

ELSA LANCOM™ Wireless L-2

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

Aachen, September 1999

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Funk-Netzwerke von ELSA sind kostengünstige Alternativen bzw. Ergänzungen von lokalen, kabelgebundenen Netzwerken (LANs). Mit mobilen Netzwerkkarten können Notebooks und PCs untereinander kommunizieren oder über Basis-Stationen Zugang zu kabelgebundenen Netzwerken und sogar zum ISDN-Netz erhalten.

Diese Dokumentation wendet sich an die Anwender der Basis-Station *ELSA LANCOM Wireless L-2*. Wir stellen Ihnen zunächst das Gerät und seine Möglichkeiten vor, helfen Ihnen beim Anschluß und bei der Installation der Software und zeigen erste Anwendungsbeispiele.

Dokumentation

Die beiliegende Dokumentation besteht aus:

- Handbuch
Hardware-Installation, Beschreibung der Funktionen und Betriebsarten und erste Konfigurationsbeispiele
- elektronischer Dokumentation auf CD
Alle Handbücher der Produktreihe, technische Grundlagen (z.B. zu Funk-Netzwerken, 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 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

Einleitung	1
Wie arbeitet ein Funk-Netzwerk?	1
Was bietet ein <i>ELSA LANCOM Wireless L-2</i> ?	4
Installation	7
Lieferumfang	7
<i>ELSA LANCOM Wireless</i> stellt sich vor	7
So schließen Sie die Basis-Station an	9
Software-Installation	10
Grundkonfiguration	10
Grundeinstellungen mit <i>ELSA LANconfig</i>	10
Grundeinstellungen setzen mit Telnet	12
Konfigurationsmöglichkeiten	13
Funk oder Kabel: Wege für die Konfiguration	13
Voraussetzungen	13
Alternativ: Adreßverwaltung mit dem DHCP-Server	13
Starten der Konfiguration über <i>ELSA LANconfig</i>	14
Starten der Konfiguration über Telnet	15
Befehle für die Konfiguration	15
Neue Firmware mit FirmSafe	16
So funktioniert FirmSafe	16
So spielen Sie eine neue Software ein	17
Konfiguration über SNMP	18
Funktionen und Betriebsarten	19
Parameter für die Funkverbindungen	19
Sicherheit für Ihre Konfiguration	21
Paßwortschutz	21
Die Login-Sperre	21
Zugangskontrolle über TCP/IP	22
Automatische Adreßverwaltung mit DHCP	22
Der DHCP-Server	23
DHCP – 'Ein', 'Aus' oder 'Auto'?	23
So werden die Adressen zugewiesen	24
Konfiguration des DHCP-Servers	27
Anhang	31
Technische Daten	31
Funkkanäle	31
Allgemeine Garantiebedingungen vom 01.06.1998	32
Konformitätserklärungen	34

Index	37
<hr/>	
Technische Grundlagen	R-1
Funk-Netzwerke nach dem IEEE-802.11-Standard	R-1
Ad-hoc-Modus	R-1
Infrastrukturmodus	R-2
Austauschbarkeit mit anderen Geräten	R-3
Netzwerktechnik	R-4
Das Netzwerk und seine Komponenten	R-4
Verbindungsarten	R-4
Netzwerk-Arten	R-6
IP-Adressierung	R-7
IP-Routing und hierarchische IP-Adressierung	R-9
Erweiterung durch lokale Netze	R-12
<hr/>	
Beschreibung der Menüpunkte	R-17
Status	R-19
Status/Aktuelle-Zeit	R-19
Status/Betriebszeit	R-19
Status/WLAN-Statistik	R-20
Status/LAN-Statistik	R-21
Status/TCP-IP-Statistik	R-22
Status/Config-Statistik	R-26
Status/Queue-Statistik	R-26
Status/PCMCIA-Status	R-27
Status/Werte löschen	R-28
Setup	R-28
Setup/LAN-Modul	R-29
Setup/TCP-IP-Modul	R-30
Setup/SNMP-Modul	R-33
Setup/DHCP-Server-Modul	R-34
Setup/Config-Modul	R-36
Setup/WLAN-Modul	R-38
Firmware	R-39
Sonstiges	R-40
<hr/>	
Protokolle	R-43

Einleitung

Die Vorteile von Funk-LANs liegen auf der Hand: Notebooks und PCs können dort aufgestellt werden, wo es sinnvoll ist – Probleme mit fehlenden Anschlüssen oder baulichen Veränderungen gehören bei der drahtlosen Vernetzung der Vergangenheit an.

Die Netzwerkanbindung in Konferenzen oder bei Präsentationen, der Zugriff auf Ressourcen in benachbarten Gebäuden und Datenaustausch mit mobilen Endgeräten sind nur einige der Anwendungsmöglichkeiten im Funk-LAN.

Die zentrale Rolle in einem vorhandenen, kabelverbundenen Netzwerk spielt dabei die Basis-Station. Über die Basis-Station erhalten alle Stationen im Funk-Netzwerk Zugang zum LAN.



In einigen europäischen Ländern ist die Nutzung von Funkfrequenzen im Bereich von 2,4 – 2,48 GHz aufgrund von nationalen Vorschriften eingeschränkt bzw. nur nach Anmeldung möglich. Die Liste der nationalen Zulassungen finden Sie auf einem Beileger.

Wie arbeitet ein Funk-Netzwerk?

In diesem Kapitel lernen Sie die grundsätzliche Arbeitsweise eines Funk-Netzwerks kennen. Die verwendeten Begriffe werden kurz erklärt und der Aufbau und die Anwendungsmöglichkeiten vorgestellt. Detaillierte technische Informationen zu diesem Bereich und zu anderen Themen finden Sie in der elektronischen Dokumentation auf der CD.

*Funk-Netzwerk-
karten
WLAN*

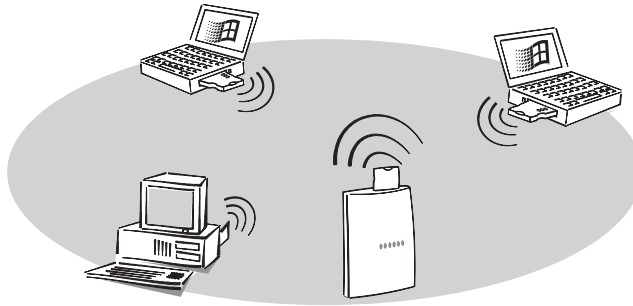
Mit Funk-Netzwerkkarten verbinden Sie einzelne Notebooks und PCs zu einem lokalen Netzwerk, einem **Local Area Network** (LAN). Da in diesem LAN das in herkömmlichen LANs übliche Netzkabel durch eine Funkverbindung ersetzt wird, nennt man diese Funk-Netzwerke auch **Wireless Local Area Network** (WLAN).

Basis-Station

Die Basis-Station bildet die Brücke zwischen LAN und WLAN. Auf der einen Seite ausgestattet mit einem Einschub für eine Funk-Netzwerkkarte (*ELSA AirLancer MC-2*), auf der anderen Seite mit einem normalen Ethernet-Anschluß, überträgt die Basis-Station alle Daten zwischen den beiden Netzen. Die Basis-Station verlängert sozusagen ein Netzkabel über eine Funkstrecke bis zu den mobilen Stationen.

Funkzelle

Der maximale Bereich, in dem Funk-Netzwerkkarten in mobilen Stationen und die Basis-Stationen sich gegenseitig erreichen können und Daten miteinander austauschen, wird als Funkzelle bezeichnet.

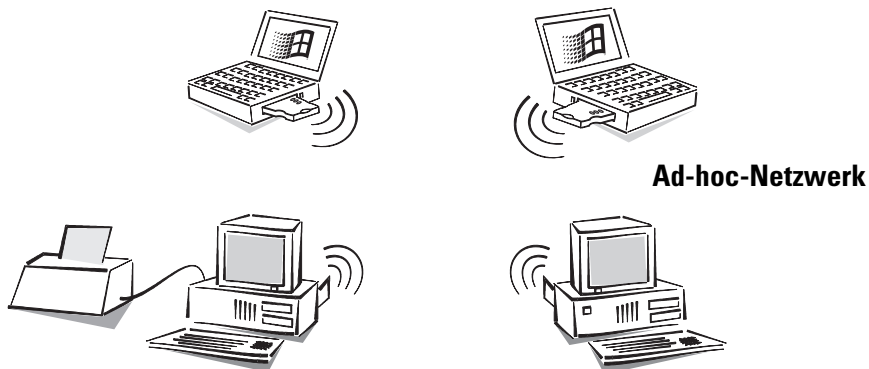


In einem Funk-Netzwerk stehen alle Funktionen eines kabelgebundenen Netzwerks zur Verfügung: Zugriff auf Dateien, Server, Drucker etc. ist ebenso möglich wie die Einbindung der mobilen Stationen in ein firmeninternes Mailsystem.

Folgende Anwendungsmöglichkeiten stehen Ihnen mit den Funk-Netzwerkkarten und Basis-Stationen von ELSA zur Auswahl:

Direkte Rechner-Verbindung

Verbinden Sie mit den Funk-Netzwerkkarten zwei oder mehrere Rechner direkt miteinander. Alle Rechner in einem WLAN können ohne weitere Hardware untereinander kommunizieren.

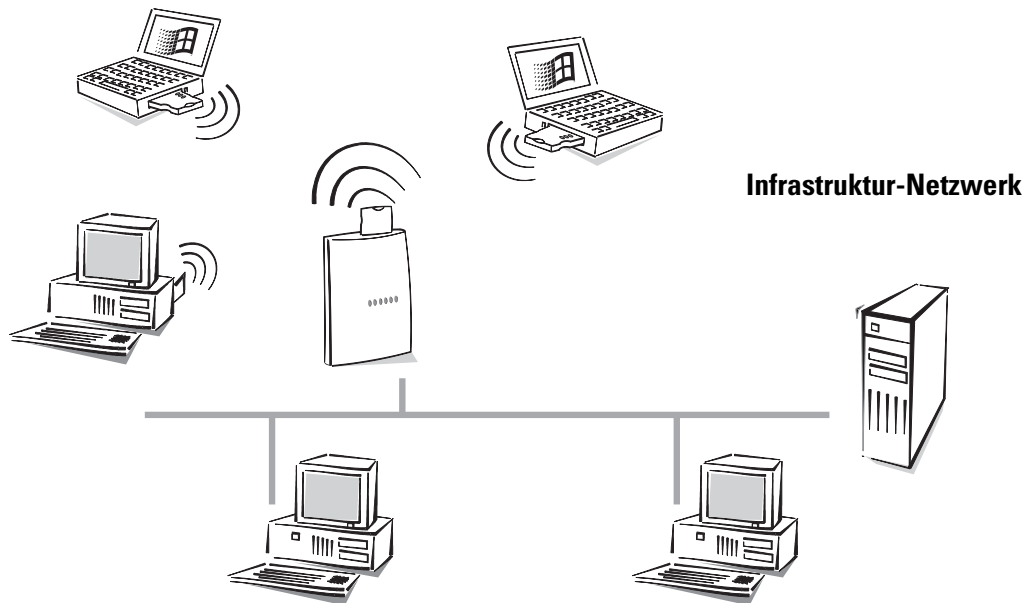
*Peer-to-Peer*

Diese Anwendung wird allgemein auch als Peer-to-Peer-Netzwerk bezeichnet, im Sprachgebrauch der Funk-Netzwerke nennt man diese Vernetzung Ad-hoc-Netzwerk.

Verbindung zum kabelgebundenen LAN

Über eine Basis-Station erhalten alle Rechner mit Funk-Netzwerkkarten Zugang zu einem kabelgebundenen Netzwerk. Die Basis-Station dient zum einen als Verbindung zwischen

LAN und WLAN. Zum anderen bildet sie die Schaltzentrale für den Datenaustausch innerhalb des WLANs.



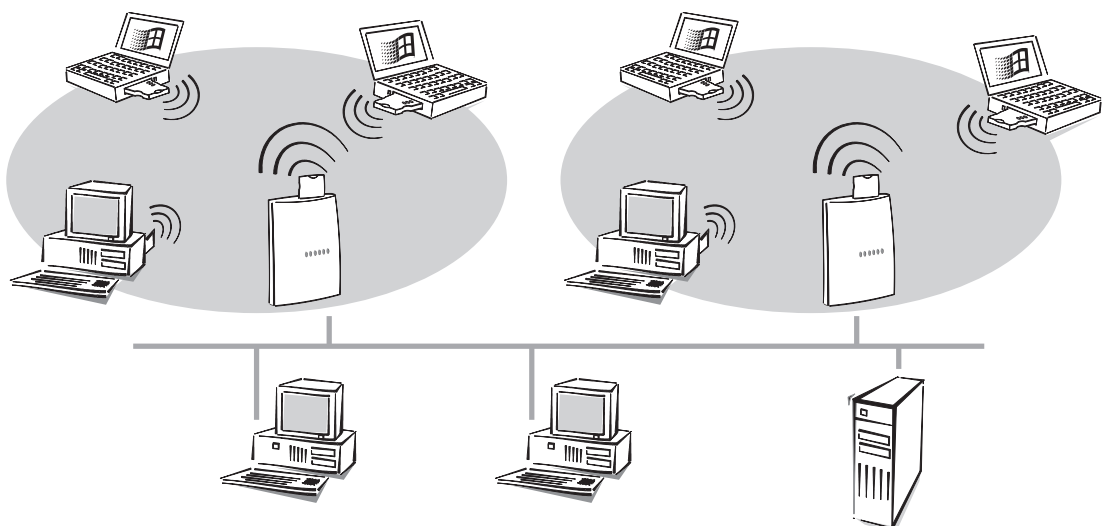
Peer-to-LAN

Ein Funk-Netzwerk mit einer Basis-Station wird allgemein auch als Peer-to-LAN-Netzwerk bezeichnet, im Sprachgebrauch der Funk-Netzwerke nennt man diese Vernetzung Infrastruktur-Netzwerk.

Dieser Netzwerk-Typ eignet sich ideal als Ergänzung zu bestehenden LANs. Bei der Erweiterung eines LANs in Bereichen, wo eine Verkabelung nicht möglich oder unwirtschaftlich ist, stellt das Infrastruktur-Netzwerk die ideale Alternative dar.

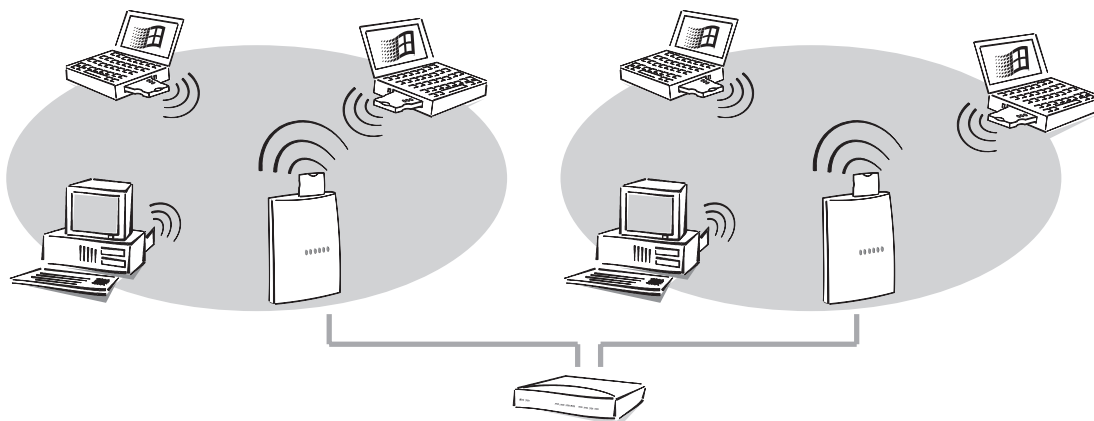
Skalierung

Wenn die Reichweite einer Funkzelle nicht mehr ausreicht, um alle mobilen Stationen zu einem Funk-Netzwerk zusammenzuschließen, können auch mehrere Basis-Stationen eingesetzt werden. Damit wird das Netzkabel des LANs zur Überbrückung der fehlenden Reichweite genutzt.



Dieses Prinzip funktioniert auch dann, wenn überhaupt kein kabelgebundenes LAN vorhanden ist, weil Sie ein neues Funk-Netzwerk aufbauen wollen. Liegen die Mobil-Stationen

nen nicht alle innerhalb der Reichweite einer Basis-Station, wird eine zweite dazugenommen. Die beiden Basis-Stationen können dann z.B. über einfache Netzkabel und einen Hub verbunden werden.



Um eine hohe Abdeckung zu erreichen, können Funkzellen auch überlappen. Damit es nicht zu Störungen im Funk-Netzwerk kommt, können für die jeweiligen Zellen unterschiedliche Kanäle (bis zu 14 verschiedene) gewählt werden.

Was bietet ein *ELSA LANCOM Wireless L-2*?

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

Einfache Installation

- *ELSA LANCOM* mit Spannung versorgen
- Verbindung zum LAN herstellen
- Einschalten
- Loslegen

LAN-Anschluß

Basis-Stationen für Funk-Netzwerke von ELSA arbeiten im Ethernet. Über den 10Base-T-Anschluß und einen Hub oder Switch verbinden Sie *ELSA LANCOM Wireless* mit dem 10-Mbit-LAN.

Funk-Netzwerk-Anschluß

Die Funk-Netzwerkkarten in den Basis-Stationen von ELSA arbeiten nach dem IEEE-Standard 802.11. Dieser Standard stellt eine Erweiterung der bereits vorhandenen IEEE-Normen für LANs dar, von denen IEEE 802.3 für Ethernet der bekannteste ist.

Für die drahtlose Datenübertragung können prinzipiell drei verschiedene physikalische Verfahren eingesetzt werden:

- Infrarotübertragung

- Funk mit Frequency Hopping
- Funk mit DSSS-Verfahren (**D**irect **S**equenz **S**pread **S**pectrum)

Bei diesem Verfahren, das auch im militärischen Bereich zur Steigerung der Abhörsicherheit verwendet wird, werden die Daten vor der Übertragung zerhackt und auf einen großen Frequenzband verteilt (spread spectrum). Damit wird eine zuverlässige und abhörsichere Übertragung gewährleistet.

Die Funk-Netzwerkkarten von ELSA setzen das DSSS-Verfahren ein. Neben den Vorteilen der Abschirmung gegen Störungen durch andere Sender, die ggf. das gleiche Frequenzband verwenden, werden die Karten damit auch kompatibel zu Systemen anderer Hersteller.

IEEE 802.11 erlaubt den Betrieb von lokalen Funk-Netzwerken über privatem und öffentlichem Gelände im ISM-Frequenzband (**I**ndustrial, **S**cientific, **M**edical: 2,4 bis 2,483 GHz).

Die maximale Bandbreite der Datenübertragung im Funk-Netzwerk beträgt 2 Mbit/s. Die Reichweite der Übertragung beträgt im Freien bis zu 300 Meter, in Gebäuden typischerweise ca. 30 Meter.

Transparentes Bridging

Datenpakete aus dem kabelgebundenen LAN werden auf das Funk-Netzwerk übertragen und umgekehrt. Darüber hinaus gibt es die Möglichkeit, den Datenverkehr auf bestimmte Protokolle und Stationen einzuschränken.

Statusanzeigen

LED-Anzeigen an der Frontseite Ihrer Basis-Station ermöglichen die Überprüfung von Ethernet-Anschlüssen sowie der aktuellen Leitungsverbindungen 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.

Der Zugriff auf das Gerät ist dabei möglich aus dem WLAN oder aus dem LAN. Dabei wird neben TFTP auch SNMP unterstützt.

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.

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

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

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

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

Installation

Diese Kapitel wird Ihnen helfen, möglichst schnell ein neues Funk-Netzwerk aufzubauen. 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.

Lieferumfang

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

- Basis-Station *ELSA LANCOM Wireless L-2*
- Netzteil
- Funk-Netzwerkkarte *ELSA AirLancer MC-2*
- LAN-Anschlußkabel
- 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 Wireless stellt sich vor

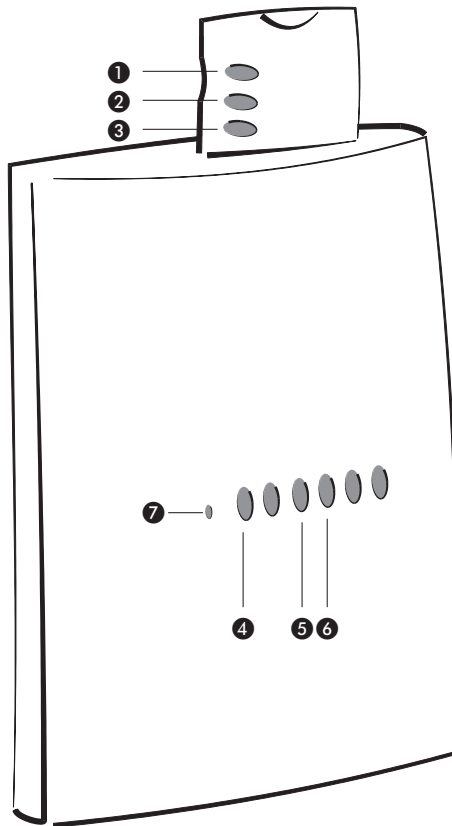
In diesem Abschnitt stellen wir Ihnen die Hardware des Geräts vor. Sie erfahren etwas über die Bedeutung der Anzeigeelemente sowie die Anschlußmöglichkeiten.

Basis-Station Die Basis-Station bildet die Verbindung zwischen dem Funk-Netzwerk und dem kabelgebundenen Netzwerk (LAN). Dazu bietet sie neben dem 10Base-T-Anschluß für das 10-Mbit-Ethernet auch einen Steckplatz für die Funk-Netzwerkkarte *ELSA AirLancer MC-2*.

PC-Karte Die Funk-Netzwerkkarte *ELSA AirLancer MC-2* ist als PC-Karte ausgeführt und wird einfach in den Steckplatz der Basis-Station eingeschoben. Die Antenne der Karte ragt über das Gehäuse der Basis-Station hinaus.

LEDs

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

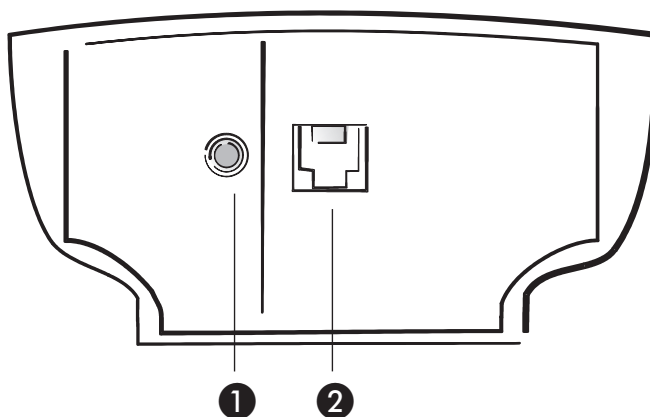


- 1 Die rote LED in der Funk-Netzwerkkarte zeigt an, daß die Verbindung zwischen der Karte und der Basis-Station hergestellt ist.
- 2 Die gelbe LED in der Funk-Netzwerkkarte zeigt die Anzahl der mobilen Stationen an, die sich bei dieser Basis-Station angemeldet haben. Bei drei angemeldeten Stationen blinkt die LED z.B. dreimal hintereinander kurz auf, dann folgt eine Pause.
- 3 Die grüne LED in der Funk-Netzwerkkarte zeigt die Aktivität auf dem Funk-Netzwerk an, also das Versenden und Empfangen von Datenpaketen. Wenn diese LED gar nicht oder aber permanent leuchtet, liegt eine Störung der Funk-Netzwerkkarte vor.
- 4 Die LED 'Power/Msg' an der Basis-Station 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
grün	1 x kurz	Bootvorgang (Test und Laden) begonnen
grün	blinkend	Anzeige eines Bootfehlers (im Blinkcode kodiert)
grün		Gerät betriebsbereit

- ⑤ Die LED 'LAN-Status' an der Basis-Station zeigt die Aktivität auf dem Funk-Netzwerk und auf dem LAN an.
- ⑥ Die LED 'LAN-Collision' an der Basis-Station zeigt eine Sendekollision auf dem LAN an.
- ⑦ Der Reset-Taster ist im Gehäuse verborgen und kann nur mit einem spitzen Gegenstand gedrückt werden (z.B. Büroklammer). Drücken Sie auf den Reset-Taster, bis alle LEDs aufleuchten. Damit wird das Gerät in den Auslieferungszustand zurückgesetzt.

Jetzt drehen Sie das Ganze mal um und sehen sich die Unterseite an. Dort finden Sie:



- ① Anschluß für das Netzteil
- ② 10Base-T-Netzwerkanschluß

So schließen Sie die Basis-Station an

- ① Verbinden Sie die Basis-Station *ELSA LANCOM Wireless L-2* mit dem LAN. Stecken Sie dazu das mitgelieferte Netzkabel in den 10Base-T-Netzwerkanschluß der Basis-Station und in eine freie Netzwerkanschlußdose Ihres lokalen Netzes (oder in eine freie Buchse eines Hubs in Ihrem LAN).
- ② Schieben Sie die Funk-Netzkarte *ELSA AirLancer MC-2* in die Basis-Station ein. Die LEDs der PC-Karte müssen dabei zur Vorderseite der Basis-Station weisen.
- ③ Versorgen Sie die Basis-Station über das Netzteil mit der benötigten Spannung. Nach einem kurzen Selbsttest des Geräts leuchtet die LED 'Power/Msg' an der Basis-Station permanent. Die rote LED in der Funk-Netzkarte zeigt an, daß die Verbindung zwischen der Karte und der Basis-Station hergestellt ist. Das Flackern der grünen LED in der Funk-Netzkarte zeigt an, daß die versucht andere Stationen im WLAN zu erreichen. Die LED 'LAN-Status' zeigt die korrekte Verbindung zwischen Basis-Station und LAN an.

Software-Installation

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



Die Parameter für das Funk-Netzwerk sind im Auslieferungszustand schon so eingestellt, daß Sie in den meisten Fällen einfach loslegen können. Nur bei speziellen Anwendungen sind Anpassungen der Konfiguration nötig.

Zum Betrieb der Konfigurationssoftware benötigen Sie entweder einen PC im kabelgebundenen LAN oder im Funk-Netzwerk.

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

Grundkonfiguration

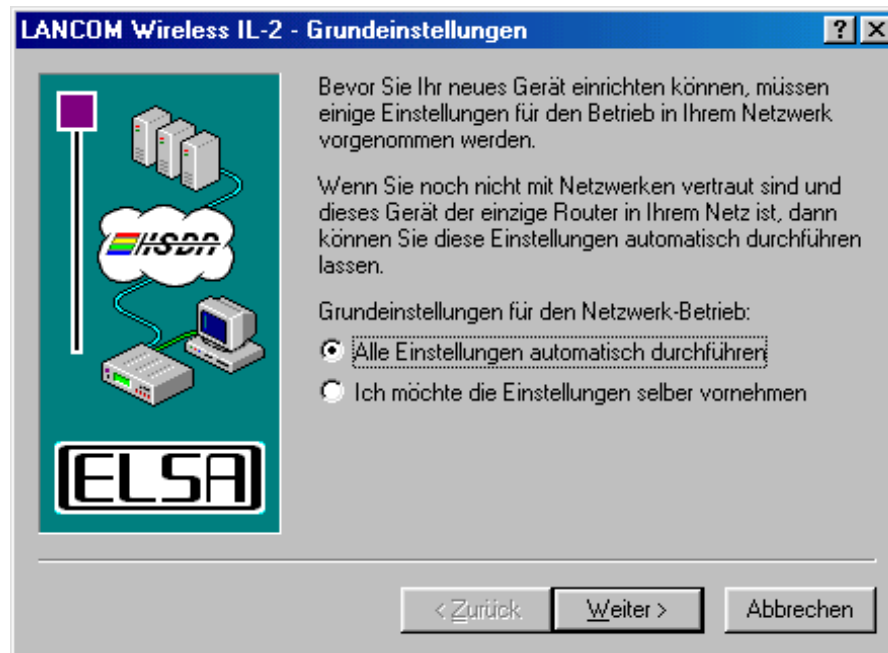
Bei der Grundkonfiguration wird die IP-Adresse für die Basis-Station festgelegt. Außerdem wird über die Verwendung des integrierten DHCP-Servers entschieden. Sie können die Grundkonfiguration mit *ELSA LANconfig* oder mit Telnet vornehmen.

Grundeinstellungen 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.

Um ein *ELSA LANCOM Wireless* in Betrieb zu nehmen, darf die IP-Adresse XXX.XXX.XXX.254 in Ihrem Netzwerk nicht belegt sein. Sollten Sie bereits ein Gerät mit dieser Adresse haben, schalten Sie es bitte für die Zeit der Inbetriebnahme des *ELSA LANCOM Wireless* aus.

- ① Starten Sie die neue Software mit **Start ▶ Programme ▶ ELSAan ▶ 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. Die Basis-Station 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 bestätigen mit **OK**. Wählen Sie im folgenden Fenster ihre Netzwerkkarte aus. Wenn im Feld 'IP-Adresse' der Wert '0.0.0.0' steht, hat die Netzwerkkarte 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 die Basis-Station

jedoch selbst festlegen und der Basis-Station 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 der Basis-Station eine freie Adresse aus dem bisher verwendeten Adreßbereich, und wählen Sie aus, ob die Basis-Station 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 Wireless-CD. Die Funktionsweise des DHCP-Servers ist weiter hinten in diesem Handbuch beschrieben.

- ④ Mit diesen wenigen Mausklicks ist Ihre Basis-Station fertig eingestellt für die grundlegende Aufgabe, mobilen Stationen Zugriff auf ein kabelgebundenes LAN zu ermöglichen.

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 Telnet-Verbindung 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 müssen Sie ggf. Ihren Router neu starten.

- ④ Evtl. DHCP-Funktion ausschalten:

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

Konfigurationsmöglichkeiten

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

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

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

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

Funk oder Kabel: Wege für die Konfiguration

Mit der Konfiguration über das Netzwerk haben Sie von jedem Rechner aus dem WLAN oder LAN aus Zugriff auf die Basis-Station. Der Zugang kann allerdings über die IP-Zugangsliste eingeschränkt oder ganz gesperrt werden. Für diese Konfiguration verwenden Sie entweder Telnet (gehört zum Lieferumfang der meisten Betriebssysteme) oder 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 Ihre Basis-Station benötigt eine IP-Adresse, mit der Sie sie ansprechen können.

Ein noch nicht konfiguriertes Gerät hört auf die IP-Adresse XXX.XXX.XXX.254. Die vielen X stehen dabei für die Netzwerk-Adresse 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, schalten sie zunächst den Rechner mit dieser IP-Adresse aus. Sobald Sie mit ELSA LANconfig oder Telnet Verbindung zur Basis-Station aufgenommen haben, geben Sie ihr eine andere, freie IP-Adresse.

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').

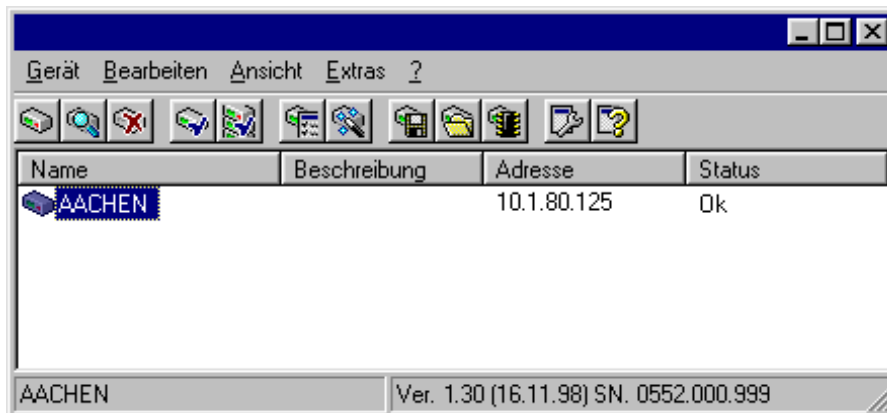
Starten der Konfiguration über *ELSA LANconfig*

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



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

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



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

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

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



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

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

Starten der Konfiguration über Telnet

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

```
telnet 10.1.80.125
```

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

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


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.

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

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)
- 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



In *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**.

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 vorherige Firmware. Die Konfiguration bleibt dabei erhalten.

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

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

Konfiguration über SNMP

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

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

Funktionen und Betriebsarten

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

- Funk-Netzwerke
- Sicherheit für die Konfiguration
- Automatische Adreßverwaltung mit DHCP

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.

Parameter für die Funkverbindungen

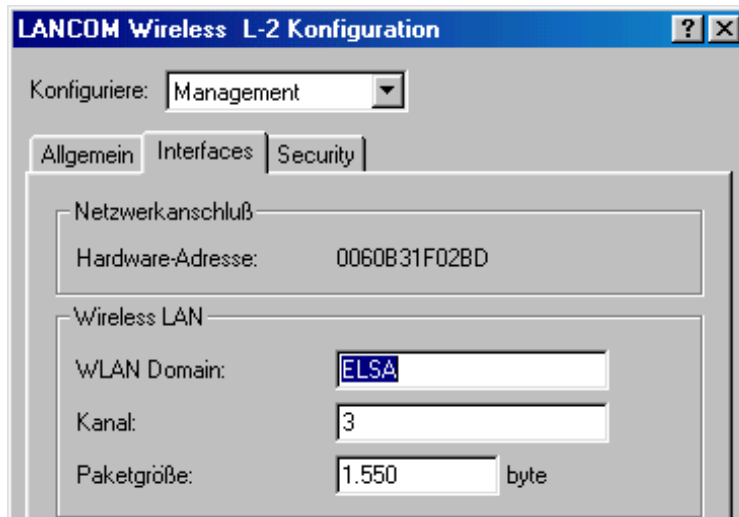
Damit die Funk-Netzkarten in den mobilen Stationen und in den Basis-Stationen sich gegenseitig erkennen und Daten untereinander austauschen können, müssen sie in verschiedenen Parametern die gleichen Werte aufweisen.

Alle Funk-Netzkarten (in Basis- oder Mobil-Stationen), die mit den gleichen Parametern arbeiten, spannen ein Funk-Netzwerk auf. Mit der Wahl der Parameter können so gezielt verschiedene Funk-Netzwerke angelegt werden, deren Datenverkehr sich gegenseitig nicht beeinflußt.

Die Parameter werden für die Funk-Netzkarten in den Basis-Stationen bei der Konfiguration über *ELSA LANconfig* oder Telnet eingestellt.

- ① Starten Sie *ELSA LANconfig* mit **Start ► Programme ► ELSAlan ► ELSA LAN-config**. *ELSA LANconfig* sucht nun automatisch nach allen Basis-Stationen im LAN und WLAN.

- ② Klicken Sie in der Liste der gefundenen Geräte auf die Basis-Station, die Sie konfigurieren möchten. Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Interfaces'.



- ③ Stellen Sie einen neuen Wert für die WLAN-Domain ein. Die WLAN-Domain muß bei allen Teilnehmern eines Funk-Netzwerks gleich sein.



Ändern Sie diesen Wert von der Voreinstellung 'ELSA' möglichst bald auf einen anderen beliebigen Wert, denn mit der WLAN-Domain schützen Sie Ihr Funk-Netzwerk wie mit einem Paßwort gegen unbefugte Eindringlinge!

- ④ Stellen Sie den Funkkanal bei allen Teilnehmern des Funk-Netzwerks gleich ein. Mit dem Funkkanal wählen Sie das Frequenzband, das die Funk-Netzwerkkarten für den Datenaustausch nutzen.

Mit der Wahl eines anderen Kanals können Sie ganz gezielt verschiedene Funk-Netzwerke nebeneinander betreiben. Theoretisch stehen zwar 14 verschiedene Kanäle zur Verfügung, durch die Frequenzüberlappung beim DSSS-Verfahren sind im ISM-Frequenzband jedoch nur drei völlig überlappungsfreie Kanäle möglich. Falls gleichzeitig mehrere Funkzellen in engem Abstand zueinander betrieben werden sollen, sollten Sie Kanäle mit größtmöglichem Abstand wählen. z.B. Kanal 1, 7 und 14 oder 3 und 13.



Beachten Sie bitte die Tabelle der erlaubten Funkkanäle in den einzelnen Ländern im Anhang.

- ⑤ Mit der Paketgröße stellen Sie die Länge der einzelnen Datenpakete ein, die über das Funk-Netzwerk versendet werden. Möglich sind Werte von 600 bis 1600 Byte. Größere Pakete müssen vor der Übertragung zerlegt (fragmentiert) werden und beim Empfänger wieder zusammengesetzt (assembliert) werden.

Kleine Pakete können in gestörten Umgebungen zu besseren Übertragungen führen, der Anteil der Nutzdaten zu den Verwaltungsinformationen eines Pakets verschlechtert sich allerdings.

- ⑥ Wechseln Sie in den Konfigurationsbereich 'WLAN-Bridge', wenn Sie
- für bestimmte mobile Stationen den Datenaustausch mit dem kabelgebundenen LAN oder
 - den Austausch von Datenpaketen mit bestimmten Protokollen sperren möchten.



*Falls der Konfigurationsbereich 'WLAN-Bridge' nicht sichtbar ist, schalten Sie im Hauptfenster von ELSA LANconfig mit **Ansicht** ► **Optionen** in die vollständige Darstellung der Konfiguration um.*

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 Wireless* 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 Wireless* 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.

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

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

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

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.

Automatische Adreßverwaltung mit DHCP

Für einen reibungslosen Betrieb in einem TCP/IP-Netzwerk benötigen alle Geräte in einem lokalen Netzwerk eindeutige IP-Adressen. Zusätzlich brauchen sie noch die Adressen von DNS- und NBNS-Servern sowie eines Standard-Gateways, über das Datenpakete von lokal nicht erreichbaren Adressen geroutet werden sollen.

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

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

Der DHCP-Server

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

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

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

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

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

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 Auto-Modus. 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.
- Wird stattdessen '0.0.0.0' eingegeben, so ermittelt der DHCP-Server selbständig die jeweiligen Adressen (Start bzw. Ende) aus den Einstellungen für die IP-Adresse im 'TCP/IP-Modul'.
- Wenn *ELSA LANCOM Wireless* keine eigene IP-Adresse hat, befindet sich das Gerät in einem besonderen Betriebszustand. Es verwendet dann selbst die IP-Adresse '10.0.0.254' und den Adreß-Pool '10.x.x.x' für die Zuweisung der IP-Adressen im Netz. In diesem Zustand weist der DHCP-Server den anderen Rechnern im Netz nur die IP-Adresse und deren Gültigkeit zu, nicht jedoch die anderen Informationen.

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

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

Zuweisung der Netzmaske

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

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 von DNS- und NBNS-Server

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



Wenn die im kabelgebundenen LAN vorhandenen DNS- oder NBNS-Server auch im Funk-Netzwerk verfügbar sein sollen, müssen die entsprechenden Adressen auf jeden Fall eingetragen werden. Die Basis-Station gibt ansonsten die eigene IP-Adresse als DNS- oder NBNS-Server an die Rechner im Funk-Netzwerk weiter, kann die Anfragen aber nicht beantworten.

Zuweisung des Default-Gateways

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



Wenn ein im kabelgebundenen LAN vorhandenes Gateway auch im Funk-Netzwerk verfügbar sein soll, muß die IP-Adresse des Gateways im DHCP-Modul als 'Gateway-Adresse' eingetragen werden. Die Basis-Station gibt ansonsten die eigene IP-Adresse als Gateway an die Rechner im Funk-Netzwerk weiter, kann die Anfragen aber nicht beantworten.

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 Netzwerkkadapter, 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 dies 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 Netzwerkkadapter 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.

Konfiguration des DHCP-Servers

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

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

Konfiguration mit *ELSA LANconfig* und den Assistenten

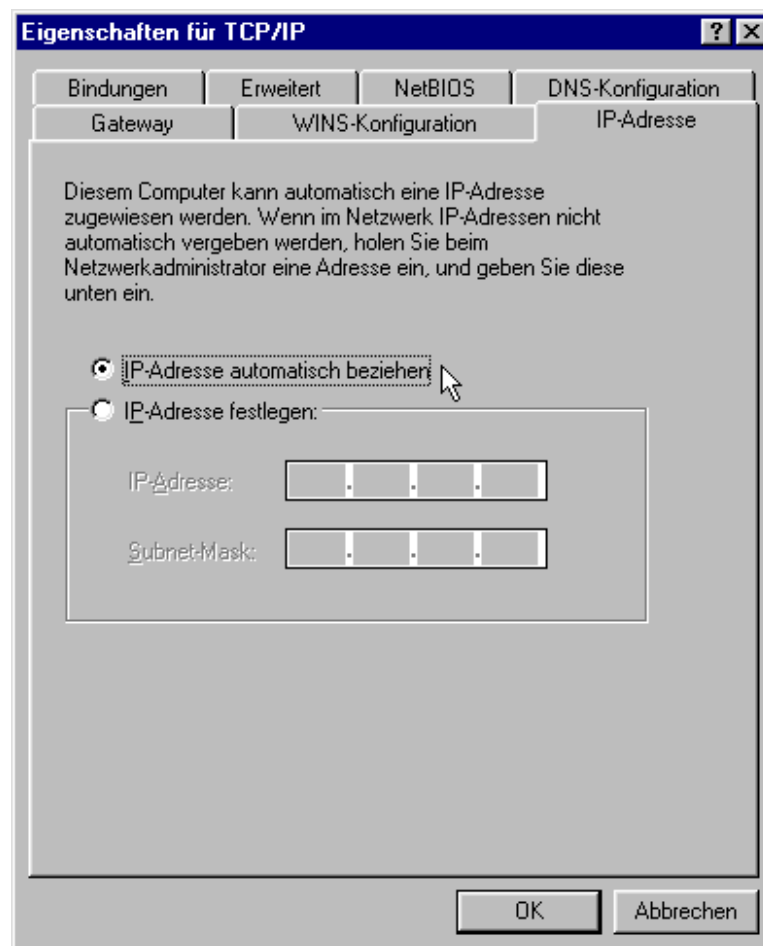
In beiden Situationen hilft Ihnen *ELSA LANconfig* mit einem Assistenten, die notwendigen Einstellungen vorzunehmen:

- ① Verbinden Sie den unkonfigurierten Router über das Netzkabel mit Ihrem lokalen Netz. Wenn Sie das Gerät dabei an einen Hub anschließen, muß der Node/Hub-Umschalter auf 'Node' stehen. Wenn Sie den Router dagegen direkt an die Netzkarte eines Rechners im Netz anschließen, muß sich der Node/Hub-Umschalter in der Position 'Hub' befinden.
- ② Schalten Sie das Gerät ein. Der Router findet dann zunächst keinen anderen DHCP-Server im Netz und aktiviert seine eigenen DHCP-Funktionen.
- ③ Falls noch nicht geschehen, installieren Sie das Protokoll 'TCP/IP' auf allen Rechnern im lokalen Netz.
 - Bei der Installation des Protokolls werden die Rechner meist standardmäßig so eingestellt, daß Sie die IP-Adresse automatisch von einem DHCP-Server bezie-

hen können. Nach einem Neustart, der mit dieser Installation verbunden ist, fordern die Rechner automatisch eine IP-Adresse vom DHCP-Server an.

- Wenn Sie das Protokoll schon installiert haben, aktivieren Sie nun die DHCP-Funktion auf allen Rechnern im lokalen Netz. Öffnen Sie dazu z.B. unter Windows 95 mit **Start ► Einstellungen ► Systemsteuerung ► Netzwerk** das Fenster zur Konfiguration der Netzwerkeigenschaften. Doppelklicken Sie den Eintrag für das Protokoll 'TCP/IP'.

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



- ④ Installieren Sie *ELSA LANconfig* auf einem der Rechner im Netz.
- ⑤ Starten Sie das Programm aus der Programmgruppe 'ELSAIlan'. Beim Start bemerkt *ELSA LANconfig*, daß sich ein unkonfigurierter Router im Netz befindet, und startet den Assistenten für die Grundeinstellungen.

- Wenn Sie bisher noch keine IP-Adressen in Ihrem Netz verwendet haben, wählen Sie in diesem Assistenten die Option 'Alle Einstellungen automatisch vornehmen', und betätigen Sie im nächsten Fenster die Schaltfläche **Fertigstellen**. Der Assistent weist dem Router nun die IP-Adresse '10.0.0.1' mit der Netzmaske '255.255.255.0' zu und schaltet den DHCP-Server ein. Aus der IP-Adresse ermittelt das Gerät dann den gültigen Adreß-Pool für die DHCP-Zuweisung.
- Wenn Sie auch vor der Umstellung auf DHCP-Betrieb IP-Adressen in Ihrem Netz verwendet haben, wählen Sie in diesem Assistenten die Option 'Ich möchte die Einstellungen selber vornehmen'. Geben Sie im nächsten Fenster eine freie IP-Adresse aus dem bisher verwendeten Adreßbereich ein, und schalten Sie den DHCP-Server ein. Der Assistent weist dem Gerät nun die eingestellte IP-Adresse mit der zugehörigen Netzmaske zu. Aus der IP-Adresse ermittelt das Gerät dann den gültigen Adreß-Pool für die DHCP-Zuweisung.
- Nach einigen Sekunden werden automatisch alle Rechner im Netz überprüft und erhalten ggf. eine neue IP-Adresse vom DHCP-Server. Zusätzlich werden den Rechnern dann auch die weiteren Parameter wie Broadcast-Adresse, DNS-Server, Default-Gateway etc. mitgeteilt.

Manuelle Konfiguration

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

Anhang

Technische Daten

Frequenzband	2400–2483,5 MHz (ISM)
Datenübertragungsrate	2 Mbit/s (mit Ausweichmöglichkeit auf 1 Mbit/s, Automatic Rate Selection)
Reichweite	bis zu 300 Meter in freien Gelände, ca. 30 Meter in geschlossenen Gebäuden (typische Reichweite)
Bitfehlerrate	Besser als 10 ⁻⁵
Norm	IEEE 802.11, DSSS (Direct Sequence Spread Spectrum)
Betriebssysteme	Windows 95, Windows 98, Windows NT 4.0, Windows 2000, Windows CE (in Vorb.)
Netzwerkprotokolle	beliebige Netzwerkprotokolle werden zwischen WLAN und LAN per Bridge übertragen
Anschlüsse	10Base-T, Power
Lieferumfang	Ausführliche Dokumentation in Deutsch, Englisch, Französisch und Italienisch Netzwerkkabel, Konfigurationssoftware
Service	Garantie: 6 Jahre
Support	über Hotline, ELSA LocalWeb und Internet

Funkkanäle

Jeder der 14 Funkkanäle, die für ein Funk-Netzwerk eingestellt werden können, hat durch die Verwendung von DSSS eine Breite von 22 MHz. Dadurch sind im ISM-Frequenzband maximal drei voneinander unabhängige Kanäle möglich. Die Tabelle gibt die Mittelfrequenzen an und zeigt, welche Kanäle in welchem Land zugelassen sind.

	Kanal-Nr.	Mittelfrequenz [MHz]	EU (ETSI)	Spanien	Frankreich
1. Funkband Kanal 3	1	2412	X		
	2	2417	X		
	3	2422	X		
	4	2427	X		
	5	2432	X		
2. Funkband Kanal 8	6	2437	X		
	7	2442	X		
	8	2447	X		
	9	2452	X		
	10	2457	X	X	X
3. Funkband Kanal 13	11	2462	X	X	X
	12	2467	X		X
	13	2472	X		X
	14	2484			

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.

Konformitätserklärungen



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

Geräteart: Wireless LAN Access Point

Type of Device:

Typenbezeichnung: LANCOM Wireless L-2

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: 1998

EN 50082-1: 1992 Teile/ parts: EN55024: 1999

EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997

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, 19. August 1999

Aachen, 19th August 1999

i.V. Stefan Kriebel

Bereichsleiter Entwicklung

VP Engineering



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

Geräteart: Wireless LAN PC card (PCMCIA)

Type of Device:

Typenbezeichnung: AirLancer MC-2

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**

ETS 300 328: 1996

ETS 300 826: 1997

EN 50081-1: 1992 Teile/ parts: EN 55022: 1998

EN 50082-1: 1992 Teile/ parts: EN 55024: 1999

EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997

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, 19. August 1999

Aachen, 19th August 1999

i.V. Stefan Kriebel

Bereichsleiter Entwicklung

VP Engineering

Index

■ Numerics

10Base-T-Anschluß	7
10-Mbit-Ethernet	7
802.11	4

■ A

Abschirmung	5
Ad-Hoc-Netzwerk	2
Administrator	R-33
Adreß-Pool	24, 29, R-34
Adreßverwaltung	22
Adreßzuweisung	14
Anschluß	R-29
Antenne	7
Apple Talk	R-6
ARP-Aging-Min	R-32
ARP-Cache	R-32
ARP-Tabelle	R-32
Assemblierung	20
Auslieferungszustand	9
Automode	23
Auto-Modus	R-34

■ B

Bandbreite	5
Basis-Station	1, 7
Betriebsarten	19
Bridging	5
Broadcast-Adresse	R-8
Broadcast-Übertragung	R-12
Brute-Force	21

■ C

Cache	R-32
Conf.-Haltezeit	R-37

■ D

Datenpakete	R-4
DHCP	6, 22, R-34
DHCP-Automode	23
DHCP-Server	6, 10, 13, 23, R-34

Konfiguration	27
Direct Sequenz Spread Spectrum	5
DNS	R-32
DNS-Backup	R-32
DNS-Forwarding	R-32
DNS-Server	22, 25
DSSS-Verfahren	5, 20
Dynamic Host Configuration Protocol	22

■ E

ELSA-Protokoll	R-28
End-Adresse	24
Ende-Adreß-Pool	R-34
Ethernet	4
10Base-T	4
Ethernet-Anschluß	1

■ F

FirmSafe	6, 16
Firmsafe	R-39
Firmware	6, R-39
Firmware-Upload	17, R-39
mit LANconfig	17
mit TFTP	18
Flash-ROM-Speicher	5, 16
Fragmentierung	20
Frequenzband	20
Funkkanal	20
Funk-Netzwerk	1, 19
Funk-Netzwerkkarte	1, 4, 7
Funkstrecke	R-4
Funkzelle	2

■ G

Gateway	22, 25
Gültigkeitsdauer	23, 25

■ H

Heap-Reserve	R-29
hierarchische IP-Adressen	R-9
Host	R-4

■ **I**

IANA	R-9
Identifikation	R-28
IEEE-Standard 802.11	4
Inband	
mit Telnet	15
Voraussetzungen	13
Infrastruktur-Netzwerk	3
Installation	4
Internet	R-6
Internetwork	R-6
Intranet-Adresse	R-30
IP-Adresse	10, 13, R-30
IP-Adressen	6, R-7
IP-Netz	R-6
IPX	R-6
IP-Zugangsliste	13
ISDN-Netz	R-7
ISDN-Zeit	R-19
ISM-Frequenzband	5

■ **K**

Kabel	R-4
Kabelnetz	R-7
Konfiguration	5
Befehle	15
SNMP	18
Konfigurationsmöglichkeiten	R-36

■ **L**

LAN	1, R-6, R-12
LAN-Anschluß	4
LAN-Anschlußkabel	7
LAN-Config	R-37
<i>LANconfig</i>	5, 10, 13, 14, 17, 19
LED	8
LAN-Collision	9
LAN-Status	9
Power/Msg	8
LED-Anzeigen	5
Lieferumfang	7
Local Area Network	1, R-6
Login	17
Login-Fehler	R-37

Login-Sperre	21, R-37
Login-Versuche	21
lokales Netzwerk	R-6

■ **M**

MAC	R-12
MAC-Adresse	R-12, R-29, R-38
MAC-Protokoll	R-12
Medium	R-4
Medium Access Control	R-12
Mehrpunkt-Verkabelungen	R-12
Multiprotokollfähigkeit	R-12

■ **N**

Name	R-28
Name-Server	R-32
NBNS	R-32
NBNS-Backup	R-32
NBNS-Server	22, 25
NetBIOS Name Server	R-32
Netzmaske	R-7
Netzteil	7
Netzwerk	R-4
Netzwerkadresse	R-7
Netzwerkanschlusses	R-29
Netzwerkkabel	R-4
Netzwerkkarte	R-4
Netzwerkprotokoll	R-6
Node-ID	R-29

■ **O**

Online-Medien	13
---------------------	----

■ **P**

Pakete	R-4
Paketgröße	20
Passw.Zwang	R-37
Paßwort	20, R-31
Paßwortschutz	21
PC-Karte	7
Peer-to-LAN-Netzwerk	3
Peer-to-Peer-Netzwerk	2
physikalisches Medium	R-4
Private Address Spaces	R-8
Protokoll	R-6

Pufferspeicher R-29, R-38
 Punkt-zu-Mehrpunkt-Verbindung R-5
 Punkt-zu-Punkt-Verbindung R-4

R

registrierte IP-Adresse R-8
 Reichweite 3, 5
 reservierte Adressbereiche R-9
 Reset-Taster 9
 Router R-4
 Routing R-9
 Routingtabelle R-9

S

Schnittstelle R-4
 Setup
 LAN-Modul R-29
 SNMP-Modul R-34
 TCP-IP-Modul R-30
 Shared Medium R-6, R-12
 Sicherheit 21
 Skalierung 3
 SNMP 18, R-33
 Software einspielen 16
 Software-Update 5
 Sonstiges R-40
 Sperre 22
 Sperr-Minuten R-37
 Sprache R-37
 Standort R-29, R-33
 Start-Adresse 24
 Start-Adreß-Pool R-34
 Status R-19
 Betriebszeit R-19
 Config-Statistik R-26
 LAN-Statistik R-21
 Ruf-Info-Tabelle R-27
 TCP-IP-Statistik R-22
 WAN-Statistik R-20
 Werte-löschen R-28

Statusanzeigen 5
 Störungen 5
 System-Boot R-40
 System-Reset R-40
 System-Upload R-41

T

TCP/IP 10, 13, R-6
 TCP/IP-Stack R-6
 TCP-Aging-Min R-33
 TCP-Max.-Verb. R-33
 Technische Daten 31
 Teilnetz R-9
 Telnet 5, 12
 Telnet-Server R-31
 TFTP 13
 TFTP-Server R-31
 Timeout R-36
 Trap-IP R-33
 Traps-senden R-33

U

Upload 6, 16

V

Versions-Tabelle R-39

W

WAN-Config R-37
 winipcfg 11
 Wireless LAN 1
 WLAN 1, 19
 WLAN-Domain 20

Z

Zeit R-19
 Zellen R-4
 Zugangskontrolle 22
 Zugangsliste R-31
 Zustand R-30

Technische Grundlagen

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

Funk-Netzwerke nach dem IEEE-802.11-Standard

Die Geräte der *ELSA LANCOM Wireless*-Reihe arbeiten nach dem Standard IEEE 802.11. Dieser Standard stellt eine Erweiterung der bereits vorhandenen IEEE-Normen für LANs dar, von denen IEEE 802.3 für Ethernet der bekannteste ist. In der Tat lassen sich nach 802.11 arbeitende Funknetze sehr leicht mit vorhandenen Ethernet-Netzen verbinden, und dies ist die wichtigste Funktion der *ELSA LANCOM Wireless*-Geräte. Nach 802.11 arbeitende Funkkarten stellen sich bis auf ein paar Zusatzparameter einem Rechner wie eine normale Ethernet-Karte dar. Dies heißt, daß Sie über ein 802.11-Funknetz alle Protokolle fahren können wie über ein kabelgebundenes Ethernet auch (IP, IPX, NetBIOS, ...). Der einzige Unterschied ist, daß Sie keine Kabel zwischen den Rechnern verlegen müssen!

Da der IEEE-Standard sich nur mit der Definition von LANs befaßt, ist die Reichweite von Funk-LAN-Systemen beschränkt; übliche Reichweiten liegen bei unter 300 Metern bei direkter Sicht, mit Gebäudewänden im allgemeinen deutlich darunter. Die Menge aller Funk-LAN-Stationen, die sich gegenseitig direkt erreichen können, bezeichnet man allgemein als Funkzelle.

Ad-hoc-Modus

Der IEEE-Standard bietet zwei Betriebsformen, die sich in der Sicherheit und der Reichweite eines so aufgebauten Funknetzes unterscheiden.

Ein Funk-LAN im Ad-hoc-Modus besteht aus einer einzelnen abgeschlossenen Funkzelle, die aus Ethernet-Sicht abgeschlossen ist, d.h., eine Verbindung nach außen ist lediglich über das Routing höherwertiger Protokolle möglich; ein Beispiel für ein solches Element wäre ein *ELSA LANCOM Wireless IL-2*, das über seinen ISDN-Port allen anderen Stationen als Internet-Access-Router dient. Ad-hoc-Netze entstehen meist spontan, wenn sich eine Arbeitsgruppe mit ihren Rechnern zusammenfindet und diese zum Datenaustausch vernetzen möchte. Rechner können zu einem solchen Netz beliebig hinzukommen und es wieder verlassen; es gibt keinen ausgezeichneten Knotenpunkt, der immer vorhanden sein muß. Eine spezielle Authentifizierung zur Teilnahme ist nicht erforderlich und auch nicht möglich, weil die zentrale Station zur Überwachung fehlt.

Was passiert aber, wenn eine Arbeitsgruppe im Nachbarbüro auf die gleiche Idee kommt und auch ein Netz aufbaut? Während man bei einem normalen Ethernet einfach zwei

Kabelstränge hat, die nicht miteinander verbunden sind, kann man Funkwellen nicht so einfach einsperren und die beiden Netzwerke würden sich gegenseitig stören. Damit das nicht passiert, gibt es in jedem IEEE-Funk-LAN einen Parameter, den Namen einer WLAN-Domain. Aus Sicht des Anwenders ist die WLAN-Domain eine beliebig wählbare Zeichenkette mit maximal 32 Zeichen. Auf Funkebene verwandelt sich dieser Name in eine zusätzliche Adressierungskomponente, so daß sich ein Datenpaket immer einer bestimmten Funkzelle zuordnen läßt. Wollen Sie in ein bestehendes Funknetz einsteigen, benötigen Sie den Namen seiner WLAN-Domain, den Sie in den erweiterten Einstellungen des Treibers für die Netzwerkkarte eintragen. Der Treiber sucht beim Start nach einem bestehenden Funknetz mit dieser Kennung. Findet er eines, klinkt er sich in dieses ein, und Sie können mit den Rechnern in diesem Funknetz kommunizieren. Findet er nichts, so spannt er eine neue Funkzelle auf.

Auch wenn auf diese Weise Funkzellen voneinander logisch getrennt werden können, so behindern sie sich immer noch physikalisch, weil ja immer nur eine Station senden kann, d.h., keine der Funkzellen würde im Überlappungsfalle die volle Bandbreite erreichen. Das können Sie verhindern, indem Sie den einzelnen Netzen nicht nur verschiedene Domain-Namen, sondern auch verschiedene Funkkanäle zuordnen: So wie zwei Funkgeräte gleichzeitig auf verschiedenen Frequenzen senden können, können zwei Funk-LANs gleichzeitig auf verschiedenen Kanälen arbeiten, ohne sich gegenseitig zu stören. Wenn zwei Funkzellen sehr nah beieinander sind, sollten die Kanäle dieser Netze 4–5 Kanäle auseinanderliegen, da eine Funkzelle die benachbarten Kanäle teilweise mit belegt.



Nicht alle vom IEEE-Standard vorgesehenen Funkkanäle sind in allen Ländern erlaubt!

Infrastrukturmodus

Die eigentliche Stärke von auf IEEE 802.11 basierenden Funknetzen ist aber die einfache Koppelbarkeit mit bestehender (Ethernet-)Vernetzung. Ein Funknetz kann genutzt werden, um mobile Station mit an ein bestendes, verkabeltes Netz anzubinden, andererseits kann ein bestehendes Netz dazu benutzt werden, mehrere Funkzellen miteinander zu koppeln, die Reichweite eines Funknetzes also zu erweitern. Dazu müssen alle Teilnehmer in einem anderen Modus betrieben werden, dem Infrastrukturmodus.

Im Infrastrukturmodus existiert neben den beweglichen Stationen ein zusätzliches Element, eine Basis-Station, die auch als Access-Point oder Distribution-System bezeichnet wird. Die *ELSA LANCOM Wireless*-Geräte wurden dazu entwickelt, die Funktion einer Basis-Station zu übernehmen. Im Infrastrukturmodus übernimmt die Basis-Station die Funktion eines „Wächters“: Domain-Name und Funkkanal sind weiterhin vorhanden, und eine Station, die neu ins Netz kommt, sucht auch weiterhin nach einer vorhandenen Funkzelle. Im Gegensatz zum Ad-hoc-Modus wird die Funkzelle jedoch immer von der Basis-Station aufgespannt, und jede Station muß sich bei der Basis-Station anmelden, bevor sie Daten in der Funkzelle austauschen darf. Der Basis-Station kommt dabei üblicherweise auch die Funktion einer 'Relaisstation' für Daten zu. Dies reduziert zwar die erreichbare Datenrate, kann bei geschickter Aufstellung der Basis-Station aber die Größe

einer Funkzelle erhöhen. Die eigentliche Aufgabe der Basis-Station ist aber die Verbindung der Funkzelle mit einem kabelgebundenen Ethernet: Erhält die Basis-Station ein Datenpaket für einen Rechner, der sich nicht bei ihr angemeldet hat, so leitet sie das Paket in das Ethernet weiter. Umgekehrt „lauscht“ sie auch ständig am Ethernet, ob Daten anliegen, die an eine bei ihr angemeldete Station gerichtet sind und leitet diese in die Funkzelle weiter. Da eine Basis-Station durch den Anmeldungszwang jederzeit genau weiß, welche Stationen sich auf ihrer Funkseite befinden, kann sie exakt entscheiden, welche Daten durchgereicht werden müssen und welche nicht. Diesen Vorgang bezeichnet man auch als Bridging.

Wie bereits erwähnt, kann ein Ethernet-Backbone auch dazu genutzt werden, die Reichweite eines Funk-LANs zu vergrößern: Dazu schließt man mehrere Basis-Stationen an einen gemeinsamen Strang an und konfiguriert diese in diesem Sonderfall alle auf die gleiche WLAN-Domain. Will eine Station ins Netz gehen, sucht sie sich unter allen erreichbaren Basis-Stationen die mit dem stärksten Signal und meldet sich bei dieser an; zwei an unterschiedlichen Basis-Stationen angemeldete Mobilstationen können so auch miteinander kommunizieren, wenn sie nicht in direkter Funkreichweite sind. Das Ethernet, über das alle Basis-Stationen verbunden sind, schließt die Lücke.

Wenn eine Station auch nach der Anmeldung kontinuierlich weiter die Funksituation überwacht, kann sie erkennen, wie die Signale von einer Basis-Station schwächer und von einer anderen stärker werden und sich für den Benutzer unmerklich ummelden. Diesen Vorgang bezeichnet man als Roaming.

Austauschbarkeit mit anderen Geräten

ELSA LANCOM Wireless-Geräte, die auf dem IEEE-802.11-Standard basieren, sind prinzipiell mit auf 802.11 basierenden Geräten anderer Hersteller interoperabel. Da der 802.11-Standard allerdings noch recht neu ist und viele Hersteller momentan erst von firmenspezifischen Funk-LAN-Lösungen auf 802.11 umstellen, kann eine Interoperabilität nicht prinzipiell garantiert werden. Die Austauschbarkeit findet spätestens beim verwendeten Modulationsverfahren ihr Ende: *ELSA LANCOM Wireless*-Geräte verwenden das sog. Direct-Sequenced-Spread-Spectrum(DSSS)-Verfahren, während andere Hersteller z.T. das Frequency-Hopping-Spread-Spectrum(FHSS)-Verfahren benutzen. Ein Datenaustausch zwischen den auf FHSS und DSS basierenden Geräten ist prinzipiell nicht möglich.

Netzwerktechnik



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

Das Netzwerk und seine Komponenten

*Netzwerk,
Übertragungs-
medium,
Schnittstellen*

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



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

*Pakete
Zellen*

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



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

Host

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

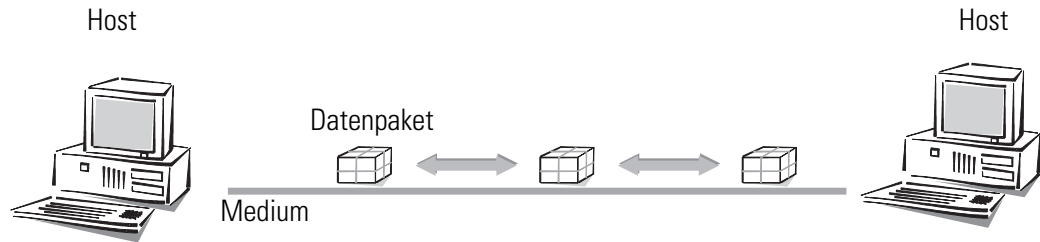
Router

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

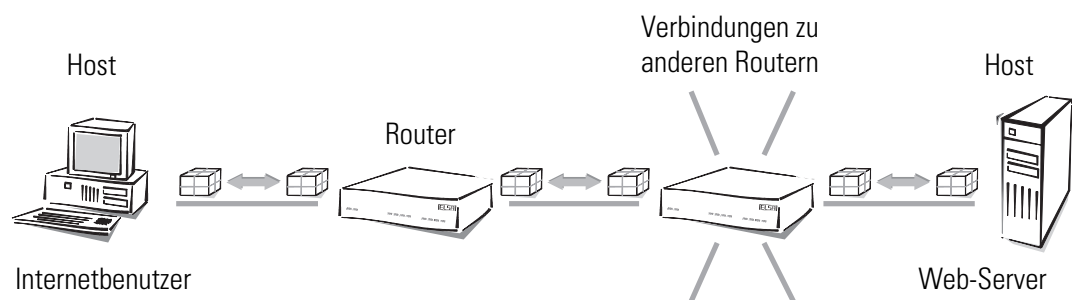
Verbindungsarten

*Punkt-zu-Punkt-
Verbindung*

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



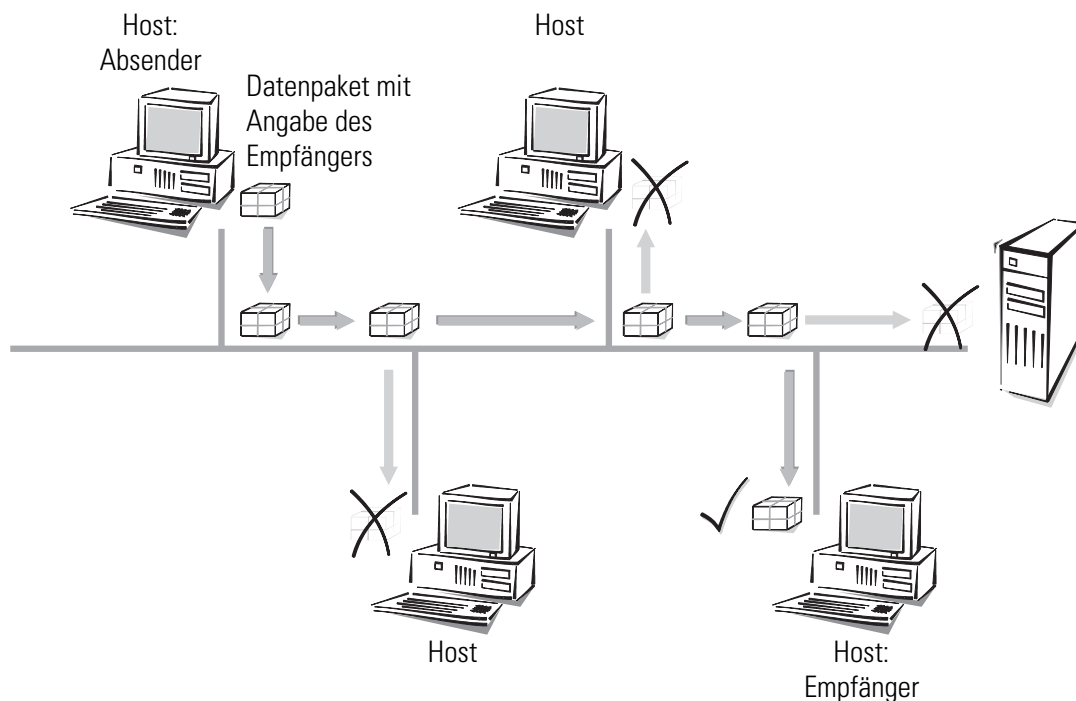
Auch bei einem Zugriff auf das Internet handelt es sich um eine Punkt-zu-Punkt-Verbindung. Die Datenpakete werden zwar vom Host beim Internetbenutzer über mehrere Router zum Host (Server) beim Internet-Provider gesendet, jedes Datenpaket hat jedoch ein ganz bestimmtes Ziel. Die Router geben die Datenpakete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



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

Punkt-zu-Mehrpunkt-Verbindung

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



Netzwerk-Arten

Protokoll

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

TCP/IP

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

IP-Netz

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

Internetwork Internet

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

Lokales Netz- werk (LAN)

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

IP-Adressierung

Paketorientierte Übertragung

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

IP-Adresse

In IP-Netzen werden IP-Adressen zur Kommunikation zwischen verschiedenen Geräten verwendet. Jeder Host hat dabei seine eigene Adresse, mit der er eindeutig identifiziert werden kann. Wie sieht nun eine IP-Adresse aus? Sie besteht aus vier Bytes, die durch Punkte getrennt sind, insgesamt also aus 32 Bits. Jedes der vier Bytes kann Werte von 0 bis 255 annehmen, z.B. 192.168.130.124.



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

Netzwerk-Adresse

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

Netzmaske

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

Beispiele:

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

Die gleiche IP-Adresse, jetzt mit einer anderen Netzmaske:

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

Sie sehen also: Eine IP-Adresse alleine ist noch nicht ausreichend. Nur im Zusammenspiel mit der Netzmaske kann ein Host eindeutig bezeichnet werden.

Und Sie sehen weiter: Je weniger Bits in der Netzmaske eine Eins enthalten, um so mehr Bits bleiben übrig zur Identifizierung der einzelnen Hosts in einem zusammenhängenden Netzwerk. Während im ersten Beispiel mit der Netzmaske 255.255.255.0 nur 254 verschiedene Adressen vergeben werden können sind es im zweiten Beispiel schon $254 \times 254 = 64.516$ verschiedene Adressen! Die erste und die letzte Ziffer eines Adreßraums sind jeweils reserviert für die Netzwerk-Adresse und die Broadcast-Adresse (Adresse für Pakete an alle Hosts in einem IP-Netz). Bei der Netzmaske 255.255.255.0 sind das die '0' für die Netzwerk-Adresse und die '255' als Broadcast-Adresse.

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

Verwaltung der IP-Adressen

Um Irrtümer zu vermeiden, müssen die IP-Adressen innerhalb eines zusammenhängenden Netzes eindeutig sein. Da auch das Internet mit vielen Millionen angeschlossener Rechner auf TCP/IP aufsetzt und damit IP-Adressen verwendet, müssen auch alle Adressen im Internet eindeutig sein. Zur Kontrolle dieser öffentlich zugänglichen Adressen gibt es Stellen, die die IP-Adressen verwalten und verteilen. Da die Anzahl der theoretisch verfügbaren IP-Adressen begrenzt ist, lassen sich die vergabeberechtigten Stellen die IP-Adressen teuer bezahlen.

Private Address Spaces

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

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

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

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

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

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

IP-Routing und hierarchische IP-Adressierung

Routing

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

Routingtabelle

Für das Routen verwaltet jeder Router eine Tabelle (Routingtabelle). Sie bezeichnet für jeden Host im Netz die Router-Schnittstelle, über die der Host am schnellsten zu erreichen ist. Es ist leicht vorstellbar, daß mit wachsender Netzgröße diese Tabellen die Kapazität der Router sprengen (das Internet als weltweiter Verbund von öffentlich erreichbaren IP-Rechnern enthält mehrere Millionen Hosts).

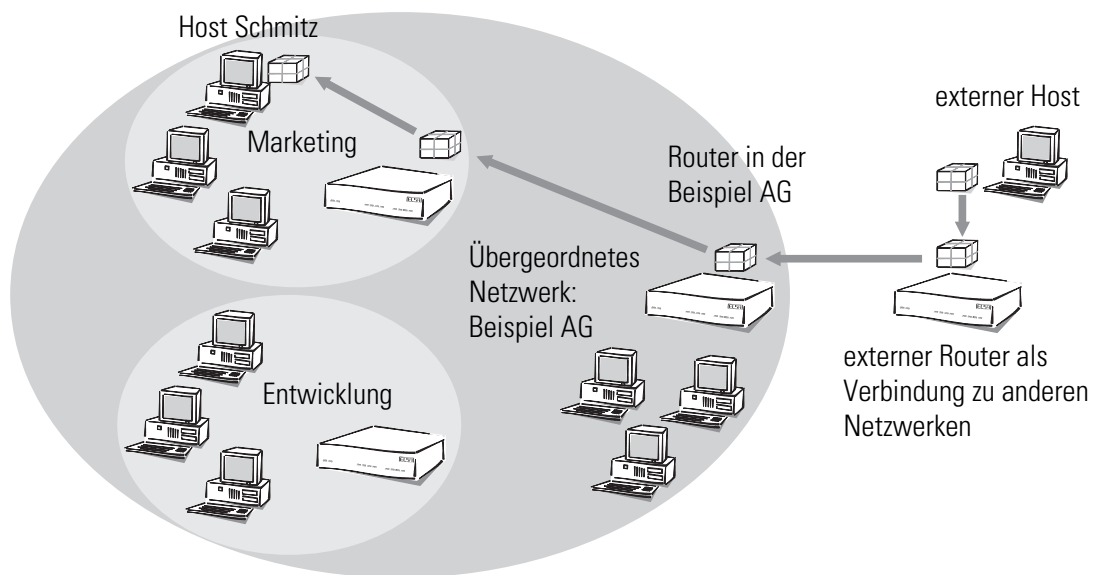
hierarchische IP-Adressen

Aus diesem Grunde wurden hierarchische IP-Adressen eingeführt. Dazu wird das IP-Netz in Teilnetze unterteilt, in denen IP-Adressen aus einem zusammenhängenden Nummernraum vergeben werden. Es sind mehrere Hierarchie-Ebenen möglich, so daß mehrere

Teilnetze zu größeren Teilnetzen zusammengefaßt werden können. Dies ist vergleichbar mit der hierarchischen Adresse bei der Briefpost, die aus Land, Stadt, Straße und Hausnummer besteht.

Die Konsequenzen dieser hierarchischen IP-Adressierung:

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



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

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

- ① Der Absender gibt dem Paket die Zieladresse „Host Schmitz – Marketing – Beispiel AG“.
- ② Ein externer Router, der die Verbindung zu anderen Netzen herstellt, muß nur wissen, wie er die Beispiel AG erreicht. Sobald er ein Paket mit der Adresse für die Beispiel AG empfängt, leitet er das Paket an den Router weiter, der für die Beispiel AG zuständig ist.
- ③ Der Router in der Beispiel AG empfängt das Paket und entnimmt der Adresse die Information, daß es für die Beispiel AG gedacht ist. Weil er selber Teil der Beispiel

AG ist, betrachtet er die Adresse genauer und sucht nach dem Namen der Abteilung. Dann leitet er das Paket weiter an den Router im Marketing.

- ④ Der Router im Marketing empfängt das Paket und entnimmt der Adresse die Information, daß es für das Marketing in der Beispiel AG gedacht ist. Weil er selber Teil dieser Abteilung ist, betrachtet er die Adresse genauer und sucht nach dem Namen des Hosts. Dann leitet er das Paket weiter an den Host von Mitarbeiter Schmitz.

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

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

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

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

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

Erweiterung durch lokale Netze

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

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

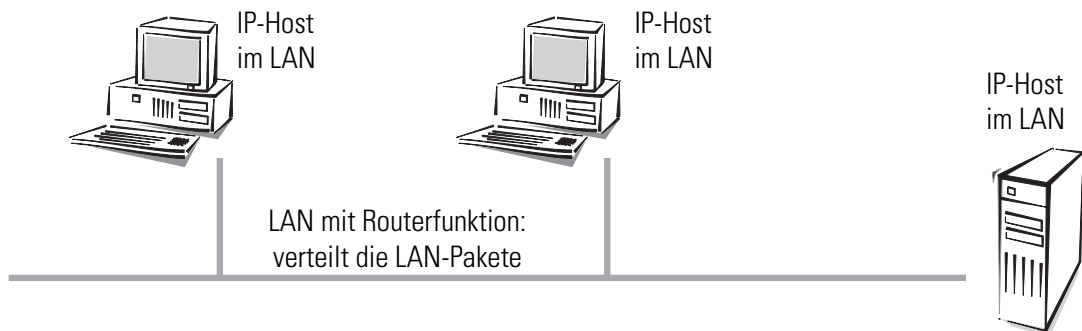
MAC-Adresse Zur Organisation der Übertragung im LAN werden spezifische LAN-Adressen verwendet, die vom Hersteller der Schnittstellenhardware fest einprogrammiert werden. Da die LAN-Adressen für die Kommunikation über das MAC-Protokoll verwendet werden, heißen Sie auch MAC-Adressen. Man kann sie sich wie einen Fingerabdruck der Schnittstellenhardware vorstellen. MAC-Adressen sehen z.B. so aus: 00-80-C7-6D-A4-6E.

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

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

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

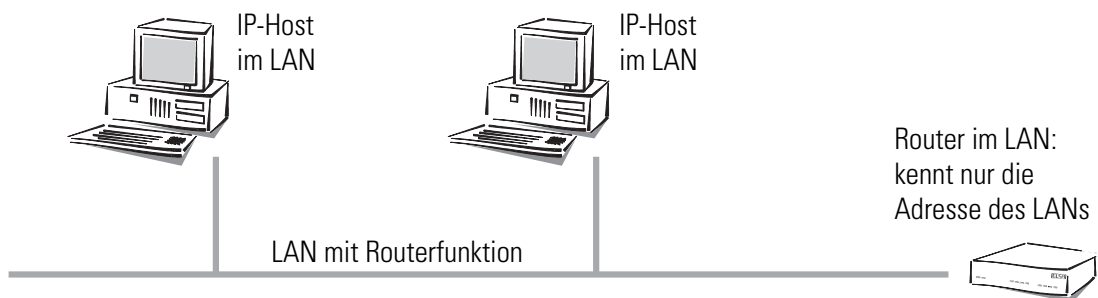
Für einen IP-Host verhält sich ein LAN so, also ob es ein eigenes Netzwerk mit einem Router wäre. Die Hosts geben die Pakete an das LAN ab, das die weitere Verteilung der Datenpakete übernimmt. Für die Kommunikation der Hosts untereinander über das IP-Protokoll dürfen in einem LAN somit nur IP-Adressen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



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

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

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



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

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

Datenübertragung im eigenen LAN

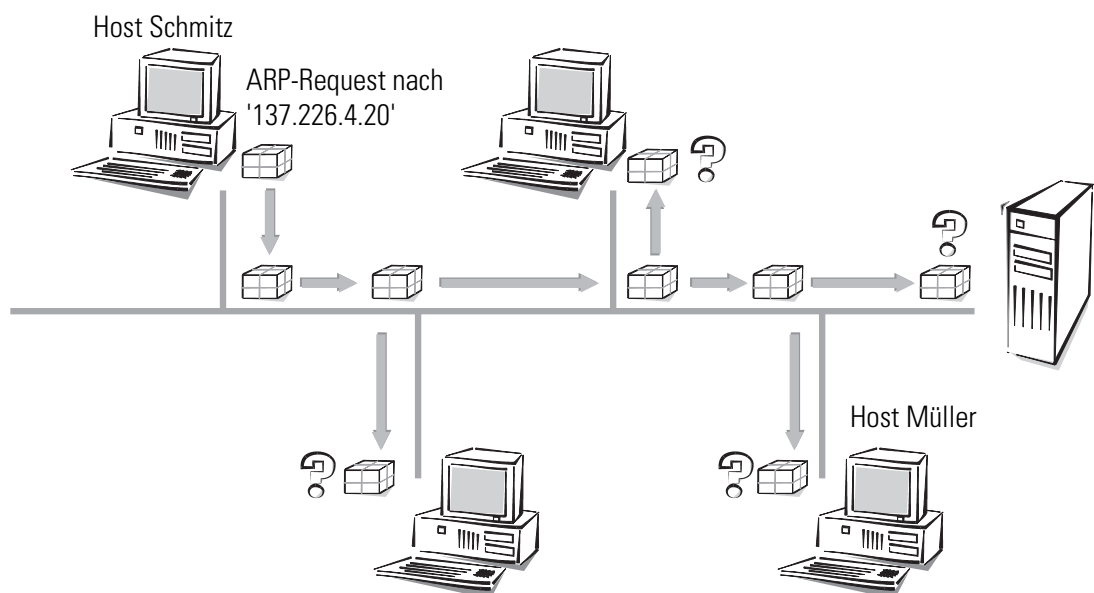
Veranschaulichen wir uns das an einem Beispiel. Stellen wir uns vor, daß die Hosts des Teilnetzes im Marketing über ein LAN verkabelt sind. Die Hosts haben IP-Adressen aus dem Nummernraum '137.226.4.1' bis '137.226.4.254' (die Adressen '137.226.4.0' und '137.226.4.255' sind reserviert), die Netzwerk-Adresse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

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

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

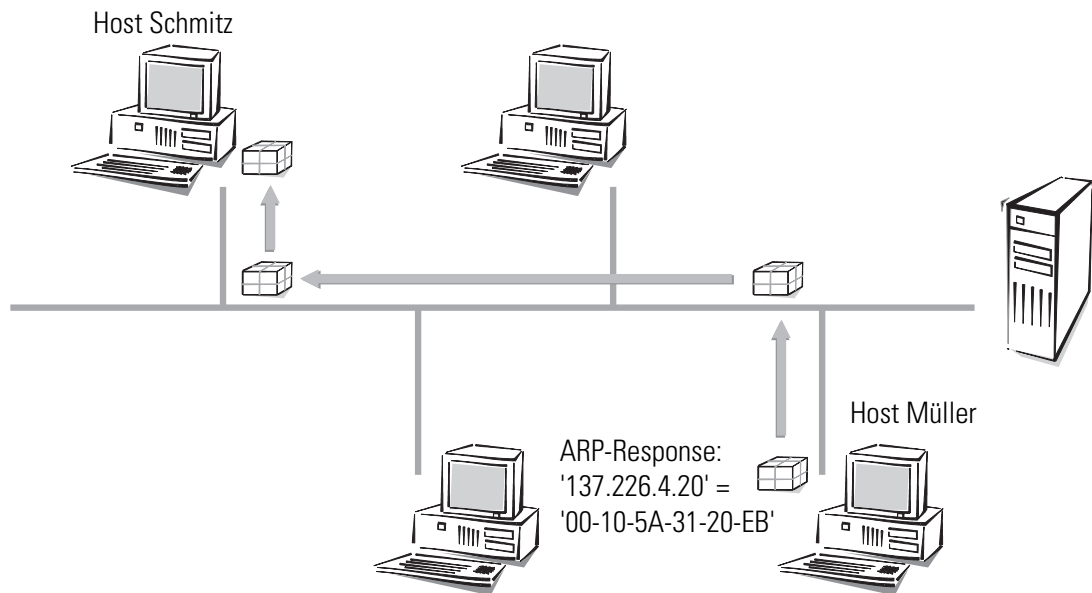
ARP

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



Dieses ARP-Request-Paket ist nichts anderes als die Frage an alle, wer denn auf die IP-Adresse '137.226.4.20' hört. Host Müller empfängt das Paket, fühlt sich angesprochen

und antwortet mit einem ARP-Response-Paket, das er direkt an Host Schmitz verschickt. Die MAC-Adresse '00-10-5A-31-20-DF' von Host Schmitz entnimmt er dem Absenderfeld im ARP-Request-Paket. Host Schmitz erkennt dies als Antwort auf seine Anfrage, entnimmt dem Absenderfeld des ARP-Response-Paketes die MAC-Adresse '00-10-5A-31-20-EB' von Host Müller und trägt sie in seine ARP-Tabelle ein.



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

Datenübertragung aus dem eigenen LAN ins Internet

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

LAN-Kopplung auf MAC-Basis

Sie wissen, daß LANs das Anschließen von Rechnern an ein lokales Netz stark vereinfachen. Daher basieren fast alle Hausnetze auf LANs. Es gibt Situationen, wo einzelne

LANs räumlich so weit ausgedehnt sind, daß die physikalischen Eigenschaften des Kabels den Anschluß weiterer Rechner behindern. Daraus ergibt sich der Bedarf, mehrere LANs so miteinander zu koppeln, daß sie elektrisch und bezüglich des MAC-Protokolls wie getrennte LANs agieren, aber gegenüber dem IP-Protokoll wie ein einziges großes LAN erscheinen.

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

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

Beschreibung der Menüpunkte

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

Zur leichteren 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.



Alle kanalbezogenen Statistiken und Menüs sind in dieser Beschreibung nur mit zwei Kanälen aufgeführt, obwohl die Geräte möglicherweise mehr als zwei Kanäle bereitstellen. Ebenso sind interfacebezogene Angaben nur für ein Interface aufgeführt. Die entsprechenden Informationen gelten für die weiteren Kanäle und Interfaces sinngemäß.

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



LAN-Modul



TCP-IP-Modul



SNMP-Modul



DHCP-Modul



Config-Modul



WLAN-Modul



Firmware



Versions-Tabelle



Tabelle-Firmsafe



Modus-Firmsafe



Timeout-Firmsafe



Firmware-Upload



Test-Firmware



Status



Aktuelle-Zeit



Betriebszeit



WLAN-Statistik



LAN-Statistik



TCP-IP-Statistik



Config-Statistik



Queue-Statistik



PCMCIA-Status



Werte löschen



Sonstiges



Manuelle Wahl



System-Reset



System-Boot











System-Upload

Status

Das Menü 'Status' enthält Informationen zum aktuellen Status und über interne Abläufe im LAN und im WAN, die sich auf die Datenübertragungsstrecke (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
Aktuelle-Zeit		Aktuelle Zeit im Gerät
Betriebszeit		Betriebszeit des Gerätes seit dem letzten Einschalten
LAN-Statistik		Statistiken des Netzwerk-Bereichs
WLAN-Statistik		Statistiken des Funk-Netzwerk-Bereichs
Config-Statistik		Statistiken der Remote-Konfiguration
TCP-IP-Statistik		Statistiken aus dem TCP/IP-Bereich
Queue-Statistik		Statistiken über die Pakete in den Queues der einzelnen Module
Werte löschen		Alle Werte außer Tabellen der untergeordnet. Statistik löschen

Status/Aktuelle-Zeit





















Hier wird die aktuelle Zeit des Gerätes angezeigt, die z.B. für die Least-Cost-Router-Berechnungen oder einige Statistiken verwendet wird. Diese Zeit kann entweder aus dem ISDN-Netz abgelesen werden (ISDN-Zeit, siehe auch Setup/Zeit-Modul) oder 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/WLAN-Statistik

Hier wird der momentane Status des WLAN-Interfaces beschrieben.

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 (Bridge/Router)
LAN-Queue-Pakete		Anzahl belegter Puffer
LAN-Queue-Fehler		Anzahl durch Puffermangel verworfener Pakete
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
LAN-Tx-Broadcasts		Anzahl vom WLAN empfangener Broadcasts
LAN-Tx-Multicasts		Anzahl vom WLAN empfangener Multicasts
LAN-Tx-Unicasts		Anzahl vom WLAN empfangener Unicasts
LAN-Wiederholungen		Anzahl der Pakete, die erst nach einer Wiederholung zugestellt werden konnten
LAN-Mehrfachwiederholungen		Anzahl der Pakete, die erst nach mehreren Wiederholungen zugestellt werden konnten
BSSID		Zahlenwert zur Unterscheidung von Funkzellen, numerische Umsetzung der WLAN-Domain. Im Infrastrukturmodus immer gleich der MAC-Adresse der Basis-Station
PHY-Kanal		Der vom Basisport momentan benutzte Funkkanal.
LAN-bereit		Erfolgreich Initialisierung der Funk-Netzwerkkarte
Stationstabelle		Anzeige der momentan angemeldeten Mobil-Stationen.











Stationstabelle Diese Tabelle zeigt Informationen zu den einzelnen Mobilstationen:









Alter	Alter der Station: Zeit seit dem letzten übertragenen Datenpaket
Phy-Signal	durchschnittliche Signalstärke der von dieser Station empfangenen Datenpakete
Node-ID	Adresse der Station. Je nach Wissensstand eine MAC-Adresse, IP-Adresse oder ein symbolischer Name, wenn diese Station DHCP benutzt.

LAN-tx-bytes und LAN-rx-bytes	bisher von bzw. zu dieser Station übertragene Datenmenge
Status	kann entweder 'None', 'Auth' oder 'Assoc' sein. Beim Einbuchen authentifiziert sich eine Station zuerst, dann „assoziiert“ sie sich, d.h. meldet sich für Datenverkehr an. Erst im Status 'Assoc' läßt der Basisport Daten durch! 'Auth' zeigt an, ob die Station auf eine Authentifizierung seitens des Basisports antwortet.
Encaps	Ethernet-Frames können im WLAN auf verschiedene Weisen in einen WLAN-Frame verpackt werden. Bei der Methode 'IEEE' wird dem kompletten Ethernet-Paket ein neuer Header vorangestellt. Eine andere Methode verwendet ein intelligenteres Verfahren, bei dem die Header ineinander umgesetzt werden und 'LLC-SNAP'-Kodierungen zur Kennzeichnung des Protokolls benutzt werden. Der Basisport erkennt beide Kodierungen automatisch. Wer wählen kann, sollte die SNAP-Kodierung benutzen, da hier der Overhead pro Frame 6 Byte kleiner ist.

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 (Bridge/Router)
LAN-NIC-Fehler		Anzahl vom NIC verworfener Datenpakete
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		Der LAN-Anschluß ist fest auf 10Base-T voreingestellt. Siehe Setup/LAN-/Anschluss.
LAN-Rx-Bytes		Anzahl vom LAN empfangener Zeichen

/LAN-Statistik		Fortlaufende Statusanzeigen
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/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
TCP-Statistik		Statistiken für TCP-Pakete von TCP-Sitzungen zum Router
TFTP-Statistik		Statistiken für TFTP-Operationen
DHCP-Statistik		Statistiken aus dem DHCP-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
Werte löschen	ARP-Statistiken löschen
Tabelle-ARP	Anzeige der ARP-Tabelle

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-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
DHCP-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
Werte löschen	DHCP-Statistik löschen












Tabelle-DHCP

In der **DHCP-Tabelle** finden Sie Einträge mit DHCP-Informationen. Sie enthält 16 (oder das 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/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/Queue-Statistik




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

/Queue-Statistik	Statistiken über die Queue	
LAN-Heap-Pakete		Anzahl verfügbarer Puffer
LAN-Queue-Pakete		Anzahl belegter Puffer
WAN-Heap-Pakete		Anzahl verfügbarer Puffer

/Queue-Statistik		Statistiken über die Queue
WAN-Queue-Pakete		Anzahl belegter Puffer
Bridge-interne Queue-Pakete		Anzahl der Bridge-Pakete aus dem LAN
Bridge-externe Queue-Pakete		Anzahl der Bridge-Pakete aus dem WAN
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
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/PCMCIA-Status

Hier finden sich einige allgemeine Informationen zur eingesteckten Karte:

LAN-Karte vorhanden		Karte eingesteckt oder nicht (das heißt nicht, daß sie funktioniert, sondern nur, daß etwas in dem PCMCIA-Slot steckt!)
Karten-ID		Der aus dem PCMCIA-Config-Space ausgelesene Kartename, also der Gerätenamen, für den Windows beim erstmaligen Einstecken einen Treiber anfordert.
Firmwareversion		Sofern die Karte korrekt initialisiert wurde, Informationen über die Firmware in der WLAN-Karte.








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
LAN-Modul		Einstellungen für das LAN
TCP-IP-Modul		Einstellungen für das TCP/IP-Modul
SNMP-Modul		Einstellungen für die Konfiguration über SNMP
DHCP-Modul		Einstellungen für den DHCP-Server
WLAN-Modul		Einstellungen für das Funknetzwerk
Config-Modul		Einstellungen für das Konfigurationsmodul

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 IPX- und IP-Router-Module, da die Router nur mit bekannten Gegenstellen Daten austauschen, sowie für die eindeutige Identifizierung einer Bridge-Gegenstelle.




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.

Da der Router in der Namenliste für den Gerätenamen nur Großbuchstaben zuläßt, wird bei einer Überprüfung durch das ELSA-Protokoll, der Name in Großbuchstaben übertragen. Sonderzeichen sollten im Gerätenamen nur verwendet werden, wenn die Gegenstelle diese verarbeiten kann.

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/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 der folgende Netzwerkanschluß ausgewählt werden:

Anschluß	Bedeutung
Auto	Standardeinstellung, da der Netzwerkanschluß fest auf 10Base-T eingestellt ist. Dieser Punkt muß nicht manuell konfiguriert werden.



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.

Intranet-Adresse Hier kann eine zweite IP-Adresse für das den Router eingegeben werden. Mit dieser zweiten IP-Adresse kann das Gerät 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 IP-Adresse) versteckt.

Intranet-Maske Hier muß die zur IP-Adresse des lokalen Netzes 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 Auswahl der IP-Adresse XXX.XXX.XXX.254 zu erreichen.

Existiert im Netz bereits eine solche IP-Adresse, muß über die Tastatur (nur ELSA LANCOM Wireless IL-2) bzw. 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 aus 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/SNMP-Modul

Über dieses Menü können Einstellungen zur Konfiguration des Geräts 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 den 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.

<i>Netzmaske</i>	<p>Die Zuweisung der Netzmaske erfolgt analog zur Adreßzuweisung:</p> <p>Entweder wird die im DHCP-Modul eingetragene Netzmaske zugewiesen, oder es wird die zum (bei der Adreßzuweisung bestimmten) lokalen Netz gehörende Netzmaske verwendet.</p>
<i>Broadcast</i>	<p>Die Zuweisung der Broadcast-Adresse erfolgt analog zur Adreßzuweisung:</p> <p>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.</p>
<i>Max.-Gültigkeit-Minute(n)</i>	<p>Hier kann die maximale Gültigkeitsdauer eingetragen werden, die der DHCP-Server einem Host zuweist.</p> <p>Der DEFAULT-Wert von 6000 Minuten entspricht ca. 4 Tagen.</p>
<i>Default-Gültigkeit-Minute(n)</i>	<p>Hier kann die Gültigkeitsdauer eingetragen werden, die zugewiesen wird, wenn der Host überhaupt keine Gültigkeitsdauer anfordert.</p> <p>Der DEFAULT-Wert von 500 Minuten entspricht ca. 8 Stunden.</p>

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/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
Fernconfig-(EAZ-MSN)		Rufnummer für die Fernkonfiguration über PPP
Conf.-Haltezeit		Zeitbeschränkung für Remote-Konfigurationsverbindungen

/Config-Modul	Einstellungen für das Konfigurationsmodul	
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 **Aus** aktiviert.

Fernconfig-(EAS-MSN) Diese Rufnummer erlaubt die Fernkonfiguration über PPP. Solange keine Nummer eingetragen ist, werden Rufe auf beliebige Nummern für die Fernkonfiguration angenommen.

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 15 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/WLAN-Modul

In diesem Menü wird der WLAN-Teil konfiguriert:

WLAN-Domaene		Hier wird die die WLAN-Domain eingetragen, d.h. der symbolische Name, mit dem Mobilstationen den Basisport finden. Ein ASCII-String mit maximal 32 Zeichen. Default ist 'ELSA'.
PHY-Kanal		Der Funkkanal, auf dem der Basisport arbeiten soll. Mögliche Werte sind 1 bis 14, die Kanäle überlappen sich aber durch das Spread-Spectrum-Verfahren, so daß sich im gesamten Funkband maximal 3 vollständig unabhängige Funkkanäle aufspannen lassen. <i>Nicht in jedem Land sind alle Kanäle erlaubt (siehe auch Tabelle mit Funkkanälen im Anhang).</i>
Paketgroesse		Ein Wert zwischen 600 und 1600, der die maximale Größe von Paketen im WLAN in Bytes angibt. Default 1550.
Zugangs-Liste		Mit dieser Liste lassen sich Stationen in WLAN explizit vom Datenverkehr mit dem LAN/Basisport ausschließen bzw. es können die Stationen definiert werden, denen Verkehr erlaubt sein soll. In die Liste sind die MAC-Adressen von Stationen einzutragen, also die auf den Karten aufgedruckten 12-stelligen Hexadezimalzahlen, allerdings ohne die Trennzeichen, aus 00-60-B3-1F-02-11 wird also z.B. 0060B31F0211. <i>Hiermit wird nur Stationen der Zugriff zum LAN bzw. WAN verwehrt, der Datentransport zwischen Stationen im WLAN, bei dem der Basisport typischerweise Relais spielt, ist davon unbeeinflusst!</i>
Zugriffsmodus		Der Positiv/Negativ-Schalter bestimmt, ob es eine Ausschußliste oder Positivliste ist. Defaultmäßig steht der Modus auf Negativ und die Zugangs-Liste ist leer, d.h. keiner Station wird Datenverkehr verwehrt.
Protokoll-Liste		Diese Liste erlaubt es, Datenpakete nach dem verwendeten Protokoll zu sperren oder freizugeben (das richtet sich wiederum nach dem Positiv/Negativ-Schalter). Jeder Ethernet-Frame beinhaltet eine 16-bit-Kennung, in welchem Layer3-Protokoll er Daten überträgt. Diese können in die Liste als Hexadezimalzahlen eingetragen werden. Gängige Protokollkennungen sind z.B.: 0800 = IP 0806 = IP/ARP 8137 = IPX F0F0, E0E0 = IPX <i>Wiederum wird hier nur der Zugang von Stationen im WLAN zum LAN bzw. WAN gesperrt, nicht jedoch der Traffic zwischen WLAN-Stationen. Siehe Protokoll-Tabelle im Anhang</i>
Protokollmodus		Positiv/Negativ-Schalter für die Protokoll-Liste
Node-ID		MAC-Layer-Adresse des Geräts
Heap-Reserve		Pufferspeicher für die Aufnahme von Datenpaketen aus dem lokalen Netzwerk

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 Wireless	1.60.0012 / 30.06.1999	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 Zustandes (aktiv oder inaktiv), die Versionsnummer, das Datum, die Größe und den Index (fortlaufende Nummer).

Position	Status	Version	Datum	Groe	Index
1	inaktiv	1.60	23061999	690	6
2	aktiv	1.60	30061999	692	7
3	<Lader>	1.60	07061999	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). 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 bestimmten (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
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 (ISDN 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 '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.

Protokolle

Dienst	Port-Nr.	Protokoll
echo	7	tcp
echo	7	udp
discard	9	tcp
discard	9	udp
systat	11	tcp
systat	11	tcp
daytime	13	tcp
daytime	13	udp
netstat	15	tcp
qotd	17	tcp
qotd	17	udp
chargen	19	tcp
chargen	19	udp
ftp-data	20	tcp
ftp	21	tcp
telnet	23	tcp
smtp	25	tcp
time	37	tcp
time	37	udp
rlp	39	udp
name	42	tcp
name	42	udp
whois	43	tcp
domain	53	tcp
domain	53	udp
nameserver	53	tcp
nameserver	53	udp
mtp	57	tcp
bootp	67	udp
tftp	69	udp
rje	77	tcp
finger	79	tcp
www	80	tcp

Dienst	Port-Nr.	Protokoll
www	80	udp
link	87	tcp
supdup	95	tcp
hostnames	101	tcp
iso-tsap	102	tcp
dictionary	103	tcp
x400	103	tcp
x400-snd	104	tcp
csnet-ns	105	tcp
pop	109	tcp
pop2	109	tcp
pop3	110	tcp
portmap	111	tcp
portmap	111	udp
sunrpc	111	tcp
sunrpc	111	udp
auth	113	tcp
sftp	115	tcp
path	117	tcp
uucp-path	117	tcp
nntp	119	tcp
ntp	123	udp
nbname	137	udp
nbdagaram	138	udp
nbssession	139	tcp
NeWS	144	tcp
sgmp	153	udp
tcprepo	158	tcp
snmp	161	udp
snmp-trap	162	udp
print-srv	170	tcp
vmnet	175	tcp
load	315	udp
vmnet0	400	tcp

Dienst	Port-Nr.	Protokoll
sytek	500	udp
biff	512	udp
exec	512	tcp
login	513	tcp
who	513	udp
shell	514	tcp
syslog	514	udp
printer	515	tcp
talk	517	udp
ntalk	518	udp
efs	520	tcp
route	520	udp
timed	525	udp
tempo	526	tcp
courier	530	tcp
conference	531	tcp
rxd-control	531	udp
netnews	532	tcp
netwall	533	udp
uucp	540	tcp
klogin	543	tcp
kshell	544	tcp
new-rwho	550	udp
remotefs	556	tcp
rmonitor	560	udp
monitor	561	udp
garcon	600	tcp
maitrd	601	tcp
busboy	602	tcp
acctmaster	700	udp
acctslave	701	udp
acct	702	udp
acctlogin	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctslave2	706	udp

Dienst	Port-Nr.	Protokoll
acctdisk	707	udp
kerberos	750	tcp
kerberos	750	udp
kerberos_master	751	tcp
kerberos_master	751	udp
passwd_server	752	udp
userreg_server	753	udp
krb_prop	754	tcp
erlogin	888	tcp
kpop	1109	tcp
phone	1167	udp
ingreslock	1524	tcp
maze	1666	udp
nfs	2049	udp
knetd	2053	tcp
eklogin	2105	tcp
rmt	5555	tcp
mtb	5556	tcp
man	9535	tcp
w	9536	tcp
mantst	9537	tcp
bnews	10000	tcp
rscs0	10000	udp
queue	10001	tcp
rscs1	10001	udp
poker	10002	tcp
rscs2	10002	udp
gateway	10003	tcp
rscs3	10003	udp
remp	10004	tcp
rscs4	10004	udp
rscs5	10005	udp
rscs6	10006	udp
rscs7	10007	udp
rscs8	10008	udp
rscs9	10009	udp
rscsa	10010	udp

Dienst	Port-Nr.	Protokoll
rscsb	10011	udp
qmaster	10012	tcp
qmaster	10012	udp

