

# ***ELSA LANCOM™ DSL/10 Office***

**Handbuch**

© 1999 ELSA AG, Aachen (Germany)

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

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

## Marken

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

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

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

ELSA AG

Sonnenweg 11

52070 Aachen

Deutschland

[www.elsa.de](http://www.elsa.de)

Aachen, September 1999

# Ein Wort vorab

## Vielen Dank für Ihr Vertrauen!

Mit dem *ELSA LANCOM DSL/10 Office* haben Sie sich für einen Router entschieden, mit dem Sie lokale Netzwerke oder einzelne Arbeitsplatzrechner über eine xDSL-Verbindung an das Internet anschließen können. Zwölfmal schneller als über einen einfachen B-Kanal im ISDN-Netz können Sie jetzt durch das Internet surfen.

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

## Dokumentation

Die beiliegende Dokumentation besteht aus:

- Handbuch  
Hardware-Installation, Beschreibung der Funktionen und Betriebsarten und Konfigurationsbeispiele
- elektronischer Dokumentation auf CD  
Technische Grundlagen (z.B. zu xDSL, allgemeiner Netzwerktechnik, TCP/IP etc.), Workshop mit ausführlichen Anwendungsbeispielen, Referenzteil zum Nachschlagen mit vollständiger Beschreibung der Menüs

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

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

Lancom.doku@elsa.de



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

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



# Inhalt

<b>Einleitung .....</b>	<b>1</b>
Was macht ein Router überhaupt? .....	1
Was bietet ein <i>ELSA LANCOM DSL/10 Office</i> ? .....	2
<b>Installation .....</b>	<b>5</b>
Lieferumfang .....	5
<i>ELSA LANCOM DSL/10 Office</i> stellt sich vor .....	5
So schließen Sie den Router an .....	7
Software-Installation .....	8
Grundkonfiguration .....	8
Grundeinstellungen vornehmen mit <i>ELSA LANconfig</i> .....	8
Grundeinstellungen setzen mit Telnet .....	10
<b>Konfigurationsmöglichkeiten .....</b>	<b>13</b>
Viele Wege führen zum <i>ELSA LANCOM DSL/10 Office</i> .....	13
Der komfortable Weg: Inband .....	13
Voraussetzungen .....	14
Alternativ: Adreßverwaltung mit dem DHCP-Server .....	14
Starten der Konfiguration über <i>ELSA LANconfig</i> .....	14
Starten der Inband-Konfiguration über Telnet .....	15
Befehle für die Konfiguration .....	15
Neue Firmware mit FirmSafe .....	17
So funktioniert FirmSafe .....	17
So spielen Sie eine neue Software ein .....	18
Konfiguration über SNMP .....	19
Allgemeines .....	19
Zugriff auf Tabellen und Parameter über SNMP .....	20
Die Management-Information-Base (MIB) .....	23
<b>Funktionen und Betriebsarten .....</b>	<b>25</b>
Sicherheit für Ihre Konfiguration .....	25
Paßwortschutz .....	25
Die Login-Sperre .....	26
Zugangskontrolle über TCP/IP .....	26
Sicherheit für Ihr LAN .....	26
Das Versteck – IP-Masquerading (NAT/ PAT) .....	27
Filter für die TCP/IP-Pakete .....	27
Gebührenmanagement .....	27
Zeitabhängige Verbindungsbegrenzung .....	28
Einstellungen im Gebührenmodul .....	28
xDSL-Verbindungen .....	28

Namenliste.....	30
PPP-Liste.....	31
IP-Routing.....	31
Die IP-Routing-Tabelle .....	31
Lokales Routing.....	33
Dynamisches Routing mit IP-RIP.....	33
IP-Masquerading (NAT, PAT) .....	35
DNS-Forwarding.....	36
Policy Based Routing.....	36
Automatische Adreßverwaltung mit DHCP .....	37
Der DHCP-Server.....	37
DHCP – 'Ein', 'Aus' oder 'Auto'?.....	37
So werden die Adressen zugewiesen.....	38
DNS.....	41
Was macht ein DNS-Server? .....	41
So stellen Sie den DNS-Server ein.....	42
<b>Anhang .....</b>	<b>45</b>
Technische Daten .....	45
Allgemeine Garantiebedingungen vom 01.06.1998 .....	46
Konformitätserklärung .....	48
<b>Index .....</b>	<b>49</b>
<b>Beschreibung der Menüpunkte (nur auf der CD) .....</b>	<b>R1</b>
Status.....	R3
Status/Verbindung .....	R4
Status/Aktuelle-Zeit.....	R4
Status/Betriebszeit .....	R4
Status/WAN-Statistik.....	R4
Status/LAN-Statistik.....	R6
Status/PPP-Statistik.....	R8
Status/TCP-IP-Statistik .....	R13
Status/IP-Router-Statistik.....	R18
Status/Config-Statistik .....	R20
Status/DSL-Statistik .....	R20
Status/DSL-Statistik/PPPoE-Statistik .....	R21
Status/Queue-Statistik .....	R22
Status/Verbindungs-Statistik.....	R23
Status/Info-Verbindung.....	R23
Status/Gegenstellen-Statistik .....	R24
Status/Kanal-Statistik.....	R24
Status/Zeit-Statistik.....	R25
Status/Werte löschen.....	R25



Setup .....	R26
Setup/WAN-Modul .....	R27
Setup/Gebühren-Modul .....	R29
Setup/LAN-Modul .....	R30
Setup/TCP-IP-Modul .....	R31
Setup/IP-Router-Modul .....	R34
Setup/SNMP-Modul .....	R42
Setup/DHCP-Server-Modul .....	R43
Setup/DNS-Modul .....	R45
Setup/Config-Modul .....	R47
Setup/Zeit-Modul .....	R48
Firmware .....	R48
Sonstiges .....	R50





# Einleitung

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

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

Mit *ELSA LANCOM DSL/10 Office* steht Ihnen ein Router zur Verfügung, der speziell für xDSL-Anschlüsse entwickelt wurde.

*ELSA LANCOM DSL/10 Office* erlaubt den Anschluß von einzelnen Arbeitsplätzen oder ganzen lokalen Netzwerken an das Internet. Mit bisher nicht gekannten Geschwindigkeiten (768 Kbit/s) können Sie Daten aus dem Internet beziehen.

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

## 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 xDSL-Verbindung bereit, die über normale Kupfer-Telefonleitungen realisiert wird.

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

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

Wann setzen Sie Router nun ganz konkret ein?

Eigentlich immer dann, wenn Rechner miteinander verbunden werden sollen und ein reiner Modem-Betrieb nicht mehr ausreicht. Das ist z.B. die Anwendung Internet im LAN.

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

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

## **Was bietet ein *ELSA LANCOM DSL/10 Office*?**

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

### **Einfache Installation**

- *ELSA LANCOM DSL/10 Office* mit Spannung versorgen
- Verbindung zum LAN herstellen
- Verbindung zum xDSL-Anschluß herstellen
- Einschalten
- Loslegen

### **LAN-Anschluß**

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

### **WAN-Anschluß**

*ELSA LANCOM DSL/10 Office* wird an die Ethernet-Schnittstelle eines xDSL-Anschlusses angeschlossen.

### **Statusanzeigen**

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

### **Konfiguration mit *ELSA LANconfig***

Die Einstellung und Anpassung der Geräte an die von Ihnen gewünschte Aufgabe erfolgt schnell und komfortabel über das mitgelieferte Konfigurationstool *ELSA LANconfig* für Windows-Betriebssysteme. Benutzer anderer Betriebssysteme verwenden Telnet oder ein beliebiges Terminalprogramm.

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

### **Software-Update**

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

### **FirmSafe**

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

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

### **DHCP**

Damit können Sie einen bestimmten Bereich von IP-Adressen zur Verfügung stellen, die der DHCP-Server dann selbständig den einzelnen Geräten im lokalen Netz zuweist.

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

### **Gebührenschatz**

Die Gebühren für die Internetnutzung werden je nach Provider zeitabhängig berechnet. Um nicht am Ende des Monats von einer unerwünscht hohen Telefonrechnung überrascht zu werden, können Sie vorher festlegen, wie viele Online-Minuten in einem bestimmten Zeitraum (z.B. 10 Stunden in 6 Tagen) über ein *ELSA LANCOM DSL/10 Office* erlaubt sind.

### **Zugriffsschutz**

Zum Schutz vor unberechtigtcm Zugriff auf das Firmen-Netz bietet der Router neben dem einfachen Paßwortschutz mit Firewall-Filtern und IP-Masquerading ein geschlossenes Sicherheitskonzept. Zusätzlich verhindert die Login-Sperre Brute-Force-Angriffe und

sperrt den Zugang zum Router nach einer einstellbaren Anzahl von Login-Versuchen mit falschem Paßwort.

### **DNS-Server**

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

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

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

# Installation

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

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

## Lieferumfang

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

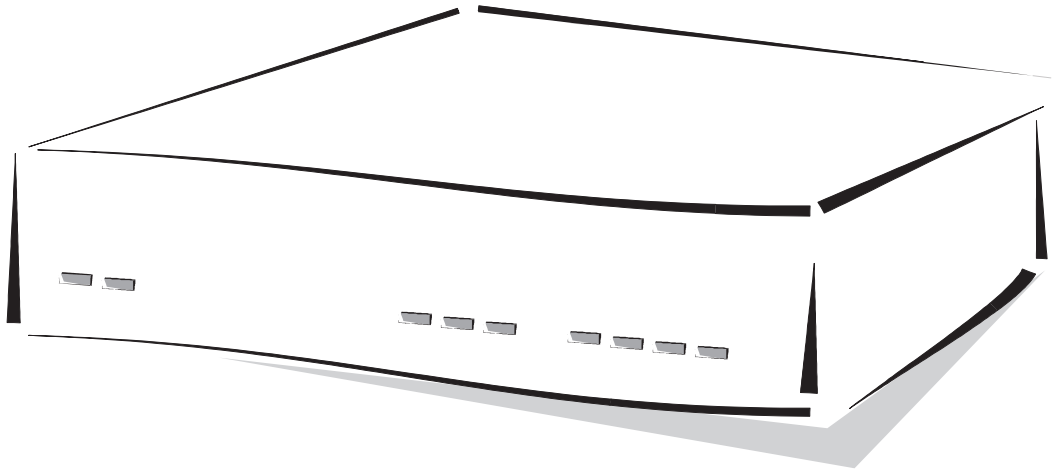
- Netzteil
- LAN-Anschlußkabel
- xDSL-Anschlußkabel
- Kabel für die Konfigurationsschnittstelle
- Adapter für Konfigurationskabel
- Dokumentation
- CD mit *ELSA LANconfig* und weiterer Software und elektronischer Dokumentation

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

## ***ELSA LANCOM DSL/10 Office stellt sich vor***

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

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



#### Power/Msg

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

aus		Gerät abgeschaltet
rot	1 x kurz	Bootvorgang (Test und Laden) begonnen
rot	blinkend	Anzeige eines Bootfehlers (im Blinkcode kodiert)
rot		Gerät betriebsbereit

#### DSL-Rx/Tx

Diese gelbe LED zeigt die Datenbewegungen auf der DSL-Verbindung an.

#### DSL-Link

Diese grüne LED zeigt an, daß die Ethernet-Verbindung zwischen *ELSA LANCOM DSL/10 Office* und DSL-Anschluß in Ordnung ist.

#### DSL-Chan

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

aus	<i>ELSA LANCOM DSL/10 Office</i> hat kein Login bei der Vermittlungsstelle angefordert
rot	<i>ELSA LANCOM DSL/10 Office</i> hat ein Login bei der Vermittlungsstelle angefordert, das Login wird durchgeführt
grün	Das Login war erfolgreich, die Verbindung zum Provider ist hergestellt.



*Solange die LED 'DSL-Chan' grün leuchtet, ist die Verbindung aktiv und gebührenpflichtig!*

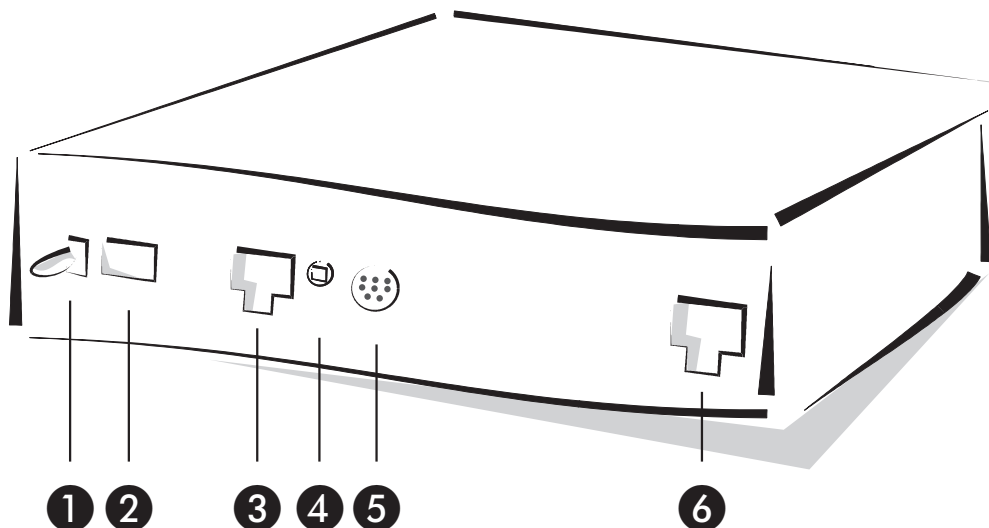
#### LAN-Tx, -Rx, LAN-Coll, -Link LAN-FDpx, -Fast

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

LAN-Rx/Tx	gelb	Datenpaket vom Gerät an das LAN oder vom LAN an das Gerät gesendet
LAN-Coll	rot	Sendekollision

LAN-Link	grün	Der Anschluß zum LAN ist hergestellt und bereit
LAN-FDpx	grün	Der Router sendet und empfängt Daten gleichzeitig
LAN-Fast	grün	<i>ELSA LANCOM DSL/10 Office</i> befindet sich im 100-Mbit-Betrieb

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



- ❶ Ein/Aus-Schalter
- ❷ Anschluß für das Netzteil
- ❸ 10/100Base-TX für 10-Mbit- oder 100-Mbit-Netze
- ❹ Node/Hub-Umschalter
- ❺ V.24-Konfigurationsschnittstelle
- ❻ 10Base-T-Anschluß für xDSL- oder Kabelmodem

## So schließen Sie den Router an

- ❶ Verbinden Sie den Router *ELSA LANCOM DSL/10 Office* mit dem LAN. Stecken Sie dazu das mitgelieferte Netzwerkabel in den 10/100Base-T-Netzwerkanschluß des Geräts und in eine freie Netzwerkanschlußdose Ihres lokalen Netzes (oder in eine freie Buchse eines Hubs in Ihrem LAN).
- ❷ Schließen Sie das Gerät an die Ethernet-Schnittstelle des xDSL- (z.B. NTBBA der Deutschen Telekom) oder Kabelmodems an.

- ③ Versorgen Sie das Gerät über das Netzteil mit der benötigten Spannung. Nach einem kurzen Selbsttest des Geräts leuchtet die LED 'Power/Msg' permanent. Die LED 'LAN-Link' zeigt an, daß Ihr Router korrekt mit dem LAN verbunden ist.



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

## Software-Installation

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

Zum Betrieb der Konfigurationssoftware benötigen Sie einen PC im LAN.

- ① Installieren Sie zuerst das Netzwerkprotokoll TCP/IP auf dem Rechner, von dem aus Sie Ihre Basis-Station einstellen möchten.
- ② Installieren Sie anschließend *ELSA LANconfig*. Wenn das Setup-Programm beim Einlegen der *ELSA LANCOM*-CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' auf der *ELSA LANCOM*-CD und folgen den weiteren Hinweisen der Installationsroutine.

## Grundkonfiguration

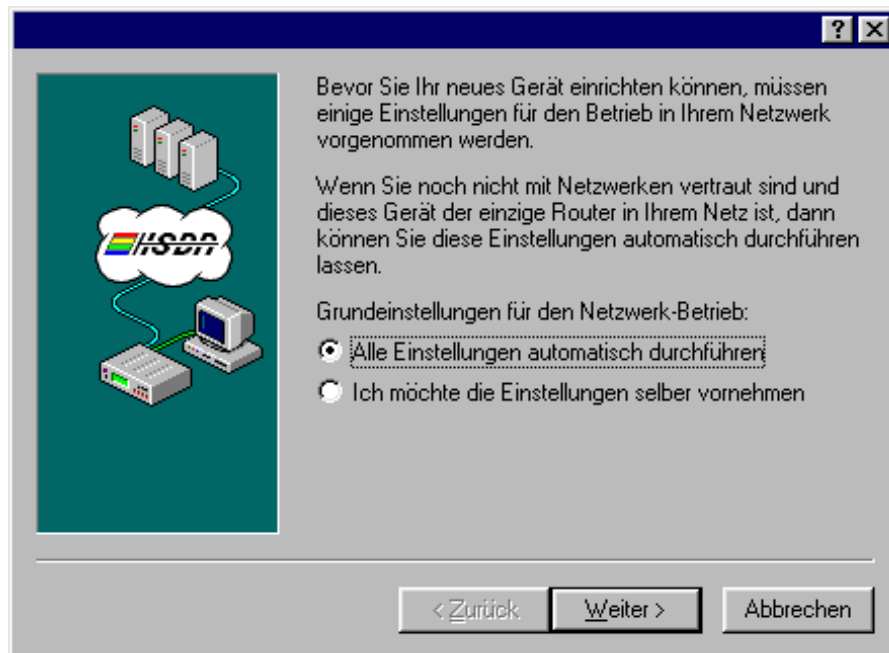
Bei der Grundkonfiguration wird die IP-Adresse für die Basis-Station festgelegt. Außerdem wird über die Verwendung des integrierten DHCP-Servers entschieden. Sie können die Grundkonfiguration mit *ELSA LANconfig* oder mit Telnet vornehmen.

### Grundeinstellungen vornehmen mit *ELSA LANconfig*

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



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



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

- Sie haben bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet, möchten das ab jetzt aber gerne tun. Welche IP-Adressen dabei verwendet werden, ist Ihnen egal. Der Router wird dann als DHCP-Server die IP-Adressen für alle Geräte im Netzwerk (LAN und WLAN) automatisch festlegen und zuweisen.

oder

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



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

*Unter Windows NT können Sie IP-Adressen mit dem Befehl `ipconfig` kontrollieren.*

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

- Sie haben bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet, möchten das ab jetzt aber gerne tun. Sie möchten die IP-Adresse für den Router jedoch selbst festlegen und geben ihm eine beliebige Adresse aus einem der für private

Zwecke reservierten Adreßbereiche, z.B. '10.0.0.1' mit der Netzmaske '255.255.255.0'. Damit legen Sie auch gleichzeitig den Adreßbereich fest, den der DHCP-Server anschließend für die anderen Geräte im Netz verwendet (sofern der DHCP-Server nicht ausgeschaltet wird).

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



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

- ④ Im Anschluß an den Assistenten für die Grundeinstellungen startet automatisch der Assistent für den Internet-Zugang. Geben Sie in diesem Assistenten nur den Benutzernamen und das Paßwort ein, das Ihr Provider Ihnen mitgeteilt hat.
- ⑤ Mit diesen wenigen Mausklicks ist Ihr Router fertig eingestellt für den Zugang zum Internet.

## Grundeinstellungen setzen mit Telnet

Wenn Sie *ELSA LANconfig* nicht verwenden möchten oder nicht verwenden können (z.B. weil Sie ein anderes Betriebssystem installiert haben), können die Grundeinstellungen auch über eine Telnet-Verbindung vorgenommen werden.

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

Geben Sie die folgenden Befehle ein:

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

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

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

- ③ Intranet-Adresse und Netzmaske:

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

```
set /Setup/TCP-IP-modul/Intranet-Maske 255.255.255.0
```



*Nach dem Ändern der Intranet-Adresse wird die telnet-Verbindung vom Router beendet und Sie müssen eine neue telnet-Verbindung zur gesetzten Intranet-Adresse aufbauen.*

- ④ Evtl. DHCP-Funktion ausschalten:

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

- ⑤ Provider in der Namenliste einrichten:

```
set /Setup/WAN-Modul/Namenliste internet 20
```

- ⑥ Zugangsdaten in der PPP-Liste eintragen:

```
set /Setup/WAN-Modul/PPP-Liste internet keine 'Ihr Paßwort'  
0 5 'Ihr Benutzername'
```

- ⑦ Route ins Internet festlegen:

```
set /Setup/IP-Router-Modul/IP-Routing-Tab. 255.255.255.255  
0.0.0.0 internet 0 Ein
```



*Auch wenn die Einträge Ihnen an dieser Stelle ohne weitere Erklärungen noch nicht allzuviel sagen, erreichen Sie damit das gleiche Ziel wie bei der Einstellung über ELSA LAN-config: Der Zugang zum Internet ist damit erstmal hergestellt!*



# Konfigurationsmöglichkeiten

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

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

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

## Viele Wege führen zum **ELSA LANCOM DSL/10 Office**

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

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

Was unterscheidet nun diese Möglichkeiten?

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

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

## Der komfortable Weg: Inband

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

## Voraussetzungen

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

Ein noch nicht konfiguriertes Gerät hört auf die IP-Adresse XXX.XXX.XXX.254. Die vielen X stehen dabei für die Netzwerkadresse in Ihrem LAN. Haben die Rechner in Ihrem Netz also z.B. Adressen wie 192.110.130.1, dann können Sie Ihr Gerät mit der Adresse 192.110.130.254 erreichen.



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

## Alternativ: Adreßverwaltung mit dem DHCP-Server

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

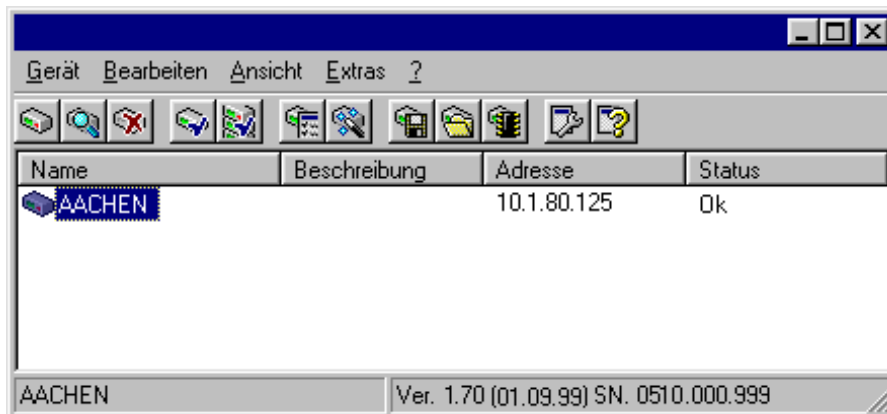
## Starten der Konfiguration über *ELSA LANconfig*

Rufen Sie *ELSA LANconfig* z.B. aus der Windows-Startleiste auf mit **Start ► Programme ► ELSAan ► ELSA LANconfig**. *ELSA LANconfig* sucht nun automatisch im lokalen Netz nach Geräten. Diese Funktion ist abschaltbar.



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

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



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

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

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



Ein Doppelklick auf den Eintrag für das markierte Gerät startet bereits die Konfiguration.

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

## Starten der Inband-Konfiguration über Telnet

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

```
telnet 10.1.80.125
```

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


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

## Befehle für die Konfiguration

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

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

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

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

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

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



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

## Neue Firmware mit FirmSafe

Die Software der 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!

### So funktioniert FirmSafe

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

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

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

## So spielen Sie eine neue Software ein

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

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



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

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

### *ELSA LANconfig*



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

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

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

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

## TFTP

Über TFTP kann eine neue Firmware mit dem Befehl **writelflash** eingespielt werden. Um eine neue Firmware, die z.B. in der Datei 'LC\_1000U.130' vorliegt, in ein Gerät mit der IP-Adresse 194.162.200.17 zu übertragen, geben Sie z.B. unter Windows NT folgenden Befehl ein:

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



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

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



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

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

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

## Konfiguration über SNMP

### Allgemeines

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

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

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

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

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

iso/org/dod/internet/private/enterprises/elsa/lancom oder 1.3.6.1.4.1.2356.1.

## Zugriff auf Tabellen und Parameter über SNMP

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

### Zugriffschutz unter SNMP V.1

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

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

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

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

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

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

### Tabellen-Zeilen löschen mit SNMP

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

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

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

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

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

### Tabellen-Zeilen hinzufügen mit SNMP

Zum Einfügen von Zeilen in einer Tabelle gibt es zwei Möglichkeiten:

- Mit dem Set-Befehl kann durch das Setzen eines neuen Indexeintrags eine neue Zeile erzeugt werden. Mit dem Befehl in der Syntax:

`someTable.1.2.2 = xyz`

Wird in der Tabelle 'someTable' eine Zeile mit dem Index '2' erzeugt, in deren zweiter Spalte der Wert 'xyz' eingetragen wird. Die '1' hinter dem Tabellennamen ist für diesen Befehl konstant und steht in der SNMP-Syntax für 'someEntry'.

- Bei SNMP-Managern, die das Einfügen von Indexwerten nicht erlauben, kann ein beliebiger schon vorhandener Indexeintrag einer Zeile auf den neuen Indexwert der neuen Zeile geändert werden. Die Zeile, die dazu als Quelle der Änderung herangezogen wird, bleibt selbst unverändert.

Praktisch läßt sich die erste Möglichkeit z.B. bei Castlerock SNMPc wie folgt realisieren:

- ① Aktivieren Sie den Unterpunkt **Display MIB Table** im Menü **Manage** des Castlerock SNMPc.
- ② Öffnen Sie die entsprechende Tabelle. Ist die Tabelle leer, werden leere Spalten angezeigt.
- ③ Klicken Sie **Edit** an. Jetzt können Werte für die einzelnen Tabellenspalten angegeben werden.
- ④ Tragen Sie den Index der Tabelle und den Wert für eine weitere zu setzende Spalte ein, und klicken Sie **Set** rechts neben der letztgenannten Spalte.

Jetzt sollte eine neue Spalte mit dem neuen Index und dem Wert für eine weitere Spalte entstanden sein.



*Es können auch Werte für alle Spalten der Zeile eingetragen und mit **Set All** alle Spalten gleichzeitig gesetzt werden.*

Diese Prozedur läßt sich auch mit **Edit MIB Vars..** im Menü **Manage** durchführen. Hier klickt man sich bis zu der Tabelle durch, klickt die zu setzende Spalte der Tabelle einmal an, trägt im Feld **Variable Name** hinter dem Namen dieser Spalte den neuen Index und in **Variable Value** den Wert ein. Nach dem Anklicken von Set sollte nun eine neue Tabellenzeile entstanden sein.

### Fehlermeldungen per SNMP-Trap

Über den Mechanismus der SNMP-Traps können Fehler- oder Warnmeldungen an eine Management-Instanz gesendet werden. Der im Router enthaltene SNMP-Agent erlaubt das Versenden von Traps an bis zu 20 SNMP-Manager. Die IP-Adressen dieser Manager werden im Konfigurations-Menü unter `/setup/SNMP-Modul/IP-Trap-Tabelle`

le konfiguriert. Das Versenden kann generell mit dem Schalter `/setup/snmp-Modul/Send-Traps` ein- und ausgeschaltet werden.

### **SNMP und *ELSA LANmonitor***

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

### **Die Management-Information-Base (MIB)**

Um SNMP-Management-Systemen Zugriff auf die Konfiguration im *ELSA LANCOM DSL/10 Office* zu geben, muß eine textuelle Darstellung der Konfigurationsstruktur (die sogenannte private MIB) mit dem Gerät ausgeliefert werden. Die Syntax dieser MIB orientiert sich an der ASN.1 (Abstract Syntax Notation One, ISO 8824). In der Regel ist im Programmpaket der SNMP-Management-Software ein sogenannter MIB-Compiler enthalten. Dieser Compiler übersetzt diese MIB-Datei in eine vom Manager benutzbare Form.

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





# Funktionen und Betriebsarten

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

- Sicherheit für die Konfiguration
- Sicherheit für das LAN
- Gebührenmanagement
- xDSL- oder Kabelverbindungen
- PPP-Unterstützung
- IP-Routing
- DHCP-Server
- DNS-Server

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

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

## Sicherheit für Ihre Konfiguration

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

Die von Ihnen einmal eingestellten Parameter sollen natürlich nicht durch Unbefugte verändert werden. Daher bietet ein *ELSA LANCOM DSL/10 Office* die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

### Paßwortschutz

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

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

## Die Login-Sperre

Die Konfiguration im *ELSA LANCOM DSL/10 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 *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security' bzw. im Menü /Setup/Config-Modul die folgenden Einträge zur Verfügung:

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

## Zugangskontrolle über TCP/IP

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

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

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

## Sicherheit für Ihr LAN

Sie mögen es sicher nicht, wenn jeder Außenstehende einfach die Daten auf Ihren Rechnern einsehen oder verändern kann. Ein *ELSA LANCOM DSL/10 Office* bietet verschiedene Möglichkeiten, den Zugriff von außen einzuschränken:

- Filterung von Datenpaketen
- IP-Masquerading (auch unter NAT/ PAT bekannt)

## Das Versteck – IP-Masquerading (NAT/ PAT)

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

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

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

## Filter für die TCP/IP-Pakete

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

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

Der Router kann sich die Ziel- und Quell-Ports von solchen Datenpaketen ansehen, die TCP oder UDP als Protokoll verwenden. Aus diesen Ports kann dann abgeleitet werden, für welchen Zweck die Daten gedacht sind. So können z.B. FTP-Zugriffe oder Telnet-Sitzungen erkannt werden.

## Gebührenmanagement

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

## Zeitabhängige Verbindungsbegrenzung

Um die Kosten zu begrenzen, 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 10 Stunden in 6 Tagen aktiv Verbindungen aufgebaut werden.



*Das Gerät zeigt diesen Zustand durch eine blinkende Power/Msg-LED und im LANmonitor an. 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 – im LANmonitor – 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.

## Einstellungen im Gebührenmodul

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

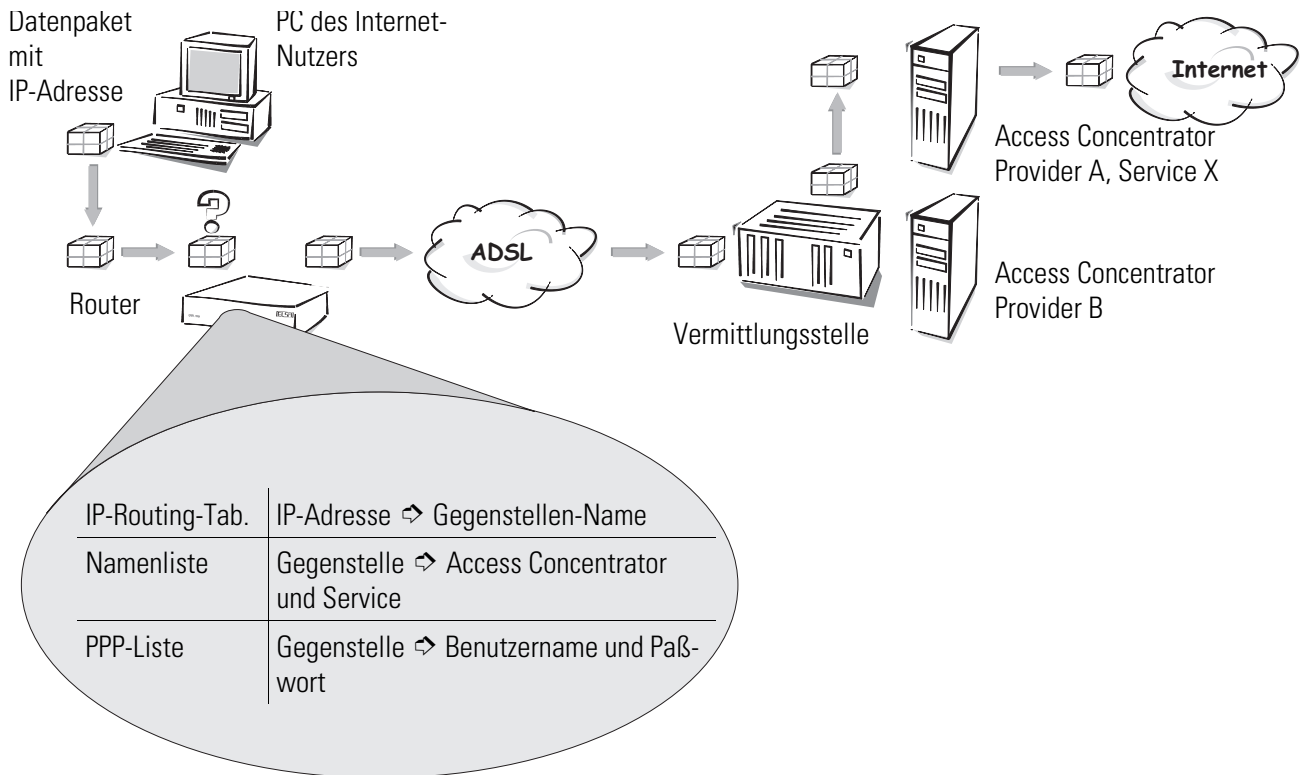


*Die Informationen über die Gebühren und Verbindungszeiten werden über einen Bootvorgang hinaus gesichert (z.B. beim Einspielen einer neuen Firmware) und gehen erst verloren, wenn das Gerät ausgeschaltet wird. Alle hier erwähnten Zeitangaben werden in Minuten gemacht.*

## xDSL-Verbindungen

Die Datenkommunikation zwischen *ELSA LANCOM DSL/10 Office* und Internet läuft über xDSL- oder Kabelverbindungen ab. 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 verdeutlichen.



Ein Datenpaket aus einem Rechner findet den Weg ins Internet in erster Linie über die IP-Adresse des Empfängers. Mit dieser Adresse schickt der Rechner das Paket los über das LAN zum Router. Der Router schaut mit der IP-Adresse zunächst in der IP-Routing-Tabelle nach und findet die Gegenstelle, die zu dieser Adresse gehört (z.B. 'Provider\_A'). Mit diesem Namen prüft der Router dann die Namenliste und findet den Namen des zugehörigen Access Concentrators (AC) 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.

Der Router kann dann eine Verbindung auf der xDSL-Leitung aufbauen und dabei angeben, daß er eine Verbindung zum Access Concentrator des Provides A haben und dort den Service X nutzen möchte. Sobald die Verbindung hergestellt ist, kann der Router das Datenpaket über die xDSL-Leitung weitergeben ins Internet.

Weitere Informationen zu IP-Netzwerken etc. finden Sie in den technischen Grundlagen.

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

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

## Namenliste

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

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

- Name

Mit diesem Namen wird die Gegenstelle in den Routermodulen identifiziert. 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!

- Access Concentrator

Der Access Concentrator steht für den Server, der über diese Verbindung erreicht werden kann. Stehen mehrere Provider zur Auswahl, die über Ihren xDSL-Anschluß genutzt werden können, wählen Sie mit dem Namen des ACs 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.



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

## PPP-Liste

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

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

- **Gegenstelle**  
Name der Gegenstelle, wie sie vorher in der Namenliste definiert wurde.
- **Username**  
Benutzername, der zur Anmeldung bei der Gegenstelle verwendet wird.
- **Paßwort**  
Paßwort, das zur Anmeldung bei der Gegenstelle verwendet wird.
- **Prüfung**  
Authentifizierungsverfahren, das der Router von der Gegenstelle verlangen soll.
- **Zeit, Wdh., Conf., Fail., Term.**  
Parameter zum Verhalten der Verbindung, die hier nicht näher beschrieben werden.

## IP-Routing

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

### Die IP-Routing-Tabelle

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

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

Was bedeuten die einzelnen Einträge in der Liste?

■ IP-Adresse und IP-Netzmaske

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

Die Route mit der IP-Adresse '255.255.255.255' mit Netzmaske '0.0.0.0' ist die Default-Route. Alle Datenpakete, die nicht durch andere Routing-Einträge geroutet werden können, werden über diese Route übertragen.

■ Router-Name

Der Router-Name gibt an, was mit den zur IP-Adresse und Netzmaske passenden Datenpaketen geschehen soll.

Routen mit dem Router-Name '0.0.0.0' bezeichnen Ausschluß-Routen. Datenpakete für diese „Null-Routen“ werden verworfen und nicht weitergeleitet. Damit werden z.B. die im Internet verbotenen Routen (Privat Address Spaces, z.B. 10.0.0.0) von der Übertragung ausgeschlossen.

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

■ Distanz

Anzahl der zwischen dem eigenen und dem Ziel liegenden Router.

Beispiele mit Erläuterungen:

IP-Adresse	IP-Netzmaske	Router-Name	Dist.	Und das passiert:
192.168.130.0	255.255.255.0	192.168.140.123	0	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.130.x werden an den lokal erreichbaren Router mit der IP-Adresse 192.168.140.123 übertragen.
192.168.0.0	255.255.0.0	0.0.0.0	0	Schließt die Übertragung aller Datenpakete in reservierte IP-Adressbereiche aus.
172.16.0.0	255.255.0.0	0.0.0.0	0	
10.0.0.0	255.0.0.0	0.0.0.0	0	
224.0.0.0	224.0.0.0	0.0.0.0	0	



## Lokales Routing

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

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

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

Manche Rechner können mit den ICMP-Redirects leider nichts anfangen. Um die Datenpakete trotzdem zustellen zu können, verwenden Sie das lokale Routing (im *ELSA LAN-config* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' oder im Menü / Setup/IP-Router-Modul/Lok.-Routing Ein). Dadurch weisen Sie den Router in Ihrem Gerät an, das Datenpaket selbst zum anderen, zuständigen Router zu senden. Außerdem werden dann keinen ICMP-Redirects mehr geschickt.

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

## 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.

### 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. Die Route wird verworfen.

### 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.

## IP-Masquerading (NAT, PAT)

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

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

### 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. Diesen Port trägt es ebenfalls in der Tabelle ein und leitet das Paket mit den neuen Angaben weiter.

Mit dem Eintrag in der internen Tabelle kann der Router diese Antwort nun wieder dem ursprünglichen Absender zuordnen.

*In den Statistiken des Routers können Sie sich diese Tabellen genau ansehen (siehe auch 'Status' im Referenzteil des Handbuchs).*



### Einfaches und inverses Masquerading

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

Der kleine Unterschied:

- Beim Zugriff aus dem LAN auf das Internet hingegen wird der Eintrag in der Tabelle mit Port- und IP-Adreß-Informationen durch den Router selbst vorgenommen.

Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also **gleichzeitig** 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

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

### **Welche Protokolle können mit IP-Masquerading übertragen werden?**

Natürlich nur solche, die auch über Ports kommunizieren. Protokolle, die ohne 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

### **DNS-Forwarding**

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

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

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

- Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist (in *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Adressen' oder im Menü */Setup/TCP-IP-Modul*). Wird er dort fündig, holt er die gewünschte Information von diesem Server.

Durch dieses Verfahren benötigen Sie keine Kenntnisse über die Adressen eines DNS-Servers. Außerdem wird damit die Adresse des DNS-Servers automatisch aktualisiert. Sollte z.B. der Provider, der diese Adresse mitteilt, seinen DNS-Server umbenennen, oder Sie sollten zu einem anderen Provider wechseln, erhält Ihr lokales Netz stets die aktuellen Informationen.

### **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-Datenpa-

kete ausgewertet, das Type-of-Service(TOS)-Feld. Diese bevorzugte Behandlung einiger Datenpakete soll z.B. die Konfiguration der Router über das WAN erleichtern, wenn gleichzeitig viele Daten übertragen werden sollen.

Weitere Informationen zu Policy Based Routing finden Sie in der 'Beschreibung der Menüpunkte' im Referenzteil des Handbuchs.



## Automatische Adreßverwaltung mit DHCP

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

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.

### Der DHCP-Server

ELSA LANCOM DSL/10 Office kann als DHCP-Server die IP-Adressen in seinem TCP/IP-Netz verwalten. Dabei teilt er den Arbeitsplatzrechnern die folgenden Parameter mit:

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

### 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.
  - 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'.

## **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.
- Es verwendet dann selbst die IP-Adresse '10.0.0.254' und den Adreß-Pool '10.x.x.x' für die Zuweisung der IP-Adressen im Netz. In diesem Zustand weist der DHCP-Server den anderen Rechnern im Netz nur die IP-Adresse und deren Gültigkeit zu, nicht jedoch die anderen Informationen.

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

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

### **Zuweisung der Netzmaske**

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

### 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.*

### Zuweisung des Default-Gateways

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

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

### Gültigkeitsdauer einer Zuweisung

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

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

#### ■ Maximale Gültigkeit in Minuten

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

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

Der Defaultwert von 6000 Minuten entspricht ca. 4 Tagen.

- Default-Gültigkeit in Minuten

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

### Vorfahrt für den DHCP-Server – Zuweisung anfordern

Standardmäßig sind fast alle Einstellungen in der Netzwerkkumgebung 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.

### Vorfahrt für den Rechner – Zuweisung überschreiben

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

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

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

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

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

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

- neu

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

- unbek.

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



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

## DNS

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

### Was macht ein DNS-Server?

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

Ohne DNS-Server im lokalen Netz wird jeder lokal unbekannte Name über die DEFAULT-Route gesucht. Durch die Verwendung eines DNS-Servers können alle Namen, die mit ihrer IP-Adresse bekannt sind, direkt bei der richtigen Gegenstelle gesucht werden. Der DNS-Server kann dabei im Prinzip ein separater Rechner im Netz sein. Folgende Gründe sprechen jedoch dafür, den DNS-Server direkt im *ELSA LANCOM DSL/10 Office* anzusiedeln:

- Ein *ELSA LANCOM DSL/10 Office* kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbständig verteilen. Der DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-Server hätte bei der dynamischen Adreßvergabe des DHCP-Servers möglicherweise Schwierigkeiten, die Zuordnung zwischen IP-Adresse und Namen aktuell zu halten.
- Der DNS-Server im *ELSA LANCOM DSL/10 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.

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.

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

## **So stellen Sie den DNS-Server ein**

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

- ① Schalten Sie den DNS-Server ein.

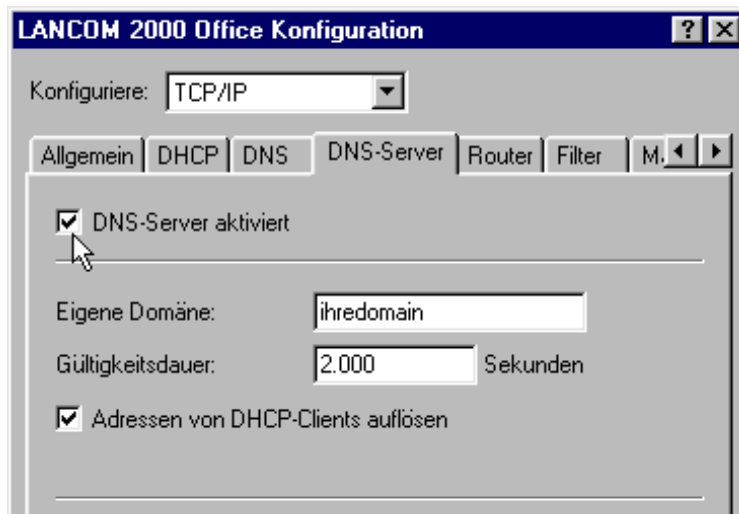
```
set setup/dns-modul/zustand ein
```

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

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

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

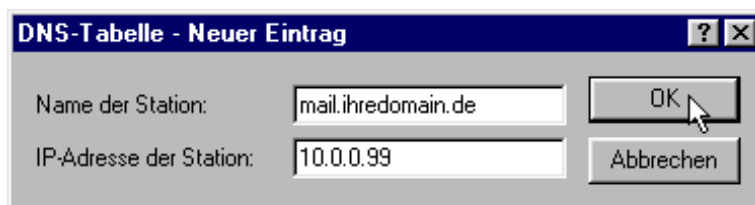
```
set setup/dns-modul/dhcp-verwenden ja
```



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

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

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



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

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

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

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

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

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

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

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

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



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

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

# Anhang

## Technische Daten

Funktionsarten	IP-Router, DHCP-Server, DHCP-Client
LAN-Anschluß	Ethernet IEEE 802.3, 10/100Base-T (RJ45, Node/Hub-Switch), Autosensing, Full-Duplex-Betrieb
Netzwerk-Protokolle	PPP über Ethernet, ARP, PROXY ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, DNS
Filter-Möglichkeiten	Quell- und Zielfilter für Netzwerke, Protokolle und Ports; WAN und LAN getrennt
WAN-Schnittstelle	Ethernet IEEE 802.3, 10Base-T (RJ45)
Gebührenschatz	Maximale Gebührenmenge oder Verbindungszeit in einem vorgegebenen Zeitraum festlegbar
Security- und Firewall-Funktionen	PAP und CHAP, Authentifizierungsmechanismen im PPP; Filtermöglichkeiten im IP-Betrieb; Schutz der Konfiguration über Zugangslisten und Paßwort; IP-Masquerading
IP-Masquerading (NAT/PAT)	IP-Adreß- und -Port-Umsetzung über eine IP-Adresse; statische/dynamische Zuweisung der IP-Adresse über PPP oder DHCP; Maskierung von TCP, UDP, ICMP, FTP; DNS-Forwarding; inverses Masquerading für IP-Dienste aus dem Intranet wie z.B. Web-Server
Management	V.24/V.28-Outband-Schnittstelle (8poliger Mini-DIN), TFTP-Konfiguration und Firmware-Upload, SNMP-Management via SNMP v.1 oder v.2, WAN- oder LAN-Zugänge getrennt aktivierbar, Diagnose-Ausgaben für Protokolle und Schnittstellen, Diagnose-Tools, Status-Anzeige <i>ELSA LANmonitor</i>
Betriebssicherheit	Hardware-Watchdogs, regelmäßige Selbsttests, FirmSafe-Konzept für Remote-Software-Upgrade
Statistiken	LAN- und WAN-Paketzähler, Fehler-, Verbindungs-, Zeit- und Gebührenzähler
Anzeigen/Bedienung	LEDs für LAN-, WAN- und Geräte-Status
Stromversorgung	12 VA mit Steckernetzteil für 230 V, 12 VA
Umgebungsbedingungen	Temperatur: 5..40°C, Luftfeuchtigkeit: 0..80%, nicht kondensierend
Ausführung und Maße	stabiles Metallgehäuse, Anschlüsse auf der Rückseite; Abmessungen 158 x 40 x 125 mm (B x H x T)
Lieferumfang	Netzteil, Kabel für Outband-Schnittstelle, zwei LAN-Twisted-Pair-Kabel, ausführliche Dokumentation und <i>ELSA LANCOM-CD</i>  <i>ELSA LANconfig</i> , <i>ELSA LANmonitor</i> zur Statusanzeige, Terminalprogramm <i>ELSA-ZOC</i>
Zulassungen:	In Vorbereitung: Deutschland, Schweiz und alle Länder der EU
Service	Garantie: 6 Jahre  Support: über Infoline, ELSA LocalWeb und Internet; Testzugänge

## Allgemeine Garantiebedingungen vom 01.06.1998

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

### 1 Garantieumfang

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

### 2 Garantiezeit

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

### 3 Abwicklung

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

### 4 Ausschluß der Garantie

Jegliche Garantieansprüche sind insbesondere ausgeschlossen,

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

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

## 5 Bedienungsfehler

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

## 6 Ergänzende Regelungen

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

# Konformitätserklärung



## KONFORMITÄTSERKLÄRUNG

### DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

**Geräteart:** Ethernet to Ethernet Router

Type of Device:

**Typenbezeichnung:** LANCOM DSL/10 Office

Product Name:

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:

This is to confirm that this product meets all essential protection requirements relating to the

**Niederspannungs Richtlinie (73/23/EWG)**

Low Voltage Directive (73/23/EEC)

**EMV Richtlinie (89/336/EWG)**

EMC Directive (89/336/EEC)

Zur Beurteilung der Konformität wurden folgende **Normen** herangezogen:

The assessment of this product has been based on the following **standards**

**EN 50081-1: 1992 Teile/ parts: EN 55022: 1994**

**EN 50082-1: 1997 Teile/ parts: EN55024: 1999**

**EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1996**

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:

On behalf of the manufacturer / importer:

**ELSA AG**

**Sonnenweg 11**

**D-52070 Aachen**

abgegeben durch: / this declaration is submitted by:

Aachen, 23. August 1999

Aachen, 23<sup>rd</sup> August 1999

i.V. Stefan Kriebel

Bereichsleiter Entwicklung

VP Engineering



# Index

## ■ Numerics

10/100Base-TX .....	7
100BASE-T .....	R30
100Mbit-Netz .....	7

## ■ A

Abbau .....	R29
Administrator .....	R42
Adreß-Pool .....	38, R44
Adreßverwaltung .....	37
Adreßzuweisung .....	14
Anschluß .....	R30
Anschlüsse .....	7
ARP-Aging-Min .....	R34
ARP-Cache .....	R34
ARP-Tabelle .....	R34
Aufbau .....	R28
Ausschluß-Routen .....	32
Authentifizierung .....	R28
Auto-Modus .....	R43

## ■ B

Betriebsarten .....	25
Brute-Force .....	3, 26
Budget .....	R29
Budget-Gebühren .....	R30

## ■ C

Cache .....	R34
Challenge Handshake Authentication Protocol	R28
CHAP .....	R28
Communities .....	19
Conf.-Haltezeit .....	R47

## ■ D

DHCP .....	3, 37, R43
DHCP-Server .....	8, 14, 37, 41, R43
Dienst .....	41
Distanz einer Route .....	32
DNS .....	36, 41, R33

DNS-Anfrage .....	R38
DNS-Backup .....	R33
DNS-Forwarding .....	36, R33
DNS-Forwarding-Mechanismus .....	42
DNS-Server .....	4, 41
Filterliste .....	44
Filtermechanismus .....	41
verfügbare Informationen .....	42
Domain Name Service .....	36, 41
Domains .....	41
Domains sperren .....	44
DSL-Anschluß .....	7
Dynamic Host Configuration Protocol .....	37
dynamische IP-Routing-Tabelle .....	R40
dynamische Zuweisung der IP-Adresse .....	R35
dynamisches Routing .....	31

## ■ E

E-Mail .....	2
End-Adresse .....	38
Ende-Adreß-Pool .....	R43
Ethernet .....	2
10/100Base-T .....	2
Fast-Ethernet .....	2

## ■ F

Fast-Ethernet .....	2
10/100Base-T .....	2
Filetransfer .....	2
Filter .....	27
Firewall .....	3
Firewall-Funktion .....	27, R38
FirmSafe .....	3, 17
Firmsafe .....	R48
Firmware .....	3, R48
Firmware-Upload .....	18, R48
mit LANconfig .....	18
mit Terminal-Programm .....	18
mit TFTP .....	19
Flash-ROM-Speicher .....	3, 17

**G**

Gateway .....	27, 39
Gebührenbegrenzung .....	27
Gebührenmanagement .....	27
Gebührenschatz .....	3, R29
Gebührensperre .....	R30
Gerätename .....	R27
Gerätenamen .....	R27
Gültigkeitsdauer .....	37, 39

**H**

Haltezeiten .....	R27
Heap-Reserve .....	R31
hohe Telefonkosten .....	27
Host .....	41

**I**

ICMP .....	R37, R42
ICMP-Routing-Methode .....	R39
Identifikation .....	R26
Inband .....	13
mit Telnet .....	15
Voraussetzungen .....	14
Inband-Konfiguration .....	13
Installation .....	2
Internet .....	2
Internet-Service-Provider .....	1
Intranet-Adresse .....	R32
Intranet-Maske .....	R32
inverses Masquerading .....	R41
IP Masquerading .....	27
IP-Adresse .....	8, 14, 27, R31
IP-Adressen .....	3
IP-Broadcast .....	R40
IP-Header .....	R39
IP-Masquerading .....	2, 3, 27, 35, R35, R41
unterstützte Protokolle .....	36
IP-Multicast .....	R40
IP-Netzmaske .....	R32
IP-Routing	
Filter .....	27
FTP .....	27
Telnet .....	27
IP-Routing-Tab .....	R35

IP-Routing-Tabelle .....	31
IP-Zugangsliste .....	13

**K**

Konfiguration .....	3
Befehle .....	15
SNMP .....	19
Verfahren .....	13
Konfigurationsmöglichkeiten .....	R47
Konfigurations-Schnittstelle .....	13

**L**

LAN-Anschluß .....	2
LAN-Anschlußkabel .....	5
LAN-Coll .....	6
LAN-Config .....	R47
LANconfig .....	3, 8, 13, 14, 18
LAN-Filtertab. ....	R36
LAN-Link .....	6
LAN-Rx .....	6
LAN-Tx .....	6
LED .....	6
LED-Anzeigen .....	2
Lieferumfang .....	5
Login .....	17
Login-Fehler .....	R47
Login-Sperre .....	26, R48
Login-Versuche .....	26
Lok.-Routing .....	R38

**M**

MAC-Adresse .....	R30
Mailserver .....	43
Management-Information-Base .....	23
Manager .....	22
manueller Verbindungsaufbau .....	R28
Masquerading .....	R32, R35, R41
Maximale-Verb. ....	R47
MIB .....	20

**N**

Name .....	R26
Namenliste .....	R27
Name-Server .....	R33
NAT .....	27, 35

NBNS .....	R34
NBNS-Backup .....	R34
NetBIOS Name Server .....	R34
Network Information Center .....	35
Netzteil .....	5, 7
Netzwerkanschlusses .....	R30
Netzwerknamen .....	41
Netzwerk-Verbindung .....	1
NIC .....	35
Node/Hub-Umschalter .....	7
Node-ID .....	R30
Nummernliste .....	R28

## O

Objekte .....	20
Online-Medien .....	13
Online-Recherchen .....	2
Outband .....	13
Outband-Konfiguration .....	13

## P

PAP .....	R28
Passw.Zwang .....	R47
Password Authentication Protocol .....	R28
Paßwort .....	R28, R32
Paßwortschutz .....	3, 25
PAT .....	27, 35
Power .....	6
PPP-Verhandlung .....	R32
Private Address Spaces .....	R36
Proxy-ARP .....	R35, R38
Pufferspeicher .....	R30

## Q

Quell-Port .....	R37
------------------	-----

## R

R1-Maske .....	R40
Rechner-Namen .....	41
registrierte IP-Adresse .....	R32
Remote Access .....	R38
reservierte Adreßbereiche .....	R36
RIP .....	R40
Router-Name .....	32
Routing-Methode .....	R39

## S

Schnittstellen .....	7
serielle Schnittstelle .....	13
Service-Tab. ....	R41
Setup	
Gebühren-Modul .....	R29
IP-Router-Modul .....	R34
LAN-Modul .....	R30
SNMP-Modul .....	R43
TCP-IP-Modul .....	R31
WAN-Modul .....	R27
Sicherheit .....	25, 26, 27
Sicherheitsfunktionen .....	2
Sicherungsverfahren .....	R28
Single User Access .....	27
SNMP .....	19, R42
Agents .....	19
Manager .....	19
MIB .....	20
Software einspielen .....	17
Software-Update .....	3
Sonstiges .....	R50
Sperre .....	26
Sperr-Minuten .....	R48
Sprache .....	R48
Standard-Route .....	R36
Standort .....	R26, R42
Start-Adresse .....	38
Start-Adreß-Pool .....	R43
statische IP-Adresse .....	R35
statisches Routing .....	31
Status .....	R3
Betriebszeit .....	R4
Config-Statistik .....	R20, R22
Info-Verbindung .....	R23
IP-Router-Statistik .....	R18
LAN-Statistik .....	R6
PPP-Statistik .....	R8
Ruf-Info-Tabelle .....	R24, R25
TCP-IP-Statistik .....	R13
Verb.-Statistik .....	R23
Verbindung .....	R4
WAN-Statistik .....	R4

Werte-löschen .....	R25
Statusanzeigen .....	2
System-Boot .....	R50
System-Reset .....	R50
System-Upload .....	R50

## ■ T

Tab.-Masquerade .....	R41
Tabelle-RIP .....	R40
Tage / Periode .....	R29
TCP .....	R37, R42
TCP/IP .....	8, 14, 31
TCP/IP-Netze .....	41
TCP-Aging-Min .....	R34
TCP-Max.-Verb. ....	R34
Technische Daten .....	45
Teleworker .....	R38
Telnet .....	3, 10
Telnet-Server .....	R33
Terminalprogramm .....	3
TFTP .....	14
TFTP-Server .....	R33
Timeout .....	R45
TOS .....	R39
Trap .....	22
Trap-IP .....	R42
Traps-senden .....	R42
Typ .....	R40
Type-of-Service .....	37, R39

## ■ U

Überprüfungen der Gegenstelle .....	R28
Überprüfungsversuche .....	R28

Überwachung .....	R30
UDP .....	R37, R42
Upload .....	3, 17
Username .....	R28

## ■ V

V.24-Konfigurationsschnittstelle .....	7
Verbindungsbegrenzung .....	28
verbotene Adreßbereiche .....	R36
Versions- Tabelle .....	R48

## ■ W

WAN-Anschluß .....	2
WAN-Config .....	R47
WAN-Filtertab. ....	R38
Wildcards .....	44
winipcfg .....	9
WWW .....	27

## ■ X

XModem .....	18
--------------	----

## ■ Z

Zeit .....	R4, R28, R48
Zeitabhängige Verbindungsbegrenzung .....	28
Zeitbudget .....	28
Ziel-Adresse .....	R38
Ziel-Netzmaske .....	R38
Zielnetzwerk .....	R35
Ziel-Port .....	R36, R37
Zugangskontrolle .....	26
Zugangsliste .....	R32
Zugriffschutz .....	3
Zustand .....	R31, R35

# Beschreibung der Menüpunkte

Der Menübaum der *ELSA LANCOM*-Konfiguration ist in sogenannte Status-Informationen, Setup-Parameter, Firmware-Informationen und Sonstiges aufgeteilt.







Zur leichten Orientierung zeigen wir Ihnen zunächst eine Übersicht über die Menüstruktur.

In der vollständigen Liste aller Menüpunkte finden Sie anschließend die genaue Beschreibung aller Anzeigen, Menüs und Aktionen mit den zugehörigen Parametern, Standardwerten und Eingabemöglichkeiten.

Sie erreichen die Menüs bei Konfigurationen über Telnet oder Terminal-Programme sowie über SNMP (siehe auch 'Konfigurationsmöglichkeiten').












Bei der Konfiguration mit *ELSA LANconfig* steht Ihnen ein integriertes Hilfesystem mit Kurzbeschreibungen zu den einzelnen Parametern zur Verfügung.

## Symbole







	Menü	zeigt ein weiteres Untermenü an.
	Info	zeigt einen Wert an, der nicht verändert werden kann.
	Wert	zeigt einen Wert an, der verändert werden kann.
	Tabelle	zeigt eine Tabelle an, deren Einträge verändert werden können.
	Info-Tabelle	zeigt eine Tabelle an, deren Einträge nicht verändert werden können.
	Aktion	führt eine Aktion aus.

## Menü-Übersicht


















### **Setup**

-  Name
-  WAN-Modul
-  Gebühren-Modul
-  LAN-Modul
-  TCP-IP-Modul
-  IP-Router-Modul
-  SNMP-Modul
-  DHCP-Modul
-  DNS-Modul
-  Config-Modul
-  Zeit-Modul





### **Firmware**

-  Versions-Tabelle
-  Tabelle-Firmsafe
-  Modus-Firmsafe
-  Timeout-Firmsafe
-  Test-Firmware
-  Firmware-Upload

### **Status**

-  Verbindung
-  Aktuelle-Zeit
-  Betriebszeit
-  WAN-Statistik
-  LAN-Statistik
-  PPP-Statistik
-  TCP-IP-Statistik
-  IP-Router-Statistik
-  Config-Statistik
-  DSL-Statistik
-  Queue-Statistik
-  Verbindungs-Statistik
-  Info-Verbindung
-  Gegenstellen-Statistik
-  Kanalstatistik
-  Zeit-Statistik
-  Werte löschen

### **Sonstiges**

-  Manuelle Wahl
-  System-Boot
-  System-Reset
-  System-Upload

## Status

Das Menü 'Status' enthält Informationen zum aktuellen Status und über interne Abläufe im LAN und im WAN, die sich auf die Datenübertragungs-Strecke (z.B. Anwahl bzw. Verbindung) oder Statistiken (z.B. Anzahl empfangener bzw. gesendeter Datenblöcke) beziehen können. Die statistischen Anzeigen bieten eine leistungsfähige Hilfestellung bei der Überprüfung der korrekten Arbeitsweise und bei der Optimierung der Parametereinstellung. Darüber hinaus liefern sie bei einem Fehlverhalten wertvolle Informationen zur Fehleranalyse.

Die meisten Statusanzeigen werden laufend aktualisiert und können mit einer im jeweiligen Menü enthaltenen **Werte löschen**-Aktion auf 0 gesetzt werden.

Das Menü besitzt den folgenden Aufbau:

Status		Fortlaufende Statusanzeigen
Verbindung		Zustand der WAN-Strecke
Aktuelle-Zeit		Aktuelle Zeit im Gerät
Betriebszeit		Betriebszeit des Gerätes seit dem letzten Einschalten
WAN-Statistik		Anzeige der WAN-Statistiken
LAN-Statistik		Statistiken des Netzwerk-Bereichs
PPP-Statistik		Statistiken des Point-to-Point-Protokolls
TCP-IP-Statistik		Statistiken aus dem TCP/IP-Bereich
IP-Router-Statistik		Statistiken aus dem IP-Router
Config-Statistik		Statistiken der Remote-Konfiguration
DSL-Statistik		Statistiken der DSL-Verbindung
Queue-Statistik		Statistiken über die Pakete in den Queues der einzelnen Module
Verbindungs-Statistik		Verbindungs-Informationen für jedes Interface
Info-Verbindung		Informationen zur letzten Verbindung für jedes Interface
Gegenstellen-Statistik		Statistik über die letzten 100 Verbindungen
Kanal-Statistik		Informationen über den Zustand der einzelnen Kanäle.
Zeit-Statistik		Informationen aus dem Zeit-Modul
Werte löschen		Alle Werte außer Tabellen der untergeordnet. Statistik löschen

## Status/Verbindung

Der Menüpunkt **Status/Verbindung** gibt die Statusmeldungen der einzelnen Kanäle wieder.

/Verbindung	Fortlaufende Statusanzeigen
Verbindung	 CH01: Bereit

## Status/Aktuelle-Zeit

Hier wird die aktuelle Zeit des Gerätes angezeigt, die z.B. für einige Statistiken verwendet wird. Diese Zeit kann manuell gesetzt werden (mit dem Befehl 'time').










## Status/Betriebszeit

Hier wird die Betriebszeit des Routers seit dem letzten Einschalten in Tagen, Stunden, Minuten und Sekunden angezeigt.

## Status/WAN-Statistik

Unter diesem Menüpunkt werden verschiedene statistische Parameter des WAN-Anschlusses angezeigt. Viele Werte über das übertragene Datenvolumen liefern nützliche Informationen über die Auslastung des WAN-Anschlusses, aufgetretene Fehler und im aktuellen Betriebszustand vorhandene interne Ressourcen der Geräte.

Das Menü **Status/WAN-Statistik** besitzt folgenden Aufbau:

/WAN-Statistik	Fortlaufende Statusanzeigen
Byte-Transport-Statistik	 Statistik für übertragene Bytes
Paket-Transport-Statistik	 Statistik für übertragene Daten-Pakete
Fehler-Statistik	 Statistik über aufgetretene Übertragungsfehler
WAN-Tx-Verworfen	 Anzahl durch Fehler/Ressourcenmangel verworfener Pakete
WAN-Heap-Pakete	 Anzahl belegter Puffer
WAN-Queue-Pakete	 Anzahl verfügbarer Puffer
WAN-Queue-Fehler	 Anzahl durch Puffermangel verworfener Datenpakete
Durchsatz-Statistik	 Statistik für die aktuell übertragenen Bytes
Werte löschen	 WAN-Statistik löschen



*Byte-Transport-Statistik*

Der Menüpunkt **Status/WAN-Statistik/Byte-Transport-Statistik** enthält für jedes verfügbare Interface eine Statistik über die auf diesem Interface übertragenen Bytes. Die dort aufgeführte Tabelle hat folgendes Aussehen:

Ifc	CRx-Bytes	Rx-Bytes	Tx-Bytes	CTx-Bytes
Ch01	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
CRx-Bytes	Anzahl der empfangenen Bytes (komprimiert)
Rx-Bytes	Anzahl der empfangenen Bytes (unkomprimiert)
Tx-Bytes	Anzahl der gesendeten Bytes (unkomprimiert)
CTx-Bytes	Anzahl der gesendeten Bytes (komprimiert)

*Paket-Transport-Statistik*

Der Menüpunkt **Status/WAN-Statistik/Paket-Transport-Statistik** enthält für jedes verfügbare Interface eine Statistik über die auf diesem Interface übertragenen Datenpakete. Die dort aufgeführte Tabelle hat folgendes Aussehen:

Ifc	Rx	Tx-gesamt	Tx-normal	Tx-gesichert	Tx-urgent
Ch01	0	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
Rx	Anzahl der empfangenen Pakete
Tx-gesamt	Anzahl der gesendeten Pakete (Daten- und Protokoll-Pakete)
Tx-normal	Anzahl der gesendeten normalen Daten-Pakete
Tx-gesichert	Anzahl der gesichert übertragenen Daten-Pakete
Tx-urgent	Anzahl der bevorzugt übertragenen Daten-Pakete (Urgent-Queue)

*Fehler-Statistik*

Der Menüpunkt **Status/WAN-Statistik/Fehler-Stat.** enthält für jedes verfügbare Interface eine Statistik über die auf diesem Interface aufgetretenen Übertragungsfehler. Die dort aufgeführte Tabelle hat folgendes Aussehen:

Ifc	Rx-L1-F.	Rx-L2-F.	Rx-L3-F.	Stack-F.	Tx-Fehler
Ch01	0	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
Rx-L1-F.	Anzahl Layer-1-Fehler bei empfangenen Daten (analog zu Layer-3-Fehlern)
Rx-L2-F.	Anzahl Layer-2-Fehler bei empfangenen Daten (d.h., analog zu den Layer-3-Fehlern, z.B. defekter PPP-Header)
Rx-L3-F.	Anzahl Layer-3-Fehler bei empfangenen Daten (d.h., der Protokoll-Header der Layer-3 ist nicht korrekt)
Stack-F.	Anzahl Stack-Fehler bei empfangenen Daten. Stack-Fehler entstehen durch empfangene Frames, die keinem internen Verarbeitungsprozeß (z.B. IP Router) zugeordnet werden können.
Tx-Fehler	Anzahl Übertragungsfehler beim Senden

*Durchsatz-Statistik*

Der Menüpunkt **Status/WAN-Statistik/Durchsatz-Statistik** enthält eine Statistik über die auf diesem Interface übertragenen Bytes. Die dort aufgeführte Tabelle hat folgendes Aussehen:







Ifc	Rx/s aktuell	Tx/s aktuell	Rx/s gemittelt	Tx/s gemittelt
Ch01	0	0	0	0

















Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
Rx/s aktuell	Durchsatz auf dem Kanal in der letzten Sekunde in Empfangsrichtung
Tx/s aktuell	Durchsatz auf dem Kanal in der letzten Sekunde in Senderichtung
Rx/s gemittelt	mittlerer Durchsatz auf dem Kanal in Empfangsrichtung
Tx/s gemittelt	mittlerer Durchsatz auf dem Kanal in Senderichtung

## Status/LAN-Statistik










Analog zum vorherigen Menüpunkt werden hier die für den LAN-Anschluß relevanten Statistiken angezeigt. Das Menü **Status/LAN-Statistik** besitzt folgenden Aufbau:

/LAN-Statistik	Fortlaufende Statusanzeigen	
LAN-Rx-Pakete		Anzahl empfangener Datenpakete
LAN-Tx-Pakete		Anzahl gesendeter Datenpakete
LAN-Rx-Fehler		Anzahl fehlerhaft empfangener Datenpakete
LAN-Tx-Fehler		Anzahl fehlerhaft gesendeter Datenpakete
LAN-Stack-Fehler		Anzahl Pakete ohne passendes Empfangsmodul (IP-Router)
LAN-NIC-Fehler		Anzahl vom NIC verworfener Datenpakete

/LAN-Statistik		Fortlaufende Statusanzeigen
LAN-Heap-Pakete		Anzahl verfügbarer Puffer
LAN-Queue-Pakete		Anzahl belegter Puffer
LAN-Queue-Fehler		Anzahl durch Puffermangel verworfener Pakete
LAN-Kollisionen		Anzahl Kollisionen während des Sendevorgangs
Verbindung-aufgebaut		Anzeige der korrekten Verbindung auf dem Ethernet (Datenübertragung möglich). Entspricht der 'Link'-LED am Gerät.
Verhandlung-abgeschlossen		Die Aushandlung der Übertragungsart zwischen Router und Gegenstelle ist abgeschlossen. Hat nur eine Bedeutung, wenn Setup/LAN-/Anschluss auf 'Auto' steht.
Anschluß		Dieser Punkt zeigt an, welche Übertragungsart momentan auf dem Ethernet-Anschluß gefahren wird: 10B-TX: 10 Mbit, halbduplex FD10B-TX: 10 Mbit, voll duplex 100B-TX: 100 Mbit, halbduplex FD100B-TX: 100 Mbit, voll duplex Wenn unter Setup/LAN- als Anschluß 'Auto' eingestellt ist, ist dies die Übertragungsart, die beide Seiten untereinander ausgehandelt haben, entspricht also den 'Fast' und 'FDpx'-LEDs am Gerät. Ist dagegen eine feste Übertragungsart eingestellt, ist dieser Wert gleich dem in Setup/LAN-/Anschluss.
LAN-Rx-Bytes		Anzahl vom LAN empfangener Zeichen
LAN-Tx-Bytes		Anzahl zum LAN gesendeter Zeichen
LAN-Rx-Broadcasts		Anzahl vom LAN empfangener Broadcast-Pakete
LAN-Rx-Multicasts		Anzahl vom LAN empfangener Multicast-Pakete
LAN-Rx-Unicasts		Anzahl vom LAN empfangener direkt adressierter Pakete
WAN-Rx-Broadcasts		Anzahl vom WAN empfangener Broadcasts
WAN-Rx-Multicasts		Anzahl vom WAN empfangener Multicasts
WAN-Rx-Unicasts		Anzahl vom WAN empfangener Unicasts
Werte löschen		LAN-Statistik löschen

## Status/PPP-Statistik

Innerhalb der PPP-Statistik werden die Zustände einzelner Sub-Protokolle des PPPs für jedes Interface separat verwaltet. Die Statistiken der übertragenen Frames einzelner Sub-Protokolle werden dagegen nur innerhalb einer gemeinsamen Statistik mitgeführt. Das Menü **Status/PPP-Statistik** besitzt daher folgenden Aufbau:

/PPP-Statistik		Fortlaufende Statusanzeigen
Zustände		Statistik über Zustand der PPP-Protokollverhandlung für jedes Interface
LCP-Statistik		Anzeige der PPP/LCP-Statistiken
PAP-Statistik		Anzeige der PPP/PAP-Statistik
CHAP-Statistik		Anzeige der PPP/CHAP-Statistik
IPCP-Statistik		Anzeige der PPP/IPCP-Statistik
CCP-Statistik		Anzeige der PPP/CCP-Statistik
Rx-Optionen		Anzeige der empfangenen LCP- und IPCP-Informationen
Tx-Optionen		Anzeige der gesendeten LCP- und IPCP-Informationen
Werte löschen		Löschen der PPP-Statistiken

Die PPP-Statistik gibt insbesondere bei Connect-Problemen mit Fremdprodukten genauen Aufschluß über den Verlauf einer PPP-Verhandlung. Sie enthält entscheidende Hinweise für eine Fehlerdiagnose.

### Zustände

Der Menüpunkt **Status/PPP-Statistik/Zustände** enthält für jedes verfügbare Interface eine Liste der aktuellen Zustände der PPP-Protokollverhandlung. Die dort aufgeführte Tabelle hat folgendes Aussehen:

Ifc	Phase	LCP	IPCP	CCP
Ch01	DEAD	Initial	Initial	Initial

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
Phase	enthält die Phase, in der sich das PPP befindet. Mögliche Werte sind <b>AUTHENTICAT</b> , <b>NETWORK</b> und <b>TERMINATE</b> .
LCP	Zustand des Subprotokolls 'Link-Control-Protokoll'. Mögliche Werte sind: <b>Initial</b> , <b>Startng</b> , <b>Stoppng</b> , <b>Stopped</b> , <b>Closing</b> , <b>Closed</b> , <b>ReqSent</b> , <b>AckRcvd</b> , <b>AckSent</b> und <b>Opened</b> .
IPCP	analog zu 'LCP' wird hier der Zustand des Subprotokolls 'IP-Control-Protocol' angezeigt.
CCP	analog zu 'LCP' wird hier der Zustand des Subprotokolls 'Compression-Control-Protocol' angezeigt.

Unter **Status/PPP-Statistik/Zustände** wird die jeweilige Phase des PPPs aktuell angezeigt. Diese Zustände sind, wie oben angegeben, Ruhezustand (Dead), Bereitschaftszustand (Establish), Überprüfung der Zugangsparameter (Authenticate) und Netzwerkphase (Network). In den Unterstatistiken werden die ausgetauschten Frames nach Art und Menge gesondert aufgeschlüsselt.

### Status/PPP-Statistik/LCP-Statistik

Das **LCP** (Link Control Protocol) verhandelt die grundlegenden Eigenschaften der PPP-Verbindungen. Die während der PPP-Verhandlung ausgetauschten LCP-Frames werden nach Art und Anzahl statistisch erfaßt und angezeigt. Sollte das LCP bei einer Verbindung nicht in den OPEN-Zustand wechseln, geben diese Statistikwerte Hinweise auf Fehler, die in der Anfangsphase der PPP-Verhandlung aufgetreten sind. Die Parameter in dieser Statistik bedeuten im einzelnen:

Rx-Fehler	Anzahl fehlerhaft empfangener PPP-Pakete
Rx-Verworfen	Anzahl verworfener PPP-Pakete
Rx-Config-Request	Anzahl empfangener Configure-Request-Pakete für LCP
Rx-Config-Ack.	Anzahl empfangener Configure-Acknowledge-Pakete für LCP
Rx-Config-Nack.	Anzahl empfangener Configure-Negative Acknowledge-Pakete
Rx-Config-Reject	Anzahl empfangener Configure-Reject-Pakete für LCP
Rx-Term-Request	Anzahl empfangener Terminate-Request-Pakete für LCP
Rx-Term-Ack	Anzahl empfangener Terminate-Acknowledge-Pakete für LCP
Rx-Code-Reject	Anzahl empfangener Code-Reject-Pakete für PPP
Rx-Protocol-Reject	Anzahl empfangener Protocol-Reject-Pakete für PPP
Rx-Echo-Request	Anzahl empfangener Echo-Request-Pakete für LCP
Rx-Echo-Reply	Anzahl empfangener Echo-Response-Pakete für LCP
Rx-Discard-Request	Anzahl empfangener Discard-Request-Pakete für LCP
Tx-Config-Request	Anzahl gesendeter Configure-Request-Pakete für LCP
Tx-Config-Ack.	Anzahl gesendeter Configure-Acknowledge-Pakete für LCP
Tx-Config-Nack.	Anzahl gesendeter Configure-Negative-Acknowledge-Pakete
Tx-Config-Reject	Anzahl gesendeter Configure-Reject-Pakete für LCP
Tx-Term-Request	Anzahl gesendeter Terminate-Request-Pakete für LCP
Tx-Term-Ack.	Anzahl gesendeter Terminate-Acknowledge-Pakete für LCP
Tx-Code-Reject	Anzahl gesendeter Code-Reject-Pakete für PPP
Tx-Protocol-Reject	Anzahl gesendeter Protocol-Reject-Pakete für PPP
Tx-Echo-Request	Anzahl gesendeter Echo-Request-Pakete für LCP
Tx-Echo-Reply	Anzahl gesendeter Echo-Response-Pakete für LCP
Tx-Discard-Request	Anzahl gesendeter Discard-Request-Pakete für LCP
Werte löschen	LCP-Statistik löschen

**Status/PPP-Statistik/PAP-Statistik**

Das **PAP** (Password Authentication Protocol) ist eines von zwei üblichen Verfahren zur Überprüfung von Gegenstellen im PPP. Es überprüft beim Verbindungsaufbau einmalig das Paßwort der Gegenstelle und läßt die Verbindung nur nach erfolgreichem Paßwort austausch zu (siehe auch Kapitel 'Point-to-Point Protocol'). Die Parameter in dieser Statistik bedeuten im einzelnen:

Rx-Verworfen	Anzahl verworfener PAP-Pakete
Rx-Request	Anzahl empfangener PAP-Request-Pakete
Rx-Success	Anzahl empfangener PAP-Success-Pakete
Rx-Failure	Anzahl empfangener PAP-Failure-Pakete
Tx-Retry	Anzahl gesendeter Wiederholungen von PAP-Request-Paketen
Tx-Request	Anzahl gesendeter PAP-Request-Pakete
Tx-Success	Anzahl gesendeter PAP-Success-Pakete
Tx-Failure	Anzahl gesendeter PAP-Failure-Pakete
Werte löschen	PAP-Statistik löschen

**Status/PPP-Statistik/CHAP-Statistik**

Das **CHAP** (Challenge Authentication Protocol) ist die zweite Möglichkeit, Gegenstellen unter PPP zu überprüfen. Dabei findet eine Paßwortüberprüfung beim Verbindungsaufbau und erneut in einstellbaren Abständen während der Verbindung statt (siehe auch Kapitel 'Point-to-Point Protocol'). Die Parameter in dieser Statistik bedeuten im einzelnen:

Rx-Verworfen	Anzahl verworfener CHAP-Pakete
Rx-Challenge	Anzahl empfangener CHAP-Challenge-Pakete
Rx-Response	Anzahl empfangener CHAP-Response-Pakete
Rx-Success	Anzahl empfangener CHAP-Success-Pakete
Rx-Failure	Anzahl empfangener CHAP-Failure-Pakete
Tx-Retry	Anzahl gesendeter Wiederholungen v. CHAP-Challenge-Paketen
Tx-Challenge	Anzahl gesendeter CHAP-Challenge-Pakete
Tx-Response	Anzahl gesendeter CHAP-Response-Pakete
Tx-Success	Anzahl gesendeter CHAP-Success-Pakete
Tx-Failure	Anzahl gesendeter CHAP-Failure-Pakete
Werte löschen	CHAP-Statistik löschen

### Status/PPP-Statistik/IPCP-Statistik

Das **IPCP** (Internet Protocol Control Protocol) zeigt bei Verwendung von IP den Zustand des Protokolls und die zur Verhandlung ausgetauschten Pakete.

Rx-verworfen	Anzahl verworfener IPCP-Pakete
Rx-Config-Request	Anzahl empfangener Configure-Request-Pakete für IPCP
Rx-Config-Ack.	Anzahl empfangener Configure-Acknowledge-Pakete für IPCP
Rx-Config-Nack.	Anzahl empfangener Configure-Negative-Acknowledge-Pakete
Rx-Config-Reject	Anzahl empfangener Configure-Reject-Pakete für IPCP
Rx-Term-Request	Anzahl empfangener Terminate-Request-Pakete für IPCP
Rx-Term-Ack.	Anzahl empfangener Terminate-Acknowledge-Pakete für IPCP
Rx-Code-Reject	Anzahl empfangener Code-Reject-Pakete für IPCP
Tx-Config-Request	Anzahl gesendeter Configure-Request-Pakete für IPCP
Tx-Config-Ack.	Anzahl gesendeter Configure-Acknowledge-Pakete für IPCP
Tx-Config-Nack.	Anzahl gesendeter Configure-Negative-Acknowledge-Pakete
Tx-Config-Reject	Anzahl gesendeter Configure-Reject-Pakete für IPCP
Tx-Term-Request	Anzahl gesendeter Terminate-Request-Pakete für IPCP
Tx-Term-Ack.	Anzahl gesendeter Terminate-Acknowledge-Pakete für IPCP
Tx-Code-Reject	Anzahl gesendeter Code-Reject-Pakete für IPCP
Werte löschen	IPCP-Statistik löschen

### Status/PPP-Statistik/CCP-Statistik

In der Statistik zum Compression Control Protocol (CCP) finden Sie die während der PPP-Verhandlung ausgetauschten Pakete zur Datenkompression.

Rx-verworfen	Anzahl aller verworfenen CCP-Pakete
Rx-Config-Request	Anzahl der empfangenen CCP-Anfragen
Rx-Config-Ack.	Anzahl der akzeptierten CCP-Anfragen
Rx-Config-Nak.	Anzahl der CCP-Anfragen, die aufgrund nicht akzeptierter Parameter der Anfrage zurückgewiesen wurden.
Rx-Config-Reject	Anzahl der CCP-Anfragen, die aufgrund anderer Gründe zurückgewiesen wurden.
Rx-Termination-Request	Anzahl der CCP-Anfragen nach einem Abbau der Kompression.
Rx-Termination-Ack.	Anzahl der bestätigten CCP-Anfragen nach einem Abbau der Kompression.
Rx-Code-Reject	Anzahl der zurückgewiesenen CCP-Anfragen, weil die Gegenstelle keine Kompression einsetzen will oder kann.
Rx-Reset-Request	Anzahl der CCP-Anfragen nach einer Synchronisation der Kompression (z.B. nach Übertragungsfehlern)

Rx-Reset-Ack	Anzahl der bestätigten CCP-Anfragen nach einer Synchronisation der Kompression
Tx-Config-Request	Anzahl der gesendeten CCP-Anfragen
Tx-Config-Ack.	Anzahl der von der Gegenstelle akzeptierten CCP-Anfragen
Tx-Config-Nak.	Anzahl der CCP-Anfragen, die von der Gegenstelle aufgrund nicht akzeptierter Parameter der Anfrage zurückgewiesen wurden.
Tx-Config-Reject	Anzahl der CCP-Anfragen, die von der Gegenstelle aufgrund anderer Gründe zurückgewiesen wurden.
Tx-Termination-Request	Anzahl der gesendeten CCP-Anfragen nach einem Abau der Kompression.
Tx-Termination-Ack.	Anzahl der gesendeten CCP-Bestätigungen für den Abau der Kompression.
Tx-Code-Reject	Anzahl der zurückgewiesenen CCP-Anfragen, weil der <i>ELSA LANCOM</i> keine Kompression einsetzen will (durch Einstellung in der Layer-Liste).
Tx-Reset-Request	Anzahl der gesendeten CCP-Anfragen nach einer Synchronisation der Kompression (z.B. nach Übertragungsfehlern)
Tx-Reset-Ack	Anzahl der gesendeten CCP-Bestätigungen für eine Synchronisation der Kompression
Werte-löschen	CCP-Statistik löschen



### Status/PPP-Statistik/Rx- und Tx-Optionen

In den Optionen der PPP-Statistik wird aufgezeichnet, welche Informationen bei der Verhandlung über LCP oder IPCP ausgetauscht werden.

*Rx-Optionen* Hier kann nachgeschaut werden, was die Gegenstelle angefordert (LCP) bzw. was dem Router zugewiesen (IPCP) wurde.

*Tx-Optionen* Hier kann nachgeschaut werden, was der Router von der Gegenstelle angefordert (LCP) bzw. was er dieser zugewiesen (IPCP) hat.

Die beiden Untermenüs besitzen jeweils den gleichen Aufbau:

/Rx- und Tx-Optionen	Anzeige	
LCP		Informationen über Paketgrößen, Steuerzeichen, Sicherungsverfahren und Rückruf
IPCP		Informationen über Adressen im IP-Netzwerk

In der Tabelle LCP sind für jeden Kanal gesondert aufgeführt:

MRU	<b>M</b> aximum <b>R</b> ecieve <b>U</b> nit, kennzeichnet die maximale Paketgröße, die die Gegenstelle empfangen kann
Authent.	verwendetes Authentifizierungsverfahren (PAP/CHAP)
Magic-Num	verwendete Magic-Number zur Erkennung von Schleifen











Zu guter Letzt stehen unter IPCP die ausgehandelten IP-Optionen wieder nach Kanal getrennt:

IP-Adresse	auch hier gilt wieder, daß in den Rx-Optionen, die Adressen stehen, die von der Gegenstelle zugewiesen wurden, und unter den Tx-Optionen die stehen, die der <i>ELSA LANCOM</i> der Gegenstelle zuweist (damit ist z.B. ganz einfach die IP-Adresse des Wahlknotens beim Internet-Provider in den Tx-Optionen abzulesen).
DNS-Default	
NBNS-Default	

## Status/TCP-IP-Statistik

Hier werden die Statistiken aus dem TCP/IP-Bereich dargestellt, gegliedert nach verschiedenen Typen von Subprotokollen des TCP/IP. In der TCP-IP-Statistik finden Sie die folgenden Parameter:

/TCP-IP-Statistik		Statistiken aus dem TCP/IP-Bereich
ARP-Statistik		Statistiken aus dem ARP-Bereich
IP-Statistik		Statistiken aus dem IP-Bereich
ICMP-Statistik		Statistiken für ICMP-Pakete
TFTP-Statistik		Statistiken für TFTP-Operationen
TCP-Statistik		Statistiken für TCP-Pakete von TCP-Sitzungen zum Router
DHCP-Statistik		Statistiken aus dem DHCP-Server
DNS-Statistik		Statistiken aus dem DNS-Server
Werte löschen		TCP/IP-Statistiken löschen

In den Unterstatistiken finden Sie dann die weiteren Parameter zu den einzelnen Menüs.

### Status/TCP-IP-Statistik/ARP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

ARP-LAN-Rx	Anzahl vom LAN empfangener ARP-Anfragen und -Antworten
ARP-LAN-Tx	Anzahl zum LAN gesendeter ARP-Anfragen und -Antworten
ARP-LAN-Fehler	Anzahl vom LAN fehlerhaft empfangener ARP-Anfragen
ARP-WAN-Rx	Anzahl vom WAN empfangener ARP-Anfragen und -Antworten
ARP-WAN-Tx	Anzahl zum WAN gesendeter ARP-Anfragen und -Antworten
ARP-WAN-Fehler	Anzahl vom WAN fehlerhaft empfangener ARP-Anfragen
Tabelle-ARP	Anzeige der ARP-Tabelle
Werte löschen	ARP-Statistiken löschen

*Tabelle-ARP*

In der **ARP-Tabelle** finden Sie 128 Einträge mit ARP-Informationen. Sie hat den folgenden Aufbau:

IP-Adresse	Node-ID	Letzter Zugriff	Anschluß
IP-Adresse, die schon einmal über ARP-Request gefunden wurde	zugehörige MAC-Adresse	Zeit seit dem letzten Zugriff in tics	lokal oder remote

### Status/TCP-IP-Statistik/IP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

IP-LAN-Rx	Anzahl vom LAN empfangener IP-Pakete
IP-LAN-Tx	Anzahl zum LAN gesendeter IP-Pakete
IP-LAN-Checksummen-Fehler	Anzahl vom LAN fehlerhaft empfangener IP-Pakete
IP-LAN-Service-Fehler	Anzahl vom LAN empfangener IP-Pakete für falschen Dienst
IP-LAN-Fragmentierungs-Fehler	Anzahl zum LAN zu sendender, unfragmentierbarer IP-Pakete
IP-LAN-Fragmentierungen	Anzahl zum LAN gesendeter, fragmentierter IP-Pakete
IP-LAN-Fragmentierungen-erzwungen	Anzahl zum LAN gesendeter IP-Pakete mit minimaler Größe
IP-WAN-Fragmentierungs-Fehler	Anzahl zum WAN zu sendender, unfragmentierbarer IP-Pakete
IP-WAN-Fragmentierungen	Anzahl zum WAN gesendeter, fragmentierter IP-Pakete
IP-WAN-Fragmentierungen-erzwungen	Anzahl zum WAN gesendeter IP-Pakete mit minimaler Größe
IP-WAN-Rx	Anzahl vom WAN empfangener IP-Pakete
IP-WAN-Tx	Anzahl zum WAN gesendeter IP-Pakete
IP-WAN-Checksummen-Fehler	Anzahl vom WAN fehlerhaft empfangener IP-Pakete
IP-WAN-Service-Fehler	Anzahl vom WAN empfangener IP-Pakete für falschen Dienst
IP-WAN-Rx-verworfen	Anzahl vom WAN durch Time-Out-Management verworfener Pakete
Werte löschen	IP-Statistiken löschen

### Status/TCP-IP-Statistik/ICMP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

ICMP-LAN-Rx	Anzahl vom LAN empfangener ICMP-Pakete
ICMP-LAN-Tx	Anzahl zum LAN gesendeter ICMP-Pakete
ICMP-LAN-Checksummen-Fehler	Anzahl vom LAN fehlerhaft empfangener ICMP-Pakete
ICMP-LAN-Service-Fehler	Anzahl vom LAN empfangener, nicht unterstützter ICMP-Pakete
ICMP-WAN-Rx	Anzahl vom WAN empfangener ICMP-Pakete
ICMP-WAN-Tx	Anzahl zum WAN gesendeter ICMP-Pakete

ICMP-WAN-Checksummen-Fehler	Anzahl vom WAN fehlerhaft empfangener ICMP-Pakete
ICMP-WAN-Service-Fehler	Anzahl vom WAN empfangener, nicht unterstützter ICMP-Pakete
Werte löschen	ICMP-Statistiken löschen

### Status/TCP-IP-Statistik/TCP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

TCP-LAN-Rx	Anzahl vom LAN empfangener TCP-Pakete
TCP-LAN-Tx	Anzahl zum LAN gesendeter TCP-Pakete
TCP-LAN-Tx-Wdh.	Anzahl zum LAN wiederholt gesendeter TCP-Pakete
TCP-LAN-Checksummen-Fehler	Anzahl vom LAN fehlerhaft empfangener TCP-Pakete
TCP-LAN-Service-Fehler	Anzahl vom LAN empfangener TCP-Pakete für falschen Port
TCP-LAN-Verbindungen	Anzahl der aktuellen TCP-Verbindungen vom LAN
TCP-WAN-Rx	Anzahl vom WAN empfangener TCP-Pakete
TCP-WAN-Tx	Anzahl zum WAN gesendeter TCP-Pakete
TCP-WAN-Tx-Wiederholungen	Anzahl zum WAN wiederholt gesendeter TCP-Pakete
TCP-WAN-Checksummen-Fehler	Anzahl vom WAN fehlerhaft empfangener TCP-Pakete
TCP-WAN-Service-Fehler	Anzahl vom WAN empfangener TCP-Pakete für falschen Port
TCP-WAN-Verbindungen	Anzahl aktueller TCP-Verbindungen vom WAN
Werte löschen	TCP-Statistiken löschen

### Status/TCP-IP-Statistik/TFTP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

TFTP-LAN-Rx	Anzahl vom LAN empfangener TFTP-Pakete
TFTP-LAN-Rx-Read-Request	Anzahl vom LAN empfangener TFTP-Read-Requests
TFTP-LAN-Rx-Write-Request	Anzahl vom LAN empfangener TFTP-Write-Requests
TFTP-LAN-Rx-Data	Anzahl vom LAN empfangener TFTP-Daten-Pakete
TFTP-LAN-Rx-Ack.	Anzahl vom LAN empfangener TFTP-Acknowledges
TFTP-LAN-Rx-Option-Ack.	Anzahl vom LAN empfangener TFTP-Option-Acknowledges
TFTP-LAN-Rx-Fehler	Anzahl vom LAN empfangener TFTP-Error-Pakete
TFTP-LAN-Rx-unb.	Anzahl vom LAN empfangener, unbekannter TFTP-Pakete
TFTP-LAN-Tx	Anzahl auf das LAN gesendeter TFTP-Pakete
TFTP-LAN-Tx-Data	Anzahl auf das LAN gesendeter TFTP-Daten-Pakete
TFTP-LAN-Tx-Ack.	Anzahl auf das LAN gesendeter TFTP-Acknowledges
TFTP-LAN-Tx-Option-Ack.	Anzahl auf das LAN gesendeter TFTP-Option-Ack
TFTP-LAN-Tx-Fehler	Anzahl auf das LAN gesendeter TFTP-Error-Pakete
TFTP-LAN-Tx-Wiederholungen	Anzahl wiederholt aufs LAN gesendeter TFTP-Pakete

TFTP-LAN-Verbindungen	Anzahl zum LAN aufgebauter TFTP-Verbindungen
TFTP-WAN-Rx	Anzahl vom WAN empfangener TFTP-Pakete
TFTP-WAN-Rx-Read-Request	Anzahl vom WAN empfangener TFTP-Read-Requests
TFTP-WAN-Rx-Write-Request	Anzahl vom WAN empfangener TFTP-Write-Requests
TFTP-WAN-Rx-Data	Anzahl vom WAN empfangener TFTP-Daten-Pakete
TFTP-WAN-Rx-Ack.	Anzahl vom WAN empfangener TFTP-Acknowledges
TFTP-WAN-Rx-Option-Ack.	Anzahl vom WAN empfangener TFTP-Option-Acknowledges
TFTP-WAN-Rx-Fehler	Anzahl vom WAN empfangener TFTP-Error-Pakete
TFTP-WAN-Rx-unb.	Anzahl vom WAN empfangener, unbekannter TFTP-Pakete
TFTP-WAN-Tx	Anzahl auf das WAN gesendeter TFTP-Pakete
TFTP-WAN-Tx-Data	Anzahl auf das WAN gesendeter TFTP-Daten-Pakete
TFTP-WAN-Tx-Ack.	Anzahl auf das WAN gesendeter TFTP-Acknowledges
TFTP-WAN-Tx-Option-Ack.	Anzahl auf das WAN gesendeter TFTP-Option-Ack
TFTP-WAN-Tx-Fehler	Anzahl auf das WAN gesendeter TFTP-Error-Pakete
TFTP-WAN-Tx-Wiederholungen	Anzahl wiederholt aufs WAN gesendeter TFTP-Pakete
TFTP-WAN-Verbindungen	Anzahl zum WAN aufgebauter TFTP-Verbindungen
Werte löschen	TFTP-Statistik löschen

### **Status/TCP-IP-Statistik/DHCP-Statistik**

In dieser Statistik werden die folgenden Werte angezeigt:

DHCP-LAN-Rx	Anzahl aus dem LAN empfangener DHCP-Pakete
DHCP-LAN-Tx	Anzahl in das LAN gesendeter DHCP-Pakete
DHCP-WAN-Rx	Anzahl aus dem WAN empfangener DHCP-Pakete
DHCP-Verworfen	Anzahl verworfener DHCP-Pakete
DHCP-Rx-Discover	Anzahl empfangener Discover-Messages
DHCP-Rx-Request	Anzahl empfangener Request-Messsges
DHCP-Rx-Dcline	Anzahl empfangener Decline-Messages
DHCP-Rx-Inform	Anzahl empfangener Inform-Messages
DHCP-Rx-Release	Anzahl empfangener Release-Messages
DHCP-Tx-Offer	Anzahl gesendeter Offer-Messages
DHCP-Tx-Ack.	Anzahl bestätigter DHCP-Pakete
DHCP-Tx-Nak	Anzahl nicht bestätigter DHCP-Pakete
DCHP-Server-Fehler	Anzahl empfangener DHCP-Pakete, die nicht für diesen Server bestimmt waren
DHCP-Zugewiesen	Anzahl aktuell zugewiesener Adressen
DHCP-MAC-Konflikte	Anzahl abgelehnter Zuweisungen aufgrund belegter IP-Adressen

Tabelle-DHCP	Tabelle mit den Zuweisungen von IP-Adressen zu MAC-Adressen
Server-Flags	Zustand des DHCP-Server (on/off)
Werte löschen	DHCP-Statistik löschen










*Tabelle-DHCP*

In der **DHCP-Tabelle** finden Sie Einträge mit DHCP-Informationen. Sie enthält 16 (oder vielfache von 16) Einträge. Die Tabelle paßt sich dynamisch an die Erfordernisse an und wächst oder schrumpft entsprechend. Sie hat den folgenden Aufbau:

IP-Adresse	Node-ID	Timeout	Rechner-name	Typ
IP-Adresse, die über DHCP zugewiesen wurde	zugehörige MAC-Adresse	Gültigkeitsdauer der Zuweisung in Minuten	Name des Rechners	Art der Zuweisung

**Status/TCP-IP-Statistik/DNS-Statistik**

Der DNS-Statistik können zusätzliche Informationen über das DNS-Modul entnommen werden. Dieses Menü hat den folgenden Aufbau:

LAN-Rx		Anzahl der DNS-Pakete, die vom LAN empfangen wurden
LAN-Tx		Anzahl der DNS-Pakete, die zum LAN gesendet wurden
WAN-Rx		Anzahl der DNS-Pakete, die vom WAN empfangen wurden
WAN-Tx		Anzahl der DNS-Pakete, die zum WAN gesendet wurden
Forwarded		Anzahl der Anfragen, die nicht beantwortet werden konnten und daher über den Forwarding-Mechanismus weitergeleitet wurden
Fehler		Anzahl von ungültigen Anfragen
DNS-Zugriffe		Gibt an, wie viele Namen aus der DNS-Tabelle aufgelöst wurden
DHCP-Zugriffe		Gibt an, wie viele Namen aus der DHCP-Tabelle aufgelöst wurden
Hit-Liste		In dieser Tabelle tauchen die 64 häufigsten Anfragen auf. Diese können dann unter Umständen über die Filterliste abgeblockt werden.

Die Hitliste hat den folgenden Aufbau

Domain	Requests	Zeit	Ip-Adresse
www.elsa.de	1	00.00.0000 00:00:29	10.0.0.123



















Die einzelnen Felder dieser Liste haben die folgende Bedeutung



Domain	Name des abgefragten Rechners
Requests	Gesamtzahl der Anfragen auf diesen Namen, seit er in die Tabelle steht
Zeit	Zeitpunkt der letzten Abfrage
IP-Adresse	Adresse des Rechners, der diesen Namen zuletzt abgefragt hat

Diese Liste ist nach Anzahl der Anfragen sortiert. Wenn die Tabelle voll ist, wird bei jeder neu eintreffenden Anfrage immer der am längsten nicht nachgefragte Name aus der Tabelle gelöscht.

## Status/IP-Router-Statistik

Hier werden die Statistiken aus dem IP-Router-Modul gesammelt.

/IP-Router-Statistik	Statistiken aus dem IP-Router-Bereich	
IPr-LAN-Rx		Anzahl vom LAN zu routender Datenpakete
IPr-LAN-Tx		Anzahl zum LAN gerouteter Datenpakete
IPr-LAN-lokales-Routing		Anzahl vom LAN empfangener und zum LAN gerouteter Pakete
IPr LAN-Netzwerk-Fehler		Anzahl LAN-Pakete, die nicht geroutet wurden
IPr-LAN-Routing-Fehler		Anzahl LAN-Pakete, die zu einem anderen Router müssen
IPr-LAN-TTL-Fehler		Anzahl LAN-Pakete mit einem abgelaufenen Time-to-Live-Wert
IPr-LAN-Filter		Anzahl der über die Filtertabelle gefilterten LAN-Pakete
IPr-LAN-verworfen		Anzahl der verworfenen LAN-Pakete
IPr-WAN-Rx		Anzahl vom WAN zu routender Datenpakete
IPr-WAN-Tx		Anzahl zum WAN gerouteter Datenpakete
IPr-WAN-Netzwerk-Fehler		Anzahl WAN-Pakete, die nicht geroutet wurden
IPr-WAN-TTL-Fehler		Anzahl WAN-Pakete mit einem abgelaufenem Time-to-Live-Wert
IPr-WAN-Filter		Anzahl der über die Filtertabelle gefilterten WAN-Pakete
IPr-WAN-verworfen		Anzahl der verworfenen WAN-Pakete
IPr-WAN-Typ-Fehler		Anzahl der Pakete vom WAN ohne IP-Router-Kennung
IPr-ARP-Fehler		Anzahl der nicht erfolgreichen Zugriffe auf den ARP-Cache
Werte löschen		IP-Router-Statistik löschen
Aufbau-Tabelle		Tabelle der letzten 100 Pakete, die eine Verbindung erforderten

/IP-Router-Statistik	Statistiken aus dem IP-Router-Bereich	
Protokoll-Tabelle		Tabelle über geroutete Pakete, protokollabhängig aufgestellt
RIP-Statistik		Statistiken aus dem IP/RIP-Bereich

*Aufbau-Tabelle* In der **Aufbau-Tabelle** sind die letzten 100 Einträge, die Informationen über die Systemzeit, Ziel-Adresse und Quell-Adresse, IP-Protokoll, Ziel-Port und Quell-Port der Datenpakete enthalten, die zu einem Verbindungsaufbau führen sollten.

Eine IP-Router-Aufbau-Tabelle kann wie folgt aussehen:

Systemzeit	Ziel-Adresse	Quell-Adresse	Protokoll	Z-Port	Q-Port
1T; 16:45:01	192.120.131.40	192.120.130.10	tcp	23	4711
1T; 10:45:10	192.120.131.50	192.120.130.10	udp	53	8123

Als 'Systemzeit' wird entweder die Betriebszeit des Geräts angezeigt, oder, falls vorhanden, die aktuelle Zeit. Die Ziel- und Quell-Adressen sind jeweils IP-Adressen, das Protokoll kann zum Beispiel auf tcp, udp oder ähnliches hinweisen und die Ziel- und Quell-Ports definieren näher die betroffenen Dienste (Telnet z.B. über TCP und Z-Port. 23, Nameserver über UDP und Z-Port 53).

*Protokoll-Tabelle*

Auch die Protokoll-Tabelle liefert wertvolle Daten über das zum LAN oder WAN übertragene Paketvolumen. Diese Werte sind aufgeschlüsselt nach den unterschiedlichen IP-Protokollen, zum Beispiel ICMP, TCP, UDP.

Eine Protokoll-Tabelle kann wie folgt aussehen:

Protokoll	LAN-Tx	WAN-Tx
tcp	14	30
udp	15	50
icmp	60	40

### Status/IP-Router-Statistik/RIP-Statistik

Hier werden die vom Gerät empfangenen IP-RIP-Pakete angezeigt. In dieser Unterstatistik finden Sie die folgenden Einträge:

RIP-Rx	Anzahl empfangener IP-RIP-Pakete
RIP-Request	Anzahl empfangener IP-RIP-Request-Pakete
RIP-Response	Anzahl empfangener IP-RIP-Response-Pakete
RIP-verworfen	Anzahl verworfener IP-RIP-Pakete
RIP-Fehler	Anzahl fehlerhafter IP-RIP-Pakete

RIP-Eintrag-Fehler	Anzahl fehlerhafter Einträge in IP-RIP-Paketen
RIP-Tx	Anzahl gesendeter IP-RIP-Pakete
Tabelle-RIP	Routing-Tabelle der durch RIP-Broadcast gelernten Routen

**Tabelle-RIP**












In der zugehörigen RIP-Tabelle stehen alle aus dem Netz gelernten Routen. Diese Tabelle wird vom Router selber verwaltet und kann nicht manuell verändert werden.

Eine IP-RIP-Tabelle kann wie folgt aussehen:

IP-Adresse	IP-Netz-Maske	Zeit	Distanz	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200

**Status/Config-Statistik**

Hier werden die Statistiken aus dem Bereich der Remote-Konfiguration angezeigt. Die Informationen über die Anzahl aller bereits gehaltenen sowie der aktuellen Konfigurationssitzungen sind jederzeit abrufbar. Die Aufschlüsselung geschieht nach LAN-, WAN- und Outband-Anschluß.

/Config-Statistik	Statistiken der Remote-Konfiguration	
LAN-Akt.-Verbindungen		Anzahl aktueller Konfigurationsverbindungen vom LAN
LAN-Ges.-Verbindungen		Anzahl bisheriger Konfigurationsverbindungen vom LAN
WAN-Akt.-Verbindungen		Anzahl aktueller Konfigurationsverbindungen vom WAN
WAN-Ges.-Verbindungen		Anzahl bisheriger Konfigurationsverbindungen vom WAN
Outband-Akt.-Verbindungen		Anzahl aktueller Outband-Konfigurationsverbindungen
Outband-Ges.-Verbindungen		Anzahl bisheriger Outband-Konfigurationsverbindungen
Outband-Bitrate		Bitrate der letzten Outband Konfigurationssitzung
Login-Fehler		Gesamtzahl der fehlerhaften Logins
Login-Sperren		Anzahl der Login-Sperrungen
Login-Ablehnungen		Anzahl der Login-Versuche, während die Login-Sperre aktiv war
Werte löschen		Config-Statistik löschen

**Status/DSL-Statistik**

In der DSL-Statistik werden Informationen über die Datenübertragung auf dem DSL-Anschluß dargestellt. Die angezeigten Werte über gesendete und empfangene Pakete,
















Pakettypen etc. helfen bei der Fehlersuche zwischen dem *LANCOM DSL/10 Office* und dem angeschlossenen xDSL- oder Kabel-Modem.

/DSL-Statistik	Statistiken des DSL-Anschlusses	
DSL-Rx-Pakete		Anzahl der vom DSL-Interface empfangenen Pakete
DSL-Tx-Pakete		Anzahl der zum DSL-Interface gesendeten Pakete
DSL-Rx-Fehler		Anzahl der vom DSL-Interface fehlerhaft empfangenen Pakete
DSL-Tx-Fehler		Anzahl der fehlerhaft zum DSL-Interface gesendeten Pakete
DSL-Rx-Keine-Verb.		Anzahl der DSL-Interface empfangenen Pakete ohne logische Verbindung
DSL-NIC-Fehler		Anzahl der internen Fehler des DSL-Interface
DSL-Queue-Pakete		Anzahl der noch zu sendenden Pakete
DSL-Queue-Fehler		Anzahl der, durch Puffermangel verworfenen, Pakete
DSL-Rx-Bytes		Anzahl der über das DSL-Interface empfangenen Zeichen
DSL-Tx-Bytes		Anzahl der über das DSL-Interface gesendeten Zeichen
DSL-Rx-Unicast		Anzahl der direkt an das LANCOM gerichteten Pakete
DSL-Tx-Broadcast		Anzahl der zum DSL-Interface gesendeten Broadcasts
DSL-Tx-Unicast		Anzahl der direkt an den AC gesendeten Pakete
Verbindung-aufgebaut		Anzeige des Link-Zustandes der DSL-Verbindung
PPPoE-Statistik		Statistiken über spezielle PPP over Ethernet Pakete
Werte löschen		DSL-Statistik löschen

## Status/DSL-Statistik/PPPoE-Statistik
















Hier werden Statistiken über den Verbindungsaufbau mit PPP über Ethernet angezeigt. Falls eine Verbindung zum Internet-Provider nicht aufgebaut werden kann, helfen diese Informationen bei der Fehlersuche.






/PPPoE-Statistik	Statistiken über spezielle PPP over Ethernet Pakete	
Tx-PADI		Anzahl der gesendeten PPP Active Discovery Indication (Verhandlungsbeginn)
Rx-PADO		Anzahl der empfangenen PPP Active Discovery Offer (AC-Angebote)
Tx-PADR		Anzahl der gesendeten PPP Active Discovery Request (AC-Anfragen)
Rx-PADS		Anzahl der empfangenen PPP Active Discovery Session-Confirm (AC-Sitzungsbestätigung)

<b>/PPPoE-Statistik</b>	<b>Statistiken über spezielle PPP over Ethernet Pakete</b>	
Tx-PADT		Anzahl der gesendeten PPP Active Discovery Terminate (Sitzungsende)
Rx-PADT		Anzahl der empfangenen PPP Active Discovery Terminate (Sitzungsende)
Tx-Protokoll		Anzahl der gesendeten Protokollpakete
Rx-Protokoll		Anzahl der empfangenen Protokollpakete
Tx-Data		Anzahl der gesendeten Nutzdatenpakete
Rx-Data		Anzahl der empfangenen Nutzdatenpakete
Rx-Bad		Anzahl der empfangenen, fehlerhaften Pakete
AC-Name		Name des ausgewählten Access-Concentrators
Service		Name des ausgehandelten Dienstes

## Status/Queue-Statistik

In dieser Statistik kann der Durchlauf der einzelnen Pakete in den verschiedenen Modulen der *ELSA LANCOM* beobachtet werden.

<b>/Queue-Statistik</b>	<b>Statistiken über die Queue</b>	
LAN-Heap-Pakete		Anzahl verfügbarer Puffer
LAN-Queue-Pakete		Anzahl belegter Puffer
WAN-Heap-Pakete		Anzahl verfügbarer Puffer
WAN-Queue-Pakete		Anzahl belegter Puffer
ARP-Query-Queue-Pakete		Anzahl der ARP-Pakete in der Query-Queue
ARP-Queue-Pakete		Anzahl der ARP-Pakete in der normalen Queue
IP-Queue-Pakete		Anzahl der IP-Pakete in der normalen Queue
IP-Urgent-Queue-Pakete		Anzahl der IP-Pakete in der gesicherten Queue
ICMP-Queue-Pakete		Anzahl der ICMP-Pakete
TCP-Queue-Pakete		Anzahl der TCP-Pakete
TFTP-Queue-Pakete		Anzahl der TFTP-Pakete
SNMP-Queue-Pakete		Anzahl der SNMP-Pakete
Prot-Heap-Pakete		Anzahl der Prot-Heap-Pakete
IPR-Queue-Pakete		Anzahl der Pakete, die noch durch den IP-Router bearbeitet werden sollen.
DHCP-Server-Queue-Pakete		Anzahl der Pakete in der Empfangs-Queue des DHCP-Servers.

/Queue-Statistik	Statistiken über die Queue	
IPR-RIP-Queue-Pakete		Anzahl der Pakete in der Empfangs-Queue des IP-RIP-Moduls (für RIP-Anfragen, RIP-Propagierungen ...).
DNS-Sende-Queue		Anzahl der Pakete, die zu DNS- oder NBNS-Servern weitergeleitet werden sollen.
DNS-Empfangs-Queue		Anzahl der Pakete, die von DNS- oder NBNS-Servern kommen und an den Host weitergeleitet werden sollen.
IP-Masq. Sende-Queue		Anzahl der Pakete, die maskiert versendet werden sollen (ins Internet).
IP-Masq. Empfangs-Queue		Anzahl der Pakete, die aus dem Internet empfangen wurden und demaskiert werden müssen.

## Status/Verbindungs-Statistik

Über dieses Menü können die Verbindungszeiten und weitere nützliche Informationen über die Auslastung des DSL-Anschlusses angezeigt werden.

Der Menüpunkt **Status/Verbindungs-Statistik** enthält für jedes verfügbare Interface eine Statistik über die auf diesem Interface aufgebauten Verbindungen. Die dort aufgeführte Tabelle hat folgendes Aussehen:

lfc	Verbindung	Fehler	Verbindungs-Zeit
Ch01	0	0	Keine Verbindung

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	bezeichnet den zugehörigen Kanal.
Verbindung	gibt die Anzahl der Verbindungen auf dem jeweiligen Kanal an.
Fehler	gibt die Anzahl der Verbindungsfehler an.
Verbindungs-Zeit	gibt die Zeit an, seit der die aktuelle Verbindung besteht. Besteht keine Verbindung, so wird „Keine Verbindungen.“ ausgegeben.

## Status/Info-Verbindung

Der Menüpunkt **Status/Info-Verbindung** enthält für jedes verfügbare Interface weitere Informationen über dessen aktuellen Verbindungszustand (logische Gegenstelle etc.). Die dort aufgeführte Tabelle hat folgendes Aussehen:

lfc	Status	Gerätename	SH-Zeit
Ch01	Bereit		0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	bezeichnet den zugehörigen Kanal.
Status	gibt den Zustand der jeweiligen Verbindung an. Mögliche Werte sind: <b>Initialisierung, Setup-WAN, Bereit, Aufbau-PPPoE, Protokoll, Verbindung, Abbau</b>
Gerätename	gibt den logischen Namen der Gegenstelle an (sofern dieser auflösbar ist).
SH-Zeit	gibt die Haltezeit (Short-Hold-Zeit) der Verbindung an.

## Status/Gegenstellen-Statistik

In dieser Tabelle werden die letzten hundert Verbindungen der *ELSA LANCOM* mit Informationen über die Gegenstelle angezeigt.

Die Tabelle hat den folgenden Aufbau:

Verb.-Start	Gegenstelle	Verb.-Zeit
OT; 00:20:57	BERLIN	50
OT; 00:20:46	CHEMNITZ	230

Die Einträge haben die folgende Bedeutung:

Verbindungsstart	Zeit, zu der die Verbindung zustande gekommen ist. Dabei wird entweder die Betriebszeit des Geräts angezeigt oder die aktuelle Zeit (falls diese vom Anwender eingegeben wurde).
Gegenstelle	Logischer Gegenstellenname
Verbindungszeit	Dauer der Verbindung in Jahren, Monaten, Tagen (optional) sowie Stunden, Minuten und Sekunden

Eine Verbindung bleibt mindestens für die Dauer ihres Bestehens in der Tabelle. Jede neue Verbindung füllt die Tabelle von oben her auf. Sollte eine bestehende Verbindung als unterster Eintrag der Tabelle stehen, so wird ggf. eine bereits abgebaute Verbindung stattdessen aus der Tabelle entfernt.

## Status/Kanal-Statistik

Diese Tabelle zeigt Ihnen Informationen über den aktuellen Zustand des DSL-Kanals. Die Informationen aus dieser Tabelle werden hauptsächlich zur Ausgabe über *ELSA LANmonitor* verwendet. Daher liegen einige Werte in einer reinen Bitdarstellung vor, die hier nicht näher erläutert wird.

Die Tabelle hat folgenden Aufbau:

Kanal	Zustand	App	Mode	Cause	Subadr.	Verb.-Zeit	Extra
Ifc-ERR	00000000	Router	akt.	0000	00000000	0	
Line	00000000	Router	akt.	0000	00000000	20	




Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Kanal	Kanal, für den der Eintrag gilt. Es wird immer nur der letzte Zustand eines Kanals angezeigt. Für Fehlermeldungen auf Kanälen wird ein eigener „Kanal“ geführt.
Zustand	Als Zustand eines Kanals wird hier z.B. 'bereit' angezeigt.
App	Applikation, die den Kanal belegt: Router
Mode	Art des letzten Verbindungsaufbaus: aktiv
Cause	Letzter aufgetretener Fehler
Subadresse	Zusatz zur Applikation, die für den Router z.B. den logischen Kanal angibt.
Verb.-Zeit	Dauer der letzten Verbindung auf diesem Kanal
Extras	Zusatzinformation zur Verbindung, z.B. der Name der Gegenstelle bei Routerverbindungen

## Status/Zeit-Statistik

In diesem Menü finden Sie Informationen über die aktuelle Zeit im Gerät sowie über den Weg, wie der *LANCOM Office*-Router zu dieser Zeit gekommen ist.

Das Menü hat folgenden Aufbau:

/Zeit-Statistik	Statistiken aus dem Zeit-Modul	
Aktuelle Zeit		Aktuelle Zeit des Geräts
Quelle		Quelle der Zeitangabe. Mögliche Werte sind: 'Manuell' für das manuelle Setzen der Zeit mit dem Befehl 'time', 'RAM' für die Übernahme der Zeit aus dem Zwischenspeicher des Gerätes nach einem Bootvorgang.
Übernahme		Anzahl der bisher erfolgten Zeit-Übernahmen aus einer der vorher genannten Quellen












## Status/Werte löschen

Hier können alle Werte der untergeordneten Statistiken bis auf die Tabellen gelöscht werden. Dazu geben Sie folgenden Befehl ein:

```
do werte-loeschen
```

## Setup

Über dieses Menü können alle Systemparameter, die für die Funktion der Geräte notwendig sind, abgefragt und geändert werden.

/Setup		Konfiguration des Systems
Name		Eingabe des Gerätenamens
WAN-Modul		Einstellungen für das WAN
Gebühren-Modul		Einstellungen für die Gebührenverwaltung
LAN-Modul		Einstellungen für das LAN
TCP-IP-Modul		Einstellungen für das TCP/IP-Modul
IP-Router-Modul		Einstellungen für das IP-Router-Modul
SNMP-Modul		Einstellungen für die Konfiguration über SNMP
DHCP-Modul		Einstellungen für den DHCP-Server
DNS-Modul		Einstellungen für den DNS-Server
Config-Modul		Einstellungen für das Konfigurationsmodul
Zeit-Modul		Einstellungen für das Zeit-Modul

### Name

Hier kann der Geräte name (maximal 16 Stellen) eingegeben werden. Der zur Verfügung stehende Zeichensatz beinhaltet Klein- und Großbuchstaben sowie einige Sonderzeichen. Den vollen Umfang können Sie sich in einer Konfigurationssitzung über den Befehl

```
set \setup\name ?
```

anzeigen lassen. Standardmäßig ist kein Name eingetragen.




Der Geräte name wird zur Identifikation benötigt und ist Voraussetzung für eine mögliche Verbindung über die IP-Router-Module, da die Router nur mit bekannten Gegenstellen Daten austauschen.

Bei PPP-Verbindungen wird entweder der Benutzername mit dem Paßwort aus der PPP-Liste oder der Geräte name während einer Überprüfung durch PAP oder CHAP als Identifikation des Gerätes zur Gegenstelle übertragen.

Die Gerätenamen sollten außerdem so vergeben werden, daß sie nicht doppelt auftreten. Empfehlenswert wäre zum Beispiel, den Gerätenamen dem Standort anzupassen (z.B. Aachen, Berlin, Provider etc.).

## Setup/WAN-Modul

Hier sind alle Einstellungen zusammengefaßt, die für die Inbetriebnahme der WAN-Interfaces und die Steuerung von Verbindungen zu logischen Gegenstellen notwendig sind.

/WAN-Modul		Einstellungen für das WAN
Namenliste		Einstellungen für die Gegenstellen
PPP-Liste		Einstellung der Parameter für PPP-Verbindungen
Manuelle-Wahl		Einstellungen für die manuelle Verbindungssteuerung

### Namenliste

Die in der Namenliste eingetragenen Gerätenamen werden vom Router benötigt, um die richtige Gegenstelle und den entsprechenden Layernamen zu ermitteln. Zusätzlich wird die Namenliste für die Rückruffunktion verwendet.

In der Namenliste können 16 verschiedene Gerätenamen verwaltet werden, die z.B. so aussehen können:

Geraetenname	SH-Zeit	AC-Name	Servicename
AACHEN	180		
BERLIN	20		

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Gerätename	In der Spalte <b>Gerätename</b> können Sie einen eigenen Gegenstellen-Namen eintragen, den Sie dann der entsprechenden Gegenstelle über den Menüpunkt <b>Name</b> des Menüs <b>Setup</b> zuweisen müssen.
SH-Zeit	In dieser Spalte können entsprechende Verbindungshaltezeiten (in Sekunden) für die DSL-Verbindung festgelegt werden. Werden nach Ablauf dieser Zeit keine Daten übertragen, wird die Verbindung auf diesem Kanal wieder abgebaut (Standard: 20).
AC-Name	Name des gewünschten Access-Concentrators. Wird hier nichts eingegeben akzeptiert das LANCOM jeden AC mit passendem Service.
Servicename	Name des gewünschten Dienstes. Ohne Angabe akzeptiert das LANCOM jeden angebotenen Dienst.

### PPP-Liste

Die in der PPP-Liste eingetragenen Gerätenamen werden vom Router benötigt, um die zur Verbindung passenden Einstellungen für das Sicherungsverfahren und die PPP-Parameter zu ermitteln. Sie enthält maximal 16 Einträge und ist wie folgt aufgebaut:

Gerätename	Authent.	Paßwort	Zeit	Wdh.	Conf	Fail	Term	Username
AACHEN	CHAP	*****	0	5	10	5	2	ELSA




Nicht alle Parameter sind über die Telnet-Konfiguration erreichbar. Verwenden Sie nach Möglichkeit *ELSA LANconfig*.

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Gerätename	In dieser Spalte können Sie den Namen eintragen, mit dem sich die Gegenstelle beim Router anmeldet. Die Groß- und Kleinschreibung wird nicht berücksichtigt!	
Authentifizierung	In dieser Spalte können Sie das Sicherungsverfahren, mit dem die Gegenstelle überprüft werden soll, eintragen. Standardwert: PAP	
	Keine	Der Router handelt beim Verbindungsaufbau keine Authentifizierung mit der Gegenstelle aus. Diese kann selbst jedoch eine Authentifizierung vom Router verlangen. Das ist z.B. bei der Anwahl an ISP der Fall.
	PAP	Die Gegenstelle wird nach dem Password Authentication Protocol überprüft.
	CHAP	Die Gegenstelle wird nach dem Challenge Handshake Authentication-Protocol überprüft.
Paßwort	In dieser Spalte kann ein Paßwort eingetragen werden, dessen Vorhandensein durch das Symbol * dargestellt wird und der zur Überprüfung der Gegenstelle dient. Er kann aus 95 Zeichen (7-Bit ASCII, auch Leerzeichen) bestehen. Standardwert: keiner. Mit dem Befehl <code>set ?</code> erhalten Sie eine Liste der erlaubten Zeichen.	
Zeit	In dieser Spalte kann der Zeitraum in Minuten zwischen zwei Überprüfungen der Gegenstelle eingetragen werden. Das Protokoll CHAP muß hierbei eingestellt sein. Standardwert: 0	
Wdh.	Hier kann die Anzahl der Wiederholungen von Überprüfungsversuchen eingestellt werden. Bei fehlgeschlagener Überprüfung wird die Verbindung sofort abgebrochen. Standardwert: 5	
Conf, Fail und Term	Durch diese Parameter kann die Arbeitsweise des PPP beeinflußt werden. Diese Parameter sind im RFC 1661 definiert und beschrieben. Die Standardwerte sind für die meisten Gegenstellen ausreichend. Wird hier nichts eingetragen, erscheinen diese Werte in der Anzeige als 0,0,0. In diesem Fall werden trotzdem die Standardwerte 10, 5, 2 benutzt. Diese Parameter können nur über SNMP oder TFTP (mit dem Konfigurationsprogramm <i>ELSA LANconfig</i> ) verändert werden!	
Username	Benutzername (max. 64 Zeichen), der der Gegenstelle während der PPP-Verhandlung übermittelt wird. Damit meldet sich der Router bei der Gegenstelle an. Wird kein Username eingetragen, gilt der Gerätename als Benutzername. Berücksichtigen Sie dabei auch die Groß- und Kleinschreibung.	

### Setup/WAN-Modul/Manuelle-Wahl

Über diesen Menüpunkt kann für Testzwecke eine manuelle Verbindungssteuerung vorgenommen werden.

/Manuelle Wahl	Einstellungen für die manuelle Verbindungssteuerung	
Aufbau		Aufbau einer Verbindung
Abbau		Abbau von Verbindungen
Status		Zeigt den aktuellen Verbindungszustand an

*Aufbau*

Parameter: Gegenstellengerätename (nur über Remote-Konfiguration).

Mit dem Befehl



Do /Setup/WAN-Modul/Manuelle-Wahl/Aufbau Gegenstelle

wird ein manueller Verbindungsaufbau über die Remote-Konfiguration initiiert. Der als Parameter angegebene Gegenstellengerätename muß dazu mit Rufnummer in der Namenliste eingetragen sein.

Soll zu einer logischen Gegenstelle eine Verbindung aufgebaut werden, für die in der Namenliste keine Rufnummer angegeben ist, so wird die Fehlermeldung 'Keine Rufnummer' angezeigt.






Abbau

Über diesen Befehl kann eine bestehende Verbindung abgebaut werden. Bei einem manuellen Verbindungsabbau kann in der Remote-Konfiguration zusätzlich der Name einer Gegenstelle angegeben werden. Es wird dann nur die Verbindung zur angegebenen Gegenstelle gelöst. Besteht keine Verbindung zur angegebenen Gegenstelle, erfolgt keine weitere Reaktion. Wird dagegen kein Gegenstellename angegeben, so werden alle bestehenden Verbindungen abgebaut.

## Setup/Gebühren-Modul

Über diesen Menüpunkt werden notwendige Einstellungen für den Gebührenschatz vorgenommen.

Standardmäßig ist der Gebührenschatz auf 10 Stunden für einen Zeitraum von sechs Tagen festgelegt. Das Menü hat folgendes Aussehen:

/Gebühren-Modul		Einstellungen für die Gebührenverwaltung
Tage/Periode		Länge einer Periode in Tagen
Minuten-Budget		Minuten, die pro Periodendauer zur Verfügung stehen
Rest-Minuten		Minuten, die noch zur Verfügung stehen
Router-Minuten		von den Router-Modulen verbrauchte Minuten
Zeit-Tabelle		Einstellungen für die lokalen Budgets der einzelnen Interfaces

Jede durch eine Verbindung anfallende Gebühreneinheit wird unmittelbar vom Minuten-Budget abgezogen, so daß hier eine Kontrolle über die noch zur Verfügung stehenden Minuten erfolgen kann.

Tage/Periode

Über diesen Menüpunkt kann der Zeitraum in Tagen (von 0 bis 255) festgelegt werden, in dem die Online-Minuten addiert und mit dem Budget verglichen werden. Der Standardwert beträgt sechs Tage. Ist dieser Zeitraum abgelaufen, beginnt die Addition der Online-Minuten neu.

Wird der Wert 0 eingegeben, kann nach Verbrauch des Minuten-Budgets keine Verbindung aufgebaut werden.

*Minuten-Budget* Über diesen Menüpunkt legen Sie fest, wieviele Online-Minuten der Gebührenüberwachung zur Verfügung stehen. Diese Minuten können nur in Zehnerschritten bis maximal 2550 eingegeben werden. Der Standardwert beträgt 600.




*Eine Gebührensperre kann entweder durch Aus- und Wiedereinschalten des Gerätes, durch Aktivierung des Menüpunktes **System-Boot** im Menü **Sonstiges** oder durch Eingabe eines neuen Gebührenbudgets aufgehoben werden.*

In der Tabelle können nur die Budget-Einheiten eingestellt werden, alle weiteren Einträge verwaltet das System selbständig.

Eine Eingabe von null Budget-Minuten deaktiviert die Gebührenüberwachung.

## Setup/LAN-Modul

Über diesen Menüpunkt werden die für das lokale Netzwerk notwendigen Einstellungen vorgenommen. Das Menü hat folgenden Aufbau:

/LAN-Modul		Einstellungen für das LAN
Anschluß		Wahl des Netzwerkanschlusses
Node-ID		MAC-Layer-Adresse des Geräts
Heap-Reserve		Pufferspeicher für die Aufnahme von Datenpaketen aus dem lokalen Netzwerk

*Anschluß* Hier kann einer der folgenden Netzwerkanschlüsse ausgewählt werden:

Anschluß	Bedeutung
Auto	Standardeinstellung, aktiviert die Autosense-Funktion des Netzwerk-Chips. Dadurch stellt sich der Router automatisch auf den verwendeten Anschluß ein, ohne das dieser Punkt manuell konfiguriert werden muß.
10BTX	10BASE-T im Halbduplex-Betrieb
FD10BTX	10BASE-T im Vollduplex-Betrieb
100BTX	100BASE-T im Halbduplex-Betrieb
FD100BTX	100BASE-T im Vollduplex-Betrieb



*Bitte beachten Sie, daß bei den Einstellungen für den Fast-Ethernet-Betrieb die entsprechenden weiteren Endgeräte das gewählte Übertragungsverfahren auch unterstützen müssen.*

*Nach dem Aus- und Einschalten bleibt der zuletzt gewählte Anschluß aktiv.*

*Node-ID* Unter diesem Menüpunkt wird die eigene Ethernet-Adresse des Routers angezeigt. Der hier angezeigte Wert wurde vom Hersteller festgelegt und kann nicht verändert werden.















Die Anzeige der Ethernet-Adresse erfolgt als zwölfstellige Hexadezimalzahl, wobei die ersten sechs Stellen '00a057' für ein ELSA Gerät stehen.

#### Heap-Reserve

Die Heap-Reserve für das lokale Netzwerk beeinflusst, wieviel Pufferspeicher ständig zur Aufnahme von Frames des lokalen Netzwerks zur Verfügung stehen. Standardmäßig ist hier ein Wert von 10 eingestellt, der garantiert, daß z.B. vier Telnet-Sitzungen jederzeit über das lokale Netzwerk aktiviert werden können.

## Setup/TCP-IP-Modul

Über dieses Menü können Einstellungen für das TCP-IP-Modul vorgenommen werden. Das Menü hat den folgenden Aufbau:

/TCP-IP-Modul		Einstellungen für das TCP/IP-Modul
Zustand		TCP/IP-Modul ein- oder ausgeschaltet
IP-Adresse		Eigene IP-Adresse
IP-Netz-Maske		Passende IP-Netzmaske des lokalen Netzes
Intranet-Adresse		Eigene Intranet-Adresse
Intranet-Maske		Passende Intranet-Netzmaske des lokalen Netzes
Zugangsliste		Einschränkung des Zugriffs auf interne Funktionen über TCP/IP
DNS-Default		Domain Name Server
DNS-Backup		Backup Domain Name Server
NBNS-Default		NetBIOS Name Server
NBNS-Backup		Backup NetBIOS Name Server
Tabelle-ARP		ARP-Tabelle für Abb. einer IP-Adresse auf eine MAC-Adresse
ARP-Aging-Min		Verweildauer für Einträge in der ARP-Tabelle
TCP-Aging-Min		Zeitbeschränkung für Konfigurations-Verbindungen, die inaktiv sind
TCP-Max.-Verbindungen.		Max. Anzahl gleichzeitiger Konfigurations-Verbindungen zum <i>ELSA LANCOM</i>

#### Zustand

Hier kann das TCP/IP-Modul des Routers ein- oder ausgeschaltet werden. Standardmäßig ist das TCP/IP-Modul aktiviert.

*Die Konfiguration über TCP/IP durch Telnet und der IP-Router können nur benutzt werden, wenn das TCP/IP-Modul eingeschaltet ist.*

#### IP-Adresse

Hier kann die IP-Adresse für den Router eingegeben werden. Die Standardadresse bei der Auslieferung ist die '0.0.0.0'.

Bei Verwendung von IP-Masquerading bekommt diese Adresse in Verbindung mit der Intranet-Adresse eine besondere Bedeutung:

Wird dem Router vom Internet-Provider die hier eingestellte IP-Adresse per PPP zugewiesen, so werden alle Rechner, die sich im durch IP-Adresse und IP-Netzmaske aufgespannten Netz befinden, normal geroutet. Diese Rechner sind dann auch direkt aus dem Internet heraus erreichbar.

*IP-Netzmaske* Hier muß die zur IP-Adresse gehörende Netzmaske eingegeben werden. Die Standardeinstellung ist 255.255.255.0 (Klasse C Netz). Eine Netzmaske von 255.255.255.255 bedeutet, daß sich in diesem Netz nur ein einziger Rechner befindet (nämlich der Router selber). Diese Einstellung (eine im Internet registrierte IP-Adresse mit voll besetzter Netzmaske) kann für das Masquerading über einen Raw-IP-Zugang, wie ihn z.B die Provider des Individual Network anbieten, verwendet werden. Bei einem solchen Zugang wird dem Router keine IP-Adresse über eine PPP-Verhandlung zugewiesen, sondern er muß eine feste, im Internet registrierte IP-Adresse besitzen.

*Intranet-Adresse* Hier kann eine zweite IP-Adresse für den Router eingegeben werden. Dadurch kann der Router einerseits für zwei logische IP-Netze als Router dienen, andererseits erhält diese Adresse eine besondere Bedeutung bei Verwendung von IP-Masquerading:

In diesem Fall werden alle Rechner, die sich im durch Intranet-Adresse und Intranet-Maske aufgespannten Netz befinden, hinter der vom Provider zugewiesenen Adresse (bzw. der Internet-Adresse (IP-Adresse)) versteckt.

Die Standardadresse bei der Auslieferung ist die '0.0.0.0'.

*Intranet-Maske* Hier muß die zur IP-Adresse gehörende Netzmaske eingegeben werden. Die Standardeinstellung ist 255.255.255.0 (Klasse C Netz).



*Wurde weder eine IP- noch eine Intranet-Adresse angegeben, reagiert das Gerät auf eine Standard-IP-Adresse, deren erste drei Stellen identisch sind mit den ersten drei Stellen des Sendegeräts XXX.XXX.XXX.YYY. Das Gerät ist dann durch Anwahl der IP-Adresse XXX.XXX.XXX.254 zu erreichen.*

*Existiert im Netz bereits eine solche IP-Adresse, muß über die Outband-Konfiguration (Terminal-Programm) eine andere Adresse eingegeben werden.*



*Wurden sowohl IP- als auch Intranet-Adresse eingegeben, so dürfen sich in dem durch IP-Adresse und IP-Netzmaske aufgespannten Netz nur Workstations (also keine Router) befinden.*

*Zugangsliste* Der Zugang zu „internen Funktionen“ der Router kann in TCP/IP-Anwendungen durch eine Zugangsliste gesteuert werden.



*Zwar sind die Konfigurationsdaten der Geräte durch ein Paßwort geschützt, jedoch wird dieses immer im Klartext übertragen, wodurch es prinzipiell möglich ist, dieses auszuspähen und von jedem beliebigen Rechner aus die Konfiguration auszulesen oder gar zu zerstören. Um dies zu verhindern, kann über die Zugriffsliste eingestellt werden, von welchen Rechnern oder aus welchen Netzen herauf auf die Konfiguration zugegriffen werden darf.*

Die Zugangskontrolle bezieht sich aus Konsistenzgründen auf alle „internen Funktionen“ der Router. Unter dem Begriff „interne Funktionen“ sind folgende zu verstehen:

- Telnet-Server: die Konfigurations-Schnittstelle auf Basis des Telnet-Protokolls.
- TFTP-Server: die Konfigurations-Schnittstelle auf Basis des TFTP-Protokolls.
- SNMP: die Konfigurations-Schnittstelle auf Basis von SNMP.

Jeder der maximal 16 Einträge in der Zugangsliste besitzt folgenden Aufbau:

IP-Adresse	IP-Netz-Maske
IP-Adresse des berechtigten Teilnehmers (oder Teilnehmerkreises)	IP-Netzwerk-Maske des Teilnehmerkreises

Sobald eine IP-Workstation mit ihrer IP-Adresse und der Netzmaske 255.255.255.255 in die Liste eingetragen ist, kann nur noch von diesem Rechner aus auf die internen Funktionen der Router zugegriffen werden. Alle Anforderungen von Geräten mit anderen IP-Adressen bleiben unbeantwortet.

Soll einem kompletten Netzwerk der Zugang zu einem *ELSA LANCOM* ermöglicht werden, kann dies für ein Netzwerk der Klasse C etwa wie folgt geschehen:

IP-Adresse	IP-Netz-Maske
192.234.222.0	255.255.255.0

Durch diesen Eintrag sind alle IP-Adressen im Klasse-C-Netzwerk 192.234.222.0 berechtigt, interne Funktionen des Routers zu benutzen.

#### DNS-Default

Der Eintrag **DNS** (Domain Name Server) wird benötigt, um Rechnern, die über PPP direkt auf den Router zugreifen, den für das eigene Netz zuständigen Name-Server bekanntzugeben.

Wenn der Router für den Zugang zum Internet über einen Internet-Service-Provider konfiguriert ist, wird der DNS-Server meist vom Provider übermittelt. Für die Einstellung im Router gibt es dann zwei verschiedene Möglichkeiten:

- Als Adresse des DNS-Servers wird die '0.0.0.0' eingetragen. Dann können alle Rechner im lokalen Netz den DNS-Server des Providers nutzen.
- Die eigene IP-Adresse des Routers wird als DNS-Server eingetragen. Dann nutzt er die DNS-Informationen des Providers nicht nur für das eigene lokale Netz, sondern gibt diese Informationen selbst weiter (DNS-Forwarding). Entfernte Gegenstellen wie z.B. Rechner, die sich über Remote-Access einwählen, können dann auch auf den DNS-Server des Providers zugreifen. Dieser Mechanismus wird auch als DNS-Forwarding bezeichnet.

#### DNS-Backup

Durch den Eintrag **DNS-Backup** kann ein zweiter Name-Server benannt werden, der bei Ausfall des DNS benutzt wird.

*NBNS-Default* Der Eintrag **NBNS** (NetBIOS Name Server) wird benötigt, um Rechnern, die über PPP direkt auf den Router zugreifen, den für das eigene Netz zuständigen NBNS bekanntzugeben.

*NBNS-Backup* Durch den Eintrag **NBNS-Backup** kann ein zweiter Server benannt werden, der bei Ausfall des NBNS benutzt wird.

*ARP-Tabelle* Hier wird die ARP-Tabelle (ARP-Cache), die zur Abbildung von IP-Adressen auf physikalische Endgeräteadressen automatisch verwaltet wird, angezeigt. Einzelne Einträge können aus dieser Tabelle entfernt, jedoch können keine neuen Einträge manuell eingegeben werden.

Die Einträge in der ARP-Tabelle könnten z.B. wie folgt aussehen, wenn verschiedene Geräte mit unterschiedlichen IP-Adressen (192.168.139.20, 192.168.130.30) mit dem Router kommuniziert haben:

IP-Adresse	Node-ID	Letzter Zugriff	Anschluß
192.168.130.20	0000c0717860	6780443 tics	lokal
192.168.130.30	0800091eebf4	6214514 tics	lokal





*ARP-Aging-Min* Hier kann eine Zeit (von 1 bis 99 Minuten) eingegeben werden, nach der die ARP-Tabelle automatisch aktualisiert wird, d.h., alle nicht angesprochenen IP-Adressen seit der letzten automatischen Aktualisierung werden entfernt. Der Standardwert beträgt 15 Minuten.






*TCP-Aging-Min* Erfolgt während einer TCP-Verbindung zum Router keine Übertragung mehr, wenn z.B. während der Remote-Konfiguration keine Daten mehr vom Benutzer eingegeben werden, baut er die TCP-Verbindung automatisch nach der hier angegebenen Zeit ab. Gültige Werte sind 1 bis 99 Minuten. Der Standardwert beträgt 15 Minuten.

*TCP-Max.-Verbindungen* Hier kann die Anzahl der maximal zulässigen, gleichzeitig möglichen Verbindungen eingestellt werden. DEFAULT-Einstellung ist '0', was gleichbedeutend ist mit „beliebig viele“.

## Setup/IP-Router-Modul

Über dieses Menü können Einstellungen für das IP-Router-Modul vorgenommen werden. Das Menü hat den folgenden Aufbau:

/IP-Router-Modul	Einstellungen für das IP-Router-Modul	
Zustand		IP-Router-Modul ein- oder ausgeschaltet
IP-Routing-Tabelle		Router-Tabelle für Zuordnung IP-Netzwerk und Gegenstelle
LAN-Filtertabelle		Negativ/Aufb.-Filtertabelle für TCP/UDP-Zielports von LAN-Pak.
WAN-Filtertabelle		Negativ-Filtertabelle für TCP/UDP-Zielports von WAN-Paketen

/IP-Router-Modul		Einstellungen für das IP-Router-Modul
Proxy-ARP		Aktivierung/Deaktivierung der Proxy-ARP-Funktion
Lok.-Routing		Ein- und Ausschalten des lokalen Routings
Routing-Methode		Routing-Verfahren für IP-Pakete
RIP-Einstellungen		Einstellungen für den Betrieb von IP-RIP
Masquerading		Einstellungen für das IP-Masquerading

Zustand

IP-Routing-  
Tabelle

Hier kann das IP-Router-Modul ein- oder ausgeschaltet werden. Standardmäßig ist das IP-Router-Modul aktiviert.

*Beim Einschalten des IP-Router-Moduls wird auch das TCP/IP-Modul aktiviert.*

In der Router-Tabelle können maximal 128 Einträge von Zielnetzwerkadressen oder direkten IP-Adressen mit dazugehörigen Netzwerkmasken und Router-Namen bzw. IP-Adressen anderer lokaler Router aufgenommen werden. Alternativ können Sie einstellen, daß Pakete zu bestimmten Ziel-IP-Adressen verworfen und auch nicht durch Proxy-ARP beantwortet werden. Dies erreichen Sie durch den Eintrag 0.0.0.0 bei dem zuständigen Router-Namen.

Das Feld 'Maskierung' gibt an, ob die Route maskiert werden soll oder nicht. Dabei werden folgende Möglichkeiten unterschieden:

- **Ein:** IP-Masquerading ist eingeschaltet und funktioniert mit dynamischer Zuweisung der IP-Adresse durch die Gegenstelle. Bei diesem Verfahren fragt der Router bei der Gegenstelle die IP-Adresse '0.0.0.0' an und bekommt daraufhin eine beliebige IP-Adresse der Gegenstelle zugewiesen, die im weiteren verwendet wird.
- **Aus:** Masquerading ist ausgeschaltet.
- **Statisch:** Masquerading ist eingeschaltet und funktioniert mit Zuweisung einer statischen, vorher vereinbarten IP-Adresse durch die Gegenstelle. Bei diesem Verfahren fragt der Router bei der Gegenstelle die unter 'Setup/TCP-IP-Modul' eingetragene IP-Adresse an und bekommt daraufhin genau diese Adresse von der Gegenstelle zugewiesen. Verwenden Sie diese Einstellung, wenn Ihnen die Gegenstelle (z.B. Ihr Internet-Provider) mit den Zugangsdaten eine feste IP-Adresse mitgeteilt hat. Dieses Verfahren funktioniert natürlich nur dann, wenn Sie diese Adresse auch als IP-Adresse im Router eingetragen haben.

Die IP-Routing-Tabelle ist im allgemeinen wie folgt sortiert:

- Die längste Netzmaske steht oben.
- Bei gleicher Netzmaske steht die kleinste IP-Adresse oben.

Zur Identifizierung der richtigen Gegenstelle durchsucht der Router anhand der empfangenen Ziel-IP-Adresse die Routing-Tabelle von oben nach unten. Wurde ein passender Eintrag gefunden, wird der gefundene Router-Name für die Verbindung verwendet.

Im Internet verbotene Adreßbereiche werden über voreingestellte Einträge in der IP-Routing-Tabelle von der Übertragung ausgeschlossen (Router-Name 0.0.0.0 bedeutet: Pakete an diese Adressen nicht übertragen). Die folgende IP-Routing-Tabelle dient als Beispiel und zeigt gleichzeitig die Standardeinträge:

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

Sollten diese Adressen trotzdem z.B. für Intranet-Benutzung benötigt werden, ist es möglich, diese vordefinierten Einträge jederzeit zu löschen. Erscheinen in dieser Routing-Tabelle keine Einträge mit Router-Namen 0.0.0.0, werden vom Router alle IP-Adressen mit gültigen Routen verarbeitet.

■ Beispiel

- Die lokale Netzwerkadresse ist 192.120.130.0.
- Datenpakete für das Zielnetz 193.140.300.0 sollen zu einem weiteren lokalen Router mit der IP-Adresse 192.120.130.200 geschickt werden.
- Zu einem Zielnetzwerk 193.140.200.0 soll überhaupt nichts übertragen werden.
- Alle anderen nicht lokalen Datenpakete sollen zum Router 'PROVIDER' beim Internet-Service-Provider geschickt werden.

Die Router-Tabelle müßte in diesem Beispiel folgende Einträge beinhalten:

IP-Adresse	IP-Netz-Maske	Router-Name	Distanz	Maskierung
193.140.200.0	255.255.255.0	0.0.0.0	0	Aus
193.140.300.0	255.255.255.0	192.120.130.200	0	Aus
255.255.255.255	0.0.0.0	PROVIDER	0	Ein

Die letzte Zeile ist ein Eintrag für die Standard-Route. Die IP-Adresse 255.255.255.255 ist gleichbedeutend mit 0.0.0.0 (0.0.0.0 kann in der ersten Spalte aus technischen Gründen nicht eingegeben werden). Durch die IP-Netzmaske 0.0.0.0 paßt diese Zeile immer, wenn alles vorher durchsucht wurde. Der Router schickt also alles, was er über andere Routen nicht übertragen kann und nicht verwerfen soll bzw. was von einem WAN-Anschluß kommt und nicht lokal ist, an den Router beim Provider.

*LAN-Filtertab.* Mit dieser Tabelle können bestimmte Ziel-Port-Bereiche gefiltert werden. Darüber hinaus kann bestimmt werden, wie diese Pakete gefiltert werden. Treffen von der LAN-Seite Pakete mit den eingetragenen Ports ein, so werden sie nicht weitergeroutet (Immer-Fil-



ter), nur, wenn die Verbindung gerade steht (Aufbau-Filter) oder nur, wenn sie über eine andere als die DEFAULT-Route gerouted werden können (I-Net-Filter).

Die LAN-Portfilter sind in einer Tabelle mit dem folgenden Aufbau definiert:

Idx.	Z-von	Z-bis	Q-von	Q-bis	Quell-Adresse	Quell-Netzmaske	Prot	Typ
WIN	0	0	137	139	255.255.255.255	0.0.0.0	TCP und UDP	Immer

Die Felder der Tabelle haben folgende Bedeutung:

- **Idx.**  
Eindeutiger Index. Dieser Eintrag ist nötig, um die Filter unterscheiden zu können. Der Index kann vier Zeichen lang sein und beliebig gewählt werden.
- **Z-von, Z-bis**  
Ziel-Port-Bereich, der gefiltert werden soll. Ein Bereich von 0 bis 0 bedeutet, daß kein Ziel-Port von diesem Filter beeinflußt wird.
- **Q-von, Q-bis**  
Quell-Port-Bereich, der gefiltert werden soll. Ein Bereich von 0 bis 0 bedeutet, daß kein Quell-Port von diesem Filter beeinflußt wird.
- **Quell-Adresse, Quell-Netzmaske**  
Hiermit kann ein Subnetz des lokalen Netzes angegeben werden, für das der Filter gelten soll. Ist die Quell-Adresse 0.0.0.0 so bedeutet das, daß der Filter auf jeden Rechner angewendet wird. Eine Netzmaske von 0.0.0.0 bedeutet, daß der Filter auf alle Netze angewendet wird (was ebenfalls alle Rechner bedeutet).
- **Prot**  
Protokoll, das gefiltert werden soll. Möglich sind **TCP, UDP, ICMP** und **alle**.  
Die Einstellung **alle** filtert jedes Paket aus dem spezifizierten Quell-Netz bzw. zum Ziel-Netz.
- **Typ**  
Art des Filters. Möglich sind Immer, Aufbau und I-Net.
  - **Immer**-Filter: Das Paket wird verworfen.
  - **Aufbau**-Filter: Das Paket wird verworfen, wenn keine Verbindung zur Gegenstelle besteht.
  - **I-Net**-Filter: Das Paket wird verworfen, wenn sein Ziel nur über die DEFAULT-Route erreichbar ist.

In der vorhergehenden Tabelle ist der Default-Filter eingetragen, der den unerwünschten und kostenintensiven Verbindungsaufbau bei Windows-Netzen auf IP unterbindet. Diese

Netze senden regelmäßig z.B. DNS-Anfragen ins lokale Netz, die ohne diesen Filter ins Internet geleitet werden.

*WAN-Filtertab.* Mit dieser Tabelle können bestimmte Ziel-Port-Bereiche angegeben werden. Treffen von der WAN-Seite Pakete mit den eingetragenen Ports ein, werden sie nicht weitergeroutet (Firewall-Funktion).

Die WAN-Portfilter sind in einer Tabelle ähnlich der LAN-Filter-Tabelle definiert:

Idx.	Z-von	Z-bis	Q-von	Q-bis	Ziel-Adresse	Ziel-Netzmaske	Prot
WIN	53	53	137	139	0.0.0.0	0.0.0.0	TCP und UDP

Die Felder der Tabelle haben die gleiche Bedeutung wie in der LAN-Filter-Tabelle, mit folgendem Unterschied:

■ Ziel-Adresse, Ziel-Netzmaske

Hiermit kann ein Subnetz des lokalen Netzes angegeben werden, für das der Filter gelten soll. Die Ziel-Adresse 0.0.0.0 bedeutet, daß der Filter auf jeden Rechner angewendet wird. Eine Netzmaske von 0.0.0.0 bedeutet, daß der Filter auf alle Netze angewendet wird (was ebenfalls alle Rechner bedeutet).

Die Tabelleneinträge sind ähnlich der IP-Router-Tabelle sortiert:

■ Die längsten Netzmasken stehen oben.

■ Bei gleicher Netzmaske steht die größte IP-Adresse oben.

Damit können Netzmasken und IP-Adressen von 0.0.0.0 als „Wildcard“ eingesetzt werden. Gleichzeitig können bestimmte Rechner und Netze gezielt gefiltert werden, während andere ungefiltert den Router passieren.

Die Tabellen werden von oben nach unten abgearbeitet. Sobald ein Filter paßt, wird das Paket entsprechend behandelt.



*Proxy-ARP* Hier kann der Proxy-ARP-Mechanismus aktiviert bzw. deaktiviert werden (Standard: 'Aus'). Diese Funktion erlaubt die Datenübertragung zu IP-Adressen im gleichen logischen Netz wie der Absender, z.B. bei der Anbindung von einzelnen Arbeitsplatzrechnern (Teleworkern) über TCP-IP an das Firmen-Netz.

*Lok.-Routing* Das lokale Routing ermöglicht es dem Router, Datenpakete über das lokale Netz weiterzuleiten. Das lokale Routing wird dann nötig, wenn der Router als Standard-Gateway der Arbeitsplatzrechner Pakete für Zielnetze empfängt, zu denen er selbst keine Verbindung aufbauen kann. Wenn dieser Router die Adresse des eigentlich zuständigen Routers nicht über ICMP an die Arbeitsplatzrechner zurückmelden kann, leitet er die Daten selbst zu dem entsprechenden Router weiter (siehe auch 'Lokales Routing'). Da diese Einstellung zu einer erhöhten Netzlast im LAN führt, ist die Standardeinstellung 'Aus'.

## Setup/IP-Router-Modul/Routing-Methode

Der Router bietet zwei Methoden für das IP-Routing an, die für IP- und ICMP-Pakete getrennt eingestellt werden können. Beide Methoden setzen auf der Auswertung des Feldes 'Type-of-Service' innerhalb des IP-Headers auf.

Das Menü hat den folgenden Aufbau:

/Routing-Methode		Einstellungen der Routing-Methode
Routing-Methode		Routing-Methode für IP-Pakete
ICMP-Routing-Methode		Routing-Methode für ICMP-Pakete

*Routing-Methode*

Mit diesem Eintrag legen Sie die Routing-Methode für IP-Pakete fest:

- Durch die Einstellung 'normal' werden alle IP-Pakete gleich behandelt, entsprechend den Routing-Vorschriften des Internet-Protocols.
- Durch die Einstellung 'TOS' werden IP-Pakete je nach Inhalt des 'TOS'-Feldes in die Urgent-Queue oder in die gesicherte Queue gestellt. Alle anderen Pakete werden in der normalen Sende-Queue abgelegt. Die Übertragung ist also garantiert, sofern sie grundsätzlich möglich ist.




*ICMP-Routing-Methode*

Mit diesem Eintrag legen Sie die Routing-Methode für ICMP-Pakete fest:

- Durch die Einstellung 'normal' werden ICMP-Pakete wie alle anderen IP-Pakete behandelt, entsprechend den Routing-Vorschriften des Internet-Protocols.
- Durch die Einstellung 'gesichert' werden alle empfangenen ICMP-Pakete in die gesicherte Queue gestellt.

## Setup/IP-Router-Modul/RIP-Einstellungen

Hierüber können Einstellungen für die Verwaltung von IP-RIP-Paketen vorgenommen werden. Das Menü hat den folgenden Aufbau:

/RIP-Einstellungen		Einstellungen für den Betrieb von IP-RIP
Typ		RIP-Kompatibilitätsschalter
R1 Maske		Verwaltung von Netzwerkmasken
Tabelle-RIP		Dynamische IP-Routing-Tabelle

*Typ* Es kann eingestellt werden, nach welchem Verfahren die IP-RIP-Pakete behandelt werden sollen. Dabei bedeutet die Einstellung:

- **Aus:** IP-RIP wird nicht unterstützt (Standard).
- **RIP-1:** RIP-1- und RIP-2-Pakete werden empfangen, aber nur RIP-1-Pakete gesendet.
- **R1komp:** Es werden ebenfalls RIP-1- und RIP-2-Pakete empfangen. Gesendet werden RIP-2-Pakete als IP-Broadcast.
- **RIP-2:** Wie **R1komp**, nur werden alle RIP-Pakete an die IP-Multicast-Adresse 224.0.0.9 gesendet.

*R1-Maske* Über diesen Menüpunkt kann, bei Verwendung von **RIP-1**, die Verwaltung der Netzwerkmasken beeinflußt werden. Diese Einstellungen werden daher nur bei Subnetting unter **RIP-1** benötigt. Dabei bedeutet die Einstellung:

- **Klasse** (Standard): Die im RIP-Paket verwendete Netzwerkmaske ergibt sich direkt aus der IP-Adresse-Klasse, d.h., für die Netzwerkklassen werden folgende Netzwerkmasken verwendet:
  - Klasse A: 255.0.0.0
  - Klasse B: 255.255.0.0
  - Klasse C: 255.255.255.0
- **Adresse:** Die Netzwerkmaske ergibt sich aus dem 1. gesetzten Bit der eingetragenen IP-Adresse. Dieses und alle höherwertigen Bits innerhalb der Netzwerkmaske werden gesetzt. Aus der IP-Adresse 127.128.128.64 ergibt sich so z.B. die IP-Netzmaske 255.255.255.192.
- **KI+Adr:** Die Netzwerkmaske wird aus der IP-Adressen-Klasse und einem angefügten Teil nach dem Adreßverfahren gebildet. Aus obiger Adresse und der Netzmaske 255.255.0.0 ergibt sich somit die IP-Netzmaske 255.128.0.0.






*Tabelle-RIP* Über diesen Menüpunkt werden die Einträge der aktuellen dynamischen IP-Routing-Tabelle angezeigt.

Eine IP-RIP-Tabelle kann z.B. wie folgt aussehen:

IP-Adresse	IP-Netz-Maske	Zeit	Distanz	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200

## Setup/IP-Router-Modul/Masquerading

In diesem Menü werden die Einstellungen für die Maskierungsfunktion vorgenommen. Das Menü hat den folgenden Aufbau:

/Masquerading		Einstellungen für das IP-Masquerading
TCP-Aging		Zeit in Sekunden bis eine TCP-Maskierung ungültig wird
UDP-Aging		Zeit in Sekunden bis eine UDP-Maskierung ungültig wird
ICMP-Aging		Zeit in Sekunden bis eine ICMP-Maskierung ungültig wird
Service-Tabelle		statische Masquerading-Tabelle
Tabelle-Masquerade		dynamische Masquerading-Tabelle

*Service-Tabelle* Bei der Verwendung des inversen Masqueradings werden durch den Eintrag bestimmter Ports in der Service-Tabelle 'Dienste' (z.B. ein Fileserver) im IP-Netz gezielt im Internet sichtbar gemacht, während alle anderen Dienste und Rechner aus dem lokalen Netz unsichtbar bleiben (siehe auch 'IP-Masquerading (NAT, PAT)'). Die Service-Tabelle (auch statische Masquerading-Tabelle) hat max. 16 Einträge nach folgendem Aufbau:

Z-Port	Intranet-Adresse
20	10.1.1.10
21	10.1.1.10

Hierbei bedeuten:

- Z-Port: Ziel-Port für diesen Eintrag
- Intranet-Adresse: Ziel-IP-Adresse des Rechners im lokalen Netz

Durch diese Zuweisung kann der entsprechende Dienst z.B. über Telnet direkt angesprochen werden. Geben Sie dazu die IP-Adresse des Routers ein und hängen die Port-Nummer, durch Doppelpunkt getrennt, an die Adresse an.

Mit dem Befehl

```
telnet 192.38.50.100:27
```

verbinden Sie sich direkt mit einem News-Server, der über einen Router mit der IP-Adresse 192.38.50.100 zu erreichen ist.

*Tabelle-Masquerade*

Beim IP-Masquerading werden die IP-Adressen von Rechnern im lokalen Netz durch eine Umsetzung der Adressen und Ports im Router nach außen hin unsichtbar gemacht. In der dynamischen Masquerading-Tabelle werden die IP-Adressen aus dem lokalen Netz

angezeigt, die aktuell vom Router maskiert werden. Die dynamische Masquerading-Tabelle hat maximal 2048 Einträge nach folgendem Aufbau:








Intranet-Adresse	Q-Port	Protokoll	Zeit
10.1.1.10	1234	TCP	10

Hierbei bedeuten:

- Intranet-Adresse: IP-Adresse des Rechners im lokalen Netz
- Q-Port: Quell-Port für diesen Eintrag
- Protokoll: verwendetes Protokoll (TCP/UDP/ICMP)
- Zeit: Zeit in Sekunden, bis der Eintrag aus der Tabelle entfernt wird

## Setup/SNMP-Modul

Über dieses Menü können Einstellungen für Konfiguration des Routers über SNMP vorgenommen werden. Das Menü hat den folgenden Aufbau:

/SNMP-Modul	Einstellungen für das SNMP-Modul	
Traps-senden		Schalter für die Ausgabe von SNMP-Traps
IP-Trap-Tabelle		Tabelle mit 20 Ziel-Adressen für Trap-Nachrichten
Administrator		Geräte-Administrator
Standort		Geräte-Standort
Register-Monitor		Befehl zum Anmelden einer Zieladresse, zu der Traps gesendet werden sollen
Loesche-Monitor		Befehl zum Löschen einer Adresse, die mit 'Register-Monitor' gesetzt wurde
Monitor-Tabelle		Tabelle mit allen aktuell aktiven Zieladressen, die mit 'Register-Monitor' gesetzt wurden

*Traps-senden* Dieser Eintrag steuert die Ausgabe von Traps (ein/aus).

*IP-Trap-Tabelle* Gibt die IP-Adressen an, zu der Trap-Nachrichten gesendet werden.

*Administrator* Name des Administrators

*Standort* Standort des Gerätes

Die letzten beiden Parameter können auch über SNMP (MIB-2) abgefragt werden.

*Register-Monitor* Mit diesem Befehl melden sich Applikationen beim Router an, um gezielte Trap-Informationen zu erhalten. Der *ELSA LANmonitor* fragt so z.B. die Kanalstatistiken ab und setzt sie (unter Windows) in eine grafische Darstellung um.

Im Prinzip können beliebige SNMP-Manager diesen Befehl nutzen, um Informationen aus dem Router zu erhalten. Mit der Syntax:

```
register-monitor ip-adresse:port mac-adresse timeout
```

wird der Router angewiesen, die angegebene Adresse in die Monitor-Tabelle aufzunehmen und Traps an sie zu senden. Bleiben die Traps für die eingestellte Haltezeit aus, wird die Adresse automatisch aus der Tabelle gelöscht. Eine Haltezeit von '0' behält den Eintrag dauerhaft in der Tabelle.

Loesche-Monitor

Mit diesem Befehl werden die Einträge aus der Monitor-Tabelle entfernt.









Monitor-Tabelle Die Monitor-Tabelle hat folgenden Aufbau:

IP-Adresse	Port	MAC-Adresse	Timeout
10.0.0.53	1057	0080c76da46e	1

Mit diesem Eintrag hat sich z.B. ein *ELSA LANmonitor* bei dem Router angemeldet.

## Setup/DHCP-Server-Modul

Über dieses Menü können Einstellungen für den DHCP-Server vorgenommen werden. Das Menü hat den folgenden Aufbau:

/DHCP-Server-Modul		Einstellungen für den DHCP-Server
Zustand		Schalter für die Aktivierung des DHCP-Moduls
Start-Adreß-Pool		Start-Adresse für den Adreßpool
Ende-Adreß-Pool		End-Adresse für den Adreßpool
Netzmaske		Netzmaske für den Adreßpool
Broadcast-Adresse		Broadcast-Adresse für das LAN
Max.-Gültigkeit-Minute(n)		Maximal-Gültigkeit der Adreßzuweisung über DHCP
Default-Gültigkeit-Minute(n)		Standard-Gültigkeit der Adreßzuweisung über DHCP
Tabelle-DHCP		Tabelle mit den aktuellen Zuweisungen über DHCP

Zustand

Ein: Das Gerät arbeitet als DHCP-Server

Aus: Das Gerät arbeitet nicht als DHCP-Server

Auto: Das Gerät überprüft regelmäßig, ob ein anderer DHCP-Server im LAN vorhanden ist. Wenn nicht, dann arbeitet es als DHCP-Server und verteilt IP-Adresse an lokale Clients.



Falls im TCP/IP-Modul keine IP- oder Intranet-Adresse eingetragen ist (z.B. Auslieferungszustand), dann verteilt der Router im Auto-Modus IP-Adressen aus dem Adreßbereich 10.0.0.2–10.0.0.253 an alle DHCP-Clients.

*Start-Adreß-Pool*  
*Ende-Adreß-Pool*

Die zugewiesene IP-Adresse wird aus dem eingestellten Adreß-Pool genommen ('Start-Adress-Pool' bis 'Ende-Adress-Pool'). Hier können beliebige im lokalen Netz gültige Adressen eingegeben werden.

Wird stattdessen '0.0.0.0' eingegeben, so ermittelt das Gerät die jeweiligen Adressen (Start bzw. Ende) aus den Einstellungen unter 'Setup/TCP-Modul'. Dabei wird wie folgt vorgegangen:

- Ist nur die IP-Adresse oder nur die Intranet-Adresse eingegeben, so wird über die zugehörige Netzmaske der Start bzw. das Ende des Pools bestimmt.
- Sind beide angegeben, so hat die Intranet-Adresse den Vorrang bei der Bestimmung des Pools.
- Als Start-Adresse des Pools wird entweder die im DHCP-Modul eingegebene Adresse verwendet oder die erste gültige Adresse im lokalen Netz.
- Als End-Adresse des Pools wird entweder die im DHCP-Modul eingegebene Adresse verwendet oder die letzte gültige Adresse im lokalen Netz.

Als IP-Adresse wird dann eine gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit bereits schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

Der DHCP-Server prüft zusätzlich, ob die Adresse, die dem Rechner zugewiesen werden soll, eindeutig im lokalen Netz ist. Dies geschieht mit einem ARP-Request auf die Adresse. Wird dieser ARP-Request beantwortet, so beginnt der DHCP-Server den Vorgang mit einer neuen Adresse. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.

*Netzmaske*

Die Zuweisung der Netzmaske erfolgt analog zur Adreßzuweisung:

Entweder wird die im DHCP-Modul eingetragene Netzmaske zugewiesen, oder es wird die zum (bei der Adreßzuweisung bestimmten) lokalen Netz gehörende Netzmaske verwendet.

*Broadcast*

Die Zuweisung der Broadcast-Adresse erfolgt analog zur Adreßzuweisung:

Entweder wird die im DHCP-Modul eingetragene Broadcast-Adresse zugewiesen, oder es wird die zum (bei der Adreßzuweisung bestimmten) lokalen Netz gehörende Broadcast-Adresse verwendet.

*Max.-Gültigkeit-Minute(n)*

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

Der DEFAULT-Wert von 6000 Minuten entspricht ca. 4 Tagen.

*Default-Gültigkeit-Minute(n)*

Hier kann die Gültigkeitsdauer eingetragen werden, die zugewiesen wird, wenn der Host überhaupt keine Gültigkeitsdauer anfordert.

Der DEFAULT-Wert von 500 Minuten entspricht ca. 8 Stunden.



*Tabelle-DHCP*

Im DHCP-Modul kann über den Punkt 'Tabelle-DHCP' die Zuweisung von IP-Adressen an die jeweiligen Rechner überprüft (bzw. nachgeschaut) werden. Diese Tabelle hat den folgenden Aufbau:

IP-Adresse	MAC-Adresse	Timeout	Rechnername	Typ
10.1.1.10	00a0570308e1	500	ELSA	neu







- IP-Adresse: zugewiesene IP-Adresse
- MAC-Adresse: Ethernet-Adresse des Rechners
- Timeout: Restzeit bis die Zuweisung ungültig wird
- Rechnername: Klartextname des Rechners, wenn er diesen in der Anfrage übermittelt
- Typ: Dieses Feld enthält weitere Informationen zu der Zuweisung.

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

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

## Setup/DNS-Modul

Hier werden die Einstellungen des DNS-Servers vorgenommen. Das Menü enthält die folgenden Einträge (inkl. Default-Einstellungen):

Zustand		Ein (Default) oder aus
Domaene		Eigene Domain, optional, maximal 32 Zeichen
DHCP-verwenden		Ja (Default) oder nein
DNS-Tabelle		Statische DNS-Tabelle zur manuellen Zuweisung von IP-Adressen und Namen, 64 Einträge
Filter-Liste		Filter-Liste zum Ausschließen verbotener Domains, 64 Einträge
Gultigkeit		Gibt an, welche Gültigkeit einem anfragenden Rechner für einen Namen mitgeteilt wird. Default: 2000

*DNS-Tabelle* Die DNS-Tabelle enthält eine einfache Zuordnung von lokalen Namen zu IP-Adressen. Dabei ist diese alphabetisch nach Namen sortiert.

Die Tabelle ist auf 64 Einträge beschränkt, da man größere Netze besser über den DHCP-Server konfiguriert und daher diesen zur Auflösung heranziehen kann. Die Tabelle hat den folgenden Aufbau:

Rechnername	Ip-Adresse
HOST10	10.0.0.10

Der Name ist hierbei auf 32 Zeichen begrenzt. Längere Namen sind im lokalen Netz auch nicht sinnvoll.

*Filter-Liste* Die Filter-Liste nimmt Einträge für zu sperrende Domains auf. Weiterhin kann konfiguriert werden, für wen diese Domain gesperrt sein soll. Dies wird über ein Paar IP-Adresse/Netzmaske angegeben. Eine IP-Adresse von 0.0.0.0 bedeutet dabei, daß diese Domain für alle Rechner gesperrt ist. Ebenso bedeutet eine Netzmaske von 0.0.0.0, daß die Domain für alle Netze gesperrt ist. Die Tabelle hat den folgenden Aufbau:

Name	Domain	Ip-Adresse	Netzmaske
F001	*xxx*	0.0.0.0	0.0.0.0

Im Feld 'Name' kann eine eindeutige ID für den jeweiligen Filter frei gewählt werden.

Das Feld 'Domain' nimmt den Namen der zu sperrenden Domain auf. Dabei sind auch Wildcards wie '?' und '\*' möglich. Der Wildcard '?' ersetzt dabei genau ein Zeichen, während '\*' für beliebig viele Zeichen steht. Der Wildcard '\*' kann dabei öfters verwendet werden. So filtert \*xxx\* z.B. alle Namen, in denen xxx vorkommt.









Über die Felder IP-Adresse und Netzmaske kann angegeben werden, für welches Subnetz diese Domain gesperrt wird.

Die Filtertabelle ist absteigend nach Netzmasken (die längste steht oben) und bei gleicher Netzmaske aufsteigend nach IP-Adressen sortiert. Bei gleichen IP-Adressen wird sie dann noch aufsteigend nach zu sperrender Domain sortiert.

Beim Durchsuchen der Tabelle wird diese nun von oben nach unten abgearbeitet. Sobald ein Filter paßt, wird eine Fehlermeldung an den anfragenden Rechner ausgegeben.

## Setup/Config-Modul

Über dieses Menü können Einstellungen für Konfigurationsmöglichkeiten des Routers vorgenommen werden. Das Menü hat den folgenden Aufbau:

/Config-Modul	Einstellungen für das Konfigurationsmodul	
LAN-Config		Schalter für Konfiguration von der LAN-Seite
WAN-Config		Schalter für Konfiguration von der WAN-Seite
Passwort-Zwang		Paßwortzwang ein/aus, wenn kein Paßwort vorhanden ist
Maximale-Verbindungen.		Maximale Anzahl gleichzeitiger Verbindungen
Conf.-Haltezeit		Zeitbeschränkung für Remote-Konfigurationsverbindungen
Login-Fehler		Anzahl für Login-Fehlversuche, bevor die Login-Sperre greift
Sperr-Minuten		Dauer der Sperrung und Zeitraum, bis alte Login-Fehler vergessen sind
Sprache		Sprache für die Konfiguration

*LAN-Config* Mit dieser Einstellung kann festgelegt werden, ob eine Konfiguration von der LAN-Seite möglich ist (**Ein**), nicht möglich ist (**Aus**) oder nur im Lese-Betrieb möglich ist (**Lese**). Standardmäßig ist die Option **Ein** aktiviert.

*WAN-Config* Mit dieser Einstellung kann festgelegt werden, ob eine Konfiguration von der WAN-Seite möglich ist (**Ein**), nicht möglich ist (**Aus**) oder nur im Lese-Betrieb möglich ist (**Lese**). Standardmäßig ist die Option **Aus** aktiviert.

*Passw.Zwang* Hier wird festgelegt, ob bei nicht vorhandenem Paßwort bei jedem Konfigurationsbeginn nach einem neuen Paßwort gefragt werden soll (**Ein**), oder ob die Paßwortabfrage unterdrückt werden soll (**Aus**). Standardmäßig ist die Option **Ein** aktiviert.

*Maximale-Verbindungen* Hier kann die maximale Anzahl der gleichzeitigen Remote-Konfigurationssitzungen zum Gerät abgelesen werden.

*Conf.-Haltezeit* Erfolgt während einer Remote-Konfiguration keine Übertragung mehr, wenn z.B. keine Daten mehr vom Benutzer eingegeben werden, baut das Gerät die Verbindung automatisch nach der hier angegebenen Zeit ab. Gültige Werte sind 1 bis 99 Minuten. Der Standardwert beträgt 5 Minuten.

*Login-Fehler* Dieser Eintrag gibt an, wie viele Fehlversuche gemacht werden dürfen, bevor die Login-Sperre aktiviert wird. Dabei wird ein leeres Paßwort (am Paßwort-Prompt einfach nur <ENTER> drücken) nicht als Versuch gewertet und löst daher auch nicht die Sperre aus.



*Der Default-Wert ist 5. Bei einem niedrigeren Wert kann es passieren, daß bei einem Zugriff über ein älteres ELSA LANconfig die Login-Sperre greift! In diesem Fall erhalten Sie eine aktuelle ELSA LANconfig-Version über unsere Online-Medien.*



*Sperr-Minuten* Dieser Eintrag hat zwei Bedeutungen. Zum einen gibt er an, wie lange der Zugang gesperrt ist, wenn die Login-Sperre aktiviert wurde. Zum zweiten wird hiermit die Zeit eingestellt, nach der das Gerät alle vorherigen Login-Fehler vergißt.

*Sprache* Stellen Sie hier ein, ob Sie die Konfiguration mit der deutschen oder der englischen Fassung der Software durchführen wollen.

## Setup/Zeit-Modul







Die Zeit kann manuell gesetzt werden (mit dem Befehl 'time').

Das Zeit-Modul hat folgenden Aufbau:

/Zeit-Modul	Einstellungen für das Zeit-Modul	
Zustand		Aktivierung des Moduls: <b>Ein, Aus</b>
Aktuelle-Zeit		Anzeige der aktuellen Zeit im Gerät

## Firmware

Über dieses Menü können die verschiedenen Firmwareparameter abgerufen werden und ein Firmware-Upload gestartet werden:

/Firmware	Einstellungen für Display-Anzeige und Tastatur	
Versions-Tabelle		Anzeige der Hardware-Releases und Seriennummern des Routers
Tabelle-Firmsafe		Informationen über die beiden im Gerät gespeicherten Firmware-Versionen und über den Bootloader.
Modus-Firmsafe		Modus der Firmware-Aktivierung
Timeout-Firmsafe		Zeit in Minuten für den Test einer neuen Firmware
Test-Firmware		Testet die inaktive Firmware
Firmware-Upload		Starten eines Firmware-Uploads

*Versions-Tabelle* In der Versions-Tabelle werden die Firmware-Version des Gerätes und die Seriennummer angezeigt.

lfc	Modul	Version	Seriennummer
lfc	LANCOM DSL/10 Office	1.70.0006 / 01.09.1999	8427.000.020

*Table-Firmsafe* In dieser Tabelle finden Sie für jede der beiden im Gerät gespeicherten Firmware-Versionen die Angaben über die Position im Speicherbereich (1 oder 2), die Angabe des Zustan-

des (aktiv oder inaktiv), die Versionsnummer, das Datum, die Größe und den Index (fortlaufende Nummer).

Position	Status	Version	Datum	Groe	Index
1	inaktiv	1.70	30081999	535	6
2	aktiv	1.70	01091999	366	7
3	<Lader>	1.60	01091999	64	0

Um eine inaktive Firmware zu aktivieren, geben Sie den Befehl





```
set <Positionsnummer> aktiv
ein.
```

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

- 'Unmittelbar': Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:
  - Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.
  - Arbeitet die neue Firmware jedoch nicht korrekt, ist das Gerät evtl. nach dem Neustart nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit das Gerät neu.
- 'Login': Um den Problemen einer fehlerhaften Firmware zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.
  - Im Unterschied zur ersten Variante wartet Firmsafe anschließend auf einen erfolgreichen Login über Outband oder Inband (per Telnet). Im Unterschied zur ersten Variante wartet Firmsafe anschließend auf einen erfolgreichen Login (per Telnet). Nur wenn dieser Login während der unter 'Timeout-Firmsafe' eingestellten Zeit erfolgt, wird die neue Firmware auch dauerhaft aktiviert.
  - Wenn das Gerät nicht mehr ansprechbar ist und ein Login somit unmöglich ist, aktiviert Firmsafe automatisch wieder die bisherige Firmware und startet damit das Gerät neu.
- 'Manuell': Auch bei der dritten Möglichkeit können Sie vorher selbst eine Zeit bestimmen (Timeout-Firmsafe), in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, daß die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird.

## Sonstiges

Über das Menü **Sonstiges** werden nachfolgende Funktionen verwaltet:

/Sonstiges	Verschiedene Funktionen	
Manuelle Wahl		Test einer Verbindung
System-Boot		Neustart des Gerätes
System-Reset		Rücksetzen auf Werkseinstellung
System-Upload		Neue Firmware laden

### Sonstiges/Manuelle-Wahl

Über diesen Menüpunkt kann für Testzwecke eine manuelle Verbindungssteuerung vorgenommen werden.

*System-Boot*

Über diesen Menüpunkt kann das Gerät neu gestartet werden.



*Vor der Ausführung des Befehls werden alle offenen Verbindungen (DSL oder TCP) abgebaut bzw. geschlossen.*

*System-Reset*

Über diesen Menüpunkt werden alle vorgenommenen Einstellungen rückgängig gemacht. Das Gerät wird in den Auslieferungszustand zurückversetzt.

Zur Sicherheit wird dabei das Paßwort zum Schutz der Konfiguration abgefragt, um eine Verwechslung mit dem Befehl `System-Boot` zu vermeiden. Ist kein Paßwort vergeben, muß ein zweites Mal die Enter-Taste gedrückt werden.

*System-Upload*

Über diesen Menüpunkt kann ein Firmware-Upload gestartet werden (siehe Kapitel 'So spielen Sie eine neue Software ein').

Die Flash-ROM-Technologie ermöglicht eine flexible und servicefreundliche Handhabung der Systemsoftware durch Einspielen unterschiedlicher Firmware-Versionen. Hierdurch können die Geräte auch auf alle zukünftigen Optionen nachgerüstet werden.