprünglich definierten acht Prioritätsstufen sind im *ELSA LANCOM 1600 Office* auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen Alarmlevel, Bedeutung und SYSLOG-Prioritäten.

Priorität	Bedeutung	SYSLOG-Priorität
Alarm	Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne dass ein Eingriff des Administrators notwendig wird (z.B. Verbindungsfehler).	ERROR

Priorität	Bedeutung	SYSLOG-Priorität
Warning	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z.B. Accounting-Informationen).	NOTICE, INFORM
Debug	Übertragung aller Debug-Meldungen. Debug-Meldungen erzeugen ein erhebliches Datenvolumen und beeinträchtigen den ordnungsgemäßen Betrieb des Geräts. Sie sollten daher im Regelbetrieb ausgeschaltet sein und nur zur Fehlersuche verwendet werden.	DEBUG

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

Facilitys

Über die Schaltfläche **Facility-Zuordnung** können alle Meldungen vom *ELSA LANCOM 1600 Office* einer Facility zugeordnet und dadurch vom SYSLOG-Client ohne zusätzlichen Aufwand in eine spezielle Log-Datei geschrieben werden.

Beispiel

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

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

alle Ausgaben des *ELSA LANCOM 1600 Office* in die Datei '/var/log/lancom.log' geschrieben.

7.5

Bürokommunikation mit **ELSA LANCAPI**



Von den Geräten der Serie ELSA LANCOM 1600 Office verfügt nur der ELSA LANCOM DSL/I-1611 Office über einen ISDN-Anschluss. Die Ausführungen dieses Abschnittes beziehen sich daher nur auf dieses Gerät.

Die *ELSA 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 Kommunikations-

programmen her. Diese Programme wiederum stellen den Rechnern Funktionen der Bürokommunikation, wie z.B. ein Fax oder einen Anrufbeantworter, bereit.

Dieser Abschnitt stellt Ihnen die *ELSA LANCAPi* und ihre Anwendung für Aufgaben der Bürokommunikation kurz vor.

7.5.1

Welche Vorteile bietet die *ELSA LANCAPi*?

Der Einsatz der *ELSA LANCAPi* bringt vor allem wirtschaftliche Vorteile. Alle Windows-Arbeitsplätze, die im LAN (Local Area Network) integriert sind, erhalten über die *ELSA LANCAPi* uneingeschränkten Zugriff auf Bürokommunikations-Funktionen wie Fax, Anrufbeantworter, Onlinebanking und Eurofile-transfer. Ohne zusätzliche Hardware an jedem einzelnen Arbeitsplatz werden alle Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsplätzen installiert.

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



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

7.5.2

Installation des *ELSA LANCAPi*-Clients

Die *ELSA LANCAPi* besteht aus zwei Komponenten, einem Server (im *ELSA LANCOM DSL/I-1611 Office*) und einem Client (auf den PCs). Der *ELSA LANCAPi*-Client wird auf allen Rechnern im lokalen Netz installiert, die die Funktionen der *ELSA LANCAPi* nutzen möchten.

- ① Legen sie die *ELSA LANCOM Office*-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' im Hauptverzeichnis der *ELSA LANCOM Office*-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 *ELSA LANCAPi* bereit, alle Aufgaben der Bürokommunikationssoftware zu übernehmen. Die *ELSA LANCAPi* ist nach erfolgreicher Installation als Icon in der Symbolleiste zu sehen. Ein Doppelklick auf dieses Symbol öffnet ein Statusfenster, in dem Sie jederzeit aktuelle Informationen zur *ELSA LANCAPi* abrufen können.

7.5.3

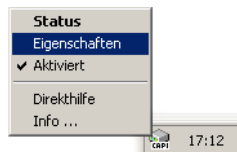
Konfiguration der *ELSA LANCAPi*-Clients

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

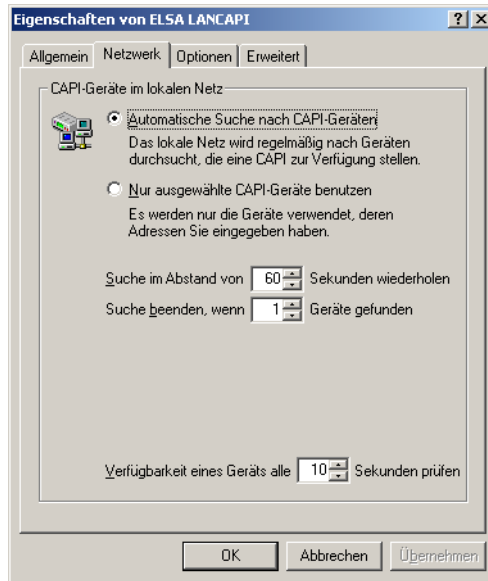
- ① Starten Sie den *ELSA LANCAPi*-Client aus der Programmgruppe 'ELSA-lan'. Auf der Registerkarte 'Allgemein' finden Sie Informationen zum Treiber zum bereitgestellten Dienst.



*Sie können den ELSA LANCAPi-Client auch aus der Windows-Taskleiste heraus aufrufen. Klicken Sie dazu einfach mit der rechten Maustaste auf das ELSA LANCAPi-Symbol in der Windows-Taskleiste neben der Uhr und wählen Sie **Eigenschaften**.*



- ② Wechseln Sie im *ELSA LANCAPi*-Client auf das Register **Netzwerk**. Hier können Sie zunächst wählen, ob der PC seinen *ELSA LANCAPi*-Server selbst suchen soll oder ob ein bestimmter Server verwendet werden soll.
 - Im ersten Fall legen Sie fest, in welchem zeitlichen Intervall der Client nach einem Server sucht. Dabei sucht er so lange, bis er die im nächsten Feld eingestellte Anzahl an Servern gefunden hat. Hat er die geforderte Zahl an Servern gefunden, hört er mit der Suche auf.
 - Wenn der Client nicht automatisch nach Servern suchen soll, geben Sie in der Liste die IP-Adressen der Server an, die der Client verwenden soll. Diese Festlegung ist z.B. dann sinnvoll, wenn Sie mehrere *ELSA LANCOM* in Ihrem LAN als *ELSA 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.



7.5.4

Konfiguration des *ELSA LANCAPI*-Servers

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

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

Der *ELSA LANCAPI*-Server wird in folgenden Menüs konfiguriert:

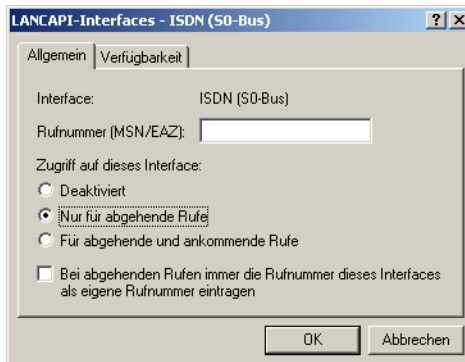
Konfigurationstool	Aufruf/Menü
<i>ELSA LANconfig</i>	LANCAPI
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► LANCAPI-Modul
Terminal/Telnet	cd /Setup/LANCAPI-Modul

Beispielkonfiguration mit *ELSA LANconfig*

- ① Öffnen Sie die Konfiguration des Routers durch einen Doppelklick auf den Gerätenamen in der Liste, und wählen Sie den Konfigurationsbereich **LANCAPI**.
- ② Wählen Sie die ISDN-Schnittstelle, die Sie einstellen wollen.



- ③ Aktivieren Sie den *ELSA LANCAPI*-Server für abgehende und ankommende Rufe, oder lassen Sie nur abgehende Anrufe zu.



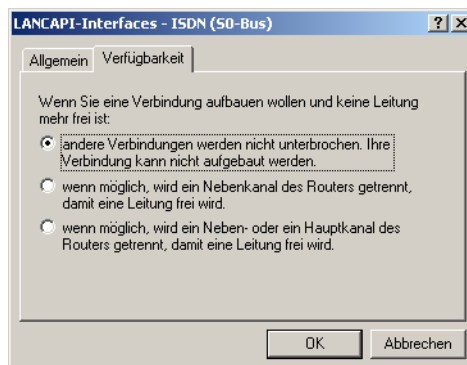
- ④ In diesem Fall reagiert die *ELSA LANCAPI* nicht auf ankommende Rufe und kann z. B. nicht zum Empfangen von Faxmitteilungen eingesetzt werden. Lassen Sie z. B. dann nur abgehende Rufe zu, wenn Sie für die *ELSA LANCAPI* keine eigene Rufnummer frei haben.
- ⑤ Wenn der *ELSA LANCAPI*-Server eingeschaltet ist, geben Sie im Feld 'Rufnummern (MSN/EAZ)' die Telefonnummern ein, auf die *ELSA*

LANCAPI reagieren soll. Mehrere Rufnummern können Sie durch Semikola getrennt eingeben. Wenn Sie hier keine Rufnummer eingeben, werden alle eingehenden Rufe an die *ELSA LANCAPI* gemeldet.

- ⑥ Der von der *ELSA LANCAPI* verwendete IP-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.
- ⑦ Falls nicht alle Rechner aus dem lokalen Netz Zugriff auf die Funktionen der *ELSA LANCAPI* haben sollen, können Sie in der Zugangsliste die berechtigten Teilnehmer (über die IP-Adressen) genau festlegen.

Wenn Sie mehrere Rufnummern für die ELSA 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.

- ⑧ Wechseln Sie auf die Registerkarte 'Verfügbarkeit'. Hier legen Sie fest, wie sich ein *ELSA LANCOM DSL/I-1611 Office* verhält, wenn über die *ELSA LANCAPI* eine Verbindung aufgebaut werden soll (ankommender oder abgehender Ruf), beide B-Kanäle jedoch besetzt sind (Prioritätensteuerung).



Die Bedeutung der angebotenen Optionen:

- 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 *ELSA LANCAP*i 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. Wenn zwei separate Routerverbindungen gleichzeitig zu zwei Gegenstellen aufgebaut sind (zwei Hauptkanäle belegt), muß die *ELSA LANCAP*i warten.
- Die Verbindung über die *ELSA LANCAP*i 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.

7.5.5

So setzen Sie die *ELSA LANCAP*i ein

Zur Verwendung der *ELSA LANCAP*i gibt es zwei Möglichkeiten:

- Sie setzen eine Software ein, die direkt auf einer CAPI-Schnittstelle (in diesem Fall der *ELSA LANCAP*i) 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 *ELSA LANCAP*i den Eintrag 'ISDN WAN Line 1'.

7.5.6

Das *ELSA CAPI Faxmodem*

Mit dem *ELSA CAPI Faxmodem* steht Ihnen unter Windows ein Faxtreiber (Fax Class 1) zur Verfügung, der als Schnittstelle zwischen *ELSA LANCAP*i und Anwendung den Betrieb von Standard-Faxprogrammen mit einem *ELSA LANCOM 1600 Office* ermöglicht.

Installation

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

Faxen über *ELSA CAPI Faxmodem*

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



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

8

Routing und WAN-Verbindungen

Dieses Kapitel beschreibt die wichtigsten Protokolle und Konfigurationseinträge, die bei WAN-Verbindungen eine Rolle spielen. Es zeigt auch Wege auf, WAN-Verbindungen über DSL, Kabelmodem oder ISDN zu optimieren.

8.1

Allgemeines über WAN-Verbindungen

WAN-Verbindungen werden für folgende Anwendungen verwendet.

- Internetzugang über DSL, Kabelmodem oder ISDN
- LAN-LAN-Kopplung über ISDN
- Remote Access über ISDN

8.1.1

Brücken für Standard-Protokolle

WAN-Verbindungen unterscheiden sich von direkten Verbindungen (beispielsweise über die *ELSA LANCAPi*) dadurch, dass die Daten im WAN über standardisierte Netzwerk-Protokolle übertragen werden, die auch im LAN Anwendung finden. Direkte Verbindungen arbeiten hingegen mit proprietären Verfahren, die speziell für Punkt-zu-Punkt-Verbindungen entwickelt worden sind.

Über WAN-Verbindungen wird ein LAN erweitert, bei direkten Verbindungen erhält nur ein einzelner PC eine Verbindung zu einem anderen PC. WAN-Verbindungen bilden gewissermaßen Brücken für die Kommunikation zwischen Netzwerken (bzw. für die Anbindung einzelner Rechner an ein LAN).

Welche Protokolle werden auf WAN-Verbindungen eingesetzt?

Auf WAN-Verbindungen über den Highspeed-Anschluss (für DSL- und Kabelmodem-Verbindungen) werden Pakete nach dem IP-Standard übertragen. Der *ELSA LANCOM DSL/I-1611 Office* unterstützt auf seiner ISDN-Schnittstelle neben IP auch IPX.

Die enge Zusammenarbeit mit den Router-Modulen

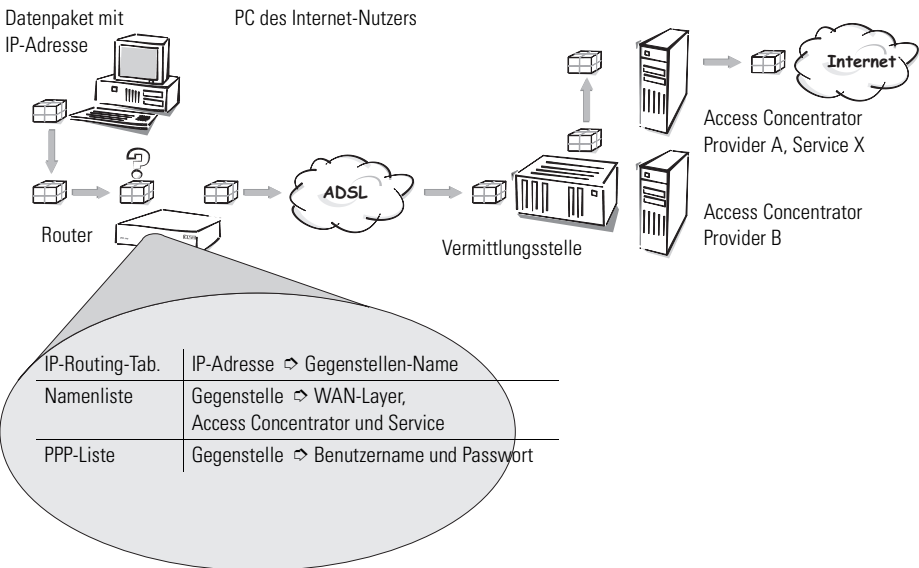
Charakteristisch für WAN-Verbindungen ist die enge Zusammenarbeit mit den Router-Modulen im *ELSA LANCOM*. Die Router-Module (IP und beim *ELSA LANCOM DSL/I-1611 Office* auch IPX) sorgen für die Verbindung von LAN und WAN. Sie bedienen sich der WAN-Module, um Anfragen von PCs aus dem LAN nach externen Ressourcen zu erfüllen.

8.1.2

Was passiert bei einer Anfrage aus dem LAN?

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

Wir wollen diesen Ablauf an einem vereinfachten Beispiel (über ADSL) verdeutlichen. Dabei gehen wir davon aus, dass die IP-Adresse des gesuchten Rechners im Internet bekannt ist.



① Auswahl der richtigen Route

Ein Datenpaket aus einem Rechner findet den Weg ins Internet in erster Linie über die IP-Adresse des Empfängers. Mit dieser Adresse schickt der Rechner das Paket los über das LAN zum Router. Der Router ermittelt in seiner IP-Routing-Tabelle die Gegenstelle, über die die Ziel-IP-Adresse erreichbar ist, z. B. 'Provider_A'.

② Authentifizierungsdaten für die Gegenstelle

Mit diesem Namen prüft der Router dann die Namenliste und findet den Namen des zugehörigen Access Concentrators und des Service, der bei diesem AC in Anspruch genommen werden soll. Außerdem erhält der Router aus der PPP-Liste Benutzernamen und Passwort, die für die Anmeldung beim Provider A notwendig sind.

③ Aufbau der WAN-Verbindung

Der Router kann dann eine Verbindung auf der ADSL-Leitung aufbauen und dabei angeben, dass er eine Verbindung zum Access Concentrator des Providers A haben und dort den Service X nutzen möchte. Er authentifiziert sich mit Benutzernamen und Passwort.

④ Weitergabe des Datenpaketes

Sobald die Verbindung hergestellt ist, kann der Router das Datenpaket über die ADSL-Leitung ins Internet weitergeben.

8.2

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 Abschnitt erfahren Sie, wie die IP-Routing-Tabelle in einem Router von ELSA aufgebaut ist und mit welchen weiteren Funktionen das IP-Routing unterstützt wird.

8.2.1

Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem Router, an welche Gegenstelle (also welchen anderen Router oder Rechner) er die Daten für bestimmte IP-Adressen oder IP-Adress-Bereiche schicken soll. So ein Eintrag heißt auch „Route“, weil der Weg der Datenpakete damit beschrieben wird. Da Sie diese Einträge selbst vornehmen und sie solange unverändert bleiben, bis Sie selbst sie wieder ändern oder löschen, heißt dieses Verfahren auch „statisches Routing“. Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing“. Dabei tauschen die Router selbständig untereinander Informationen über die Routen aus und erneuern diese fortlaufend. Die statische Routing-Tabelle kann bis zu 256 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 Grundein-

stellung für die 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.

Konfiguration der Routing-Tabelle

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	IP-Router ► Routing ► Routing-Tabelle
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► IP-Router-Modul ► IP-Routing-Tab.
Terminal/Telnet	cd /Setup/IP-Router/IP-Routing-Tab.

Eine IP-Routing-Tabelle kann beispielsweise so aussehen:

IP-Adresse	IP-Netzmaske	Router-Name	Distanz	Maskierung
192.168.120.0	255.255.255.0	MAIN	2	Ein
192.168.125.0	255.255.255.0	NODE1	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' und der 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 (private Adressräume, z. B. '10.0.0.0') von der Übertragung ausgeschlossen.

Wird als Router-Name eine IP-Adresse eingetragen, handelt es sich dabei um einen lokal erreichbaren Router, der für die Übertragung der entsprechenden Datenpakete zuständig ist.

- Distanz

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

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

- Maskierung

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

Weitere Informationen finden Sie im Abschnitt 'Das Versteck – IP-Masquerading (NAT, PAT)' auf Seite 63.

8.2.2

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 Standard-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. Dadurch weisen Sie den Router in Ihrem Gerät an, das Datenpaket selbst zum anderen, zuständigen Router zu senden. Außerdem werden dann keine ICMP-Redirects mehr geschickt. Die Einstellung erfolgt unter:

Konfigurationstool	Aufruf
<i>ELSA LANconfig</i>	IP-Router ► Allgemein ► Pakete im lokalen Netz weiterleiten
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► IP-Router-Modul ► Lok.-Routing
Terminal/Telnet	set /Setup/IP-Router/Lok.-Routing Ein

Lokales Routing kann im Einzelfall sehr hilfreich sein, sollte aber auch nur im Einzelfall verwendet werden. Denn lokales Routing 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.

8.2.3

Dynamisches Routing mit IP-RIP

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

Welche Informationen werden über IP-RIP propagiert?

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

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

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

- Solange der Router eine Verbindung zu einer Gegenstelle aufgebaut hat, gibt er alle über diese Route erreichbaren Netze in den RIPs mit der Distanz '1' weiter. Damit werden andere Router im LAN darüber informiert, dass hier bei diesem Router eine bestehende Verbindung zu dieser Gegenstelle genutzt werden kann. So kann zusätzlicher Verbindungsaufbau von Routern mit Wählverbindungen verhindert und ggf. Verbindungskosten reduziert werden.
- Wenn darüber hinaus in diesem Router keine weitere Verbindung zu einer anderen Gegenstelle aufgebaut werden kann, werden alle anderen Routen mit der Distanz '16' im RIP weitergemeldet. Die '16' steht dabei für „Im Moment ist diese Route nicht erreichbar“. Dass ein Router neben der bestehenden Verbindung keine weitere aufbauen kann, liegt an einer der folgenden Ursachen:
 - Auf allen anderen Kanälen ist schon eine andere Verbindung hergestellt (auch über *ELSA LANCAPi*).
 - Die Y-Verbindungen für den S₀-Anschluss sind in der Interface-Tabelle ausdrücklich ausgeschlossen.
 - Die bestehende Verbindung benutzt alle B-Kanäle (Kanalbündelung).

- Bei der bestehenden Verbindung handelt es sich um eine Festverbindung. Nur wenige ISDN-Anbieter ermöglichen es, neben einer Festverbindung auf dem ersten B-Kanal eine Wählverbindung auf dem zweiten B-Kanal aufzubauen.

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

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

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

Was bedeuten die Einträge?

IP-Adresse und Netzmaske bezeichnen das Ziel-Netz, die Distanz gibt die Anzahl der zwischen Sender und Empfänger liegenden Router an, die letzte Spalte zeigt an, welcher Router diese Route 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. Wenn ein Gerät so die Verschlechterung seiner eigenen statischen Routing-Tabelle bekanntmacht (z.B. durch den Abbau einer Verbindung steigt die Distanz von '1' auf '2', siehe unten), dann glaubt der Router ihm das und nimmt den schlechteren Eintrag in seine dynamische Tabelle auf.



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

Zusammenspiel: statische und dynamische Tabelle

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

Router ohne IP-RIP-Unterstützung

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

Skalierung durch IP-RIP

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

Konfiguration der IP-RIP-Funktion

Konfigurationstool	Menü/Tabelle
<i>ELSA LANconfig</i>	IP-Router ► Allgemein ► RIP-Optionen
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► IP-Router-Modul ► RIP-Einstellung
Terminal/Telnet	<code>cd /Setup/IP-Router-Modul/RIP-Einstellung</code>

- Im Feld 'RIP-Unterstützung' (bzw. 'RIP-Typ') gibt es folgende Auswahl:
 - 'Aus': IP-RIP wird nicht verwendet (Standard).
 - 'RIP-1': RIP-1- und RIP-2-Pakete werden empfangen, aber nur RIP-1-Pakete gesendet.
 - 'RIP-1 kompatibel': es werden ebenfalls RIP-1- und RIP-2-Pakete empfangen. Gesendet werden RIP-2-Pakete als IP-Broadcast.
 - 'RIP-2': Wie 'RIP-1 kompatibel', nur werden alle RIP-Pakete an die IP-Multicast-Adresse 224.0.0.9 gesendet.
- Der Eintrag unter 'RIP-1-Maske' (bzw. 'R1-Maske') kann auf folgende Werte gesetzt werden:
 - 'Klasse' (Standard): Die im RIP-Paket verwendete Netzwerkmaske ergibt sich direkt aus der IP-Adress-Klasse, d.h., für die Netzwerk-klassen werden folgende Netzwerkmasken verwendet:

Klasse A	255.0.0.0
Klasse B	255.255.0.0
Klasse C	255.255.255.0

- 'Adresse': Die Netzwerkmaske ergibt sich aus dem 1. gesetzten Bit der eingetragenen IP-Adresse. Dieses und alle höherwertigen Bits innerhalb der Netzwerkmaske werden gesetzt. Aus der IP-Adresse 127.128.128.64 ergibt sich so z.B. die IP-Netzmaske 255.255.255.192.
- 'Klasse+Adresse': Die Netzwerkmaske wird aus der IP-Adressen-Klasse und einem angefügten Teil nach dem Adreßverfahren gebildet. Aus obiger Adresse und der Netzmaske 255.255.0.0 ergibt sich somit die IP-Netzmaske 255.128.0.0.



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.

8.2.4

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.

Policy Based Routing kann wie folgt ein- und ausgeschaltet werden:

Konfigurationstool	Menü/Tabelle
ELSA LANconfig	IP-Router ► Allgemein ► Type-Of-Service-Feld berücksichtigen
ELSA WEBconfig	Experten-Konfiguration ► Setup ► IP-Router-Modul ► Routing-Methode ► Routing-Methode
Terminal/Telnet	cd /Setup/IP-Router-Modul/Routing-Methode set Routing-Methode TOS (ein) set Routing-Methode NORMAL (aus)

8.2.5

SYN/ACK-Speedup

Das SYN/ACK-Speedup-Verfahren dient der Beschleunigung des IP-Datenverkehrs. Beim SYN/ACK-Speedup werden IP-Kontrollzeichen (SYN für Synchronisation und ACK für Acknowledge) innerhalb des Sendebuffers gegenüber einfachen Datenpaketen bevorzugt behandelt. Dadurch wird die Situation vermieden, dass Kontrollzeichen länger in der Sendeschlange hängen bleiben und die Gegenstelle deshalb aufhört, Daten zu senden.

Der größte Effekt tritt beim SYN/ACK-Speedup bei schnellen Verbindung ein, wenn in beiden Richtungen mit hoher Geschwindigkeit Datenmengen übertragen werden.

Werkseitig ist der SYN/ACK-Speedup eingeschaltet.

Ausschalten in Problemfällen

Durch die bevorzugte Behandlung einzelner Pakete wird die ursprüngliche Paketreihenfolge geändert. Obwohl TCP/IP keine bestimmte Paketreihenfolge gewährleistet, kann es in einzelnen Anwendungen zu Problemen kommen. Das betrifft nur Anwendungen, die abweichend vom Protokollstandard

eine bestimmte Paketreihenfolge voraussetzen. Für diesen Fall kann der SYN/ACK-Speedup ausgeschaltet werden:

Konfigurationstool	Menü/Tabelle
<i>ELSA LANconfig</i>	IP-Router ► Allgemein ► TCP SYN- und ACK-Pakete bevorzugt weiterleiten
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► IP-Router-Modul ► Routing-Methode ► SYN/ACK-Speedup
Terminal/Telnet	cd /Setup/IP-Router-Modul/Routing-Methode set SYN/ACK-Speedup AUS

8.3 Die Konfiguration von Gegenstellen

Gegenstellen werden in zwei Tabellen konfiguriert:

- In der Namenliste (bzw. den Namenlisten) werden alle Informationen eingestellt, die individuell für nur eine Gegenstelle gelten.
- Parameter für die unteren Protokollebenen (unterhalb von IP bzw. IPX) werden in der Kommunikations-Layer-Tabelle definiert.



In diesem Abschnitt wird die Konfiguration der Authentifizierung (Protokoll, Benutzername, Passwort) nicht behandelt. Informationen zur Authentifizierung finden Sie im Abschnitt 'Verbindungsaufbau mit PPP' auf Seite 120.

8.3.1 Namenliste

Die verfügbaren Gegenstellen werden in der Namenliste mit einem geeigneten Namen und zusätzlichen Parametern angelegt.

Geräte vom Typ *ELSA LANCOM DSL/I-1611 Office* verfügen über zwei Namenlisten, eine für DSL- (bzw. Kabelmodem-) und eine weitere für ISDN-Gegenstellen. *ELSA LANCOM 1600 Office* ohne ISDN-Anschluss verfügen nur über die DSL-Namenliste.

Konfigurationstool	Menü/Tabelle
<i>ELSA LANconfig</i>	Kommunikation ► Gegenstellen ► Namenliste (DSL) Kommunikation ► Gegenstellen ► Namenliste (ISDN)
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► WAN-Modul ► DSL-Namenliste bzw. ISDN-Namenliste
Terminal/Telnet	<code>cd /Setup/WAN-Modul</code> <code>set DSL-Namenliste [...]</code> <code>set ISDN-Namenliste [...]</code>

- Für eine DSL-Gegenstelle sind folgende Parameter erforderlich:

Namenliste	Parameter	Bedeutung
DSL	Name	Mit diesem Namen wird die Gegenstelle in den Routermodulen identifiziert. Sobald das Routermodul anhand der IP-Adresse ermittelt hat, bei welcher Gegenstelle das gewünschte Ziel erreicht werden kann, können aus der Namenliste die zugehörigen Verbindungsparameter ermittelt werden.
	Haltezeit	Diese Zeit gibt an, wie lange die Verbindung aktiv bleibt, nachdem keine Daten mehr übertragen wurden. Wird eine Null als Haltezeit angegeben, wird die Verbindung nicht automatisch beendet. Bei einer Haltezeit von 9999 Sekunden werden abgebrochen Verbindungen selbstständig wiederhergestellt (siehe 'Dauerverbindung für Flatrates – Keep-Alive' auf Seite 127).
	Access Concentrator	Der Access Concentrator (AC) steht für den Server, der über diese Gegenstelle erreicht werden kann. Stehen mehrere Provider zur Auswahl, die über Ihren ADSL-Anschluss genutzt werden können, wählen Sie mit dem Namen des AC den Provider aus, der für den IP-Adresskreis dieser Gegenstelle zuständig ist. Der Wert für den AC wird Ihnen von Ihrem Provider mitgeteilt. Wird kein Wert für den AC eingetragen, wird jeder AC angenommen, der den geforderten Service anbietet.
	Service	Tragen Sie hier den Dienst ein, den Sie bei Ihrem Provider nutzen möchten. Das kann z. B. einfaches Internet-Surfen sein oder aber auch Video-Downstream. Der Wert für den Service wird Ihnen von Ihrem Provider mitgeteilt. Wird kein Wert für den Service eingetragen, wird jeder Service angenommen, den der geforderte AC anbietet.

Namenliste	Parameter	Bedeutung
ISDN	Layername	Wählen Sie den Kommunikations-Layer aus, der für diese Verbindung verwendet werden soll. Die Konfiguration dieser Layer ist im folgenden Abschnitt beschrieben.
	Name	Wie in der DSL-Namenliste.
	Rufnummer	Eine Rufnummer wird nur benötigt, wenn die Gegenstelle angerufen werden soll. Das Feld kann leer bleiben, wenn lediglich Rufe angenommen werden sollen. Mehrere Rufnummern für dieselbe Gegenstelle können in der Round-Robin-Liste eingetragen werden.
	Haltezeit	Wie in der DSL-Namenliste.
	Haltezeit für Bündelung	Der zweite B-Kanal in einer Bündelung wird abgebaut, wenn er für die eingestellte Dauer nicht benutzt wurde.
	Layername	Wie in der DSL-Namenliste.
	Automatischer Rückruf	Der automatische Rückruf ermöglicht eine sichere Verbindung und senkt die Kosten für den Anrufer. Nähere Informationen finden Sie im Abschnitt 'Rückruf-Funktionen' auf Seite 128.



Werden in der DSL-Namenliste weder Access Concentrator noch Service angegeben, stellt der Router eine Verbindung zum ersten AC her, der sich auf die Anfrage über die Vermittlungsstelle meldet.

8.3.2

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 Kommunikations-Layer finden Sie unter:

Konfigurationstool	Liste
ELSA LANconfig	Kommunikation ► Allgemein ► Kommunikations-Layer
ELSA WEBconfig	Experten-Konfiguration ► Setup ► WAN-Modul ► Layer-Liste
Terminal/Telnet	<code>cd /Setup/WAN-Modul</code> <code>set Layer-Liste [...]</code>

In der Kommunikations-Layer-Liste sind die gängigen Protokollkombinationen bereits vordefiniert. Änderungen oder Ergänzungen sollten Sie nur vorneh-

men, wenn Gegenstellen inkompatibel zu den vorhandenen Layern sind. Die möglichen Optionen finden Sie in der folgenden Übersicht:

Parameter	Bedeutung
Layername	Unter diesem Namen wird der Layer in den Namenlisten ausgewählt.
Encapsulation	Die Datenpakete können oberhalb von Schicht 3 des OSI-Modells zusätzlich als Ethernet-Pakete gekapselt werden. Diese Einstellung ist zur Kommunikation mit älteren <i>ELSA LANCOM</i> -Geräten notwendig. In der Einstellung 'Transparent' werden die Pakete nicht speziell gekapselt.
Layer-3	Folgende Optionen stehen für die Vermittlungsschicht (oder Netzwerkschicht) zur Verfügung:
	'Transparent' Es wird kein zusätzlicher Header eingefügt.
	'PPP' Der Verbindungsaufbau erfolgt nach dem PPP-Protokoll (im synchronen Modus, d. h. bitorientiert). Die Konfigurationsdaten werden der PPP-Tabelle entnommen.
	'AsyncPPP' Wie 'PPP', nur wird der asynchrone Modus verwendet. PPP arbeitet also zeichenorientiert.
	'... mit Script' Alle Optionen können wahlweise mit eigenem Script ausgeführt werden. Das Script wird in der Script-Liste angegeben.
	'ELSA' ELSA-eigenes Verfahren für die Verbindungsverhandlung.
Layer-2	'DHCP' Zuordnung der Netzwerkparameter über DHCP.
	In diesem Feld wird der obere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Folgende Optionen stehen zur Verfügung:
	'Transparent' Es wird kein zusätzlicher Header eingefügt.
	'X.75LAPB' Verbindungsaufbau nach X.75 und LAPM (Link Access Procedure Balanced).
Optionen	'PPPoE' Die PPP-Verhandlung läuft über Ethernet ab. Dazu werden die PPP-Pakete in Ethernet-Frames gekapselt. Dieses Verfahren wird häufig für DSL-Verbindungen benutzt.
	Hier können Sie die Kompression der übertragenen Daten und die Bündelung von Kanälen aktivieren. Die gewählte Option wird nur dann wirksam, wenn sie sowohl von den verwendeten Schnittstellen als auch von den gewählten Layer-2- und Layer-3-Protokollen unterstützt wird. Weitere Informationen finden Sie im Abschnitt 'Kanalbündelung mit MLPPP' auf Seite 132.

Parameter	Bedeutung
Layer-1	In diesem Feld wird der untere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Folgende Optionen stehen zur Verfügung:
'ETH-10'	Transparentes 10-Mbit-Ethernet nach IEEE 802.3.
'HDLC'	Sicherung und Synchronisation der Datenübertragung nach HDLC (im 7- oder 8-Bit-Modus).
'V.110'	Übertragung nach V.110 mit maximal 38.400 bit/Sekunde.

8.4 Verbindungsaufbau mit PPP

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.

8.4.1 Das Protokoll

Was ist PPP?

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

- Passwortschutz nach PAP, CHAP oder MS-CHAP
- Rückruf-Funktionen (nur *ELSA LANCOM DSL/I-1611 Office*)
- Aushandlung der über die aufgebaute Verbindung zu benutzenden Netzwerkprotokolle (z.B. IP). Dazu gehören auch für diese Protokolle notwendige Parameter wie z.B. IP-Adressen. Diese Verhandlung läuft über das Protokoll IPCP (IP Control Protocol) ab.
- Überprüfung der Verbindung mit dem LCP (Link Control Protocol)
- Bündelung von mehreren ISDN-Kanälen (Multilink PPP – nur *ELSA LANCOM DSL/I-1611 Office*)

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

Wozu wird PPP verwendet?

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

- aus Kompatibilitätsgründen z.B. bei Kommunikation mit Fremdroutern
- Remote Access von entfernten Arbeitsplatzrechnern mit ISDN-Adaptern (nur *ELSA LANCOM DSL/I-1611 Office*)
- Internet-Access (mit der Übermittlung von Adressen)

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

Die Phasen einer PPP-Verhandlung

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

● Establish-Phase

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

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

● Authenticate-Phase

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

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

- Network-Phase

Im *ELSA LANCOM 1600 Office* sind die Protokolle IPCP und IPXCP (letzteres nur im *ELSA LANCOM DSL/I-1611 Office*) implementiert.

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

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

- Terminate-Phase

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

Die PPP-Verhandlung im *ELSA LANCOM*

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

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

```
trace + ppp
```

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

8.4.2

Alles o.k.? Leitungsüberprüfung mit LCP

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

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

Verbindung zuverlässig und stabil. Zur dauerhaften Überprüfung der Verbindung wird dieser Request in bestimmten Abständen wiederholt.

Was passiert nun, wenn der Reply ausbleibt? Zuerst werden einige Wiederholungen der Anfrage gestartet, um kurzfristige Störungen der Leitung auszuschließen. Wenn alle diese Wiederholungen unbeantwortet bleiben, wird die Leitung abgebaut und ein Ersatzweg gesucht. Streikt beispielsweise die Highspeed-Verbindung, kann als Backup eine vorhandene ISDN-Schnittstelle den Weg ins Internet bahnen.



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



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

8.4.3

Zuweisung von IP-Adressen über PPP

Zur Verbindung von Rechnern, die TCP/IP als Netzwerkprotokoll einsetzen, benötigen alle Beteiligten eine gültige und eindeutige IP-Adresse. Wenn nun eine Gegenstelle keine eigene IP-Adresse hat (z.B. der einzelne Arbeitsplatzrechner eines Teleworkers), dann kann der *ELSA LANCOM 1600 Office* ihm für die Dauer der Verbindung eine IP-Adresse zuweisen und so die Kommunikation ermöglichen.

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



Die Zuweisung einer IP-Adresse wird nur dann möglich, wenn der ELSA LANCOM 1600 Office die Gegenstelle beim Eintreffen des Anrufs über die Rufnummer oder den Namen identifizieren kann, d.h. die Authentifizierung erfolgreich war.

Beispiele

● Remote Access

Die Zuweisung der Adresse wird durch einen speziellen Eintrag in der IP-Routing-Tabelle ermöglicht. Neben dem Eintrag der IP-Adresse, die der Gegenstelle aus dem Feld 'Router-Name' zugewiesen werden soll, wird als Netzmaske die 255.255.255.255 angegeben. Der Routername ist in diesem Fall der Name, mit dem sich die Gegenstelle beim *ELSA LANCOM 1600 Office* anmelden muss.

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

Damit das Ganze funktioniert, muss die Gegenstelle natürlich auch so eingestellt sein, dass sie die IP-Adresse und die Namensserver vom *ELSA LANCOM 1600 Office* bezieht. Das geschieht z.B. im DFÜ-Netzwerk von Windows durch die Einträge in den 'TCP-Einstellungen' unter 'IP-Adresse' bzw. 'DNS-Konfiguration'. Hier werden die Optionen 'Vom Server zugewiesene IP-Adresse' und 'Vom Server zugewiesene Namensserveradressen' aktiviert.

● Internetzugang

Wird über den *ELSA LANCOM 1600 Office* der Zugang zum Internet für ein lokales Netz realisiert, kann die Zuweisung von IP-Adressen den umgekehrten Weg nehmen. Hierbei sind Konfigurationen möglich, in denen der *ELSA LANCOM 1600 Office* selbst keine im Internet gültige IP-Adresse hat und sich für die Dauer der Verbindung eine vom Internet-Provider zuweisen lässt. Neben der IP-Adresse erhält der *ELSA LANCOM 1600 Office* während der PPP-Verhandlung auch Informationen über DNS-Server beim Provider.

Im lokalen Netz ist der *ELSA LANCOM 1600 Office* nur mit seiner intern gültigen Intranet-Adresse bekannt. Alle Arbeitsplatzrechner im lokalen Netz können dann auf den gleichen Internet-Account zugreifen und auch z.B. den DNS-Server erreichen.

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

8.4.4 Einstellungen in der PPP-Liste

In der PPP-Liste können Sie für jede Gegenstelle, die mit Ihrem Netz Kontakt aufnimmt, eine eigene Definition der PPP-Verhandlung festlegen.

Konfigurationstool	Liste
<i>ELSA LANconfig</i>	Kommunikation ► Protokolle ► PPP-Liste
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► WAN-Modul ► PPP-Liste
Terminal/Telnet	<code>cd /Setup/WAN-Modul</code> <code>set PPP-Liste [...]</code>

Die PPP-Liste kann bis zu 64 Einträge aufnehmen und die folgende Werte enthalten:

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

In dieser Spalte der PPP-Liste tragen Sie folgende Werte ein:
Wiederholungen (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 <i>ELSA LANconfig</i> , SNMP oder TFTP verändert werden!

8.5

DSL-Verbindungsaufbau mit PPTP

Immer mehr DSL-Anbieter ermöglichen die Einwahl nicht nur über PPPoE, sondern auch über PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol). Bei diesem PPTP handelt es sich um eine Protokoll-Erweiterung von PPP, die vorrangig von Microsoft entwickelt wurde.

PPTP ermöglicht es, „Tunnel“ über IP-Netze zu einer Gegenstelle aufzubauen. Unter einem Tunnel versteht man eine logisch abgeschirmte Verbindung, die die übertragenen Daten vor dem unbefugten Zugriff Dritter schützen soll. Dazu wird der Verschlüsselungsalgorithmus RC4 eingesetzt.

Konfiguration von PPTP

Im *ELSA LANCOM 1600 Office* werden alle notwendigen PPTP-Parameter vom Internetzugangs-Assistenten abgefragt, sobald der Internetzugang über PPTP ausgewählt wird. Zusätzlich zu den Eingaben, die auch beim normalen PPPoE-Zugang abgefragt werden, ist dabei nur die IP-Adresse des PPTP-Gateways anzugeben. Beim PPTP-Gateway handelt es sich zumeist um das DSL-Modem. Genauere Informationen stellt Ihnen Ihr DSL-Anbieter zur Verfügung.

Änderungen an der Konfiguration werden in der PPTP-Liste vorgenommen:

Konfigurationstool	Liste
<i>ELSA LANconfig</i>	Kommunikation ► Protokolle ► PPTP-Liste
<i>ELSA WEBconfig</i>	Experten-Konfiguration ► Setup ► WAN-Modul ► PPTP-Liste
Terminal/Telnet	cd /Setup/WAN-Modul set PPTP-Liste [...]

Die PPTP-Konfiguration besteht aus drei Parametern:

- 'Gegenstelle' – Die Bezeichnung aus der DSL-Namensliste.
- 'IP-Adresse' – IP-Adresse des PPTP-Gateways, zumeist die Adresse des DSL-Modems
- 'Port' – IP-Port, über den das PPTP-Protokoll läuft. Dem Protokollstandard gemäß sollte immer Port '1.723' angegeben sein.

8.6

Dauerverbindung für Flatrates – Keep-Alive

Als Flatrates bezeichnet man pauschale Verbindungsstarifen, die nicht nach Verbindungszeiten, sondern pauschal für feste Perioden abgerechnet werden. Bei Flatrates lohnt sich der Verbindungsabbau nicht mehr. Im Gegenteil: Neue Mails sollen direkt am PC gemeldet werden, der Heimarbeitsplatz soll kontinuierlich mit dem Firmennetzwerk verbunden sein und man möchte für Freunde und Kollegen über Internet Messenger Dienste (ICQ und ähnliche) pausenlos erreichbar sein. Es ist also wünschenswert, dass Verbindungen ununterbrochen aufrecht gehalten werden.

Beim *ELSA LANCOM 1600 Office* sorgt das Keep-Verfahren dafür, dass Verbindungen immer dann aufgebaut werden, wenn die Gegenstelle sie gekappt hat.

Konfiguration des Keep-Alive-Verfahrens

Das Keep-Alive-Verfahren wird in den Namenslisten (für DSL und beim *ELSA LANCOM DSL/I-1611 Office* auch für ISDN) konfiguriert.

Wird die Haltezeit auf 0 Sekunden gesetzt, so wird die Verbindung nicht aktiv vom *ELSA LANCOM 1600 Office* beendet. Der automatische Abbau von Verbindungen, über die längere Zeit keine Daten mehr übertragen wurden, wird mit einer Haltezeit von 0 Sekunden deaktiviert. Unterbrochene Verbindungen werden in dieser Einstellung allerdings nicht automatisch wiederhergestellt.

Bei einer Haltezeit von 9999 Sekunden wird die Verbindung immer dann wiederhergestellt, wenn sie ursprünglich von der eigenen Seite aufgebaut wurde und die Gegenseite sie abgebaut hat.

8.7

Rückruf-Funktionen

Der *ELSA LANCOM DSL/I-1611 Office* unterstützt über seine ISDN-Schnittstelle den automatischen Rückruf.



Von den Geräten der Serie ELSA LANCOM 1600 Office verfügt nur der ELSA LANCOM DSL/I-1611 Office über einen ISDN-Anschluss. Die Ausführungen dieses Abschnittes beziehen sich daher nur auf dieses Gerät.

Neben dem Rückruf über den D-Kanal wird auch das von Microsoft spezifizierte CBCP (**C**allback **C**ontrol **P**rotocol) sowie der Rückruf über PPP nach RFC 1570 (PPP LCP Extensions) angeboten. Zusätzlich besteht die Möglichkeit eines besonders schnellen Rückrufs über ein von ELSA entwickeltes Verfahren. PCs mit Windows-Betriebssystem können nur über das CBCP zurückgerufen werden.

8.7.1

Rückruf nach Microsoft CBCP

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

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

Über das CBCP ist es möglich, von einem Rechner mit einem Windows-Betriebssystem eine Verbindung zum *ELSA LANCOM DSL/I-1611 Office* aufzunehmen und sich von diesem zurückrufen zu lassen. Die drei möglichen Einstellungen werden über den Rückruf-Eintrag sowie den Rufnummern-Eintrag in der ISDN-Namenliste ausgewählt.

Namenliste (ISDN) - Neuer Eintrag

Name:

Rufnummer:

Haltezeit: Sekunden

Haltezeit für Bündelung: Sekunden

Layername:

Automatischer Rückruf:

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

Keinen Rückruf durchführen

Für diese Einstellung muss der Rückruf-Eintrag bei der Konfiguration über *ELSA WEBconfig* oder in der Konsole den Wert 'Aus' haben.

Rückrufnummer vom Anrufer bestimmt

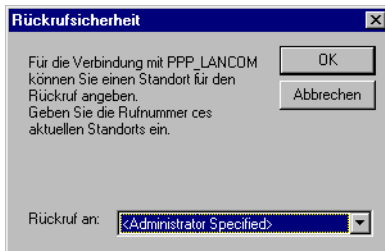
Für diese Einstellung muss der Rückruf-Eintrag auf 'Die Gegenstelle nach Überprüfung des Namens zurückrufen' stehen (bzw. in *ELSA WEBconfig* oder in der Konsole den Wert 'Name' haben). In der Namenliste darf **keine** Rufnummer angegeben sein.

Nach der Authentifizierung erscheint beim Anrufer in Windows ein Eingabefenster, das ihn nach der ISDN-Rufnummer des PC fragt.

Rückrufnummer im *ELSA LANCOM DSL/I-1611 Office* bestimmt

Für diese Einstellung muss der Rückruf-Eintrag auf 'Die Gegenstelle nach Überprüfung des Namens zurückrufen' stehen (bzw. in *ELSA WEBconfig* oder in der Konsole auf den Wert 'Name' gesetzt sein). In der Namenliste muss **eine** Rufnummer angegeben sein.

Einige Windows-Versionen (insbesondere Windows 98) fordern den Benutzer mit einem Eingabefenster auf, den Rückruf an die im *ELSA LANCOM DSL/I-1611 Office* hinterlegte Rufnummer ('Administrator Specified') zu bestätigen. Andere Windows-Version informieren den Benutzer nur darüber, dass der PC auf den Rückruf vom *ELSA LANCOM DSL/I-1611 Office* wartet.



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

8.7.2

Schneller Rückruf mit dem ELSA-Verfahren

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

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



Für den schnellen Rückruf nach ELSA-Verfahren muss die Nummernliste für die Rufannahme auf beiden Seiten gepflegt sein.

8.7.3

Rückruf nach RFC 1570 (PPP LCP Extensions)

Der Rückruf nach 1570 ist das Standardverfahren für den Rückruf von Routern anderer Hersteller. Diese Protokollerweiterung beschreibt fünf Möglichkeiten, einen Rückruf anzufordern. Alle Versionen werden vom *ELSA LANCOM DSL/I-1611 Office* akzeptiert. Es wird jedoch bei allen Varianten gleich verfahren:

Der *ELSA LANCOM DSL/I-1611 Office* baut nach der Authentifizierung der Gegenstelle die Verbindung ab und ruft diese dann einige Sekunden später zurück.

Konfiguration

Für den Rückruf nach PPP wählen Sie in *ELSA LANconfig* die Option 'Die Gegenstelle zurückrufen' bzw. 'Auto' bei Konfiguration über *ELSA WEBconfig*, Terminalprogramm oder Telnets.



Für den Rückruf nach PPP muss die Nummernliste für die Rufannahme im ELSA LANCOM DSL/I-1611 Office gepflegt sein.

8.7.4

Konfiguration der Rückruf-Funktion im Überblick

In der ISDN-Namenliste stehen unter *ELSA WEBconfig* und Terminalprogramm/Telnets für den Rückruf-Eintrag folgende Optionen zur Verfügung:

Mit diesem Eintrag stellen Sie den Rückruf so ein:
'Aus'	Es wird nicht zurückgerufen.
'Auto' (nicht bei Windows-Betriebssystemen, s.u.)	Wenn die Gegenstelle in der Nummernliste gefunden wird, so wird diese zurückgerufen. Hierzu wird der Ruf zunächst abgelehnt und, sobald der Kanal wieder frei ist, zurückgerufen (Dauer ca. 8 Sekunden). Wird die Gegenstelle nicht in der Nummernliste gefunden, so wird sie zunächst als DEFAULT-Gegenstelle angenommen, und der Rückruf wird während der Protokollverhandlung ausgehandelt. Dabei fällt eine Gebühr von einer Einheit an.
'Name'	Bevor ein Rückruf erfolgt, wird immer eine Protokollverhandlung durchgeführt, auch wenn die Gegenstelle in der Nummernliste gefunden wurde (z.B. für Rechner mit Windows, die sich auf dem Gerät einwählen). Dabei fallen geringe Gebühren an.
'ELSA'	Wenn die Gegenstelle in der Nummernliste gefunden wird, wird der schnelle Rückruf durchgeführt, d.h., der <i>ELSA LANCOM 1600 Office</i> sendet ein spezielles Signal zur Gegenstelle und ruft sofort zurück, wenn der Kanal wieder frei ist. Nach ca. 2 Sekunden steht die Verbindung. Nimmt die Gegenstelle den Ruf nicht unmittelbar nach dem Signal zurück, so erfolgt zwei Sekunden später ein Rückfall auf das normale Rückrufverfahren (Dauer wieder ca. 8 Sekunden). Dieses Verfahren steht nur an DSS1-Anschlüssen zur Verfügung.

Mit diesem Eintrag stellen Sie den Rückruf so ein:
'Looser'	Benutzen Sie die Option 'Looser', wenn von der Gegenstelle ein Rückruf erwartet wird. Diese Einstellung erfüllt zwei Aufgaben gleichzeitig. Zum einen sorgt sie dafür, dass ein eigener Verbindungsaufbau zurückgenommen wird, wenn ein Ruf von der gerade angerufenen Gegenstelle hereinkommt, zum anderen wird mit dieser Einstellung die Funktion aktiviert, auf das schnelle Rückruf-Verfahren reagieren zu können. D.h., um den schnellen Rückruf nutzen zu können, muss sich der Anrufer im 'Looser'-Modus befinden, während beim Angerufenen der Rückruf auf 'ELSA' eingestellt sein muss.



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



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

8.8

Kanalbündelung mit MLPPP

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



Von den Geräten der Serie ELSA LANCOM 1600 Office verfügt nur der ELSA LANCOM DSL/I-1611 Office über einen ISDN-Anschluss. Die Ausführungen dieses Abschnittes beziehen sich daher nur auf dieses Gerät.

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

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

Zwei Methoden der Kanalbündelung

- Statische Kanalbündelung

Wenn eine Verbindung mit statischer Kanalbündelung aufgebaut wird, versucht der *ELSA LANCOM DSL/I-1611 Office* nach dem ersten B-Kanal sofort, auch den zweiten B-Kanal aufzubauen. Gelingt dies nicht, weil z.B. dieser Kanal schon durch ein anderes Gerät oder durch eine andere Verbindung im *ELSA LANCOM DSL/I-1611 Office* besetzt ist, wird dieser Aufbauversuch automatisch und regelmäßig solange wiederholt, bis auch der zweite Kanal für diese Verbindung zur Verfügung steht.

- Dynamische Kanalbündelung

Bei einer Verbindung mit dynamischer Kanalbündelung baut der *ELSA LANCOM DSL/I-1611 Office* zunächst nur einen B-Kanal auf und beginnt mit der Datenübertragung. Wenn er dann während der Verbindung feststellt, dass der Durchsatz eine Weile über einem bestimmten Schwellwert liegt, versucht er den zweiten Kanal dazuzunehmen.

Wenn der zweite Kanal aufgebaut ist und der Datendurchsatz wieder unter den Grenzwert zurückgeht, wartet der *ELSA LANCOM DSL/I-1611 Office* noch die eingestellte B2-Haltezeit ab und schließt den Kanal dann automatisch wieder. Dabei werden die begonnenen Gebühreneinheiten ausgenutzt, sofern die Gebühreninformationen während der Verbindung übermittelt werden. Der *ELSA LANCOM DSL/I-1611 Office* benutzt den zweiten B-Kanal also nur, wenn und solange er ihn auch wirklich braucht!

So stellen Sie die Kanalbündelung ein

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

- ① Wählen für die Gegenstelle einen Kommunikations-Layer aus der Layer-Liste aus, der in den Layer-2-Optionen die Bündelung aktiviert hat. Wählen Sie unter folgenden Layer-2-Optionen:
 - **compr.** nach dem LZS-Datenkompressionsverfahren (Stac) reduziert das Datenvolumen, wenn die Daten nicht schon vorher komprimiert waren. Dieses Verfahren wird auch von Routern anderer Hersteller und von ISDN-Adaptern unter Windows-Betriebssystemen unterstützt.
 - **buendeln** verwendet zwei B-Kanäle für eine Verbindung.

- **bnd+cmpr** nutzt beides (Komprimierung und Kanalbündelung) und stellt damit die maximal mögliche Übertragungsleistung zur Verfügung.
- ② Erstellen Sie nun einen neuen Eintrag in der ISDN-Namenliste. Achten Sie dabei auf die Haltezeiten für die Verbindung. Beachten Sie folgende Regeln:
 - Die B1-Haltezeit sollte je nach Anwendungsfall so groß gewählt werden, dass die Verbindung nicht durch das kurzzeitige Ausbleiben von Paketen zu früh abgebaut wird. Erfahrungsgemäß sind Werte zwischen 60 und 180 Sekunden für den Beginn eine gute Basis, die man im Betrieb dann weiter anpassen kann.
 - Die B2-Haltezeit entscheidet darüber, ob es sich um eine statische oder dynamische Kanalbündelung handelt (siehe oben). Mit einer B2-Haltezeit von '0' oder '9999' wird die Bündelung statisch, mit Werten dazwischen schaffen Sie die Möglichkeit der dynamischen Kanalbündelung. Die B2-Haltezeit definiert, wie lange der Datendurchsatz unter der Schwelle für die dynamische Kanalbündelung liegen darf, ohne dass der zweite B-Kanal automatisch abgebaut wird.
- ③ Legen Sie in der Router-Interface-Liste mit dem Eintrag für die Y-Verbindung fest, was geschehen soll, wenn während einer laufenden Verbindung mit Kanalbündelung der Wunsch nach einer zweiten Verbindung zu einer anderen Gegenstelle angemeldet wird.

ELSA WEBconfig	Experten-Konfiguration ► Setup ► WAN-Modul ► Router-Interface-Liste
Terminal/Telnet	cd /Setup/WAN-Modul set Router-Interface-Liste [...]

- Y-Verbindung **Ein**: Der Router unterbricht die Bündelverbindung, um die zweite Verbindung zur anderen Gegenstelle aufzubauen. Wenn der zweite Kanal wieder frei wird, holt sich die Bündelverbindung diesen Kanal automatisch wieder zurück (bei statischer Bündelung immer, bei dynamischer nur bei Bedarf).
- Y-Verbindung **Aus**: Der Router hält die bestehende Bündelverbindung, die zweite Verbindung muss warten.



Bitte beachten Sie, dass bei Verwendung der Kanalbündelung die Kosten für zwei Verbindungen anfallen. Dabei sind keine weiteren Verbindungen über die ELSA LANCAPI möglich! Setzen Sie die Kanalbündelung also nur dann

ein, wenn die doppelte Übertragungsleistung auch tatsächlich ausgenutzt werden kann.

9

Technische Daten

9.1

Leistungs- und Kenndaten

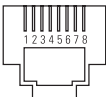
	<i>ELSA LANCOM 1600 Office</i>
Funktionsarten	alle Geräte: IP-Router, DNS-Server, DHCP-Server; gleichzeitiger Betrieb aller Funktionsarten möglich zusätzlich <i>ELSA LANCOM DSL/I-1611 Office</i> : IPX-Router, CAPI-Server, Least-Cost-Router für Router- und CAPI-Verbindungen
10Base-T-WAN-Anschluss	Ethernet IEEE 802.3, 10Base-T (RJ45) mit PPP-over-Ethernet (PPPoE) oder PPTP als Kommunikationsprotokoll
ISDN-Schnittstelle (nur <i>ELSA LANCOM DSL/I-1611 Office</i>)	Anschluss: ISDN-S _g -Bus, Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-Konfiguration, I.430; D-Kanal: 1TR6, Euro-ISDN (DSS1), Autosensing, optional Festverbindungsunterstützung Gruppe 0 (D64S, D64S2, D64SY); B-Kanal: PPP (asynch./synch.), MLPPP, X.75, HDLC, V.110, CAPI 2.0 über <i>ELSA LANCAPI</i> , Stac-Datenkompression
LAN-Anschluss	Ethernet IEEE 802.3, 10/100Base-TX (RJ45, Node/Hub, Switch), Autosensing, Vollduplex
Netzwerk-Protokolle	alle Geräte: IP-Router: ARP, Proxy ARP, DHCP-Server, IP, ICMP, UDP, TCP, RIP-1, RIP-2, Proxy DNS zusätzlich <i>ELSA LANCOM DSL/I-1611 Office</i> : Proxy NetBIOS/IP IPX-Router: IPX, SPX, RIP, SAP, Novell NetBIOS, Novell-Burst-Mode
Security-Funktionen	alle Geräte: PAP, CHAP und MS-CHAP zur Beglaubigung unter PPP; Filtermöglichkeiten im Router-Betrieb, Schutz der Konfiguration über Zugangslisten und Passwort, Aufzeichnung der letzten Verbindungsinformationen, IP-Masquerading zusätzlich <i>ELSA LANCOM DSL/I-1611 Office</i> : Auswertung der Rufnummer der Gegenstelle (CLIP); automatischer Rückruf über ISDN;
Filter-Möglichkeiten (Firewall)	alle Geräte: IP-Router: Quell- und Zielfilter für Netzwerke, Protokolle und Ports, MAC-Adress-Filter zusätzlich <i>ELSA LANCOM DSL/I-1611 Office</i> – IPX-Router: RIP, SAP, IPX- und SPX-Watchdog, Sockets, Routen, Propagated Packets
IP-Masquerading	Übersetzung von internen IP-Adressen und Ports auf eine externe IP-Adresse; statische/dynamische Zuweisung der IP-Adresse via PPP; Maskierung von TCP, UDP, ICMP und FTP; DNS-Forwarding; inverse Maskierung für Dienste im Intranet wie z.B. Web-Server (DMZ)
Spoofing (nur <i>ELSA LANCOM DSL/I-1611 Office</i>)	IPX-Router: RIP- und SAP-Packets; IPX- und SPX-Watchdogs, Novell NetBIOS, Keep-alive-Packets

	ELSA LANCOM 1600 Office
CAPI-Server (nur <i>ELSA LANCOM DSL/I-1611 Office</i>)	virtuelle CAPI 2.0 für Windows-Betriebssysteme, NDIS-WAN-Treiber, Fax-Class 1
Leistungssteuerung, Übertragungsoptimierung	alle Geräte: Keep-Alive auf WAN-Verbindungen, Policy Based Routing, SYN/ACK-Speedup zusätzlich <i>ELSA LANCOM DSL/I-1611 Office</i> – automatischer Rückruf über ISDN mit oder ohne Verbindungsaufbau; Line-on-Demand (dynamische Kanalbündelung), Short-Hold-Modus, Round-Robin-Auswahl, Fast Call Back, Dial-Backup für Festverbindungen
Gebührenschatz	Maximale Onlinezeit oder Gebühren pro Periode
Management	alle Geräte: via LAN oder V.24, Managementsoftware <i>ELSA LANconfig</i> und <i>ELSA LANmonitor</i> für Windows, Konfiguration über SNMP v.1, TFTP, Telnet oder Terminal möglich zusätzlich <i>ELSA LANCOM DSL/I-1611 Office</i> – via ISDN (Fernwartung)
Betriebssicherheit	Hardware-Watchdogs, regelmäßige Selbsttests, <i>ELSA FirmSafe</i> -Konzept für Remote-Software-Upgrade
Statistiken	Zähler für LAN/WAN getrennt, Pakete, Fehler, Verbindungen und Online-Zeit; Logging der Verbindungssteuerung und Online-Zeit mit <i>ELSA LANmonitor</i> und SYSLOG; Accounting der Verbindungen, Online-Zeit, Volumen pro IP mit <i>ELSA LANmonitor</i> ; Trace von Protokollen zur Diagnose
Anzeigen/Bedienung	LEDs für Power, WAN- und LAN-Status, Security/VPN; Reset-Schalter, Node/Hub-Schalter
Stromversorgung	12 V AC mit Steckernetzteil für 230 V, 12 VA
Umgebungsbedingungen	Temperatur: 5–40°C, Luftfeuchtigkeit: 0–80%, nicht kondensierend
Ausführung und Maße	stabiles Metallgehäuse, Anschlüsse auf der Rückseite; Abmessungen 230 x 38 x 228 mm (B x H x T)
Lieferumfang	Netzteil, Kabel für Outband-Schnittstelle, ISDN-Anschlusskabel (nur <i>ELSA LANCOM DSL/I-1611 Office</i>), zwei LAN-Twisted-Pair-Kabel, ausführliche Dokumentation und <i>ELSA LANCOM Office-CD</i> ; <i>ELSA LANconfig</i> , <i>ELSA LANmonitor</i> , <i>ELSA LANCAPI</i> , ELSA CAPI Faxmodem, Bürokommunikationssoftware ELSA-RVS-COM, LapLink Pro
Zulassungen	für Deutschland, Schweiz und alle Länder der EU
Service und Garantie	6 Jahre Garantie
Support	über Hotline und Internet

9.2 Anschlussbelegung

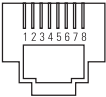
9.2.1 Ethernet-Schnittstellen 10/100Base-T (LAN) und 10Base-T (WAN)

8-polige RJ45-Buchsen, entsprechend ISO 8877, EN 60603-7

Steckverbindung	RJ45-Pin	Leitung
	1	T+
	2	T-
	3	R+
	4	–
	5	–
	6	R-
	7	–
	8	–

9.2.2 ISDN-S₀-Schnittstelle


8-polige RJ45-Buchse, entsprechend ISO 8877, EN 60603-7

Steckverbindung	RJ45-Pin	Leitung	IAE
	1	–	–
	2	–	–
	3	T+	2a
	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	–	–
	8	–	–

9.2.3

Konfigurationsschnittstelle (Outband)

8-polige Mini-DIN-Buchse

Steckverbindung	Mini-DIN 8polig	Leitung
	1	CTS
	2	RTS
	3	RxD
	4	RI
	5	TxD
	6	DSR
	7	DCD
	8	DTR
	U	GND

Allgemeine Garantiebedingungen

Diese Garantie vom 01.06.1998 gewährt die ELSA AG den Erwerbern von ELSA-Produkten nach ihrer Wahl zusätzlich zu den ihnen zustehenden gesetzlichen Gewährleistungsansprüchen nach Maßgabe der folgenden Bedingungen:

1 Garantieumfang

- a) Die Garantie erstreckt sich auf das gelieferte Gerät mit allen Teilen. Sie wird in der Form geleistet, daß Teile, die nachweislich trotz sachgemäßer Behandlung und Beachtung der Gebrauchsanweisung aufgrund von Fabrikations- und/oder Materialfehlern defekt geworden sind, nach unserer Wahl kostenlos ausgetauscht oder repariert werden. Alternativ hierzu behalten wir uns vor, das defekte Gerät gegen ein Nachfolgeprodukt auszutauschen oder dem Käufer den Original-Kaufpreis gegen Rückgabe des defekten Geräts zu erstatten. Handbücher und evtl. mitgelieferte Software sind von der Garantie ausgeschlossen.
- b) Die Kosten für Material und Arbeitszeit werden von uns getragen, nicht aber die Kosten für den Versand vom Erwerber zur Service-Werkstätte und/oder zu uns.
- c) Ersetzte Teile gehen in unser Eigentum über.
- d) Wir sind berechtigt, über die Instandsetzung und den Austausch hinaus technische Änderungen (z.B. Firmware-Updates) vorzunehmen, um das Gerät dem aktuellen Stand der Technik anzupassen. Hierfür entstehen dem Erwerber keine zusätzlichen Kosten. Ein Rechtsanspruch hierauf besteht nicht.

2 Garantiezeit

Die Garantiezeit beträgt für dieses ELSA-Produkt sechs Jahre. Die Garantiezeit beginnt mit dem Tag der Lieferung des Gerätes durch den ELSA-Fachhändler. Garantieleistungen bewirken weder eine Verlängerung der Garantiefrist, noch setzen sie eine neue Garantiefrist in Lauf. Die Garantiefrist für eingebaute Ersatzteile endet mit der Garantiefrist für das ganze Gerät.

3 Abwicklung

- a) Zeigen sich innerhalb der Garantiezeit Fehler des Gerätes, so sind Garantieansprüche unverzüglich, spätestens jedoch innerhalb von sieben Tagen geltend zu machen.
- b) Transportschäden, die äußerlich erkennbar sind (z.B. Gehäuse beschädigt), sind unverzüglich gegenüber der Transportperson und uns geltend zu machen. Äußerlich nicht erkennbare Schäden sind unverzüglich nach Entdeckung, spätestens jedoch innerhalb von sieben Tagen nach Anlieferung, schriftlich gegenüber der Transportperson und uns zu reklamieren.
- c) Der Transport zu und von der Stelle, welche die Garantieansprüche entgegennimmt und/oder das instandgesetzte Gerät austauscht, geschieht auf eigene Gefahr und Kosten des Erwerbers.
- d) Garantieansprüche werden nur berücksichtigt, wenn mit dem Gerät das Rechnungsoriginal vorgelegt wird.

4 Ausschluß der Garantie

Jegliche Garantieansprüche sind insbesondere ausgeschlossen,

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

- b) wenn das Gerät unter Bedingungen gelagert oder betrieben wurde, die außerhalb der technischen Spezifikationen liegen;
- c) wenn die Schäden durch unsachgemäße Behandlung – insbesondere durch Nichtbeachtung der Systembeschreibung und der Betriebsanleitung – aufgetreten sind;
- d) wenn das Gerät durch hierfür nicht von uns ermächtigte Personen geöffnet, repariert oder modifiziert wurde;
- e) wenn das Gerät mechanische Beschädigungen irgendwelcher Art aufweist;
- f) wenn Schäden an der Bildröhre eines ELSA-Monitors festgestellt werden, die insbesondere durch mechanische Belastungen (Verschiebung der Bildröhrenmaske durch Schockeinwirkung oder Beschädigungen des Glaskörpers), starke Magnetfelder in unmittelbarer Nähe (bunte Flecken auf dem Bildschirm), permanente Darstellung des gleichen Bildes (Einbrennen des Phosphors) hervorgerufen wurden;
- g) wenn und soweit sich die Luminanz der Hintergrundbeleuchtung bei TFT-Panels im Laufe der Zeit allmählich reduziert;
- h) wenn der Garantieanspruch nicht gemäß Ziffer 3a) oder 3b) gemeldet worden ist.

5 Bedienungsfehler

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

6 Ergänzende Regelungen

- a) Die vorstehenden Bestimmungen regeln das Rechtsverhältnis zu uns abschließend.
- b) Durch diese Garantie werden weitergehende Ansprüche, insbesondere solche auf Wandlung oder Minderung, nicht begründet. Schadensersatzansprüche, gleich aus welchem Rechtsgrund, sind ausgeschlossen. Dies gilt nicht, soweit z.B. bei Personenschäden oder Schäden an privat genutzten Sachen nach dem Produkthaftungsgesetz oder in Fällen des Vorsatzes oder der groben Fahrlässigkeit zwingend gehaftet wird.
- c) Ausgeschlossen sind insbesondere Ansprüche auf Ersatz von entgangenem Gewinn, mittelbaren oder Folgeschäden.
- d) Für Datenverlust und/oder die Wiederbeschaffung von Daten haften wir in Fällen von leichter und mittlerer Fahrlässigkeit nicht.
- e) In Fällen, in denen wir die Vernichtung von Daten vorsätzlich oder grob fahrlässig verursacht haben, haften wir für den typischen Wiederherstellungsaufwand, der bei regelmäßiger und gefahrensprechender Anfertigung von Sicherheitskopien eingetreten wäre.
- f) Die Garantie bezieht sich lediglich auf den Erstkäufer und ist nicht übertragbar.
- g) Gerichtsstand ist Aachen, falls der Erwerber Vollkaufmann ist. Hat der Erwerber keinen allgemeinen Gerichtsstand in der Bundesrepublik Deutschland oder verlegt er nach Vertragsabschluß seinen Wohnsitz oder gewöhnlichen Aufenthaltsort aus dem Geltungsbereich der Bundesrepublik Deutschland, ist unser Geschäftssitz Gerichtsstand. Dies gilt auch, falls Wohnsitz oder gewöhnlicher Aufenthalt des Käufers im Zeitpunkt der Klageerhebung nicht bekannt ist.
- h) Es findet das Recht der Bundesrepublik Deutschland Anwendung. Das UN-Kaufrecht gilt im Verhältnis zwischen uns und dem Erwerber nicht.

10.2

Konformitätserklärung Europäische Union (CE)

Die CE-Konformitätserklärungen für die *ELSA LANCOM 1600 Office* finden Sie im Download-Bereich der ELSA-Homepage (www.elsa.de/download).



11 Index

- **Ziffern**
 - 10/100Base-TX22
 - 100Mbit-Netz22
 - 10Base-T-Anschluss22
- **A**
 - Adress-Pool79
 - Adressverwaltung77
 - Anlagenanschluß13
 - Anrufbeantworter12
 - Anruferkennung71
 - Anschlussbelegung139
 - Ethernet-Schnittstelle139
 - ISDN-S₀-Schnittstelle139
 - Konfigurationsschnittstelle140
 - LAN-Schnittstelle139
 - Outband140
 - WAN-Schnittstelle139
 - Anschlüsse22
 - AOCD92
 - Ausschluss-Routen109
 - Authentifizierung17, 129
 - Automodus78
 - Autosensing22
- **B**
 - BACP18
 - Benutzername47, 72, 125
 - B-Kanal
 - Protokoll73
 - Verbindungszustand14
 - Brute-Force13, 61
 - Bürokommunikation97
- **C**
 - Calling Line Identifier Protocol74
 - CAPI Faxmodem102
 - CAPI-Schnittstelle96
 - CBCP128
 - Challenge Handshake
 - Authentication Protocol72
 - CHAP72
 - CLIP17, 73, 74
 - Common ISDN Application Programming
 - Interface96
 - Conf126
- **D**
 - Datenkompressionsverfahren
 - LZS133
 - Datenübertragung133
 - DFÜ-Netzwerk45, 72
 - DHCP52, 77
 - Automodus78
 - für WINS-Auflösung82
 - DHCP-Server77, 83
 - Dienst83
 - Distanz einer Route109
 - D-Kanal52, 73
 - DNS52, 83
 - DNS-Forwarding84, 85
 - DNS-Server13, 77, 80, 83
 - Filterliste89
 - Filtermechanismus84
 - verfügbare Informationen84
 - DNS-Tabelle88, 89
 - Domain83, 89
 - sperrern89
 - Domain Name Service83
 - DSL-Anschluss22
 - DSL-Modem10, 12
 - Durchsatz133
 - Dynamic Host Configuration Protocol77

Dynamische Kanalbündelung 18, 133
 Dynamisches Routing 107

E

ELSA CAPI Faxmodem 17
ELSA Dynamic VPN 17
 ELSA FirmSafe 15, 54
ELSA LANCAPI 14, 17, 46
ELSA LANconfig 40, 46, 55
ELSA LANmonitor 49
 Anzeige-Optionen 49
 Internet-Verbindung kontrollieren .. 50
 System-Informationen 49
ELSA WEBconfig 55
 ELSA-Protokoll 73
 ELSA-RVS-COM 12
 ELSA-ZOC 12
 E-Mail 10
 End-Adresse 79
 Ethernet 12
 10/100Base-T 12
 Fast-Ethernet 12
 Eurofiletransfer 17

F

Fail 126
 FAQs (Frequently Asked Questions) 3
 Fast Call Back 74
 Fast-Ethernet 12
 10/100Base-T 12
 Fax 12, 17, 102
 Fax Class 1 102
 Faxmodem 17
 Faxtreiber 102
 Faxübertragung 103
 Fehlende Gebühreninformationen 92
 Fehlersuche 49
 Fernkonfiguration 16, 39
 Fernverbindung 46
 Fernzugang 45

Festverbindungen 11, 18
 Filetransfer 10
 Filter 62
 Filter-Liste 70
 Filtermechanismen 11
 Firewall 13, 62, 63, 97
 Firewall-Filter 10
 Firmware 3, 15
 Firmware-Update 15
 Firmware-Upload 55
 mit *ELSA LANconfig* 56
 mit *ELSA WEBconfig* 56
 mit Terminalprogramm 56
 mit TFTP 57
 Flash-ROM-Speicher 15, 54
 Flatrate 127
 Frequently Asked Questions 3

G

Garantiebedingungen 141
 Gateway 63, 77, 80
 Gebührenbegrenzung 90
 Gebühreneinheiten 92, 133
 Gebühreninformation 92, 133
 Gebührenmanagement 90
 Gebührenschatz 16
 Gebührenüberwachungsfunktion 97
 Gegenstelle 125
 Gerätenamen 125
 Gültigkeitsdauer 78, 81

H

Haltezeit 133, 134
 Hohe Telefonkosten 90
 Home-Office 11
 Host 83

I

Identifikationskontrolle 71
 Identifizierung des Anrufers 71

Inband	39
mit Telnet	44
Inband-Konfiguration	39
Installation	12
Internet	10, 63
Internet Service Provider	10
Internet-Adresse	64
Internetzugang	35, 124
Intranet-Adresse	64
Inverses Masquerading	65
IP-Adressbereich	67
IP-Adresse	50, 63, 123
IP-Adressverwaltung	77
IP-Broadcast	114
IP-Masquerading	10, 13, 52, 62, 63
einfaches Masquerading	65
unterstützte Protokolle	66
IP-Multicast	114
IP-Parameter selber festlegen	33
IP-Port	101
IP-Routing	13
Standard-Router	110
IP-Routing-Tabelle	107
ISDN	
B-Kanal	73
D-Kanal	13, 74
S ₀ -Anschluss	22
ISDN-Kabel	12
ISDN-Zeit	18

K

Kabelmodem	10, 12
Anschluss	22
Kanalbündelung	18, 132
Dynamisch	18, 133
Statisch	18, 133
Keep-Alive	127
KnowledgeBase	3
Kompression	18

Konfiguration	15
SNMP	45
Verfahren	39
Konfigurationskabel	23
Konfigurations-Schnittstelle	39
Kosten begrenzen	90

L

LAN-Anschluss	12
LAN-Anschlusskabel	23
LAN-LAN-Kopplung	11
LCP-Echo-Reply	122
LCP-Echo-Request	122
LCR	18, 92
Least-Cost-Routing	18, 92
LED-Anzeigen	14, 19
Leitungsaufbau	13
Leitungsverwaltung	13
Lieferumfang	23
Line-Management	11
Login	55
Login-Sperre	61
Login-Versuche	61
LZS-Datenkompression	133

M

MAC-Adresse	67
MAC-Adress-Filter	13
Mailserver	88
Media Access Control	67
Mehrgeräteanschluß	13
MLPPP	18, 132
MS-CHAP	120, 121
Multilink PPP	120, 132

N

NAT	62, 63
NBNS-Server	77, 80, 82
NetBIOS	52, 84
NetBIOS-Netze	84

NetBIOS-Proxy	16
Netzteil	22, 23
Netzwerknamen	83
Node/Hub-Umschalter	22

● O

Objekt-Tabelle	69
Online-Minuten	90
Online-Recherchen	10
Outband	39
Outband-Konfiguration	39

● P

Paket-Dump	52
PAP	72
passwd	61
Password Authentication Protocol	72
Passwort	48, 50, 71, 72, 125
Passwortschutz	17, 59
PAT	62, 63
Peer-to-Peer-Netzwerke	16
Periode	90
Point-to-Point Tunneling Protocol	126
Policy Based Routing	115, 138
Port	101
Port-Nr.	66
Power	19
PPP	16, 50, 72, 132
LCP Extensions	130
Leitungsüberprüfung mit LCP	122
Rückruf-Funktionen	128
Verhandlungsphase	47
Zuweisung von IP-Adressen	123
PPP-Client	40, 46
PPP-Liste	72
PPP-Verbindung	47
PPTP	126
Prioritätensteuerung	101
Punkt-zu-Mehrpunkt-Konfiguration	13
Punkt-zu-Punkt-Konfiguration	13

● R

Rechner-Namen	83
Regel-Tabelle	69
Remote Access	11, 124
Reset-Schalter	22
RIP	52
Router-Interface-Liste	134
Router-Name	108
Rückruf	11, 71, 73
Fast Call Back	74
Rückruf-Funktion	17
Rufnummernerkennung	17

● S

S ₀ -Schnittstelle	13
Schnittstellen	22
Schutz der Konfiguration	59
Schutz für das LAN	62
Schutz für die Konfiguration	59
Serielle Schnittstelle	39
Sicherheit	59, 62, 63
Sicherheits-Checkliste	74
Sicherheitseinstellungen	60
Sicherheitsfunktionen	10
Sicherung	125
Sicherungsverfahren	72
Single User Access	63
SNMP	45
Software einspielen	54
Sperre	61
Stac	133
Stac-Datenkompression	18
Standard-Faxprogramme	102
Start-Adresse	79
Stations-Namen-Tabelle	87
Statische Kanalbündelung	18, 133
Statisches Routing	107
Statistiken	16
Statusanzeigen	14

Support 3
 SYN/ACK-Speedup 115, 138

● T

TCP/IP 107
 TCP/IP-Netze 83
 Technische Daten 137
 Telnet 15, 46
 Term 126
 Terminalprogramm 15, 56
 TFTP 44
 Timeout 133
 Trace
 Ausgaben 51
 Beispiele 53
 Schlüssel und Parameter 51
 starten 51
 Treiber 3
 Type-of-Service 115

● U

Übertragungsraten 14, 51
 Überwachung 49
 Upload 15, 55
 Username 125

● V

V.24-Konfigurationsschnittstelle 22
 Verbindungsbegrenzung 92
 Verbindungsdauer 14
 Verfügbarkeit 101

Virtuelle Private Netzwerke 11, 14
 VPN 11, 14

● W

Wählleitungen 11
 WAN-Anschluss 12
 WAN-Anschlusskabel 23
 Wdh 126
 Wiederholungen 126
 Wildcards 89
 Windows-Netz 16, 82
 WINS-Konfiguration 82
 Wissensdatenbank 3

● Y

Y-Verbindung 134

● Z

Zeit 125
 Zeitabhängige Verbindungs-
 begrenzung 92
 Zeitbudget 92
 Zeitkontrolle 18
 Zeit-Limit 90
 Zugang zum Internet einrichten 35
 Zugangskontrolle 62
 Zugangsschutz 71
 Name 71
 Name oder Nummer 71
 Nummer 71
 zusätzliches Limit 91

