ELSA LANCOM™ Wireless IL-2

Handbuch

ELSA AG

Sonnenweg 11

52070 Aachen

Deutschland

www.elsa.de

Aachen, Oktober 1999

Art.-Nr. 20943/1099

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 IL-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\ELSASIDE\index.htm.

Inhalt

Deutsch

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, Datenaustausch mit mobilen Endgeräten sind nur einige der Anwendungsmöglichkeiten im Funk-LAN.

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

Über den eingebauten IP-Router und die ISDN-Schnittstelle verbinden Sie Ihr gesamtes LAN mit der Außenwelt. Der Zugriff auf das Internet für das ganze LAN oder Office-Funktionen wie Fax und Anrufbeantworter an allen Arbeitsplätzen sind nur einige der Vorteile, die Ihnen der ISDN-Router bietet.

In einigen europäischen Ländern ist die Nutzung von Funktfrequenzen 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-Netzwerkkarten WLAN

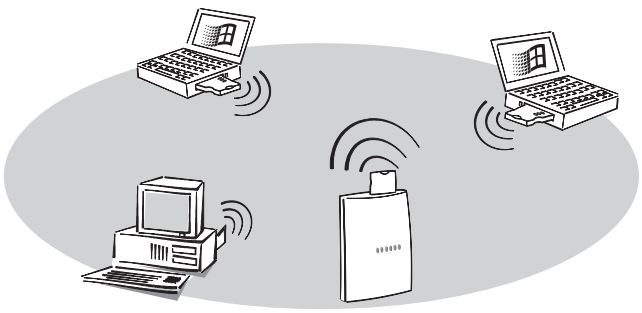
Mit Funk-Netzwerkkarten verbinden Sie einzelne Notebooks und PCs zu einem lokalen Netzwerk, einem **L**ocal **A**rea **N**etwork (LAN). Da in diesem LAN das in herkömmlichen LANs übliche Netzwerkkabel durch eine Funkverbindung ersetzt wird, nennt man diese Funk-Netzwerke auch **W**ireless **L**ocal **A**rea **N**etwork (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 Netzwerkkabel 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.

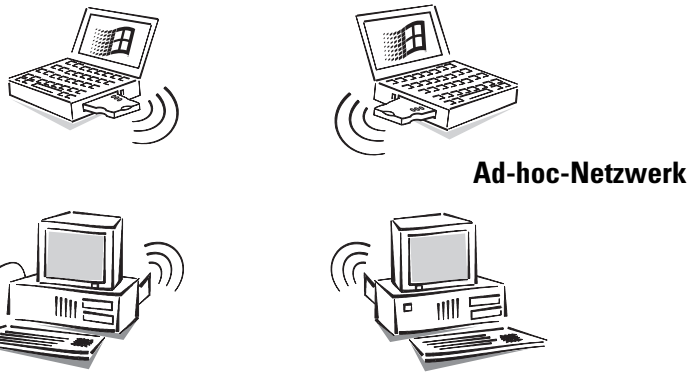


In einem Funk-Netzwerk stehen alle Funktionen eines kabelgebundenen Netzwerks zur Verfügung: Zugriff auf Dateien, Server, Drucker etc. ist ebenso möglich wie die Einbindung der mobilen Stationen in ein firmeninternes Mailssystem.

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.



Ad-hoc-Netzwerk

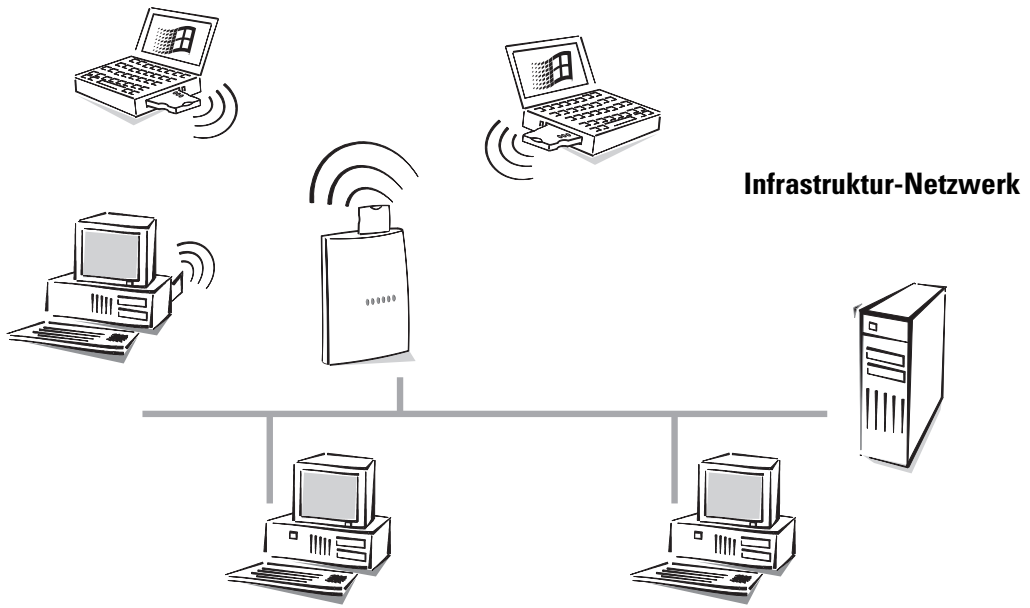
Peer-to-Peer

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 einem als Verbindung zwischen

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



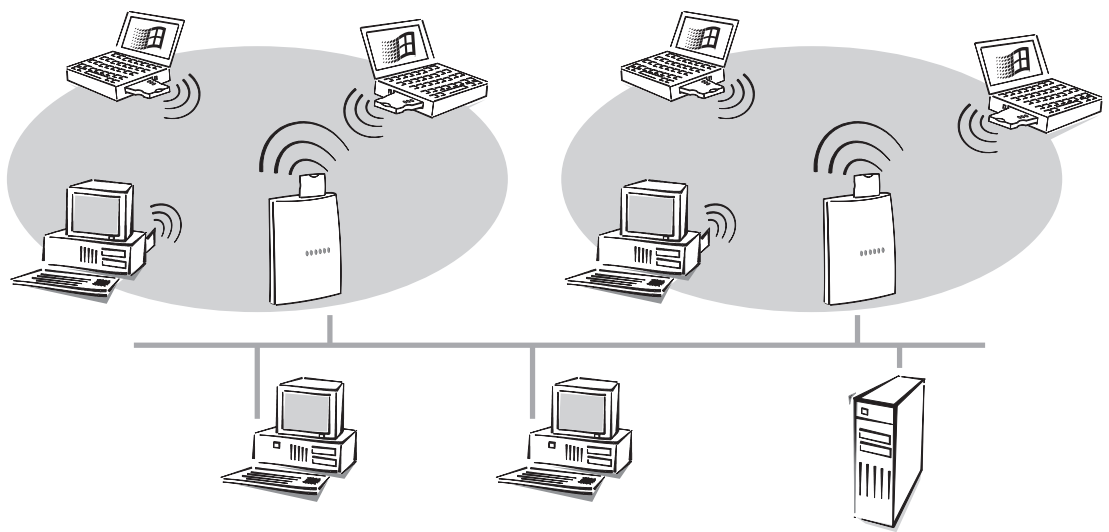
Peer-to-LAN

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.

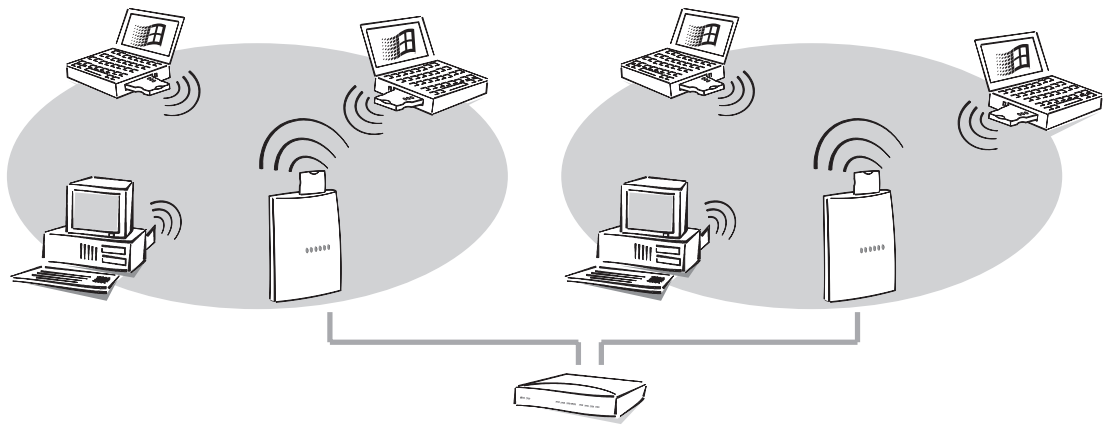
Skalierung

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 Netzwerkkabel 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-Statio-

nen nicht alle innerhalb der Reichweite einer Basis-Station, wird eine zweite dazugenommen. Die beiden Basis-Stationen können dann z.B. über einfache Netzwerkkabel 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.

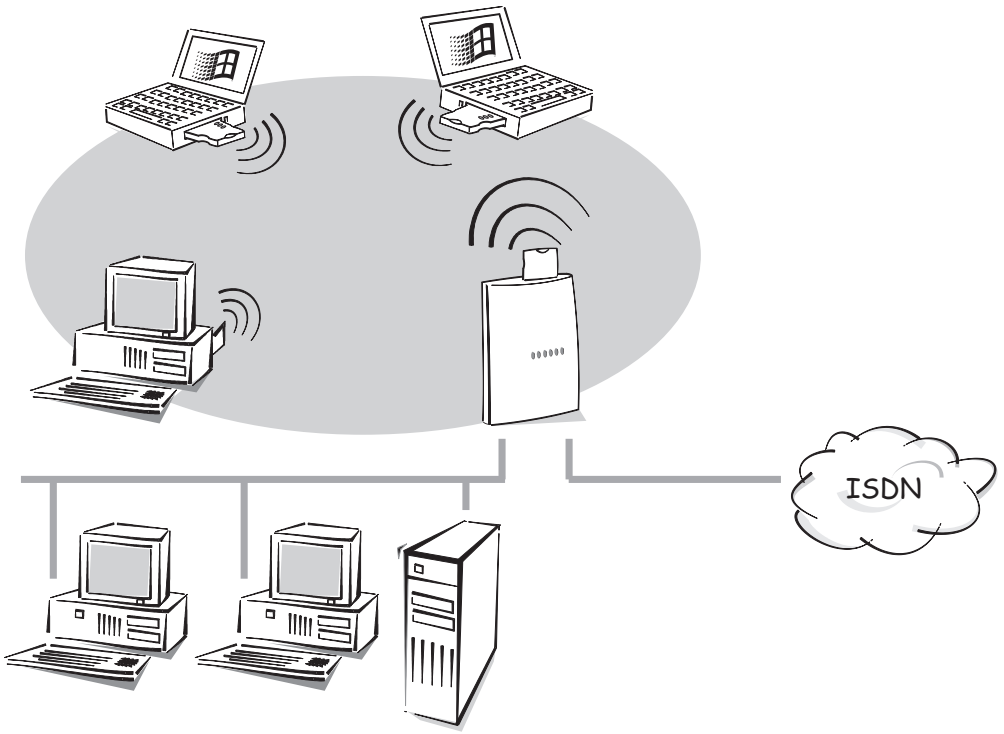
Roaming

Roaming ist der transparente Wechsel zwischen verschiedenen Funkzellen. Die Benutzer können von einer Zelle zur anderen wechseln, ohne die Netzwerkverbindung zu verlieren. Die Basis-Stationen tauschen dabei ständig die Informationen zu den angemeldeten Funkstationen über das kabelgebundene LAN aus.

Voraussetzung für erfolgreiches Roaming ist, daß alle daran beteiligten Basis-Stationen an ein gemeinsames Ethernet-Netz angeschlossen sind. Bridges, Switches und Repeater zwischen den Basis-Stationen sind erlaubt, Router nicht!

ISDN-Anschluß

Eine besondere Zusatzfunktion bietet die Basis-Station *ELSA LANCOM Wireless IL-2*. Über die ISDN-Schnittstelle verbindet die Basis-Station nicht nur das Funk-Netzwerk mit dem kabelgebundenen LAN, sondern gleichzeitig mit dem ISDN-Netz.



Zusammen mit dem Funktionsumfang eines IP-Routers sind damit weitere Anwendungen wie der Zugriff auf das Internet für alle Rechner im LAN und WLAN möglich.

Was bietet ein *ELSA LANCOM Wireless IL-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
- ISDN-Kabel einstecken
- 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 vohandenen 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**ndustiral, **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.

WAN-Anschluß

Ein *ELSA LANCOM Wireless* wird an die S_0-Schnittstelle(n) eines ISDN-Anschlusses in Punkt-zu-Mehrpunkt-Konfiguration (Mehrgeräteanschluß) oder in Punkt-zu-Punkt-Konfiguration (Anlagenanschluß) angeschlossen. Der Router erkennt Ihren Anschlußtyp und das verwendete D-Kanal-Protokoll automatisch. Wählverbindungen mit DSS1 oder 1TR6 können ebenso verwendet werden wie Festverbindungen. Festverbindungen sind ein zusätzliches Feature, das Sie bei ELSA anfordern können.

Kanalbündelung und Kompression

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

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 ISDN- und Ethernet-Anschlüssen sowie der aktuellen Leitungsverbindungen und erleichtern somit die Diagnose bei möglichen Systemstörungen.

ELSA LANmonitor

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

- Verbindungszustand für jeden B-Kanal
- Name der verbundenen Gegenstelle
- Welches Modul aus dem Gerät ist verbunden (Router, *LANCAPI*)
- Verbindungsdauer und Übertragungsraten
- Auszüge aus der Statistik des Geräts (z.B. Informationen aus der PPP-Verhandlung)

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

Gebührenschutz

Bei freigeschalteter „Gebühreninformation während der Verbindung" im ISDN-Netz (nach AOCD) können die verfügbaren Gebühreneinheiten für einen bestimmten Zeitraum festgelegt werden. So haben Sie immer Kontrolle über Ihre Telefonrechnung.

Falls an Ihrem ISDN-Anschluß keine Gebühreninformationen übermittelt werden, können Sie ersatzweise auch die aktive Verbindungszeit für einen definierten Zeitraum einschränken. Nach Ablauf dieser Zeit läßt der Router dann keinen eigenen Verbindungsaufbau mehr zu.

Least-Cost-Routing

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

Automatische Zeitkontrolle

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

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 WAN (über ISDN), aus dem WLAN oder aus dem LAN. Bei Konfigurationen aus dem LAN oder WLAN wird neben TFTP auch SNMP unterstützt.

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

Zugriffschutz

Zum Schutz vor unberechtigtem Zugriff auf das Firmen-Netz bietet der Router neben dem Paßwortschutz und der Rufnummernerkennung (CLIP) auch eine Rückruf-Funktion, die nur den Verbindungsaufbau zu vorher festgelegten Telefonanschlüssen zuläßt. Firewall-Filter und IP-Masquerading runden das Sicherheitskonzept ab. Zusätzlich verhindert die Login-Sperre „Brute-Force-Angriffe“ und sperrt den Zugang zum Router nach einer einstellbaren Anzahl von Login-Versuchen mit falschem Paßwort.

Kompatibilität durch PPP

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

Fernkonfiguration über PPP

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

Software-Update

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

Die aktuelle Version steht immer in unseren Online-Medien für Sie bereit und kann über das LAN, das WLAN oder das WAN (ISDN) 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.

ELSA LANCAPI und *ELSA CAPI Faxmodem*

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

Alle Workstations, die im LAN (Local Area Network) integriert sind, erhalten über die *LANCAPI* uneingeschränkten Zugriff auf Bürokommunikations-Funktionen wie Fax und EuroFileTransfer. Ohne zusätzliche Hardware an den Arbeitsstationen werden alle Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsstationen installiert.

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

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

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.

NetBIOS-Proxy

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

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

DNS-Server

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

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

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

Installation

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 IL-2*
- Netzteil
- Funk-Netzwerkkarte *ELSA AirLancer MC-2*
- LAN-Anschlußkabel
- ISDN-Anschlußkabel
- Dokumentation
- CD mit *ELSA LANconfig* und weiterer Software und elektronischer Dokumentation

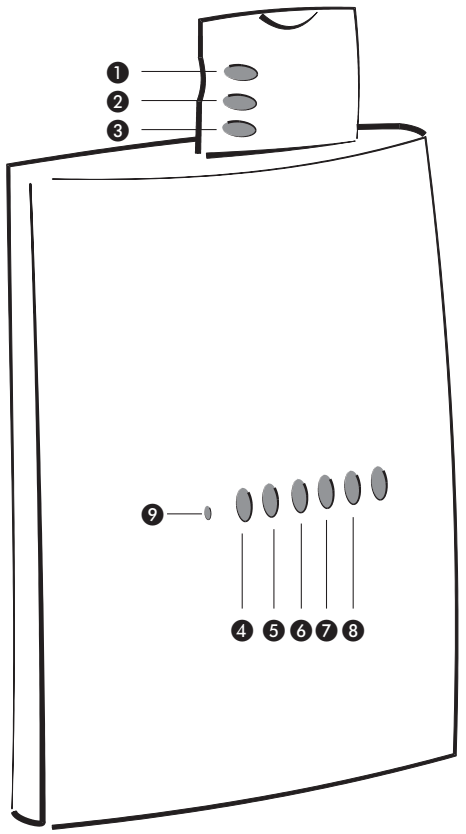
Falls etwas fehlen sollte, wenden Sie sich bitte direkt an Ihren Händler.

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.

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

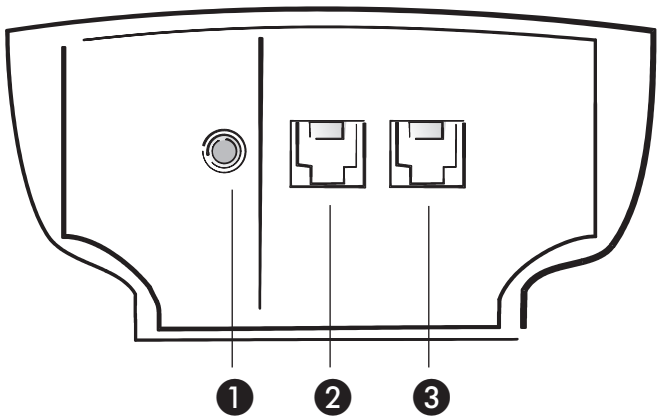
5. Die LED 'S_0-Status' an der Basis-Station zeigt die Aktivität des D-Kanals an.

❻ Die LED 'WAN-Channel-1' an der Basis-Station zeigt die Aktivität des ersten B-Kanals auf der ISDN-Schnittstelle an.

❼ Die LED 'WAN-Channel-2' an der Basis-Station zeigt die Aktivität des zweiten B-Kanals auf der ISDN-Schnittstelle an.

❽ 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:



❶ Anschluß für das Netzteil

❷ 10Base-T Netzwerkanschluß

❸ ISDN-S_0-Anschluß

So schließen Sie die Basis-Station an

① Verbinden Sie die Basis-Station *ELSA LANCOM Wireless IL-2* mit dem LAN. Stecken Sie dazu das mitgelieferte Netzwerkkabel 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 Schließen Sie den Router an einen ISDN-S_0-Mehrgeräteanschluß oder Anlagenanschluß (Punkt-zu-Mehrpunkt- oder Punkt-zu-Punkt-Konfiguration). Um den Gebührenschutz und die Gebührenstatistik zu nutzen, beantragen Sie bei Ihrer Telefongesellschaft das ISDN-Merkmal 'Gebührenübertragung **während** der Verbindung' (nach AOCD).

③ Schieben Sie die Funk-Netzwerkkarte *ELSA AirLancer MC-2* in die Basis-Station ein. Die LEDs der PC-Karte müssen dabei zur Vorderseite der Basis-Station weisen.

④ 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-Netzwerkkarte zeigt an, daß die Verbindung zwischen der Karte und der Basis-Station hergestellt ist. Das Flackern der grünen LED in der Funk-Netzwerkkarte 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 vornehmen mit *ELSA LANconfig*

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

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

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

– Sie haben bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet, möchten das ab jetzt aber gerne tun. Welche IP-Adressen dabei verwendet werden, ist Ihnen egal. 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 Inband-Konfiguration (Konfiguration über das Netzwerk) haben Sie von jedem Rechner aus dem WLAN, LAN oder WAN (ISDN) 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 Netzwerkadresse in Ihrem LAN. Haben die Rechner in Ihrem Netz also z.B. Adressen wie 192.110.130.1, dann können Sie Ihr Gerät mit der Adresse 192.110.130.254 erreichen.

Haben Sie bereits einen Rechner mit der Adresse XXX.XXX.XXX.254 in Ihrem Netz stehen, 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

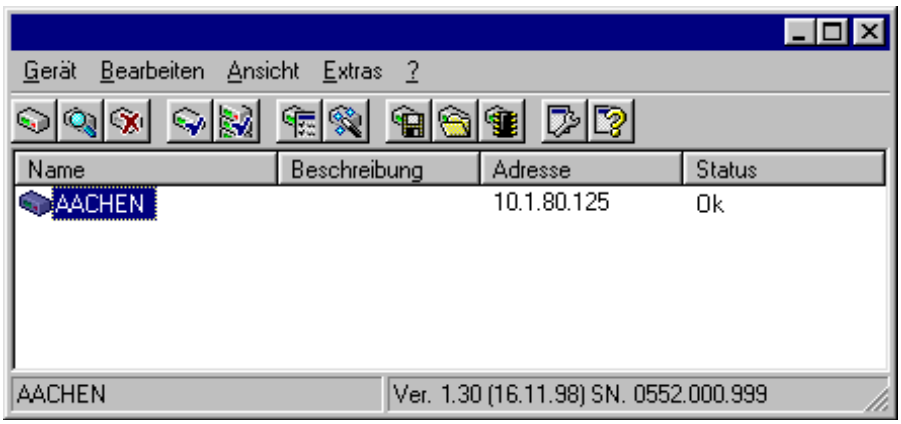
Netz automatisch einstellen lassen (siehe auch Kapitel 'Automatische Adreßzuweisung mit DHCP').

Starten der Konfiguration über *ELSA LANconfig*

Rufen Sie das Konfigurations-Tool *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 Konfigration 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 von 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.	set ip-adresse 192.110.120.140 setzt eine neue IP-Adresse.
	Bei Tabellenzeilen geben Sie alle Einträge getrennt durch Leerzeichen ein. Ein * läßt den Eintrag unverändert.	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 Betriebs-Software 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 bestimmten, in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, daß die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird.

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

Beim Konfigurations-Tool *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 **writeflash** 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 writeflash

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

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

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-Verbindungen
- Sicherheit für die Konfiguration
- Sicherheit für das LAN
- Gebührenmanagement
- ISDN-Verbindungen
- PPP-Unterstützung
- IP-Routing
- Automatische Adreßverwaltung mit DHCP
- DNS-Server
- NetBIOS-Proxy
- *ELSA LANCAPI*
- Zeitkontrolle
- Least-Cost-Router

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

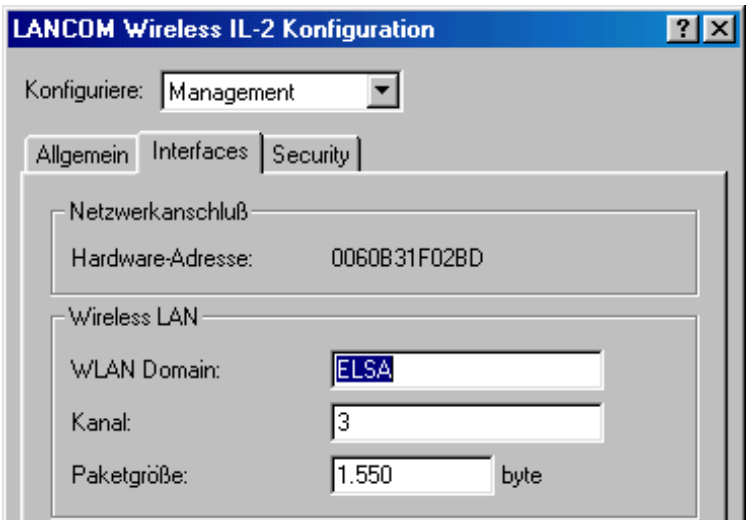
Damit die Funk-Netzwerkkarten in den mobilen Stationen und in den Basis-Stationen sich gegenseitig erkennen und Daten untereinander austauschen können, müssen sie in verschiedenen Parametern die gleichen Werte aufweisen.

Alle Funk-Netzwerkkarten (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-Netzwerkkarten in den Basis-Stationen bei der Konfiguration über *ELSA LANconfig* oder Telnet eingestellt.

① Starten Sie *ELSA LANconfig* mit **Start** ▶ **Programme** ▶ **ELSAlan** ▶ ***ELSA LANconfig***. *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-Frequezband 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 Aktivieren Sie die Funktion 'Roaming', wenn Sie mehrere Funkzellen an einem gemeinsamen Ethernet-Strang betreiben und den „nahtlosen“ Übergang von einer Funkzelle zur anderen ermöglichen wollen. Stellen Sie die WLAN-Domain und den Funkkanal bei allen Basis-Stationen, die am Roaming beteiligt werden sollen, gleich ein.

⑦ 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 im Konfigurationstool *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Bei einer Terminal- oder Telnetsitzung schalten Sie die Paßwortabfrage im Menü `/Setup/Config-Modul/Passw.Zwang` ein. Das Paßwort selbst wird in diesem Fall mit dem Befehl `passwd` gesetzt.

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 ungerechtigter Benutzer ein Paßwort zu „knacken“, und so Zugang zu einem Netzwerk, einem Rechner oder einem anderen Gerät zu erlangen. Dazu spielt z.B. ein Rechner automatisch alle möglichen Kombinationen aus Buchstaben und Zahlen durch, bis das richtige Paßwort gefunden wurde.

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

Diese Parameter gelten global für alle Konfigurationsmöglichkeiten (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 im Konfigurationstool *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 im Konfigurationstool *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein' bzw. im Menü `/Setup/TCP-IP-Modul/Zugangsliste`.

Sicherheit für Ihr LAN

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

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

Die Kontrolle

Welcher „Identifier" zur Erkennung des Anrufers verwendet werden soll, wird im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Rufannahme' bzw. im Menü `/`

`Setup/WAN-Modul/Schutz` eingestellt. Zur Auswahl stehen die folgenden Möglichkeiten:

- keiner: Anrufe aller Gegenstellen werden angenommen.
- Name: Es werden nur Anrufe von solchen Gegenstellen angenommen, die in der Namenliste eingetragen sind.

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

Überprüfung des Namens

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

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

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

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

Und woher kommen Name und Paßwort des Anrufers?

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

Überprüfung der Nummer

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

Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen. Ist ein Schutz im *ELSA LANCOM* über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekannten Rufnummern abgelehnt.

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

Der Rückruf

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

Mit den Einstellungen in Namen- und Nummernliste und der Auswahl des Protokolls können Sie das Rückrufverhalten Ihrer Router steuern:

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

Und ganz nebenbei steuern Sie über die Einstellungen die Verteilung der Kosten für die Verbindung. Ist in der Namenliste ein Rückruf 'Nach Name' vereinbart, übernimmt der rückrufende Router alle Gebühren bis auf eine, die für die Namensübermittlung benötigt wird. Ebenfalls eine Einheit fällt für den Router an, wenn der Anrufer nicht über CLI identifiziert wird. Ist dagegen eine Identifizierung über die Rufnummer des Anrufers erlaubt und möglich, kommt der Anrufer sogar ganz ohne Kosten weg.

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

Das Versteck – IP-Masquerading (NAT, PAT)

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

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

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

Gebührenmanagement

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

Zeitabhängige Verbindungsbegrenzung

Um die Kosten begrenzen zu können, kann die maximale Verbindungsdauer mit Hilfe der Zeit gesteuert werden. Dazu wird ein Zeitbudget für eine Periode vereinbart. Im Default-Zustand dürfen z.B. für maximal 210 Minuten pro Woche aktiv Verbindungen aufgebaut werden.

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

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

Einstellungen im Gebührenmodul

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

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

ISDN-Verbindungen

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

Die Routermodule ermitteln zunächst nur, zu welcher Gegenstelle ein Datenpaket übertragen werden soll. Damit die entsprechende Verbindung ausgewählt und ggf. aufgebaut werden kann, müssen verschiedene Parameter für alle notwendingen ISDN-Verbindun-

gen vereinbart werden. Diese Parameter sind in unterschiedlichen Listen abgelegt, deren Zusammenspiel die richtigen Verbindungen erlaubt.

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

Namenliste

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

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

- Name

  Mit diesem Namen wird die Gegenstelle in den Routermodulen identifiziert.

- Rufnummer

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

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

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

- Haltezeiten

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

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

- Layername

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

- Rückruf

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

  – normaler Rückruf
  – Rückruf nach dem schnellen ELSA-Verfahren

– Rückruf nach Überprüfung des Namens
– selbst den Rückruf der Gegenstelle nach dem schnellen ELSA-Verfahren erwarten

Interface-Einstellungen

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

In den Interface-Einstellungen legen Sie für jedes Interface (also jeden S_0-Anschluß) die allgemeinen Parameter fest. Diese Parameter gelten für alle Betriebsarten der Geräte. Es sind im einzelnen:

- Das D-Kanal-Protokoll, das an diesem S_0-Anschluß verwendet wird.

  Automatische Erkennung, DSS1 (Euro-ISDN), DSS1 Punkt-zu-Punkt, 1TR6, Festverbindung Gruppe 0

- Festverbindungsoption

  B-Kanal, der ggf. für die Festverbindung verwendet werden soll.

- Anwahlpräfix

  Nummer, die bei abgehenden Rufen der Rufnummer vorangestellt wird, z.B. die Amtskennziffer beim Betrieb an TK-Anlagen.

Router-Interface-Einstellungen

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

In den Router-Interface-Einstellungen legen Sie für jedes Interface (also jeden S_0-Anschluß) die Parameter fest, die in der Betriebsart als Router verwendet werden. Diese Parameter gelten nicht für die anderen Betriebsarten der Geräte. Es sind im einzelnen:

- Rufnummern (MSN/EAZ)

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

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

- Option für Y-Verbindung

  Schalten Sie diese Option ein, wenn die beiden B-Kanäle des Anschlusses parallel Verbindungen zu unterschiedlichen Gegenstellen aufbauen können sollen.

- Unterdrückung der eigenen Rufnummer

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

Diese Funktion muß vom Netzbetreiber unterstützt werden.

LANCAPI-Interface-Einstellungen

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

In den Router-Interface-Einstellungen legen Sie für jedes Interface (also jeden S_0-Anschluß) die Parameter fest, die für die *LANCAPI* verwendet werden. Diese Parameter gelten nicht für die anderen Betriebsarten der Geräte. Es sind im einzelnen:

- Rufnummern (MSN/EAZ)

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

- Zugriff auf die *LANCAPI*

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

- Übertragung der eigenen Rufnummer

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

Layer-Liste

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

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

- Layername

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

- Encapsulation

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

- Layer-3

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

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

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

- Layer-2

  Layer-2-Protokoll für die Verbindung.

- Optionen

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

- Layer-1

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

Round-Robin-Liste

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

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

- Gegenstelle

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

- Round-Robin

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

- Anfangen mit:

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

PPP-Liste

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

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

- Gegenstelle

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

- Username

  Benutzername, der zur Anmeldung bei der Gegenstelle verwendet wird.

- Paßwort

  Paßwort, das zur Anmeldung bei der Gegenstelle verwendet wird.

- Prüfung

  Authentifizierungsverfahren, das der Router von der Gegenstelle verlangen soll.

- Zeit, Wdh., Conf., Fail., Term.

  Parameter zum Verhalten der Verbindung, die hier nicht näher beschrieben werden.

Script

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

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

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

- Gegenstelle

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

- Script

  Tragen Sie hier das Script ein, wie im Referenzteil der Dokumentation beschrieben.

Rufannahme

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

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

- Alle

  Alle Rufe werden angenommen.

- Name

  Alle Rufe werden zunächst angenommen. In der Protokollverhandlung wird der Name ermittelt und geprüft, ob dieser Name in der Namenliste vorhanden ist. Nur dann bleibt die Verbindung bestehen, ansonsten wird sie wieder abgebaut.

- Nummer

  Der Anruf wird nur angenommen, wenn die Gegenstelle in der Nummernliste eingetragen ist und die Rufnummer der Gegenstelle übermittelt wird.

- Name oder Nummer

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

Nummernliste

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

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

- Rufnummer

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

- Gegenstelle

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

Point-to-Point Protocol

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

Und gerade weil das PPP nicht einer bestimmten Betriebsart der Router zugeordnet werden kann und natürlich auch wegen der großen und in Zukunft noch weiter steigenden

Bedeutung dieser Protokoll-Familie, möchten wir Ihnen die Funktionen der Geräte im Zusammenhang mit dem PPP hier in einem eigenen Abschnitt vorstellen.

Das Protokoll

Was ist PPP?

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

- Paßwortschutz nach PAP oder CHAP
- Aushandlung der über die aufgebaute Verbindung zu benutzenden Netzwerkprotokolle (z.B. IP). Dazu gehören auch für diese Protokolle notwendigen Parameter wie z.B. IP-Adressen. Diese Verhandlung läuft über das Protokoll IPCP (IP Control Protocol) ab.
- Überprüfung der Verbindung mit dem LCP (Link Control Protocol)

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

Wozu wird PPP verwendet?

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

- aus Kompatibilitätsgründen z.B. bei Kommunikation mit Fremdroutern
- Internet-Access (mit der Übermittlung von Adressen)

Die Phasen einer PPP-Verhandlung

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

- Establish-Phase

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

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

- Authenticate-Phase

Falls notwendig, werden danach die Paßworte ausgetauscht. Bei Authentifizierung nach PAP wird das Paßwort nur einmalig übertragen. Bei Benutzung von CHAP wird ein verschlüsseltes Paßwort periodisch in einstellbaren Abständen gesendet.

- Network-Phase

  Ist die Verhandlung der Parameter erfolgreich verlaufen, können von den Router-Modulen IP-Pakete auf der geöffneten (logischen) Leitung übertragen werden.

- Terminate-Phase

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

Die PPP-Verhandlung im *ELSA LANCOM*

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

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

```
trace + ppp
```

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

Die PPP-Liste

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

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

In dieser Spalte der PPP-Liste ...	... tragen Sie folgende Werte ein:
Gerätename	Name der Gegenstelle, mit dem sie sich bei Ihrem Router anmeldet
Sicherung	Verfahren zur Sicherung der PPP-Verbindung ('PAP', 'CHAP' oder 'keine'). Ihr eigener Router verlangt von der Gegenstelle die Einhaltung dieses Verfahrens! Nicht etwa umgekehrt. Daher bietet sich die Sicherung nach 'PAP' oder 'CHAP' nicht an bei Verbindungen zu Internet-Service-Providern, die uns vielleicht kein Paßwort übermitteln wollen. Für solche Verbindungen wählen Sie 'keine' Sicherung.
Paßwort	Paßwort, das von Ihrem Router an die Gegenstelle übertragen wird (falls gefordert). * in der Liste zeigen an, daß ein Eintrag vorhanden ist.

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

Alles o.k.? Leitungsüberprüfung mit LCP

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

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

Was passiert nun, wenn der Reply ausbleibt? Zuerst werden einige Wiederholungen der Anfrage gestartet, um kurzfristige Störungen der Leitung auszuschließen. Wenn alle diese Wiederholungen unbeantwortet bleiben, wird die Leitung abgebaut und ein Ersatzweg gesucht.

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

IP-Routing

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

Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem Router, an welche Gegenstelle (also welchen anderen Router oder Rechner) er die Daten für bestimmte IP-Adressen oder IP-Adreß-Bereiche schicken soll. So ein Eintrag heißt auch „Route“, weil der Weg der Datenpakete damit beschrieben wird. Da Sie diese Einträge selbst vornehmen und sie solange unverändert bleiben, bis Sie selbst sie wieder ändern oder löschen, heißt dieses Verfahren auch „statisches Routing“. Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing“. Dabei tauschen die Router selbständig untereinander Informationen über die Routen aus und erneuern diese fortlaufend. Die statische Routing-Tabelle kann bis zu 64 Einträge aufnehmen, die dynamische Tabelle 128. Bei aktiviertem IP-RIP beachtet der IP-Router beide Tabellen.

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

Was bedeuten die einzelnen Einträge in der Liste?

- IP-Adresse und IP-Netzmaske

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

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

- Router-Name

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

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

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

- Distanz

  Anzahl der zwischen dem eigenen und dem Ziel liegenden Router.

Beispiele mit Erläuterungen:

IP-Adresse	IP-Netzmaske	Router-Name	Dist.	Und das passiert:
192.168.130.0	255.255.255.0	192.168.140.123	0	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.130.x werden an den lokal erreichbaren Router mit der IP-Adresse 192.168.140.123 übertragen.
192.168.0.0	255.255.0.0	0.0.0.0	0	Schließt die Übertragung aller Datenpakete in 10er-Netze aus.
172.16.0.0	255.255.0.0	0.0.0.0	0	
10.0.0.0	255.0.0.0	0.0.0.0	0	
224.0.0.0	224.0.0.0	0.0.0.0	0	

Filter für die TCP/IP-Pakete

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

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

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

Proxy-ARP

Eine Besonderheit im IP-Router stellt die Möglichkeit des Proxy-ARP dar. „Proxy“ ist ein englischer Begriff und heißt auf deutsch „Stellvertreter”. Dieser Stellvertreter wird dann eingesetzt, wenn die Datenübertragung zu IP-Adressen im gleichen logischen Netz wie der Absender erfolgt, die Zieladresse dennoch über einen Router zu erreichen ist. Das ist z.B. bei der Anbindung von einzelnen Arbeitsplatzrechnern (Teleworkern) über TCP/IP an das Firmen-Netz der Fall. Der Teleworker hat dann eine IP-Adresse, die im gleichen lokalen Netz liegt wie alle anderen Rechner im LAN. Normalerweise würde ein Datenpaket aus dem LAN für den Teleworker also nur lokal einen Abnehmer suchen, leider aber nicht finden.

Um diese Funktion zu nutzen, muß die Option 'Proxy-ARP' eingeschaltet werden (im LANconfig im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' oder im Menü / `setup/IP-Router-Modul` *bei anderen Konfigurationsmöglichkeiten).*

Mit folgendem Eintrag in der Routing-Tabelle wird der Router zum Stellvertreter des Teleworkers:

IP-Adresse	IP-Netzmaske	Router-Name	Distanz	IP-Masquerading
192.168.110.123	255.255.255.255	Teleworker01	0	aus

Da der Router auf einen ARP-Request für den Proxy-Rechner mit seiner eigenen MAC-Adresse antwortet, werden Proxy-Hosts in einem RIP-Paket nicht propagiert. In der Routing-Tabelle wird die Distanz auf '0' gesetzt, um das zu verdeutlichen.

Der Router beantwortet nun die Frage nach der MAC-Adresse zur IP-Adresse 192.168.110.123 mit seiner eigenen MAC-Adresse. Dadurch werden alle Pakete für den Teleworker im LAN nun automatisch zum Router geschickt, der die Daten zum Rechner auf der anderen Seite der Verbindung weiterleitet.

Lokales Routing

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

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

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

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

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

Dynamisches Routing mit IP-RIP

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

Welche Informationen werden über IP-RIP propagiert?

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

- Routen, die mit der Router-Einstellung '0.0.0.0' verworfen werden.
- Routen, die auf andere Router im lokalen Netz lauten.

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

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

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

Was bedeuten die Einträge?

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

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

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

Zusammenspiel: statische und dynamische Tabelle

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

IP-Masquerading (NAT, PAT)

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

Die Lösung heißt hier IP-Masquerading. Bei diesem Verfahren tritt nur ein Router des LANs mit einer IP-Adresse im Internet in Erscheinung. Diese IP-Adresse wird dem Router z.B. fest vom NIC oder temporär von einem Internet-Provider zugewiesen. Alle anderen Rechner im Netz „verstecken" sich dann hinter dieser einen IP-Adresse. Neben dem

angenehmen Spareffekt bildet das IP-Masquerading auch einen sehr effektiven Schutz gegen Zugriffe aus dem Internet auf das lokale Netz.

Zwei Adressen für den Router

- 'aus': Es wird keine Maskierung durchgeführt.

Wie funktioniert IP-Masquerading?

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

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

In den Statistiken des Routers können Sie sich diese Tabellen genau ansehen (siehe auch 'Status' im Referenz-Handbuch).

Einfaches und inverses Masquerading

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

Der kleine Unterschied:

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

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

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

Welche Protokolle können mit IP-Masquerading übertragen werden?

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

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

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

DNS-Forwarding

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

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

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

- Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist (im Konfigurationstool *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Adressen' oder im Menü `/Setup/TCP-IP-Modul`). Wird er dort fündig, holt er die gewünschte Information von diesem Server.
- Gibt es keinen eingetragenen DNS-Server im *ELSA LANCOM Wireless*, versucht der Router auf einer evtl. bestehenden PPP-Verbindung (z.B. zum Internet-Provider) einen DNS-Server zu erreichen und holt die Zuordnung der IP-Adresse zum Namen von dort. Das gelingt natürlich nur dann, wenn während der PPP-Verhandlung die Adresse eines DNS-Servers an den *ELSA LANCOM Wireless* übermittelt worden ist.

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

Policy Based Routing

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

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

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-Automode die IP-Adressen für sich selbst und für die Rechner im Netz selbständig festlegen.

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

DHCP – 'Ein', 'Aus' oder 'Auto'?

Der DHCP-Server kann drei verschiedene Zustände annehmen:

- 'Ein': Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adreß-Pools) überprüft.
  - Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an.
  - Bei einer fehlerhaften Konfiguration (z.B. ungültige Pool-Grenzen) wird der DHCP-Server wieder abgeschaltet und wechselt in den Zustand 'Aus'.
- 'Aus': Der DHCP-Server ist dauerhaft abgeschaltet.
- 'Auto': Der Server befindet sich im Automodus. In diesem Zustand sucht das Gerät nach dem Einschalten im lokalen Netz nach anderen DHCP-Servern.
  - Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Damit wird u.a. verhindert, daß ein unkonfiguriertes Gerät nach dem Einschalten im Netz Adressen vergibt, die nicht im lokalen Netz liegen.
  - Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein.

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

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

So werden die Adressen zugewiesen

Zuweisung von IP-Adressen

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

- Die IP-Adresse kann aus dem eingestellten Adreß-Pool genommen werden (Start-Adreß-Pool bis End-Adreß-Pool). Hier können beliebige im lokalen Netz gültige Adressen eingegeben werden.
- Es verwendet dann selbst die IP-Adresse '10.0.0.254' und den Adreß-Pool '10.x.x.x' für die Zuweisung der IP-Adressen im Netz. In diesem Zustand weist der DHCP-Server den anderen Rechnern im Netz nur die IP-Adresse und deren Gültigkeit zu, nicht jedoch die anderen Informationen.

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

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

Zuweisung der Netzmaske

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

Zuweisung der Broadcast-Adresse

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

Die Änderung der Voreinstellung für die Broadcast-Adresse wird nur für erfahrene Netzwerk-Spezialisten empfohlen.

Zuweisung von DNS- und NBNS-Server

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

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

Zuweisung des Default-Gateways

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

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

Gültigkeitsdauer einer Zuweisung

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

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

- Maximale Gültigkeit in Minuten

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

  Fordert ein Host eine Gültigkeit an, die die maximale Dauer 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 Netzwerkumgebung von Windows so eingestellt, daß die benötigten Parameter über DHCP angefragt werden. Überprüfen Sie die Einstellungen mit einem Klick auf **Start** ▶ **Einstellungen** ▶ **Systemsteuerung** ▶ **Netzwerk**. Wählen Sie den Eintrag für 'TCP/IP' an Ihrem Netzwerkadapter, und öffnen Sie die **Eigenschaften**.

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

Vorfahrt für den Rechner – Zuweisung überschreiben

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

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

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

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

Im DHCP-Modul kann über den Punkt 'Setup/DHCP/Tabelle-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 das Konfigurationstool *ELSA LANconfig* mit einem Assistenten, die notwendigen Einstellungen vorzunehmen:

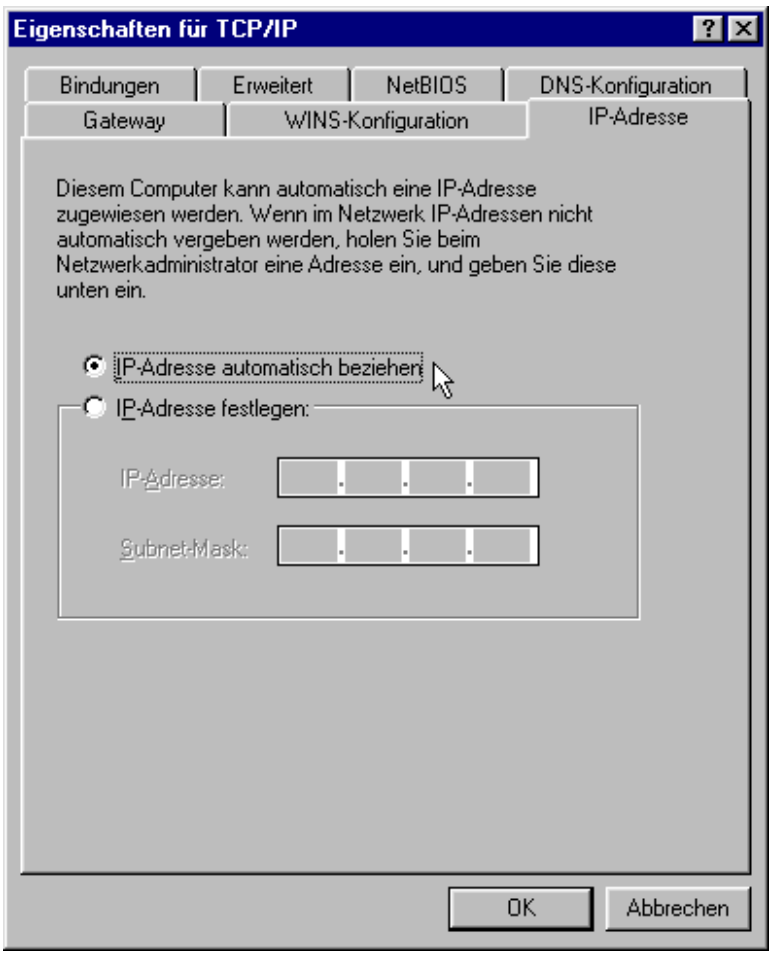
① Verbinden Sie das unkonfigurierte Gerät über das Netzwerkkabel mit Ihrem lokalen Netz.

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

③ Falls noch nicht geschehen, installieren Sie das Protokoll 'TCP/IP' auf allen Rechnern im lokalen Netz.

  – Bei der Installation des Protokolls werden die Rechner meist standardmäßig so eingestellt, daß Sie die IP-Adresse automatisch von einem DHCP-Server beziehen wollen. Nach einem Neustart, der mit dieser Installation verbunden ist, fordern die Rechner automatisch eine IP-Adresse vom DHCP-Server an.

– Wenn Sie das Protokoll schon installiert haben, aktivieren Sie nun die DHCP-Funktion auf allen Rechnern im lokalen Netz. Öffnen Sie dazu z.B. unter Windows 95 mit **Start** ▶ **Einstellungen** ▶ **Systemsteuerung** ▶ **Netzwerk** das Fenster zur Konfiguration der Netzwerkeigenschaften. Doppelklicken Sie den Eintrag für das Protokoll 'TCP/IP'.
Aktivieren Sie die Option 'IP-Adresse automatisch beziehen'. Wechseln Sie auf die Registerkarte 'DNS-Konfiguration', und löschen Sie alle vorhandenen DNS-Adressen. Löschen Sie dann auf der Registerkarte 'Gateway' alle evtl. vorhandenen Einträge und schließen alle Fenster mit **OK**. Nach einem Neustart, der mit dieser Einstellung verbunden ist, fordern die Rechner automatisch eine IP-Adresse aus dem Adreß-Pool des DHCP-Servers an.



④ Installieren Sie das Konfigurationstool *ELSA LANconfig* auf einem der Rechner im Netz.

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

– Wenn Sie bisher noch keine IP-Adressen in Ihrem Netz verwendet haben, wählen Sie in diesem Assistenten die Option 'Alle Einstellungen automatisch vorneh-

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

– Wenn Sie auch vor der Umstellung auf DHCP-Betrieb IP-Adressen in Ihrem Netz verwendet haben, wählen Sie in diesem Assistenten die Option 'Ich möchte die Einstellungen selber vornehmen'. Geben Sie im nächsten Fenster eine freie IP-Adresse aus dem bisher verwendeten Adreßbereich ein, und schalten Sie den DHCP-Server ein.
Der Assistent weist dem Gerät nun die eingestellte IP-Adresse mit der zugehörigen Netzmaske zu. Aus der IP-Adresse ermittelt das Gerät dann den gültigen Adreß-Pool für die DHCP-Zuweisung.

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

Manuelle Konfiguration

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

DNS

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

Was macht ein DNS-Server?

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

Ohne DNS-Server im lokalen Netz wird jeder lokal unbekannte Name über die DEFAULT-Route gesucht. Durch die Verwendung eines DNS-Servers können alle Namen, die mit ihrer IP-Adresse bekannt sind, direkt bei der richtigen Gegenstelle gesucht werden. Der

DNS-Server kann dabei im Prinzip ein separater Rechner im Netz sein. Folgende Gründe sprechen jedoch dafür, den DNS-Server direkt im *ELSA LANCOM Wireless* anzusiedeln:

- Ein *ELSA LANCOM Wireless* kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbständig verteilen. Der DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-Server hätte bei der dynamischen Adreßvergabe des DHCP-Servers möglicherweise Schwierigkeiten, die Zuordnung zwischen IP-Adresse und Namen aktuell zu halten.
- Beim Routing von Windows-Netzen über NetBIOS kennt ein *ELSA LANCOM Wireless* außerdem die Rechnernamen und IP-Adressen in den anderen angeschlossenen NetBIOS-Netzen. Außerdem melden sich auch die Rechner mit fest eingestellter IP-Adresse ggf. in der NetBIOS-Tabelle an und sind damit mit Name und Adresse bekannt.
- Der DNS-Server im *ELSA LANCOM Wireless* kann gleichzeitig als sehr komfortabler Filtermechnismus eingesetzt werden. Anfragen nach bestimmten Domains, die nicht besucht werden dürfen, können durch die einfache Angabe des Domain-Namens für das ganze LAN, nur für Teilnetze (Subnetze) oder sogar für einzelne Rechner gesperrt werden.

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

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

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

So stellen Sie den DNS-Server ein

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

① Schalten Sie den DNS-Server ein.

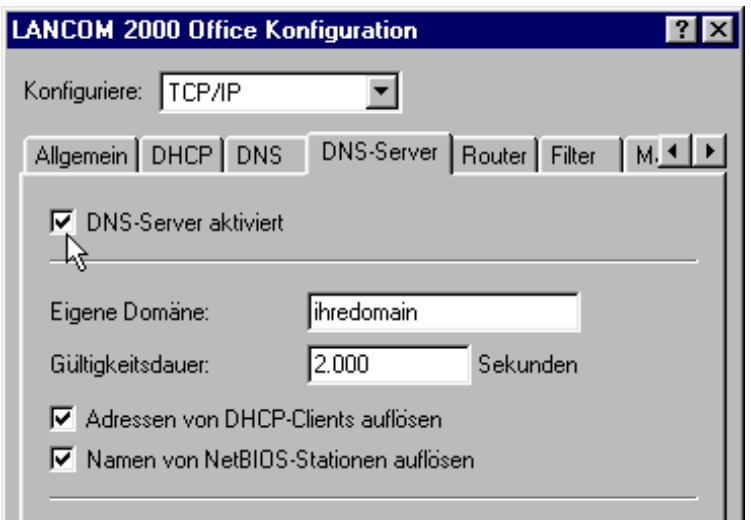
```
set setup/dns-modul/zustand ein
```

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

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

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

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

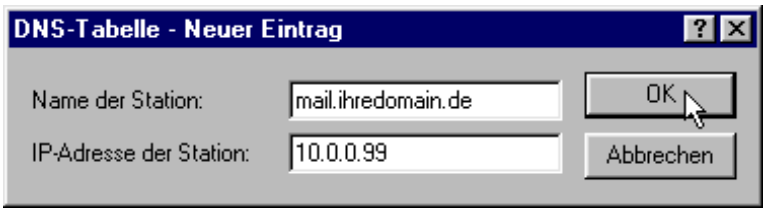


④ Der DNS-Server dient hauptsächlich dazu, Anfragen nach Namen im Internet von den Anfragen nach Namen bei anderen Gegenstellen zu trennen. Tragen Sie daher alle Rechner in die DNS-Tabelle ein,

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

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

Sie ein:




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

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

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

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


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

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

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

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

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

NetBIOS-Proxy

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

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

Kurz und bündig: Was ist NetBIOS?

NetBIOS dient dazu, mehrere Rechner einfach und unkompliziert zu vernetzen. Ein wichtiger Vertreter eines NetBIOS-Netzes ist das Windows-Netz, über das sich mehrere Windows-3.11-, Windows-9x- und Windows-NT-Rechner einfach vernetzen lassen und in dem die Ressourcen der jeweiligen Rechner (Laufwerke oder Drucker) für alle anderen freigegeben werden können.

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

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

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

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

Behandlung von NetBIOS-Paketen

Das äußerst „gesprächige" Verhalten der Windows-Rechner kann bei der Verbindung über ISDN-Leitungen hohe Gebühren verursachen, da jedes NetBIOS-Paket mit Namens-

informationen automatisch zum Verbindungsaufbau führt (z.B. zum bereits eingerichteten ISP). Durch diese Pakete bleibt die Leitung ständig aufgebaut und es fallen entsprechend hohe Gebühren an, ohne daß wirklich eine Nutzdatenübertragung stattfindet.

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

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

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

Welche Voraussetzungen müssen erfüllt sein?

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

Installierte Komponenten

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

- Netzwerkprotokoll

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

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

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

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

- Client

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

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

- Dienst

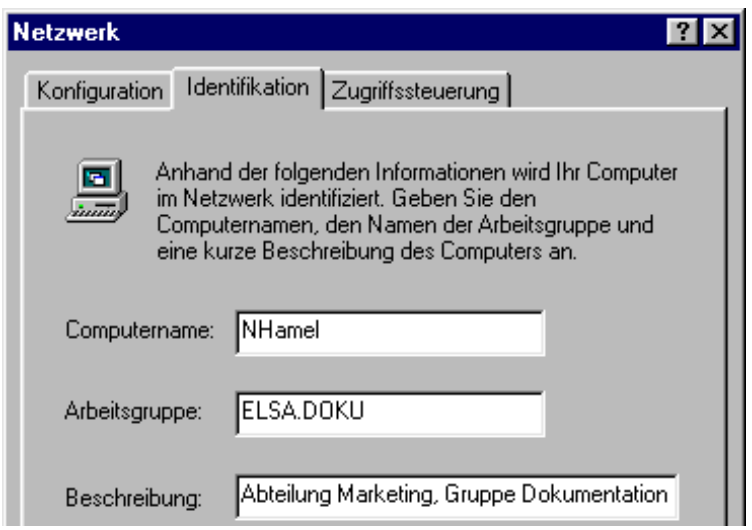
  Die Datei- und Druckerfreigabe ermöglicht das Freigeben von Laufwerken oder Druckern für andere Benutzer im Windows-Netz.

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

Einstellungen im Windows-Netzwerk

- Namen und Gruppenbezeichnung

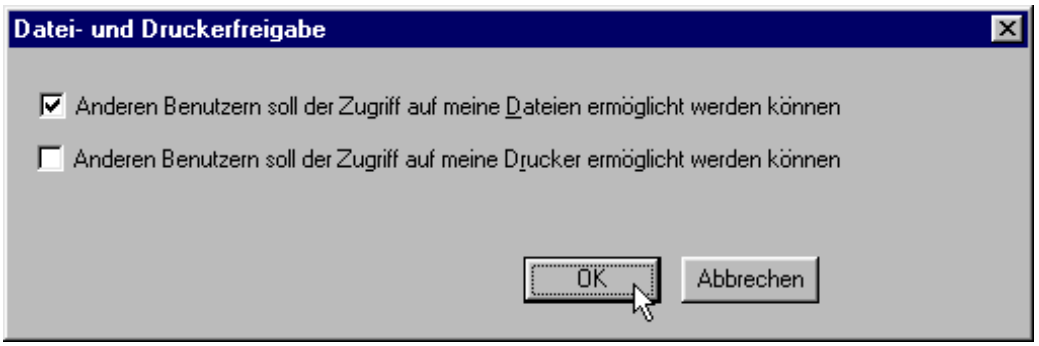
  Klicken Sie auf **Start** ▶ **Einstellungen** ▶ **Systemsteuerung** ▶ **Netzwerk**, und wechseln Sie auf die Registerkarte **Identifikation**.



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

- Datei- und Druckerfreigabe

  Prüfen Sie nach der Installation, ob die Datei- und Druckerfreigabe aktiviert ist. Klikken Sie dazu **Start** ▶ **Einstellungen** ▶ **Systemsteuerung** ▶ **Netzwerk** ▶ **Datei- und Druckerfreigabe**. Wählen Sie aus, ob die anderen Benutzer im Windows-Netz den Drucker und/oder die Dateien von diesem Rechner nutzen können.



Alle Benutzer, die auf die freigegebenen Ressourcen zugreifen wollen, müssen sich beim Start von Windows mit Name und Paßwort anmelden.

Klicken Sie dann im Explorer mit der rechten Maustaste die Laufwerke, Ordner oder Drucker, die Sie für die Benutzung durch andere Netzteilnehmer freigeben wollen, und wählen Sie den Punkt **Freigabe** aus dem Kontextmenü.

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

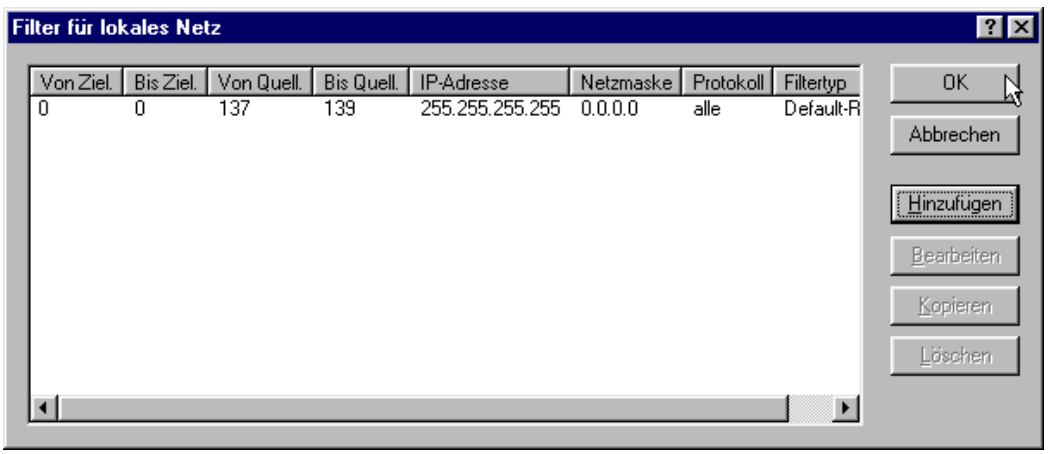
Ob die Einstellungen im Windows-Netzwerk korrekt erfolgt sind, können Sie leicht prüfen: Der eigene Rechner muß in der Netzwerkumgebung mit seinem Namen angezeigt werden.

So verbinden Sie zwei Windows-Netze über ISDN

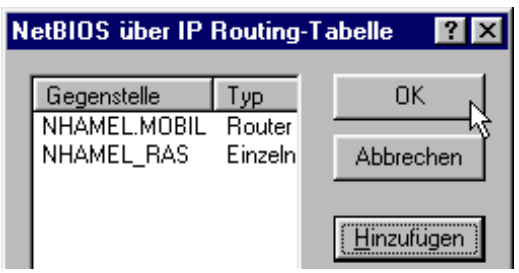
Nachdem alle Vorbereitungen abgeschlossen sind, können Sie nun zwei Windows-Netze verbinden. Die Einstellungen für Arbeitsgruppennetze und Domänen-Netze (Windows NT) sind dabei ähnlich. Die folgenden Schritte sind für beide Seiten der Verbindung auszuführen.

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

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



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



Bei der Konfiguration über Telnet geben Sie alternativ ein:

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

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

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

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

⑤ Wenn alle Gegenstellen eingetragen sind, aktivieren Sie die NetBIOS-Funktion.

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

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

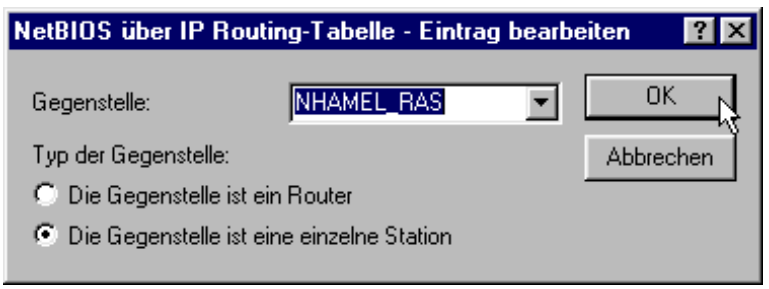
So wählt sich ein Remote-Access-Rechner ein

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

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

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

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




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

```
set nhamel.ras workstation
```

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

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

Gesucht – Gefunden: Die Netzwerkumgebung

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

NetBIOS-Routing über LAN-LAN-Kopplung

Nachdem die Netze nach dem Einschalten der NetBIOS-Module gegenseitig die Informationen über die verfügbaren Rechner ausgetauscht haben, ist im *ELSA LANCOM Wireless* nun eine Liste mit diesen Rechnernamen verfügbar. Über Telnet kann mit

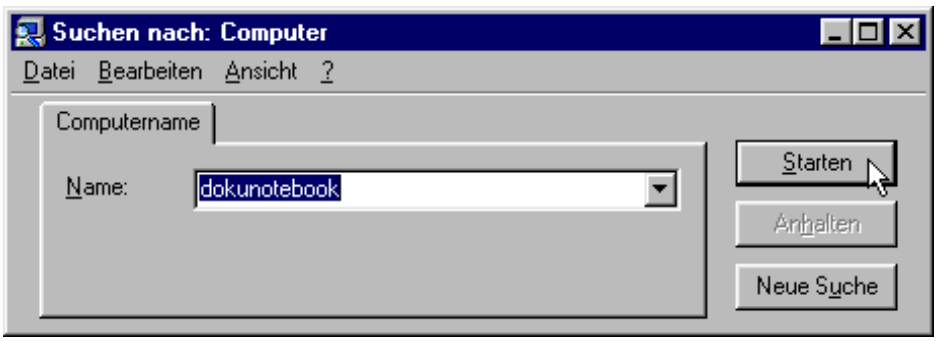
```
dir /Setup/NetBIOS-Modul/host-liste
```

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

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

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

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



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

NetBIOS-Routing über RAS-Zugang

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

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

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

Bürokommunikation und *ELSA LANCAPI*

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

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

ELSA LANCAPI

Welche Vorteile bietet die *LANCAPI*?

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

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

Das dynamische Konzept der *LANCAPI* ermöglicht dabei auch eine leichte Skalierbarkeit der Kommunikationswege. Wenn mehr B-Kanäle benötigt werden, um die anfallenden Aufgaben zu bewältigen, werden einfach mehrere Router im Netz installiert. Alle Geräte im lokalen Netz teilen sich dann die anfallende Arbeit.

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

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

Installation des *LANCAPI*-Clients

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

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

② Wählen Sie den Eintrag 'LANCOM Software installieren'.

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

Nach dem evtl. erforderlichen Neustart des Rechners ist die *LANCAPI* bereit, alle Aufgaben der Bürokommunikationssoftware entgegenzunehmen. Die *ELSA LANCAPI* ist nach erfolgreicher Installation als Icon in der Symbolleiste zu sehen. Ein Doppelklick auf dieses

Symbol öffnet ein Statusfenster, in dem Sie jederzeit aktuelle Informationen zur *ELSA LANCAPI* abrufen können.

Einstellen des *LANCAPI*-Clients

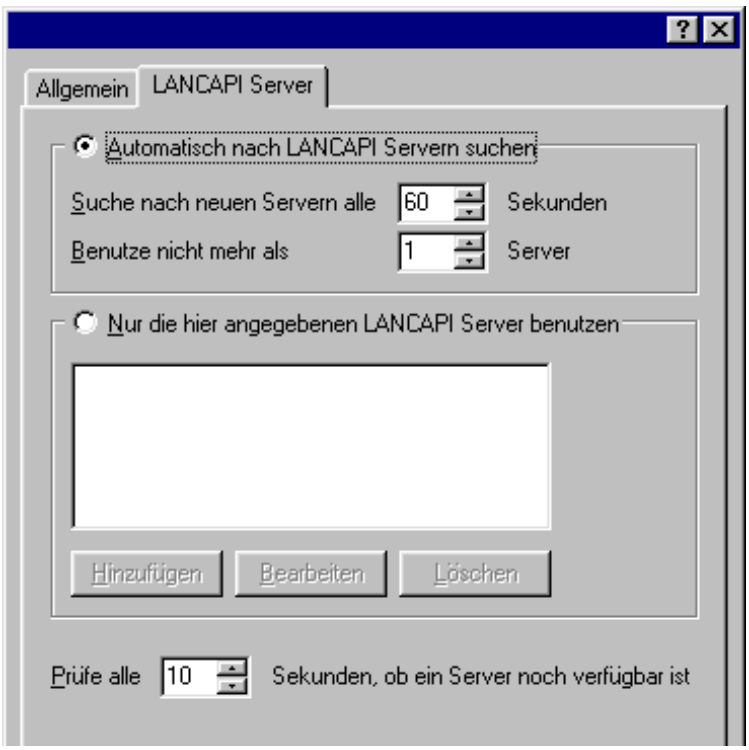
Bei der Einstellung des Clients für die *LANCAPI* legen Sie fest, welche *LANCAPI*-Server verwendet werden sollen und wie diese überprüft werden. Wenn Sie nur ein *ELSA LANCOM Wireless* in Ihrem LAN als *LANCAPI*-Server betreiben, können Sie im Prinzip alle Parameter in den Voreinstellungen belassen.

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

② Wechseln Sie auf das Register 'LANCAPI-Server'. Hier können Sie zunächst wählen, ob der PC seinen *LANCAPI*-Server selbst suchen oder ob ein bestimmter Server verwendet werden soll.

- Im ersten Fall legen Sie fest, in welchem zeitlichen Intervall der Client nach einem Server sucht. Dabei sucht er solange, bis er die im nächsten Feld eingestellte Anzahl an Servern gefunden hat. Hat er die geforderte Zahl an Servern gefunden, hört er mit der Suche auf.
- Wenn der Client nicht automatisch nach Servern suchen soll, geben Sie in der Liste die IP-Adressen der Server an, die der Client verwenden soll. Diese Festlegung ist z.B. dann sinnvoll, wenn Sie mehrere *ELSA LANCOM Wireless* in Ihrem LAN als *LANCAPI*-Server betreiben und eine Gruppe von PCs einen bestimmten Server verwenden sollen.

– Für beide Optionen können Sie dazu noch einstellen, in welchem Intervall der Client prüft, ob die gefundenen oder per Liste definierten Server noch aktiv sind.



Einstellen des *LANCAPI*-Servers

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

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

So stellen Sie die entsprechenden Parameter ein:

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

② Schalten Sie den *LANCAPI*-Server ein, oder lassen Sie nur abgehende Anrufe zu. In diesem Fall reagiert die *LANCAPI* nicht auf ankommende Rufe und kann z.B. nicht zum Empfangen von Faxmitteilungen eingesetzt werden. Lassen Sie z.B. dann nur abgehende Rufe zu, wenn Sie für die *ELSA LANCAPI* keine eigene Rufnummer frei haben.

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

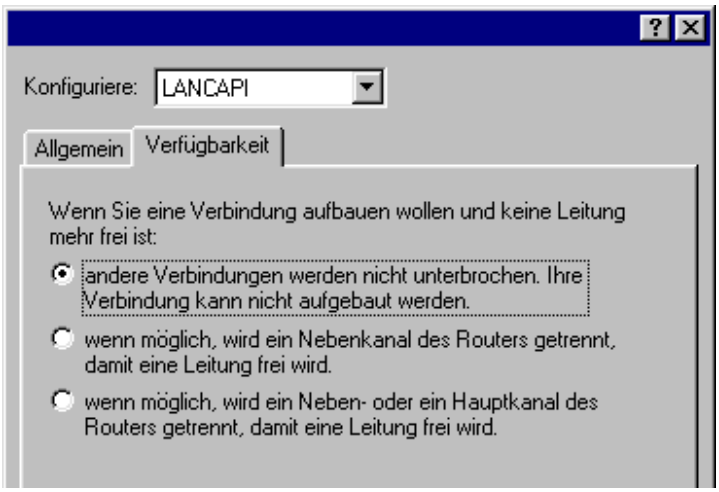
④ Der von der *LANCAPI* verwendete Port ist auf '75' (any private telephony service) voreingestellt. Verändern Sie diese Einstellung nur dann, wenn dieser Port in Ihrem lokalen Netz schon für andere Dienste verwendet wird.

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

Wenn Sie mehrere Rufnummern für die LANCAPI eingeben, können Sie den einzelnen Arbeitsplätzen z.B. ein persönliches Fax oder einen persönlichen Anrufbeantworter bereitstellen. Dazu geben Sie bei der Installation der Kommunikationsprogramme wie z.B. ELSA-RVS-COM an verschiedenen Arbeitsplätzen jeweils verschiedene Rufnummern an, auf die das Programm reagieren soll.

Wechseln Sie auf die Registerkarte 'Verfügbarkeit'. Hier legen Sie fest, wie sich ein *ELSA LANCOM Wireless* verhält, wenn über die *LANCAPI* eine Verbindung aufgebaut werden

soll (ankommender oder abgehender Ruf), beide B-Kanäle jedoch besetzt sind (Prioritätensteuerung). Mögliche Optionen sind hier:



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

So verwenden Sie die *LANCAPI*

Zur Verwendung der *LANCAPI* gibt es zwei Möglichkeiten:

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

Der Least-Cost-Router

Seit der Liberalisierung des Telefonmarktes in Deutschland und in Europa stehen dem Benutzer von Telekommunikationsdiensten eine Reihe von Providern (Netzbetreiber) zur Auswahl, die sich durch z.T. sehr unterschiedliche Tarife unterscheiden. Die Provider unterscheiden sich außerdem danach, ob man fest mit diesem Anbieter verbunden ist

und automatisch immer dessen Netz verwendet (Preselection) oder ob man sich bei jedem Anruf frei entscheidet, welchen Provider man nutzen möchte (Call-by-Call). Um eine Verbindung über einen Call-by-Call-Provider aufzubauen, wählt man nach dem Abheben zunächst die passende Vorwahl, um in das entsprechende Leitungsnetz zu kommen. Erst nach dieser Netzkennziffer wählt man die normale Telefonnummer, um seine Gegenstelle zu erreichen.

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

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

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

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

Der LCR benötigt also folgende Eingaben:

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

Die ersten Versuche

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

Sie wissen z.B., daß man insbesondere bei Fern- oder Auslandsverbindungen mit dem Call-by-Call-Verfahren sparen kann. Sie haben sich außerdem bei einigen Call-by-Call-

Anbietern (CbC) erkundigt und die jeweils günstigsten Tarife herausgesucht. Die ersten Einträge in der LCR-Tabelle sehen dann z.B. folgendermaßen aus:

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

Diese Einträge bedeuten, daß alle Verbindungen am Wochenende nach München (oder andere Nummern, die mit '089' beginnen), über den Provider mit der Netzkennzahl '01097' geführt werden. Wochentags wird für diese Rufe in der Zeit zwischen 8:00 Uhr und 18:00 Uhr der Provider mit der Netzkennzahl '01098' verwendet. Auslandsgespräche am Sonntag gehen über den Provider mit der Netzkennzahl '01097'.

Für Fortgeschrittene: LCR mit System

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

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

- Einige Ortsnetze erreichen Sie zwar über eine Vorwahl, trotzdem aber zum normalen Ortstarif. Falls Sie diese Bereiche mit einem allgemeinen Eintrag umgeleitet haben, können Sie die Vorwahlen mit Ortstarif über die Vorwahl Ihrer Telefongesellschaft umleiten (z.B. '01033' für das Netz der Deutschen Telekom). Ein leerer Eintrag für die Netzkennzahl bedeutet ebenfalls „keine Umleitung“.

- Vielleicht geht der größte Teil Ihrer ISDN-Verbindungen in die gleichen Ortsnetze. Wenn die meisten Ihrer Gegenstellen in München liegen, können Sie diese Gegenstellen über einen bestimmten Anbieter erreichen.
- Untersuchen Sie die verschiedenen Tarifzonen. Welche Vorwahlen in welche Zone gehören, können Sie z.B. unter www.billiger-telefonieren.de im Internet nachsehen.

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

So stellen Sie den Least-Cost-Router ein

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

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

Um diese Fragen zu beantworten, gehen Sie so vor:

① Wechseln Sie im *ELSA LANconfig* im Konfigurationsbereich 'Least-Cost-Router' auf die Registerkarte 'Allgemein'.

② Aktivieren Sie die Funktion des Least-Cost-Routers. Der Least-Cost-Router läßt sich nur dann aktivieren, wenn die Zeit des Geräts entweder manuell gesetzt wurde oder wenn schon einmal eine gültige Zeit aus dem ISDN-Netz übermittelt wurde (siehe auch 'Die Uhrzeit für die Auswahl' weiter unten). Schalten Sie den LCR je nach Bedarf für die folgenden Betriebsarten ein:

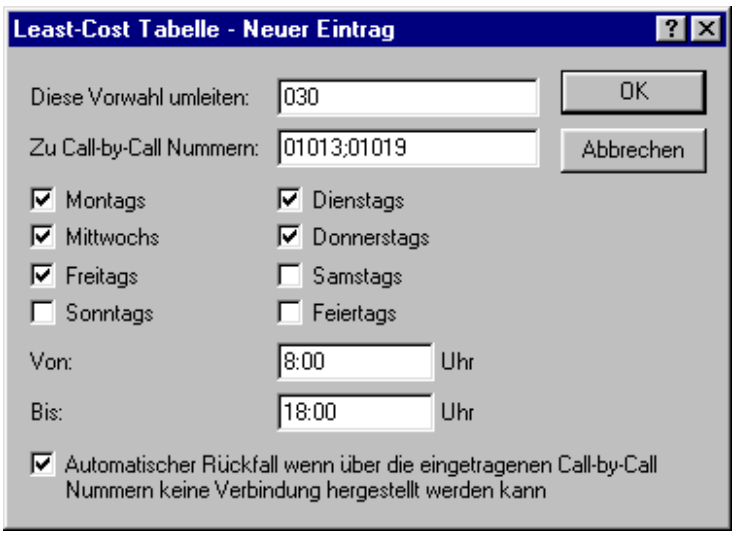
   – Router
   – *LANCAPI*

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

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

   – Welche Vorwahl soll umgeleitet werden?

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



④ Wenn Sie in der LCR-Tabelle auch Einträge für Feiertage gemacht haben, öffnen Sie anschließend die Liste der **Feiertage**. Tragen Sie jeden Feiertag mit dem vollständigen Datum ein (TT.MM.JJJJ).

⑤ Kontrollieren Sie die interne Uhr des Geräts (inkl. Datum), damit der LCR auch zur richtigen Zeit die Umleitungen aktiviert (siehe auch weiter unten, 'Die Uhrzeit für die Auswahl').

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

Die Uhrzeit für die Auswahl

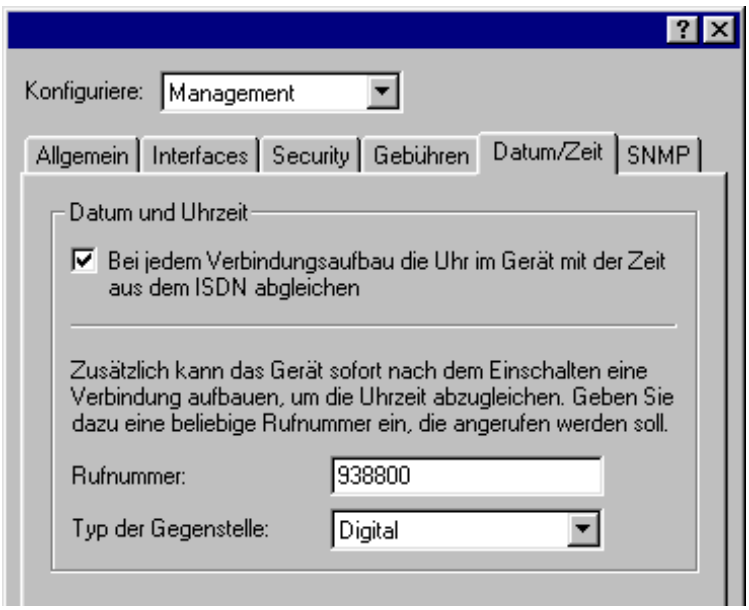
Damit der Least-Cost-Router mit Hilfe der Tabelleneinträge tatsächlich die richtige Verbindung auswählt, muß die interne Uhr im *ELSA LANCOM Wireless* natürlich immer auf dem aktuellen Stand sein. Aber auch hier hilft sich der Router selbst: Er kann entweder

bei jedem Verbindungsaufbau oder bei jedem Einschalten des Geräts die interne Uhrzeit mit der aktuellen Zeit im ISDN-Netz abgleichen.

① Wechseln Sie im *ELSA LANconfig* im Konfigurationsbereich 'Management' auf die Registerkarte 'Datum/Zeit'.

② Aktivieren Sie ggf. die Option für den automatischen Zeitabgleich bei jedem Verbindungsaufbau. Falls Sie die Zeit lieber manuell eintragen möchten, schalten Sie diese Option aus.

③ Beim Ausschalten verliert das Gerät die aktuelle Zeit. Geben Sie die Rufnummer einer beliebigen Gegenstelle ein, wenn das Gerät direkt nach dem Einschalten eine Verbindung aufbauen und so die Zeit mit dem ISDN-Netz abgleichen soll. Wählen Sie dabei aus, ob es sich um eine digitale Gegenstelle (z.B. Mailboxen oder Internet-Provider) handelt oder um eine analoge Gegenstelle (Telefonansage oder Sprachdienst).



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

Anhang

Technische Daten

Hardware-Spezifikationen

Frequenzband:	2400–2483,5 MHz (ISM)
Hardware:	Prozessor: Hitachi SH3, 60 MHz, 4 MByte RAM, 2 MByte Flash-ROM
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)
LAN-Anschluß:	Ethernet IEEE 802.3, 10Base-T (RJ45)
WAN-Anschluß:	ISDN-S_0-Bus (RJ45), entsprechend I.430
Anzeigen/Bedienung:	LEDs für LAN-, WAN- und Gerätestatus
Zertifizierung:	CE-Zeichen (EG), Zulassungen für alle Länder der EU und Schweiz
Sicherheit:	Paßwortschutz, Verschlüsselung (WEP, in Vorb.), IP-Masquerading (NAT), Firewall-Filter
Anschlüsse:	10Base-T, ISDN S0, Power
Garantieservice:	6 Jahre
Support:	über Hotline, ELSA LocalWeb und Internet

Software-Spezifikationen

Funktionsarten:	IP-Router, DHCP-Server, DHCP-Client, DNS-Server, transparentes Bridging zwischen WLAN und LAN, *LANCAPI*-Server, NetBIOS-Spoofing
Netzwerk-Protokolle	ARP, Proxy-ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, NetBIOS über IP
Filter:	Quell- und Zielfilter für Netzwerke, Protokolle und Ports; WAN und LAN getrennt
Gebührenschutz:	maximale Gebührenhöhe oder Verbindungszeit in einem vorggegebenen Zeitraum; festlegbare Security- und Firewall-Funktionen
ISDN-D-Kanal-Protokolle:	DSS1, 1TR6, Punkt-zu-Mehrpunkt- und Punkt-zu Punkt-Konfiguration, automatische Umschaltung zwischen DSS1 und 1TR6 (abschaltbar), CLIP, MSN, EAZ, DDI

ISDN-B-Kanal-Protokolle:	Router: Layer 1: HDLC Kbit/s, HDLC 64 Kbit/s Layer 2: X.75 LAPB, transparent Layer 3: transparent, PPP, synchron und asynchron LZS-Datenkompression Stac, Hi/Fn Kanalabündelung ML-PPP (statisch und dynamisch, inkl. BACP) Skriptverarbeitung für CompuServe CAPI-Betrieb: Layer 1: HDLC Kbit/s, HDLC 64 Kbit/s Layer 2: ISO 776 (X.75 SLP), transparent Layer 3: transparent, T.90NL (mit T.70NL-Kompatibilität)
IP-Masquerading NAT/PAT):	IP-Adreß- und Port-Umsetzung über eine IP-Adresse; statische und dynamische Zuweisung der IP-Adresse über PPP oder DHCP; Maskierung von TCP, UDP, ICMP und FTP; DNS-Forwarding; inverses Masquerading für IP-Dienste aus dem Intranet (z.B. Web-Server)
Management:	TFTP-Konfiguration und Firmware-Upload, SNMP-Management vias SNMP v.1 oder v.2, WAN- und LAN-Zugänge getrennt aktivierbar und konfigurierbar; Konfigurationszugang für WLAN, getrennt schaltbar, Diagnose-Tools, Status-Anzeige *ELSA LANmonitor*
Betriebssicherheit:	Hardware-Watchdogs, regelmäßige Selbsttests, FirmSafe für Remote-Software-Upgrades
Sicherheit:	Paßwortschutz, PAP/CHAP, Verschlüsselung (WEP in Vorb.), IP-Masquerading (NAT/PAT), Firewall-Filter, Schutz über Zugangslisten, WLAN-Verschlüsselung, WLAN-Filter
Statistiken:	LAN- und WAN-Paktezähler, Fehler-, Verbindungs-, Zeit- und Gebührenzähler

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 gefahrentsprechender Anfertigung von Sicherheitskopien eingetreten wäre.

f) Die Garantie bezieht sich lediglich auf den Erstkäufer und ist nicht übertragbar.

g) Gerichtsstand ist Aachen, falls der Erwerber Vollkaufmann ist. Hat der Erwerber keinen allgemeinen Gerichtsstand in der Bundesrepublik Deutschland oder verlegt er nach Vertragsabschluß seinen Wohnsitz oder gewöhnlichen Aufenthaltsort aus dem Geltungsbereich der Bundesrepublik Deutschland, ist unser Geschäftssitz Gerichtsstand. Dies gilt auch, falls Wohnsitz oder gewöhnlicher Aufenthalt des Käufers im Zeitpunkt der Klageerhebung nicht bekannt ist.

h) Es findet das Recht der Bundesrepublik Deutschland Anwendung. Das UN-Kaufrecht gilt im Verhältnis zwischen uns und dem Erwerber nicht.

Konformitätserklärungen

CE

KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

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

Geräteart: **Wireless ISDN / LAN Access Point**
Type of Device:
Typenbezeichnung: ***LANCOM Wireless IL-2***
Product Name:
EG-Baumusterprüfbescheinigungsnummer: D801136L
Registration No.:
Benannte Stelle: **CETECOM ICT Services GmbH**
Notified Body: CE 0682 X

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)
Netzzulassungsrichtlinie (98/515/EG)
Commission Decision (98/515/EC)
ISDN Richtlinie (97/346/EWG)
ISDN Directive (97/346/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
TBR 3: Nov. 1995

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, 9. September 1999
Aachen, 9th September 1999

i.V. Stefan Kriebel
Bereichsleiter Entwicklung
VP Engineering

CE

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**: 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

Index

I

K

L

M

N

O

P

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 IEEE-802.11-Standard. Dieser Standard stellt eine Erweiterung der bereits vohandenen 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 Funktionen der *ELSA LANCOM Wireless*-Geräte. Nach 802.11 arbeitende Funkkarten stellen sich bis auf ein paar Zusatzparameter einem Rechner dar 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 usw.). 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, das heißt, 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*, daß 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, das heißt, 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 Funk-Kanäle 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 auch die benachbarten Kanäle teilweise mitbelegt.

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, kabelgebundenes 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 Basistation 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 Zwang zur Anmeldung 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.

Wichtig: Da im Ad-hoc-Modus keine Anmeldung erforderlich ist, ist dieses Bridging (das sich für den Anwender völlig automatisch vollzieht), nur im Infrastrukturmodus möglich. Der Betrieb eines ELSA LANCOM Wireless im Ad-hoc-Modus ist daher nicht vorgesehen.

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 sogenannte Direct-Sequenced-Spread-Spectrum-Verfahren (DSS), während andere Hersteller zum Teil das Frequency-Hopping-Spread-Spectrum-Verfahren (FHSS) benutzen. Ein Datenaustausch zwischen FHSS- und DSS-basierten 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, Übertragungsmedium, 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.

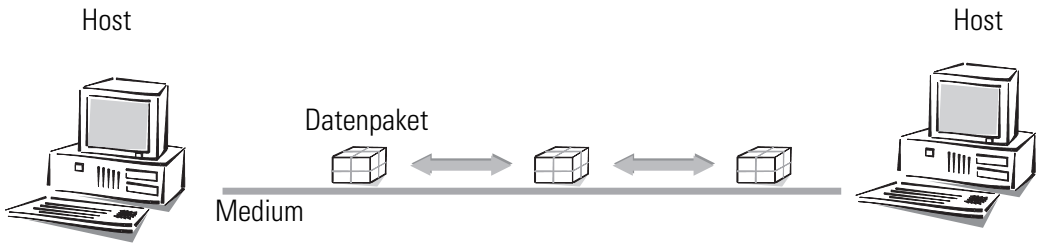
Router

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.

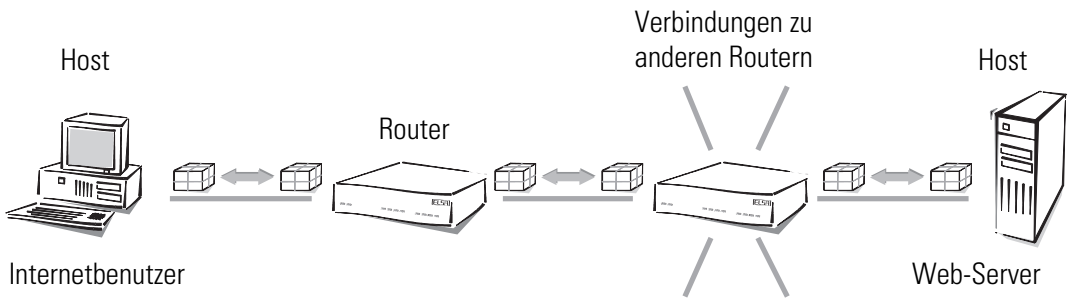
Verbindungsarten

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).



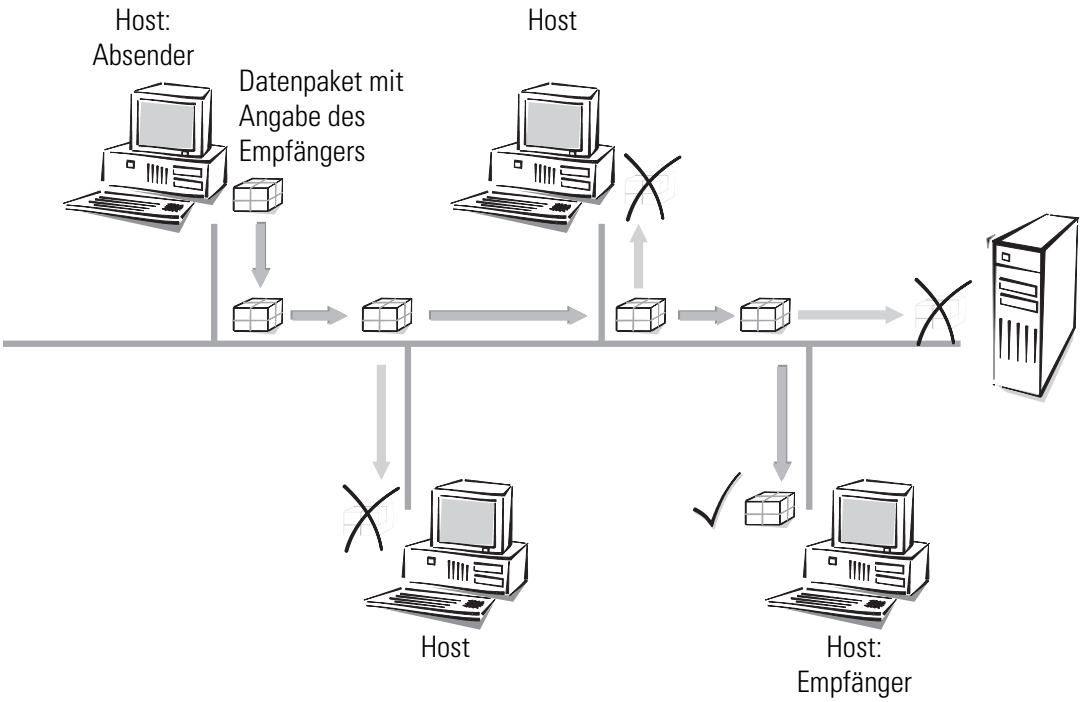
Auch bei einem Zugriff auf das Internet handelt es sich um eine Punkt-zu-Punkt-Verbindung. Die Datenpakete werden zwar vom Host beim Internetbenutzer über mehrere Router zum Host (Server) beim Internet-Provider gesendet, jedes Datenpaket hat jedoch ein ganz bestimmtes Ziel. Die Router geben die Datenpakete 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 Netzwerk (LAN)

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

IP-Adressierung

Paketorientierte Übertragung

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

IP-Adresse

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

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

Netzwerk-Adresse

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

Netzmaske

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

Beispiele:

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

Die gleiche IP-Adresse, jetzt mit anderer Netzmaske:

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

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

Und Sie sehen weiter: Je weniger Bits in der Netzmaske eine Eins enthalten, um so mehr Bits bleiben übrig zur Identifizierung der einzelnen Hosts in einem zusammenhängenden Netzwerk. Während im ersten Beispiel mit der Netzmaske 255.255.255.0 nur 254 verschiedene Adressen vergeben werden können sind es im zweiten Beispiel schon 254x254= 64516 verschiedene Adressen! Die erste und die letzte Ziffer eines Adreßraums sind jeweils reserviert für die Netzwerk-Adresse und die Broadcast-Adresse (Adresse für Pakete an alle Hosts in einem IP-Netz). Bei der Netzmaske 255.255.255.0 sind das die '0' für die Netzwerk-Adresse und die '255' als Broadcast-Adresse.

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

Verwaltung der IP-Adressen

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

Private Address Spaces

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

Diese reservierten IP-Adressen dürfen jedoch **nicht** nach außen (ins Internet) 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; das heißt, ein Anschluß an das Internet ist nur mit zusätzlichen Hilfsmitteln (z.B. IP-Masquerading) möglich.
- Im Internet werden Pakete für diese IP-Adressen nicht geroutet, 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).

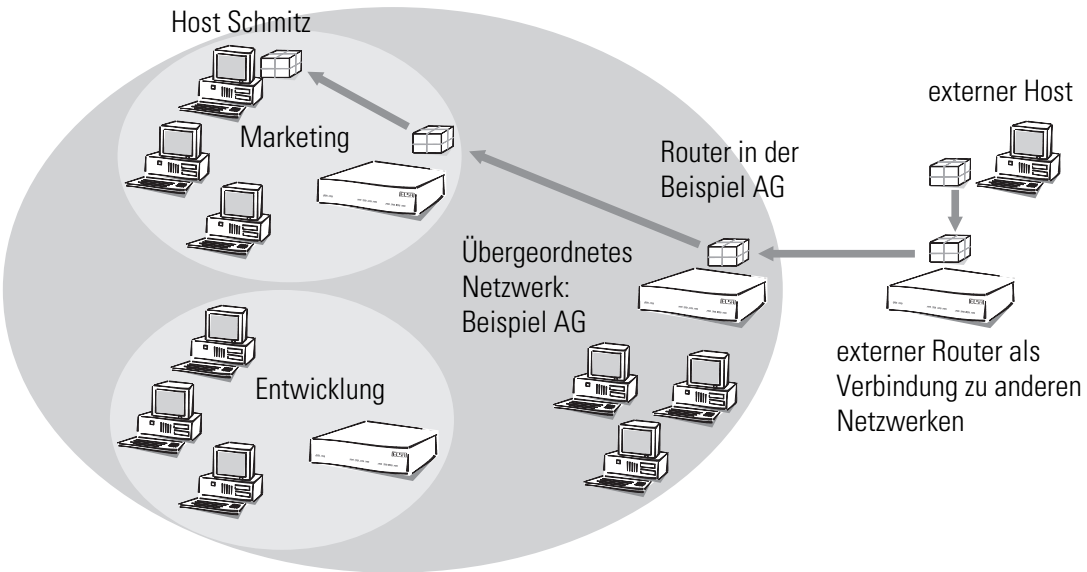
hierarchische IP-Adressen

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 zusammensetzen aus der Adresse der Firma und der Abteilung.

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

① Der Absender gibt dem Paket die Zieladresse „Host Schmitz – Marketing – Beispiel AG".

② Ein externer Router, der die Verbindung zu anderen Netzen herstellt, muß nur wissen, wie er die Beispiel AG erreicht. Sobald er ein Paket mit der Adresse für die Beispiel AG empfängt, leitet er das Paket an den Router weiter, der für die Beispiel AG zuständig ist.

③ Der Router in der Beispiel AG empfängt das Paket und entnimmt der Adresse die Information, daß es für die Beispiel AG gedacht ist. Weil er selber Teil der Beispiel

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

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

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

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

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

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

① Wenn ein Host im Teilnetz der Entwicklung ein Datenpaket an Herrn Schmitz senden möchte, gibt der Absender dem Paket die Zieladresse „Host Schmitz – Marketing – Beispiel AG".

② Der Router in der Entwicklung empfängt das Paket und entnimmt der Adresse die Information, daß es für das Marketing in der Beispiel AG gedacht ist. Weil er selber Teil der Beispiel AG, nicht jedoch der Abteilung Marketing ist, leitet er das Paket weiter an den Router im übergeordneten Netzwerk.

③ Der Router in der Beispiel AG empfängt das Paket und entnimmt der Adresse die Information, daß es für die Beispiel AG gedacht ist. Weil er selber Teil der Beispiel AG ist, betrachtet er die Adresse genauer und sucht nach dem Namen der Abteilung. Dann leitet er das Paket weiter an den Router im Marketing, wo das Paket an den Empfänger weitergeleitet wird.

Erweiterung durch lokale Netze

Medium Access Control

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

LAN und IP-Netz

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

MAC-Adresse

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

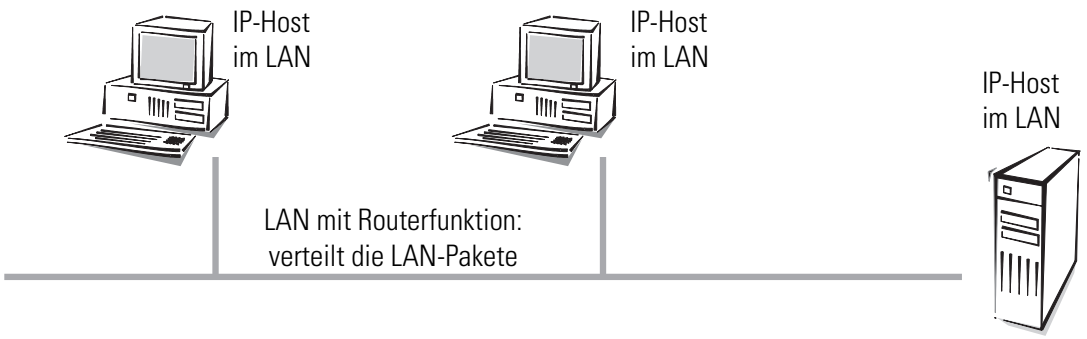
MAC-Adressen sind unabhängig von IP-Adressen. Ein IP-Host, dessen Schnittstelle über ein LAN arbeitet, hat eine IP- und eine MAC-Adresse. Während IP-Adressen durch ihre Postadressen-ähnliche Struktur dafür ausgelegt wurden, das Routen in riesigen IP-Netzen zu vereinfachen, wurden Fingerabdruck-ähnliche 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).

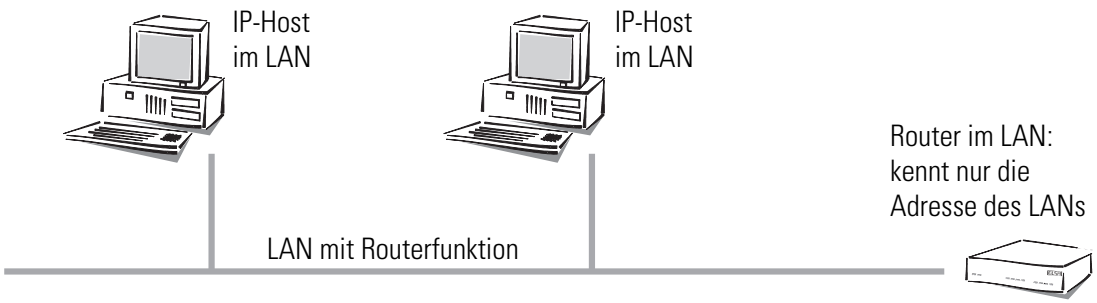
Für einen IP-Host verhält sich ein LAN so, also ob es ein eigenes Netzwerk mit einem Router wäre. Die Hosts geben die Pakete an das LAN ab, das die weitere Verteilung der Datenpakete übernimmt. Für die Kommunikation der Hosts untereinander über das IP-Protokoll dürfen in eim LAN somit nur IP-Adressen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

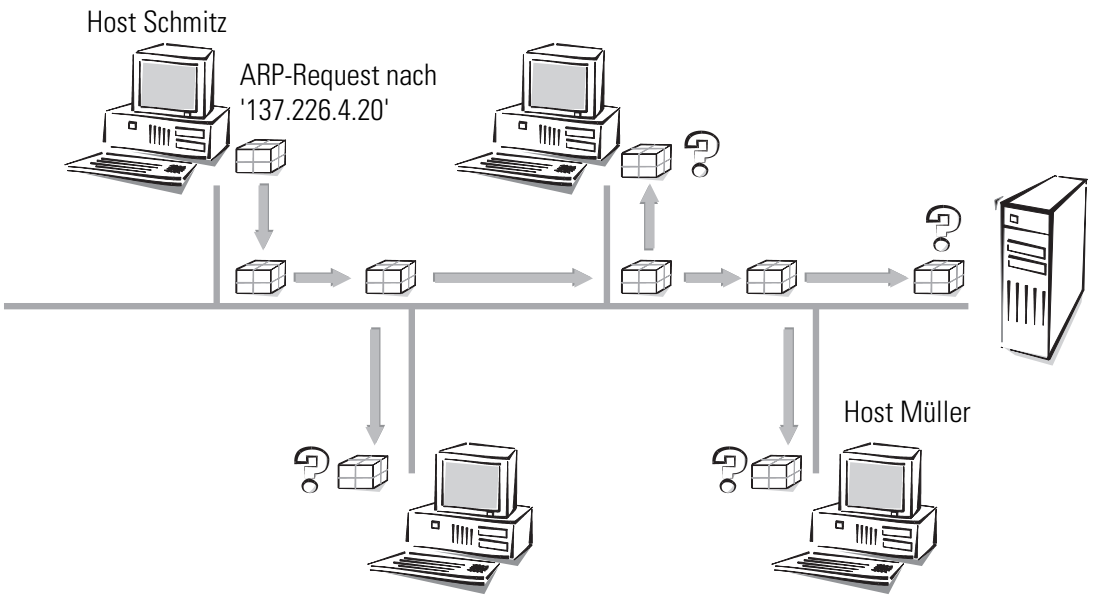
Veranschaulichen wir uns das an einem Beispiel. Stellen wir uns vor, daß die Hosts des Teilnetzes im Marketing über ein LAN verkabelt sind. Die Hosts haben IP-Adressen aus dem Nummernraum '137.226.4.1' bis '137.226.4.254' (die Adressen '137.226.4.0' und '137.226.4.255' sind reserviert), die Netzwerk-Adresse 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.

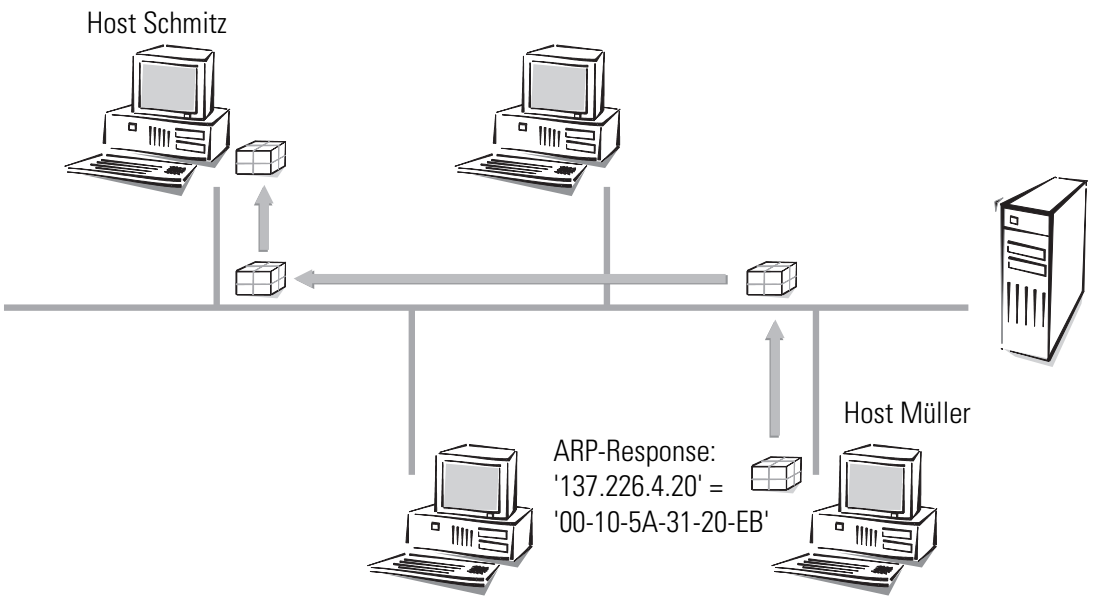
ARP

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-Adressen aller Rechner im gesamten LAN kennen.

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

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.

Symbole

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

Menü-Übersicht

- **Setup**
  - Name
  - WAN-Modul
  - Gebühren-Modul
  - LAN-Modul
  - TCP-IP-Modul
  - IP-Router-Modul
  - SNMP-Modul
  - DHCP-Modul
  - DNS-Modul
  - NetBIOS-Modul
  - Config-Modul
  - WLAN-Modul
  - LANCAPI-Modul
  - LCR-Modul
  - Zeit-Modul
- **Firmware**
  - Versions-Tabelle
  - Tabelle-Firmsafe
  - Modus-Firmsafe
  - Timeout-Firmsafe
  - Firmware-Upload
  - Test-Firmware
- **Status**
  - Verbindung
  - Aktuelle-Zeit
  - Betriebszeit
  - WLAN-Statistik
  - WAN-Statistik
  - LAN-Statistik
  - PPP-Statistik
  - TCP-IP-Statistik
  - IP-Router-Statistik
  - Config-Statistik
  - Queue-Statistik
  - Verbindungs-Statistik
  - Info-Verbindung
  - Layer-Verbindung
  - Ruf-Info-Tabelle
  - Gegenstellen-Statistik
  - S_0-Bus
  - Kanal-Statistik
  - Zeit-Statistik
  - LCR-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**
Verbindung		Zustand der WAN-Strecke
Aktuelle-Zeit		Aktuelle Zeit im Gerät
Betriebszeit		Betriebszeit des Gerätes seit dem letzten Einschalten
S_0-Bus		Zustand der S_0-Schnittstelle
WAN-Statistik		Anzeige der WAN-Statistiken
LAN-Statistik		Statistiken des Netzwerk-Bereichs
WLAN-Statistik		Statistiken des Funk-Netzwerk-Bereichs
PPP-Statistik		Statistiken des Point-to-Point-Protokolls
Bridge-Statistik		Statistiken des Bridge-Bereichs
TCP-IP-Statistik		Statistiken aus dem TCP/IP-Bereich
IP-Router-Statistik		Statistiken aus dem IP-Router
Config-Statistik		Statistiken der Remote-Konfiguration
Queue-Statistik		Statistiken über die Pakete in den Queues der einzelnen Module
Verbindungs-Statistik		Verbindungs-Informationen für jedes Interface
Info-Verbindung		Informationen zur letzten Verbindung für jedes Interface
Layer-Verbindung		Informationen über das verwendete B-Kanal-Protokoll für jedes Interface
Ruf-Info-Tabelle		Informationen über die letzten 10 angekommenen Rufe
Gegenstellen-Statistik		Statistik über die letzten 10 Verbindungen
Kanal-Statistik		Informationen über den Zustand der einzelnen Kanäle. Bei *ELSA LANCOM Wireless L-2* auch Informationen über die a/b-Ports.
Zeit-Statistik		Informationen aus dem Zeit-Modul

Status		Fortlaufende Statusanzeigen
LCR-Statistik		Informationen aus dem Least-Cost-Router
PCMCIA-Status		Informationen zum PCMCIA-Status
Werte löschen		Alle Werte außer Tabellen der untergeordnet. Statistik löschen

Status/Verbindung

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

/Verbindung		Fortlaufende Statusanzeigen
Verbindung		CH01: Bereit; CH02: Bereit

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/S_0-Bus

Unter diesem Menüpunkt wird der aktuelle Zustand der S_0-Schnittstelle angezeigt. Die Statistik hat den folgenden Aufbau:

/S_0-Bus		Fortlaufende Statusanzeigen
D-Info		Übersicht über den Zustand eines D-Kanals.
D2-Statistik		Aufschlüsselung der Layer-2-Informationen des D-Kanals für die einzelnen B-Kanäle.

D-Info

Diese Tabelle zeigt allgemeine D-Kanal-Informationen:

Kanal	Kennzeichnung des B-Kanals.
Protokoll	D-Kanal-Protokoll. Entweder das in der Interface-Tabelle fest eingestellte Protokoll oder das bei der Einstellung 'Auto' am ISDN-Anschluß detektierte Protokoll.

Layer-2	Aktivierung der Schicht 2 des D-Kanals ('Ja' oder 'Nein')
TEI	TEI zugewiesen ('Ja' oder 'Nein')
S_0-Aktivierung	Zustandsanzeige der Aktivierung ('Ja' oder 'Nein')

D2-Statistik

Diese Tabelle zeigt Layer-2-Informationen zu den einzelnen B-Kanälen:

Kanal	Kennzeichnung des B-Kanals.
TEI	Von der Vermittlungsstelle zugewiesener **T**erminal **E**quipment **I**dentifier.
L2-Aktivierung	Aktivierung der Schicht 2 des D-Kanals ('Ja' oder 'Nein').
Verbindungen	Anzahl der Verbindungen, die über die angezeigte TEI abgewickelt wurden.

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 WAN empfangener Broadcasts
LAN-Tx-Multicasts		Anzahl vom WAN empfangener Multicasts
LAN-Tx-Unicasts		Anzahl vom WAN empfangener Unicasts
LAN-Tx-Verworfen		Anzahl vom LAN verworfener Pakete
LAN-Wiederholungen		Anzahl der Pakete, die erst nach einer Wiederholung zugestellt werden konnten
LAN-Mehrfachwieder-holungen		Anzahl der Pakete, die erst nach mehreren Wiederholungen zugestellt werden konnten

LAN-bereit		Erfolgreich Initialisierung der Funk-Netzwerkkarte
Stationstabelle		Anzeige der momentan angemeldeten Mobil-Stationen.
WLAN-Parameter		Parameter des Funk-Netzwerks

Stationstabelle Diese Tabelle zeigt Informationen zu den einzelnen Mobilstationen:

Kanal	Kennzeichnung des B-Kanals.
Index	zeigt die Reihenfolge der Einträge in der Tabelle an.
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 wird. 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.

WLAN-Parameter Diese Tabelle zeigt die aktuellen Parameter des Funk-Netzwerks an:

BSSID		Zahlenwert zur Unterscheidung von Funkzellen, numerische Umsetzung der WLAN-Domain. Im Infrastrukturmodus immer gleich der MAC-Adresse der Basis-Station
PHY-Kanal		Der von der Basis-Station momentan benutzte Funkkanal.
Regulatory Domain		Der Frequenzbereich, den die Firmware der WLAN-Karte zuläßt
PHY-Type		Verwendetes Funkverfahren, steht fest auf DSSS.

Status/WAN-Statistik

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

Die WAN-Statistik wird interfacebezogen geführt, das heißt, für jedes Interface existiert eine eigene Statistik, in welcher übertragene Daten und Fehler registriert werden. Das Menü **Status/WAN-Statistik** besitzt folgenden Aufbau:

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

Byte-Transport-Statistik

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

Ifc	CRx-Bytes	Rx-Bytes	Tx-Bytes	CTx-Bytes
Ch01	0	0	0	0
Ch02	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

Paket-Transport-Statistik

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

Ifc	Rx	Tx-gesamt	Tx-normal	Tx-gesichert	Tx-urgent
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

Fehler-Statistik

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

Ifc	Rx-L1-F.	Rx-L2-F.	Rx-L3-F.	Stack-F.	Tx-Fehler
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

Durchsatz-Statistik

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

Ifc	Rx aktuell	Tx aktuell	Rx gemittelt	Tx gemittelt
Ch01	0	0	0	0
Ch02	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

Status/LAN-Statistik

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

/LAN-Statistik	Fortlaufende Statusanzeigen	
LAN-Rx-Pakete		Anzahl empfangener Datenpakete
LAN-Tx-Pakete		Anzahl gesendeter Datenpakete
LAN-Rx-Fehler		Anzahl fehlerhaft empfangener Datenpakete
LAN-Tx-Fehler		Anzahl fehlerhaft gesendeter Datenpakete
LAN-Stack-Fehler		Anzahl Pakete ohne passendes Empfangsmodul (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 (Daten-übertragung möglich). Entspricht der 'Link'-LED am Gerät.
LAN-Rx-Bytes		Anzahl vom LAN empfangener Zeichen
LAN-Tx-Bytes		Anzahl zum LAN gesendeter Zeichen
LAN-Rx-Broadcasts		Anzahl vom LAN empfangener Broadcast-Pakete
LAN-Rx-Multicasts		Anzahl vom LAN empfangener Multicast-Pakete
LAN-Rx-Unicasts		Anzahl vom LAN empfangener direkt adressierter Pakete
WAN-Rx-Broadcasts		Anzahl vom WAN empfangener Broadcasts
WAN-Rx-Multicasts		Anzahl vom WAN empfangener Multicasts
WAN-Rx-Unicasts		Anzahl vom WAN empfangener Unicasts
Werte löschen		LAN-Statistik löschen

Status/PPP-Statistik

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

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

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

Zustände

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

Ifc	Phase	LCP	IPXCP	IPCP	CCP
Ch01	DEAD	Initial	Initial	Initial	Initial
Ch02	DEAD	Initial	Initial	Initial	Initial

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

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

Status/PPP-Statistik/LCP-Statistik

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

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

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

Status/PPP-Statistik/PAP-Statistik

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

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

Status/PPP-Statistik/CHAP-Statistik

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

Rx-Verworfen	Anzahl verworfener CHAP-Pakete
Rx-Challenge	Anzahl empfangener CHAP-Challenge-Pakete
Rx-Response	Anzahl empfangener CHAP-Response-Pakete
Rx-Success	Anzahl empfangener CHAP-Success-Pakete

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

Status/PPP-Statistik/IPCP-Statistik

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

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

Status/PPP-Statistik/CBCP-Statistik

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

Rx-Request	Anzahl empfangener CBCP-Request-Pakete
Rx-Response	Anzahl empfangener CBCP-Response-Pakete
Rx-verworfen	Anzahl verworfener CBCP-Pakete
Rx-Ack	Anzahl empfangener CBCP-Acknowledge-Pakete
Tx-Request	Anzahl gesendeter CBCP-Request-Pakete

Tx-Response	Anzahl gesendeter CBCP-Response-Pakete
Tx-Ack	Anzahl gesendeter CBCP-Acknowledge-Pakete
Werte löschen	IPCP-Statistik löschen

Status/PPP-Statistik/CCP-Statistik

In der Statistik zum CCP (**C**ompression **C**ontrol **P**rotocol) finden Sie die während der PPP-Verhandlung ausgetauschten Pakete zur Datenkompression.

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

Status/PPP-Statistik/ML-Statistik

Die Statistik zum MLPPP gibt hauptsächlich Auskunft darüber, wie bei einer gebündelten PPP-Verbindung die Gegenstelle die einzelnen Pakete behandelt.

Buendel-Verb	Anzahl der Verbindungen, die MLPPP verwendet haben
Rx-Seq-Verlust	Anzahl der Pakete, bei denen ein Fehler in der Reihenfolge der Sequenznummern aufgetreten ist.
Rx-Seq-Wiederholung	Anzahl der Pakete, die der reihenfolge der Sequenznummern nach verspätet eingetroffen sind.
Rx-Mrru-Ueberlauf	Anzahl der Pakete, bei denen nach dem Zusammenbauen eine Verletzung der in der PPP-Verhandlung ausgehandelten MRRU (maximal received reassembled unit) festgestellt wurde.
Rx-Header-Fehler	Anzahl der Pakete mit fehlerhaftem Header.
Rx-verworfen	Anzahl aller verworfenen MLPPP-Pakete.
Rx-Frag-Start	Anzahl der Pakete mit gesetztem Start-Flag (erster Teil eines fragmentierten Pakets).
Rx-Frag-Mid	Anzahl der Pakete mit gesetztem Mid-Flag (mittlerer Teil eines fragmentierten Pakets).
Rx-Frag-Ende	Anzahl der Pakete mit gesetztem End-Flag (letzter Teil eines fragmentierten Pakets).
Rx-unfragmentiert	Anzahl der Pakete mit gesetztem Start- und End-Flag (unfragmentierte Pakete).
Werte-löschen	ML-Statistik löschen

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

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

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

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

Die beiden Untermenüs besitzen jeweils den gleichen Aufbau:

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

In der Tabelle LCP sind für jeden Kanal gesondert aufgeführt:

MRU	**M**aximum **R**eceive **U**nit, kennzeichnet die maximale Paketgröße, die die Gegenstelle empfangen kann
ACCM	**A**synchron **C**ontrol **C**haracter **M**ap, kennzeichnet die Zeichen im asynchronen Datenstrom, die als Steuerzeichen interpretiert werden
Authent.	verwendetes Authentifizierungsverfahren (PAP/CHAP)
Callback	Art der Rückruf-Verhandlung

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

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

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
NetBIOS-Statistik		Statistiken aus dem NetBIOS-Modul
DNS-Statistik		Statistiken aus dem DNS-Server
Werte löschen		TCP/IP-Statistiken löschen

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

Status/TCP-IP-Statistik/ARP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

ARP-LAN-Rx	Anzahl vom LAN empfangener ARP-Anfragen und -Antworten
ARP-LAN-Tx	Anzahl zum LAN gesendeter ARP-Anfragen und -Antworten
ARP-LAN-Fehler	Anzahl vom LAN fehlerhaft empfangener ARP-Anfragen
ARP-WAN-Rx	Anzahl vom WAN empfangener ARP-Anfragen und -Antworten
ARP-WAN-Tx	Anzahl zum WAN gesendeter ARP-Anfragen und -Antworten
ARP-WAN-Fehler	Anzahl vom WAN fehlerhaft empfangener ARP-Anfragen
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-Fragmentierungs-Fehler	Anzahl vom LAN fehlerhaft empfangener Fragmentierungen
IP-LAN-Fragmentierungen	Anzahl vom LAN empfangener Fragmentierungen
IP-LAN-Fragmentierung-erzwungen	Anzahl vom LAN erzwungener Fragmentierungen
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-Fragmentierungs-Fehler	Anzahl vom WAN fehlerhaft empfangener Fragmentierungen
IP-WAN-Fragmentierungen	Anzahl vom WAN empfangener Fragmentierungen
IP-WAN-Fragmentierung-erzwungen	Anzahl vom WAN erzwungener Fragmentierungen

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-Acknowleges
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-Decline	Anzahl empfangener Decline-Messages
DHCP-Rx-Inform	Anzahl empfangener Inform-Messages
DHCP-Rx-Release	Anzahl empfangener Release-Messages
DHCP-Tx-Offer	Anzahl gesendeter Offer-Messages
DHCP-Tx-Ack.	Anzahl bestätigter DHCP-Pakete
DHCP-Tx-Nak	Anzahl nicht bestätigter DHCP-Pakete
DCHP-Server-Fehler	Anzahl empfangener DHCP-Pakete, die nicht für diesen Server bestimmt waren
DHCP-Zugewiesen	Anzahl aktuell zugewiesener Adressen
DHCP-MAC-Konflikte	Anzahl abgelehnter Zuweisungen aufgrund belegter IP-Adressen
Tabelle-DHCP	Tabelle mit den Zuweisungen von IP-Adressen zu MAC-Adressen
Server-Flags	Ein/Ausschalten der Server-Flags
Werte löschen	DHCP-Statistik löschen

Tabelle-DHCP

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

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

Status/TCP-IP-Statistik/NetBIOS

Über das Menü /Status/TCP-IP-Statistik/NetBIOS-Statistik können zusätzliche Informationen über das NetBIOS-Modul erhalten werden. Dieses Menü hat den folgenden Aufbau:

LAN-Rx, WAN-Rx		Anzahl der NetBIOS-Pakete, die vom LAN bzw. WAN empfangen wurden
LAN-Tx, WAN-Tx		Anzahl der NetBIOS-Pakete, die auf das LAN bzw. WAN gesendet wurden
Registrierungen		Anzahl der erfolgten Namenregistrierungen
Konflikte		Anzahl der festgestellten Namenskonflikte. Da das NetBIOS-Modul nur eine Art schwarzes Brett ist, an dem jeder Rechner seinen Namen anheftet, überprüft es auch nicht die Konsistenz der Daten. Daher wird der Zähler nur erhöht, wenn ein Host selbst einen Konflikt festgestellt hat und dieses über einen Broadcast im Netz bekannt macht
Freigaben		Anzahl der erfolgten Namensfreigaben
Erneuerungen		Anzahl der erfolgten Namenserneuerungen (Refresh)
Timeouts		Anzahl der durch Alterung herausgefallenen Namen
B-Knoten		Anzahl der gerade aktiven B-Knoten (Broadcast) im Netz
P-Knoten		Anzahl der gerade aktiven P-Knoten (Peer-to-Peer) im Netz
M-Knoten		Anzahl der gerade aktiven M-Knoten (Mixed-Mode) im Netz
W-Knoten		Anzahl der gerade aktiven W-Knoten (Hybrid) im Netz

B-Knoten Broadcast-Knoten. Ein B-Knoten führt die Namenverhandlung ausschließlich über Broadcasts durch. Ein solcher Rechner ist über eine Routerverbindung hinweg nicht zu sehen, da Broadcasts nicht geroutet werden dürfen.

P-Knoten Point-To-Point-Knoten. Ein P-Knoten benötigt zur Namensverhandlung einen NetBIOS-Nameserver (NBNS) sowie zur Datagrammübermittlung über einen Router hinweg einen NetBIOS-Datagram-Distribution-Server (NBDD).

M-Knoten Mixed-Knoten. Dieser Knoten-Typ stellt eine Mischung aus B- und P-Knoten dar. Im lokalen Netz verhält er sich wie ein B-Knoten, ist der gewünschte Kommunikationspartner nicht im lokalen Netz zu finden, so wird versucht ihn über eine NBNS-Anfrage aufzulösen (P-Knoten-Verhalten).

W-Knoten Diese Art von Knoten ist nach RFC nicht zulässig, trotzdem hat Microsoft sie als Hybrid-Knoten eingeführt.

Status/TCP-IP-Statistik/DNS-Statistik

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

LAN-Rx		Anzahl der DNS-Pakete, die vom LAN empfangen wurden
LAN-Tx		Anzahl der DNS-Pakete, die zum LAN gesendet wurden
WAN-Rx		Anzahl der DNS-Pakete, die vom WAN empfangen wurden
WAN-Tx		Anzahl der DNS-Pakete, die zum WAN gesendet wurden
Forwarded		Anzahl der Anfragen, die nicht beantwortet werden konnten und daher über den Forwarding-Mechanismus weitergeleitet wurden
Fehler		Anzahl von ungültigen Anfragen
DNS-Zugriffe		Gibt an, wie viele Namen aus der DNS-Tabelle aufgelöst wurden
DHCP-Zugriffe		Gibt an, wie viele Namen aus der DHCP-Tabelle aufgelöst wurden
NetBIOS-Zugriffe		Gibt an, wie viele Namen aus den NetBIOS-Tabellen aufgelöst wurden
Filter		Anzahl der über die Filtertabelle gefilterten DNS-Pakete
Hit-Liste		In dieser Tabelle tauchen die 16 häufigsten Anfragen auf. Diese können dann unter Umständen über die Filterliste abgeblockt werden.

Die Hitliste hat den folgenden Aufbau:

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

Die einzelnen Felder dieser Liste haben die folgende Bedeutung:

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

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

Status/IP-Router-Statistik

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

/IP-Router-Statistik		Statistiken aus dem IP-Router-Bereich
IPr-LAN-Rx		Anzahl vom LAN zu routender Datenpakete
IPr-LAN-Tx		Anzahl zum LAN gerouteter Datenpakete
IPr-LAN-lokales-Routing		Anzahl vom LAN emfangener und zum LAN gerouteter Pakete
IPr LAN-Netzwerk-Fehler		Anzahl LAN-Pakete, die nicht geroutet wurden
IPr-LAN-Routing-Fehler		Anzahl LAN-Pakete, die zu einem anderen Router müssen
IPr-LAN-TTL-Fehler		Anzahl LAN-Pakete mit einem abgelaufenen Time-to-Live-Wert
IPr-LAN-Filter		Anzahl der über die Filtertabelle gefilterten LAN-Pakete
IPr-LAN-verworfen		Anzahl der verworfenen LAN-Pakete
IPr-WAN-Rx		Anzahl vom WAN zu routender Datenpakete
IPr-WAN-Tx		Anzahl zum WAN gerouteter Datenpakete
IPr-WAN-Netzwerk-Fehler		Anzahl WAN-Pakete, die nicht geroutet wurden
IPr-WAN-TTL-Fehler		Anzahl WAN-Pakete mit einem abgelaufenem Time-to-Live-Wert
IPr-WAN-Filter		Anzahl der über die Filtertabelle gefilterten WAN-Pakete
IPr-WAN-verworfen		Anzahl der verworfenen WAN-Pakete
IPr-WAN-Typ-Fehler		Anzahl der Pakete vom WAN ohne IP-Router-Kennung
IPr-ARP-Fehler		Anzahl der nicht erfolgreichen Zugriffe auf den ARP-Cache
Werte löschen		IP-Router-Statistik löschen
Aufbau-Tabelle		Tabelle der letzten 20 Pakete, die eine Verbindung erforderten
Protokoll-Tabelle		Tabelle über geroutete Pakete, protokollabhängig aufgestellt
RIP-Statistik		Statistiken aus dem IP/RIP-Bereich

Aufbau-Tabelle

In der **Aufbau-Tabelle** sind die letzten 20 Einträge, die Informationen über die Systemzeit, Ziel-Adresse und Quell-Adresse, IP-Protokoll, Ziel-Port und Quell-Port der Datenpakete enthalten, die zu einem Verbindungsaufbau führen sollten.

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

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

Als 'Systemzeit' wird entweder die Betriebszeit des Geräts angezeigt oder die Systemzeit des ISDN-Netzes (falls diese vom ISDN-Anschluß zur Verfügung gestellt wird). Die Ziel- und Quell-Adressen sind jeweils IP-Adressen, das Protokoll kann zum Beispiel auf tcp, udp oder ähnliches hinweisen und die Ziel- und Quell-Ports definieren näher die betroffenen Dienste (Telnet z.B. über TCP und Z-Port. 23, Nameserver über UPD und Z-Port 53).

Protokoll-Tabelle

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

Eine Protokoll-Tabelle kann wie folgt aussehen:

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

Status/IP-Router-Statistik/RIP-Statistik

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

RIP-Rx	Anzahl empfangener IP-RIP-Pakete
RIP-Request	Anzahl empfangener IP-RIP-Request-Pakete
RIP-Response	Anzahl empfangener IP-RIP-Response-Pakete
RIP-verworfen	Anzahl verworfener IP-RIP-Pakete
RIP-Fehler	Anzahl fehlerhafter IP-RIP-Pakete
RIP-Eintrag-Fehler	Anzahl fehlerhafter Einträge in IP-RIP-Paketen
RIP-Tx	Anzahl gesendeter IP-RIP-Pakete
Tabelle-RIP	Routing-Tabelle der durch RIP-Broadcast gelernten Routen
Werte löschen	IP-RIP-Statistik löschen

Tabelle-RIP

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

Eine IP-RIP-Tabelle kann wie folgt aussehen:

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

Status/Config-Statistik

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

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

Status/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
WAN-Queue-Pakete		Anzahl belegter Puffer
ARP-Query-Queue-Pakete		Anzahl der ARP-Pakete in der Query-Queue

/Queue-Statistik	Statistiken über die Queue	
ARP-Queue-Pakete	0	Anzahl der ARP-Pakete in der normalen Queue
IP-Queue-Pakete	0	Anzahl der IP-Pakete in der normalen Queue
IP-Urgent-Queue-Pakete	0	Anzahl der IP-Pakete in der gesicherten Queue
ICMP-Queue-Pakete	0	Anzahl der ICMP-Pakete
TCP-Queue-Pakete	0	Anzahl der TCP-Pakete
TFTP-Queue-Pakete	0	Anzahl der TFTP-Pakete
SNMP-Queue-Pakete	0	Anzahl der SNMP-Pakete
Prot-Heap-Pakete	0	Anzahl der Prot-Heap-Pakete
IPR-Queue-Pakete	0	Anzahl der Pakete, die noch durch den IP-Router bearbeitet werden sollen.
DHCP-Server-Queue-Pakete	0	Anzahl der Pakete in der Empfangs-Queue des DHCP-Servers.
IPR-RIP-Queue-Pakete	0	Anzahl der Pakete in der Empfangs-Queue des IP-RIP-Moduls (für RIP-Anfragen, RIP-Propagierungen ...).
DNS-Sende-Queue	0	Anzahl der Pakete, die zu DNS- oder NBNS-Servern weitergeleitet werden sollen.
DNS-Empfangs-Queue	0	Anzahl der Pakete, die von DNS- oder NBNS-Servern kommen und an den Host weitergeleitet werden sollen.
IP-Masq. Sende-Queue	0	Anzahl der Pakete, die maskiert versendet werden sollen (ins Internet).
IP-Masq. Empfangs-Queue	0	Anzahl der Pakete, die aus dem Internet empfangen wurden und demaskiert werden müssen.
WLAN-Management-Heap-Pakete	0	Anzahl der im Puffer verfügbaren Pakete.

Status/Verbindungs-Statistik

Über dieses Menü können die Verbindungszeiten, alle angefallene Gebühren und weitere nützliche Informationen über die Auslastung des ISDN-Anschlusses angezeigt werden.

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

Ifc	Verbindung	aktiv	passiv	Fehler	Verbindungs-Zeit	Gebuehren
Ch01	0	0	0	0	Keine Verbindung	0
Ch02	0	0	0	0	Keine Verbindung	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
Verbindung	gibt die Anzahl der Verbindungen auf dem jeweiligen Kanal an.
aktiv	gibt die Anzahl der aktiven Verbindungsaufbauten für den Kanal an.
passiv	gibt die Anzahl der Verbindungen durch eingegangene Rufe für den Kanal an.
Fehler	gibt die Anzahl der Verbindungsfehler an.
Verbindungs-Zeit	gibt die Zeit an, seit der die aktuelle Verbindung besteht. Besteht keine Verbindung, so wird „Keine Verbindungen." ausgegeben.
Gebühren	gibt die Zahl der Gebühren der aktuellen Verbindung an. Dieser Wert wird bei einem erneuten Verbindungsaufbau wieder auf Null gesetzt.

Die gesamten angefallenen Gebühren werden nicht unmittelbar angezeigt. Es wird jedoch intern eine Summierung der Gebühren durchgeführt, um das Gebührenbudget verwalten zu können (siehe auch **Setup/Gebühren-Modul**).

Status/Info-Verbindung

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

Ifc	Status	Mode	Rufnummer	Gerätename	B1-HZ	B2-HZ
Ch01 Ch02	Bereit Bereit				0 0	0 0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
Status	gibt den Zustand der jeweiligen Verbindung an. Mögliche Werte sind: **Initialisierung**, **Setup-WAN**, **Bereit**, **Anwahl**, **Anliegender-Ruf**, **Protokoll**, **Verbindung**, **Rückruf** sowie **Bündelung** und **Reserviert**. Der Status **Bündelung** wird im Display (nur *ELSA LANCOM Wireless IL-2*) durch Anfügen von „**/2**" in Spalte 15 und 16 der zugehörigen Displayzeile ebenfalls angezeigt. **Bündelung** erscheint für das zweite Interface, wenn entweder auf dem ersten Interface eine Bündelverbindung aktiviert wurde oder eine Festverbindung mit zwei B-Kanälen eingestellt wurde. **Reserviert** wird das zweite Interface, wenn auf dem ersten B-Kanal eine Verbindung besteht und die Y-Verbindung deaktiviert wurde.
Mode	gibt die Art des Aufbaus wieder. Möglich sind: **Akt.** (aktiver Verbindungsaufbau = Anwahl) **Pas.** (passiver Verbindungsaufbau = Anruf) **RR** (Aufbau durch Rückruf)
Rufnummer	gibt die Rufnummer der Gegenstelle aus der Namenliste an.

Gerätename	gibt den logischen Namen der Gegenstelle an (sofern dieser auflösbar ist). Der Gerätename wird ebenfalls auf dem Display in der entsprechenden Displayzeile mit angezeigt, sobald eine logische Verbindung besteht.
B1-HZ	gibt die Haltezeit (Short-Hold-Zeit) der Verbindung an.
B2-HZ	gibt die Haltezeit (Short-Hold-Zeit) für gebündelte Kanäle dieser Verbindung an.

Status/Layer-Verbindung

Der Menüpunkt **Status/Layer-Verbindung** enthält für jedes verfügbare Interface Informationen über das auf dem jeweiligen Interface benutzte B-Kanal-Protokoll. Die Einträge dieser Tabelle entsprechen denen der Layerliste **Setup/WAN-Modul/Layer-Liste** im WAN-Modul. Zusätzlich existiert noch ein Eintrag für das Interface selbst. Das Menü hat folgendes Aussehen:

Ifc	Layername	Encaps	Lay-3	Lay-2	L2-Opt.	Lay-1
Ch01 Ch02	DEFAULT PPPHDLC	ETHER TRANS	ELSA TRANS	X.75ELSA PPP	compr. Keine	HDLC64K HDLC64K

Status/Ruf-Info-Tabelle

In dieser Tabelle werden die letzten zehn angekommenen Rufe angezeigt, und zwar unabhängig davon, ob der Router den Ruf angenommen hat oder nicht.

Dadurch ist es z.B. möglich, beim Betrieb an einer TK-Anlage herauszufinden, welche interne MSN verwendet wird. Die Tabelle hat den folgenden Aufbau:

Systemzeit	Ifc	CLIP-Anrufer	Wahl-Anrufer	Dienst	B-Kanal
0T; 00:20:57	S_0	5678	1234	HDLC64K	2
0T; 00:20:46	S_0	4321	1234	HDLC64K	1
0T; 00:19:47	S_0	4321	1234	HDLC64K	1
0T; 00:11:33	S_0	5678	1234	HDLC64K	1
0T; 00:01:13	S_0	4321	1234	HDLC64K	2
0T; 00:01:02	S_0	4321	1234	HDLC64K	1
0T; 00:00:06	S_0	5678	1234	HDLC64K	1

Die Einträge haben die folgende Bedeutung:

Systemzeit	Zeitpunkt, zu dem der Ruf ankam. Dabei wird entweder die Betriebszeit des Geräts angezeigt oder die Systemzeit des ISDN-Netzes (falls diese vom ISDN-Anschluß zur Verfügung gestellt wird).
Ifc	Bezeichnet das zugehörige Interface.
CLIP-Anrufer	Die Rufnummer (CLIP) des Anrufers

Wahl-Anufer	Die vom Anrufer gewählte MSN/EAZ
Dienst	Hier ist der vom Anrufer gewünschte Dienst eingetragen. Mögliche Werte sind HDLC64K, HDLC56K und unbekannt. Ein analoger Ruf wird hier also als unbekannt angezeigt. *LANCOM Office*-Router können zusätzlich die Werte A-3kHz (analog 3kHz), Sprache (für normale Sprachübertragung) und Fax-G2/3 (für analoge Faxübertragungen nach Gruppe 2 oder 3) angezeigt werden.
B-Kanal	Hier wird der benutzte B-Kanal eingetragen. Ein Wert von 0 bedeutet, daß alle Kanäle bereits belegt sind, es sich also um ein Anklopfen handelt.

Ein Tip für den Fall, daß ein Router in einer Nebenstellenanlage verwendet wird: Nach einem Anruf mit einem beliebigen ISDN-Endgerät unter der Nummer des ISDN-Busses, wird unter 'Wahl-Anrufer' genau die MSN/EAZ angezeigt, die im Router an der Stelle / Setup/WAN-Modul/Router-Interface-Liste/MSN-EAZ eingetragen werden muß, damit ein Ruf von außen korrekt angenommen werden kann.

Status/Gegenstellen-Statistik

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

Die Tabelle hat den folgenden Aufbau:

Verb.-Start	Gegenstelle	Anw.	Ifc	Verb.-Zeit	Gebühren
0T; 00:20:57	BERLIN	Akt.	Ch01	50	5
0T; 00:20:46	CHEMNITZ	Pas.	Ch02	230	10

Die Einträge haben die folgende Bedeutung:

Verbindungsstart	Zeit, zu der die Verbindung zustande gekommen ist. Dabei wird entweder die Betriebszeit des Geräts angezeigt oder die Systemzeit des ISDN-Netzes (falls diese vom ISDN-Anschluß zur Verfügung gestellt wird).
Gegenstelle	Logischer Gegenstellenname
Anwahl	Art des Verbindungsaufbaus: Akt. – die Verbindung wurde aktiv vom Gerät aufgebaut Pas. – das Gerät wurde angerufen RR – das Gerät hat die Gegenstelle zurückgerufen
Ifc	Interface, auf dem die Verbindung zustande gekommen ist (Ch01, Ch02).
Verbindungszeit	Dauer der Verbindung in Sekunden
Gebühren	Für diese Verbindung angefallene Gebühren in Einheiten

Eine Verbindung bleibt mindestens für die Dauer ihres Bestehens in der Tabelle. Jede neue Verbindung füllt die Tabelle von oben her auf. Sollte eine bestehende Verbindung

als unterster Eintrag der Tabelle stehen, so wird ggf. eine bereits abgebaute Verbindung stattdessen aus der Tabelle entfernt.

Status/Kanal-Statistik

Diese Tabelle zeigt Ihnen Informationen über den aktuellen Zustand der beiden B-Kanäle. Beim *ELSA LANCOM Wireless IL-2* werden auch Informationen über die a/b-Ports angezeigt. Die Informationen aus dieser Tabelle werden hauptsächlich zur Ausgabe über *ELSA LANmonitor* verwendet. Daher liegen einige Werte in einer reinen Bitdarstellung vor, die hier nicht näher erläutert wird.

Die Tabelle hat folgenden Aufbau:

Kanal	Zustand	App	Mode	Cause	Rufnummer	Subadr.	Geb.	Verb.-Zeit	Extra	ISDN-Anzeige
S_0-ERR	00000000	Router	akt.	0000	0241123456	00000000	3	0		
S_0-B1	00000000	a/b	akt.	0000	0241123457	00000000	2	20		
S_0-B2	00000000	Lancapi	pass.	0000	0241123458	00000000	4	180		

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Kanal	Kanal (oder a/b-Port), für den der Eintrag gilt. Es wird immer nur der letzte Zustand eines Kanals angezeigt. Für Fehlermeldungen auf Kanälen wird ein eigener „Kanal“ geführt.
Zustand	Als Zustand eines Kanals wird hier z.B. 'bereit' angezeigt.
App	Applikation, die den Kanal belegt: Router, *LANCAPI* oder a/b-Port
Mode	Art des letzten Verbindugsaufbaus: aktiv oder passiv
Cause	Letzter aufgetretener Fehler
Rufnummer	Rufnummer der Gegenstelle: bei aktivem Aufbau die gewählte Nummer, bei eingehenden Rufen die Nummer, die übermittelt wird.
Subadresse	Zusatz zur Applikation, die für den Router z.B. den logischen Kanal angibt. Für die *LANCAPI* z.B. die IP-Adresse des Clients, der die CAPI nutzt.
Geb.	Anzahl der Gebühreneinheiten, die für diese Verbindung angefallen sind
Verb.-Zeit	Dauer der letzten Verbindung auf diesem Kanal
Extras	Zusatzinformation zur Verbindung, z.B. der Name der Gegenstelle bei Routerverbindungen
ISDN-Anzeige	Informationen von der Vermittlungsstelle, z.B. Fehlermeldungen, beim Anschluß an TK-Anlage evtl. auch Name des Anrufers etc.

Status/Zeit-Statistik

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

Das Menü hat folgenden Aufbau:

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

Status/Zeit-Statistik/ISDN

In dieser Statistik werden die folgenden Werte angezeigt:

Verbindung	Anzahl der Versuche, eine Zeitinformation aus dem ISDN-Netz abzulesen
Informationen	Anzahl der aus dem ISDN-Netz erhaltenen Zeitinformationen
Infofehler	Anzahl der fehlerhaften Zeitinformationen aus dem ISDN-Netz

Status/LCR-Statistik

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

Das Menü hat folgenden Aufbau:

/LCR-Statistik		Statistiken aus dem Least Cost Router
Gesamtaufrufe		Gesamtzahl der Aufrufe des LCR
Erfolge		Anzahl der Aufrufe, bei denen der LCR eine passende Regel in seinen Tabellen fand und die Nummer erfolgreich umgeleitet wurde
nicht-gefunden-Fehler		Anzahl der Aufrufe, bei denen der LCR keine passende Regel in seinen Tabellen fand und die Nummer deswegen nicht umgeleitet wurde
fehlende-Zeit-Fehler		Anzahl der Aufrufe, bei denen der LCR mangels fehlender Zeit nicht eingreifen konnte
Provider-Statistik		Eine Tabelle mit allen angerufenen Providern (bzw. deren Vorwahlen), die Anzahl der erfolgreichen bzw. fehlgeschlagenen Anrufe
Werte löschen		LCR-Statistik löschen

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 Kartenname, also der Gerätename, 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
WAN-Modul		Einstellungen für das WAN
Gebühren-Modul		Einstellungen für die Gebührenverwaltung
LAN-Modul		Einstellungen für das LAN
WLAN-Modul		Einstellungen für das WLAN
TCP-IP-Modul		Einstellungen für das TCP/IP-Modul
IP-Router-Modul		Einstellungen für das IP-Router-Modul
SNMP-Modul		Einstellungen für die Konfiguration über SNMP
DHCP-Modul		Einstellungen für den DHCP-Server
Config-Modul		Einstellungen für das Konfigurationsmodul
DNS-Modul		Einstellungen für den DNS-Server
NetBIOS-Modul		Einstellungen für das NetBIOS-Modul

/Setup		Konfiguration des Systems
LANCAPI-Modul		Einstellungen für die *ELSA LANCAPI*
LCR-Modul		Einstellungen für den Least-Cost-Router
Zeit-Modul		Einstellungen für das Zeit-Modul

Name

Hier kann der Gerätename (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 Gerätename 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 Gerätename 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/WAN-Modul

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

/WAN-Modul		Einstellungen für das WAN
Interface-Liste		Einstellungen für das S_0-Interface
Router-Interface-Liste		Einstellungen für das Interface der Routermodule
Namenliste		Einstellungen für die Gegenstellen
Round-Robin-Liste		Einstellungen verschiedener Gegenstellen-Nummern
Layerliste		Einstellungen der verwendeten Layer-Kombinationen
PPP-Liste		Einstellung der Parameter für PPP-Verbindungen

/WAN-Modul		Einstellungen für das WAN
Nummernliste		Einstellung der zugangsberechtigten Rufnummern
Script-Liste		Einstellung der Anwahl-Scripte
Manuelle-Wahl		Einstellungen für die manuelle Verbindungssteuerung
Schutz		Schutz für die Annahme von eingehenden Rufen
RR-Versuche		Anzahl der Rückrufversuche, wenn die Gegenstelle besetzt ist

Interface-Liste

Diese Tabelle enthält die Interface-Einstellungen, die für alle Betriebsarten (Module) der Geräte gelten.

Ifc	Protokoll	FV-B-Kanal	Anwahl-Prae
S0	Auto	1	0

Zusätzlich können für die einzelnen Module noch weitere, spezielle Interface-Einstellungen vorgenommen werden, z.B. die Rufnummern, auf die ein Modul reagieren soll, siehe auch

`setup/wan-modul/Router-Interface-Liste`

`setup/lancapi-modul`

`setup/ab-modul/port-liste`

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	Bezeichnet das zugehörige Interface.
Protokoll	Einstellung des D-Kanal-Protokolls. Mögliche Werte sind: **Auto**: automatische Erkennung des D-Kanal-Protokolls **DSS1**: Euro-ISDN **1TR6**: nationales ISDN **GRP0**: Festverbindung Gruppe 0 **GRP2**: Festverbindung Gruppe 2 **P2P-DSS1**: Anlagenanschluß
FV-B-Kanal	Einstellung des B-Kanals, auf dem eine Festverbindung ablaufen soll. Mögliche Werte sind: **kein**: Keine Zuweisung der Festverbindung auf einen bestimmten Kanal. **1** oder **2**: Festverbindung läuft über den angegebenen B-Kanal. Bitte beachten Sie auch die Hinweise zur Einstellung dieser Parameter in der Beschreibung der Festverbindung. Die Funktion der Festverbindungen gehört nicht zur Grundausstattung der *ELSA LANCOM Wireless*.
Anwahl-Prae	Globales Anwahlpräfix für alle Module des Geräts. Die hier eingetragenen Ziffern (maximal 8) werden automatisch bei jeder Anwahl vor die gewählte Rufnummer gestellt. Verwenden Sie dieses Präfix z.B. dann, wenn Ihr Router an eine TK-Anlage angeschlossen ist.

Router-Interface-Liste

Diese Tabelle enthält die Interface-Einstellungen, die für die Router-Module der *ELSA LANCOM* gelten.

Ifc	MSN/EAZ	YV.	CLIP
S0	123456	Aus	Ein

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	Bezeichnet das zugehörige Interface.
MSN-EAZ	Wenn Sie Ihr Gerät an einem ISDN-Anschluß mit 1TR6 angeschlossen haben, geben Sie hier die EAZ ein, auf die das Interface reagieren soll. Wenn Sie Ihr Gerät an einem ISDN-Anschluß mit DSS1 angeschlossen haben, so wird hier die MSN angegeben, auf die das Interface reagieren soll. Soll das Interface auf mehrere MSNs reagieren, so können diese hier mit Semikola getrennt angegeben werden. Ein '#' in der Liste erlaubt beliebige eingehende MSNs. Die erste MSN in dieser Liste wird bei abgehenden Rufen an die Gegenstelle gemeldet. Wenn keine MSN eingetragen wird, überträgt die Vermittlungsstelle die Haupt-MSN des Anschlusses.
YV.	Über diesen Eintrag kann die Fähigkeit des Interfaces, Y-Verbindungen aufzubauen, gesteuert werden. Mögliche Einstellungen sind: **Ein:** Y-Verbindung wird unterstützt, es können mehrere Verbindungen gleichzeitig aufgebaut werden (Default). Eine Verbindung mit Kanalbündelung wird abgebaut, wenn eine zweite Verbindung zu einer anderen Gegenstelle aufgebaut werden soll. Beachten Sie auch die Einstellungen für die Verfügbarkeit der *LANCAPI* und der Telefonanlage beim *ELSA LANCOM Wireless IL-2*. **Aus:** Y-Verbindung wird nicht unterstützt, es kann nur eine Verbindungen aufgebaut werden. Die zweite Verbindung wird blockiert. Wenn eine Verbindung zu einer weiteren Gegenstelle aufgebaut werden soll, wird dieser Aufbau zurückgewiesen. Eine Verbindung mit Kanalbündlung wird nicht beeinträchtigt.
CLIP	Calling Line Identification Protocol: Unterdrückung der abgehenden MSN. Mögliche Werte: **Ja**: CLIR aktivieren, keine MSN übertragen. **Nein**: CLIR deaktivieren, MSN zur Gegenstelle übertragen. Bitte beachten Sie: Die „Fallweise Unterdrückung der Rufnummernübermittlung“ muß als Dienstmerkmal ggf. bei der Telefongesellschaft beantragt werden.

Namenliste

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

In der Namenliste können 64 verschiedene Gerätenamen verwaltet werden, die z.B. so aussehen können:

Geraetename	Rufnummer	B1-HZ	B2-HZ	Layername	Rückruf
AACHEN	875463	180	0	PPPHDLC	ein
BERLIN	040785647	20	20	DEFAULT	aus

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Gerätename	In der Spalte **Gerätename** können Sie einen eigenen Gegenstellen-Namen eintragen, den Sie dann der entsprechenden Gegenstelle über den Menüpunkt **Name** des Menüs **Setup** zuweisen müssen.
Rufnummer	In dieser Spalte können Sie die anzurufende Rufnummer hinterlegen und evtl. mit Wahlsonderzeichen ergänzen (s.u., Standard: keine).
B1-HZ	In dieser Spalte können entsprechende Verbindungshaltezeiten (in Sekunden) für den ersten B-Kanal festgelegt werden. Werden nach Ablauf dieser Zeit keine Daten übertragen, wird die Verbindung auf diesem Kanal wieder abgebaut (Standard: 20). Werden dabei über das ISDN-Netz die Gebühreninformationen während der Verbindung übermittelt, nutzt der *ELSA LANCOM* eine angefangene Gebühreneinheit vollständig aus und beendet die Verbindung erst kurz vor dem Beginn der nächsten Einheit. Diese Funktion wird auch als dynamischer Short-Hold bezeichnet.
B2-HZ	In dieser Spalte können entsprechende Verbindungshaltezeiten für den zweiten B-Kanal festgelegt werden (analog B1-HZ, Standard: 20). Die B2-Haltezeit steuert bei einer Kanalbündelung das Verhalten der Bündelung. Werte von 0 oder 9999 kennzeichnen eine statische Bündelung, Werte dazwischen eine dynamische Bündelung.
Layername	In dieser Spalte wird ein Name hinterlegt, der in der Layerliste ebenfalls eingetragen sein sollte. Damit wird die für diese Verbindung notwendige Einstellung des Übertragungs-Protokolls festgelegt.
Rückruf	In dieser Spalte können Sie festlegen, ob ein Rückruf für die entsprechende Gegenstelle erfolgen soll (Aus/Name/Auto/Looser/ELSA; Standard: Aus).

- Rückrufoptionen

Aus	Es erfolgt kein Rückruf.
Looser	Der Router bricht eigene Aufbauversuche ab, wenn ein Ruf von dieser Gegenstelle anliegt (gegenseitiger Verbindungsaufbau). Diese Einstellung muß benutzt werden, wenn ein Rückruf von der Gegenstellen erwartet wird.
Auto (nicht Windows 9x oder Windows NT)	Wenn die Gegenstelle in der Nummernliste eingetragen ist, so wird die Verbindung abgelehnt und ein direkter Rückruf gestartet. Dabei fallen für den Anrufer keine Gebühren an. Ist die Gegenstelle nicht in der Nummernliste eingetragen, so wird in einer Protokollverhandlung (ELSA oder PPP) Rückruf ausgehandelt. Dabei fällt eine Gebühr von einer Einheit an.
Name	Diese Einstellung erzwingt eine Protokollverhandlung. Damit kann über die Nummernliste ein Rufnummernschutz eingestellt und zusätzlich über die Protokollverhandlung ein Rückruf gestartet werden. Dabei fällt eine Gebühr von einer Einheit an.
ELSA	Diese Einstellung ermöglicht ein besonders schnelles Rückrufverfahren. Die zurückgerufene Gegenstelle muß die Einstellung 'Looser' verwenden.

- Die Wahlsonderzeichen der folgenden Tabelle können mit den Rufnummern in der Namen- oder Round-Robin-Liste oder im logischen Anwahlpräfix eingegeben wer-

den. Sie steuern die Amtsholung, die Verwendung einer semipermanenten Festverbindung oder bestimmten das für die Verbindung zu verwendende Interface:

#	Amtsholung (nur bei einigen TK-Anlagen)
F	Die Gegenstelle wird über die Festverbindung erreicht. Syntax: F[Kanal:][Rufnummer] Sowohl Angabe von Kanal als auch Rufnummer sind optional. Der Kanal gibt bei mehreren Festverbindungen den zu verwendenden B-Kanal an. Die Rufnummer gibt je nach Einstellung in der Kanalliste an, ob über die Wählverbindung eine dynamische Kanalbündelung oder eine Backup-Leitung realisiert werden soll.

Durch Anhängen von **S** oder **S2** an die Rufnummer wird die semipermanente Verbindung (SPV) beim D-Kanal-Protokoll 1TR6 aktiviert.

Eine SPV muß bei der Telefongesellschaft beantragt werden und wird pauschal berechnet.

*Wird das Anhängen von **S** oder **S2** vergessen, verhält sich eine SPV wie eine normale Wählleitung, und es entstehen unnötig hohe Gebühren. Die Telekom berechnet Ihnen dann die Pauschalgebühr und die entstandenen Wählleitungsgebühren für die Dauer der Leitungsnutzung.*

Round-Robin-Liste

Die Round-Robin-Liste ermöglicht es, eine Gegenstelle unter mehreren Rufnummern zu erreichen. Sie ist wie folgt aufgebaut:

Gerätename	Round-Robin	Anf.
AACHEN	4321-5555-6666	last

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Gerätename	In der Spalte Gerätename können Sie einen Gegenstellennamen aus der Namenliste eintragen. Sollte eine Zeile in der Round-Robin-Liste nicht für alle gewünschten Rufnummern ausreichen, kann diese Zeile wie folgt verlängert werden: Der Gerätename wird um das Zeichen # und einen eindeutigen Index (z.B. AACHEN#1) verlängert und in die nächste Zeile aufgenommen.
Round-Robin	Hier sind die Durchwahlnummern aller möglichen Gegenstellen unter dem entsprechenden Gerätenamen einzugeben. Die einzelnen Durchwahlnummern sind hierbei durch Bindestriche getrennt anzugeben.
Anf.	In der Spalte **Anf.** sind folgende Einträge möglich: **last**: Der nächste Verbindungsaufbau beginnt mit der Durchwahl, bei der die letzte Verbindung erfolgreich aufgebaut wurde (Default). **frst**: Der nächste Verbindungsaufbau beginnt immer mit der ersten Durchwahlnummer. Dieses Feld kann für eine logische Gegenstelle nur über deren **ersten** Eintrag in der Tabelle geändert werden. Bei allen weiteren Einträgen für diese Gegenstelle wird das Feld automatisch angepaßt.

Layerliste

In der Layerliste können durch Kombination unterschiedlicher ISDN-Layer verschiedene B-Kanal-Protokolle frei definiert werden. Hierdurch kann die Kompatibilität zu Geräten anderer Hersteller, die unterschiedliche B-Kanal-Protokolle verwenden, hergestellt werden.

Für *LANCOM Office*-Router gelten die folgenden Standardeinstellungen:

Layer-Name	Encaps	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	TRANS	PPP	TRANS	compr.	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	keine	HDLC64K
RAWHDLC	TRANS	TRANS	TRANS	keine	HDLC64K
BRIDGE	ETHER	TRANS	X.75LAPB	keine	HDLC64K

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Layer-Name	In dieser Spalte können Sie einen eigenen Namen für die von Ihnen verwendete Layer-Kombination aufnehmen. Diese Namen können dann entsprechend ihrer Schreibweise in der Spalte 'Layername' der Namenliste verwendet werden, um das Protokoll einzustellen. Ist in dieser Spalte ein Eintrag mit der Bezeichnung **DEFAULT** festgelegt, werden die dort abgelegten Einstellungen immer verwendet, wenn kein Layername zugeordnet werden kann (z.B. weil ein Anrufer seine Rufnummer nicht übermittelt). Ebenfalls wird dieser Eintrag verwendet, wenn eine Festverbindung der Gruppe 0 aufgebaut wird. Ist der Eintrag **DEFAULT** nicht vorhanden, wird standardmäßig ein von ELSA entwickeltes B-Kanal-Protokoll verwendet. Jeder der hier vordefinierten Layer ist vom Benutzer lösch- oder veränderbar.	
Encaps	In der Spalte **Encaps** können zusätzliche Informationen zu den zu übertragenden Daten festgelegt werden. Folgende Eintragungen sind möglich:	
	ETHER	Die Daten werden mit einem Ethernet-Header versehen. Diese Einstellung ist zur Kommunikation mit älteren *ELSA LANCOM*-Geräten oder im Bridge-Betrieb notwendig.
	TRANS	Bei dieser Einstellung wird kein Ethernet-Header ausgegeben. Es werden z.B. reine IP-Datenpakete übertragen. Diese Einstellung sorgt für den größtmöglichen effektiven Datendurchsatz.
Lay-3	In der Spalte Lay-3 können zusätzliche Header für die Datenübertragung im ISDN definiert werden. Folgende Einstellungen sind wählbar:	
	TRANS	Es wird kein zusätzlicher Header eingefügt (größter Datendurchsatz). Diese Einstellung ist immer zu wählen, wenn die Gegenstelle die Daten transparent auf ISDN-Layer-3 verschickt, (z.B. transparent HDLC, transparent X.75LAPB).
	ELSA	Die Daten werden mit einem ELSA-Header versehen. Zusätzlich wird bei einem Verbindungsaufbau eine Protokollverhandlung durchgeführt, in der die Gegenstellen ihre Namen austauschen. Nur mit dieser Einstellung ist ein Anrufschutz über den Namen möglich. Ohne ELSA-Einstellung kann ein Anrufschutz nur über die Rufnummer verwendet werden. Diese Einstellung ist zur Kommunikation mit älteren *ELSA LANCOM*-Geräten oder den Workstation-Treibern notwendig.
	PPP	Es wird eine Verhandlung nach dem Point-to-Point Protocol durchgeführt.

	APPP	Es wird eine Verhandlung nach dem asynchronen PPP durchgeführt. APPP wird dann verwendet, wenn synchrones PPP nicht möglich ist, weil die Verbindung keine synchrone Übertragung zuläßt (z.B. beim analogen Modembetrieb).
	SCPPP	Nach Abschluß der Scriptverarbeitung wird eine synchrone PPP-Verhandlung gestartet.
	SCAPPP	Nach Abschluß der Scriptverarbeitung wird eine asynchrone PPP-Verhandlung gestartet.
	SCTRANS	Nach Abschluß der Scriptverarbeitung besteht die Verbindung zur Gegenstelle. Es wird keine weitere Protokoll-Verhandlung durchgeführt.
Lay-2	In dieser Spalte wird das Protokoll für ISDN-Layer-2 eingestellt:	
	TRANS	Die Daten werden direkt in HDLC-Pakete verpackt. Diese Einstellung ist immer dann zu wählen, wenn die Kommunikation über transparent HDLC geschehen soll.
	X.75LAPB	Der Datenaustausch erfolgt im X.75-gesicherten Format. Wählen Sie diese Einstellung immer dann, wenn die Gegenstelle mit einer X.75-Datensicherung arbeiten soll.
L2-Opt.	Die Spalte L2-Opt. ermöglicht die Einstellung einer Option für die Datenübertragungseinstellung unter Lay-2 mit einem weiteren *ELSA LANCOM*.	
	keine	Es erfolgt keine Datenkompression oder Kanalbündelung.
	compr.	Es erfolgt eine Datenkompression nach V.42bis (*ELSA LANCOM Wireless IL-2*) oder Stac. Datenkompression nach V.42bis ist nur in Verbindung mit X.75ELSA oder X.75LAPB möglich. Kompression nach Stac (Hi/fn) muß in Verbindung mit PPP oder Multilink-PPP verwendet werden. Stac-Kompression kann auch in Verbindung mit Windows-Gegenstellen genutzt werden.
	bündeln	Es erfolgt eine Kanalbündelung über mehrere B-Kanäle. Die Kanalbündelung ist nur für die Lay-2-Einstellungen 'PPP' möglich. Die statische bzw. dynamische Kanalbündelung ist abhängig von der B2-Verbindungshaltezeit. Mit einer B2-Haltezeit von '0' oder '9999' stellen Sie eine statische Kanalbündelung ein, in der immer beide Kanäle verwendet werden. Bei der dynamischen Kanalbündelung mit anderen B2-Haltezeiten wird der zweite Kanal nur dann aktiviert, wenn der Datendurchsatz über einem bestimmten Schwellwert liegt.
	bnd+cmpr	Es erfolgt eine Kanalbündelung und Datenkompression über zwei B-Kanäle.
Lay-1	Die Spalte Lay-1 ermöglicht die Festlegung der Geschwindigkeit, mit der die Daten im ISDN geschickt werden.	
	HDLC64K	Die Daten werden mit 64.000 bit/s übertragen.
	HDLC56K	Die Daten werden mit 56.000 bit/s übertragen. Diese Einstellung ist besonders für Verbindungen in die USA von Bedeutung.

*Für die korrekte Arbeitsweise als Bridge muß auf jeden Fall im Feld **Encaps** der Eintrag **ETHER** eingestellt werden. Wird der ELSA LANCOM als Router eingesetzt, ist der Eintrag frei wählbar und passend zur Gegenstelle einzustellen.*

Für die Anbindung an Geräte anderer Fabrikate erkundigen Sie sich bitte bei dem Hersteller nach dem dort verwendeten Datenformat (PPP wird fast immer unterstützt).

Beim Internet-Zugang und Remote-Access ist in der Regel PPP vorgegeben.

PPP-Liste

Die in der PPP-Liste eingetragenen Gerätenamen werden vom Router benötigt, um die zur Verbindung passenden Einstellungen für das Sicherungsverfahren und die PPP-Parameter zu ermitteln. Sie ist enthält maximal 64 Einträge und ist wie folgt aufgebaut:

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

Username	Benutzername (max. 64 Zeichen), der der Gegenstelle während der PPP-Verhandlung übermittelt wird. Damit meldet sich der Router bei der Gegenstelle an. Wird kein Username eingetragen, gilt der Gerätename als Benutzername. Berücksichtigen Sie dabei auch die Groß- und Kleinschreibung.

Nummernliste

Unter diesem Menüpunkt wird eine Nummernliste verwaltet, in der 64 verschiedene Rufnummern mit dazugehörigen Gerätenamen eingetragen werden können. Damit können die von den Gegenstellen übermittelten Rufnummern (CLI) zu den Gegenstellen-Namen zugeordnet werden.

Einträge in der Nummernliste könnten für zwei anrufende Geräte AACHEN und BERLIN wie folgt aussehen, damit über die mitgeteilte Rufnummer deren Name erkannt und gegebenenfalls ein Rückruf (wenn gewünscht) über die Namenliste durchgeführt werden kann:

Rufnummer	Gerätename
875463	AACHEN
040785647	BERLIN

Diese Nummernliste ist für den passiven Verbindungsaufbau nötig. Die Rufnummern der Gegenstellen müssen ohne führende Nullen eingetragen werden.

Bei einem Rufnummerntest wird dann das momentan aktive D-Kanal-Protokoll berücksichtigt.

Falls die Einstellung 'Schutz Nummer' eingestellt ist und ein Anruf einer Gegenstelle erfolgt, wird die dabei übermittelte Rufnummer der Gegenstelle mit den Einträgen in der Nummernliste verglichen. Sind die übermittelte Rufnummer und ein Listeneintrag identisch, ist der Anrufer berechtigt, und die Verbindung wird aufgebaut.

Falls die Einstellung 'Schutz Nummer oder Name' eingestellt ist und ein Anruf einer Gegenstelle erfolgt, wird die dabei übermittelte Rufnummer der Gegenstelle mit den Einträgen in der Nummernliste verglichen. Sind die übermittelte Rufnummer und ein Listeneintrag identisch, ist der Anrufer zum Verbindungsaufbau berechtigt. Aus der Nummernliste kann außerdem der Name der Gegenstelle ermittelt werden und damit der Layer, der für diese Verbindung verwendet werden soll. Mit diesem Layer wird dann die Verbindung aufgebaut und die Namensüberprüfung mit dem gefundenen Layer gestartet (bzw. mit dem Default-Layer, wenn keiner gefunden wurde).

Wenn der Name der Gegenstelle (und damit der zu verwendende Layer) nicht über die Nummernliste ermittelt werden kann, wird der Ruf mit dem DEFAULT-Layer angenommen und nach der Protokoll-Verhandlung (PPP) geprüft, ob ein passender Eintrag in der Namenliste ist.

Script-Liste

Einige Internet-Provider (z.B. CompuServe) führen vor einer PPP-Verhandlung einen scriptgesteuerten Anmeldevorgang durch. Um auch solche Verbindung aufbauen zu kön-

nen, ist im *ELSA LANCOM* eine einfache Scriptverarbeitung implementiert (siehe 'Script-Verarbeitung').

In dieser Tabelle werden die Scripts definiert und den Gegenstellen zugewiesen. Die Tabelle hat den folgenden Aufbau:

Gerätename	Script
CSERVE	<>[Host]<CIS>[User]$U[Password]$P[PPP]$C

Die Einträge in der Script-Liste haben die folgende Bedeutung:

- Gerätename: Name der logischen Gegenstelle
- Script: Alle auszuführenden Befehle – Maximal 58 Zeichen stehen pro Zeile zur Verfügung. Sollte die notwendige Befehlsfolge länger sein, so kann ähnlich wie in der Round-Robin-Liste ein weiterer Eintrag für die logische Gegenstelle hinzugefügt werden. Die Syntax hierfür ist: Gerätename gefolgt von '#' und einer Zahl. Die Einträge werden von oben nach unten abgearbeitet.

Setup/WAN-Modul/Manuelle-Wahl

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

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

Aufbau Parameter: Gegenstellengerätename (nur über Remote-Konfiguration).

Mit dem Befehl

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

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

Bei Aktivierung der Funktion von der Tastatur der *ELSA LANCOM* aus erfolgt jeweils unmittelbar die Anzeige der Fehlermeldung 'Keine Gegenst.', weil dabei kein Name eingegeben werden kann. Diese Funktion ist also von der Tastatur der *ELSA LANCOM* nicht zu verwenden! Soll zu einer logischen Gegenstelle eine Verbindung aufgebaut werden, für die in der Namenliste keine Rufnummer angegeben ist, so wird die Fehlermeldung 'Keine Rufnummer' angezeigt.

Abbau Über diesen Befehl kann eine bestehende Verbindung abgebaut werden. Bei einem manuellen Verbindungsabbau kann in der Remote-Konfiguration zusätzlich der Name einer

Gegenstelle angegeben werden. Es wird dann nur die Verbindung zur angegebenen Gegenstelle gelöst. Besteht keine Verbindung zur angegebenen Gegenstelle, erfolgt keine weitere Reaktion. Wird dagegen kein Gegenstellenname angegeben, so werden alle bestehenden Verbindungen abgebaut.

Setup/WAN-Modul/Schutz

Hier kann eingestellt werden, unter welchen Voraussetzungen am Übertragungsmodul anliegende Rufe angenommen werden sollen.

- Ist der Schutz auf 'keiner' eingestellt, werden grundsätzlich alle anliegenden Rufe angenommen, solange die Gegenseite das Verbindungsprotokoll unterstützt.
- Mit der Einstellung 'Name' werden nur Rufe von Gegenstellen akzeptiert, für die ein Eintrag in der Namenliste vorhanden ist. Durch diese Überprüfung wird ein zusätzlicher Schutz gewährleistet. Diese Überprüfung steht nur bei Verwendung von PPP zur Verfügung.
- Bei der Einstellung 'Nummer' werden nur solche Gegenstellen akzeptiert, die in der Nummernliste als berechtigte Gegenstellen eingetragen sind.
- Auch ein Kombinationsschutz aus Namenliste oder Nummernliste ist mit 'Nr./Name' einstellbar. Damit wird zunächst geprüft, ob ein Eintrag in der Nummernliste vorhanden ist. Wenn das nicht möglich ist, versucht der Router den Namen über die Protokollverhandlung zu ermitteln.

Setup/WAN-Modul/RR-Versuche

Hierüber kann eingestellt werden, wie oft (von 1 bis 9) ein Rückruf wiederholt werden soll, wenn die Gegenstelle besetzt ist. Bei internationalen Verbindungen sollte ein Wert zwischen 3 und 5 eingegeben werden, um die Rückruffunktionen zu optimieren. Der Standardwert beträgt 3.

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

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 *ELSA LANCOM*

Zustand

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

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

IP-Adresse

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

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

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

IP-Netzmaske

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

Intranet-Adresse

Hier kann eine zweite IP-Adresse für 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 Anwahl 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 herauf auf die Konfiguration zugegriffen werden darf.

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

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

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

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

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

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

IP-Adresse	IP-Netz-Maske
192.234.222.0	255.255.255.0

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

DNS-Default

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

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

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

den DNS-Server des Providers zugreifen. Dieser Mechanismus wird auch als DNS-Forwarding bezeichnet.

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

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

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

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

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

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

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

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

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

Setup/IP-Router-Modul

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

/IP-Router-Modul	Einstellungen für das IP-Router-Modul	
Zustand		IP-Router-Modul ein- oder ausgeschaltet
IP-Routing-Tabelle		Router-Tabelle für Zuordnung IP-Netzwerk und Gegenstelle
LAN-Filtertabelle		Negativ/Aufb.-Filtertabelle für TCP/UDP-Zielports von LAN-Pak.
WAN-Filtertabelle		Negativ-Filtertabelle für TCP/UDP-Zielports von WAN-Paketen
Proxy-ARP		Aktivierung/Deaktivierung der Proxy-ARP-Funktion
Lok.-Routing		Ein- und Ausschalten des lokalen Routings
Routing-Methode		Routing-Verfahren für IP-Pakete
RIP-Einstellungen		Einstellungen für den Betrieb von IP-RIP
Masquerading		Einstellungen für das IP-Masquerading

Zustand

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

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

IP-Routing-Tabelle

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

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

- **Ein**: IP-Masquerading ist eingeschaltet und funktioniert mit dynamischer Zuweisung der IP-Adresse durch die Gegenstelle. Bei diesem Verfahren fragt der Router bei der Gegenstelle die IP-Adresse '0.0.0.0' an und bekommt daraufhin eine beliebige IP-Adresse der Gegenstelle zugewiesen, die im weiteren verwendet wird.
- **Aus**: Masquerading ist ausgeschaltet.
- **Statisch**: Masquerading ist eingeschaltet und funktioniert mit Zuweisung einer statischen, vorher vereinbarten IP-Adresse durch die Gegenstelle. Bei diesem Verfahren fragt der Router bei der Gegenstelle die unter 'Setup/TCP-IP-Modul' eingetragene IP-Adresse an und bekommt daraufhin genau diese Adresse von der Gegenstelle zugewiesen. Verwenden Sie diese Einstellung, wenn Ihnen die Gegen-

stelle (z.B. Ihr Internet-Provider) mit den Zugangsdaten eine feste IP-Adresse mitgeteilt hat. Dieses Verfahren funktioniert natürlich nur dann, wenn Sie diese Adresse auch als IP-Adresse im Router eingetragen haben.

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

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

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

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

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

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

- Beispiel
  - Die lokale Netzwerkadresse ist 192.120.130.0.
  - Drei Endgeräte sollen über Proxy-ARP mit den IP-Adressen 192.120.130.10, 192.120.130.11 und 192.120.130.12 über einen *ELSA LANCOM* 'Dresden' erreichbar sein.
  - Es gibt zwei erreichbare Zielnetze 192.120.131.0 und 192.120.132.0 für die Gegenstellen 'AACHEN' und 'BERLIN'.
  - Datenpakete für das Zielnetz 193.140.300.0 sollen zu einem weiteren lokalen Router mit der IP-Adresse 192.120.130.200 geschickt werden.
  - Zu einem Zielnetzwerk 193.140.200.0 soll überhaupt nichts übertragen werden.
  - Alle anderen nicht lokalen Datenpakete sollen zum Router 'PROVIDER' beim Internet-Service-Provider geschickt werden.

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

IP-Adresse	IP-Netz-Maske	Router-Name	Distanz	Maskierung
192.120.130.10	255.255.255.255	DRESDEN	0	Aus
192.120.130.11	255.255.255.255	DRESDEN	0	Aus
192.120.130.12	255.255.255.255	DRESDEN	0	Aus
192.120.131.0	255.255.255.0	AACHEN	0	Aus
192.120.132.0	255.255.255.0	BERLIN	0	Aus
193.140.200.0	255.255.255.0	0.0.0.0	0	Aus
193.140.300.0	255.255.255.0	192.120.130.200	0	Aus
255.255.255.255	0.0.0.0	PROVIDER	0	Ein

Wenn die Verbindung zur gewählten Gegenstelle über eine PPP-Verbindung realisiert wird, müssen in der PPP-Tabelle für den entsprechenden Eintrag die Rechte für IP aktiviert sein!

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

LAN-Filtertab.

Mit dieser Tabelle können bestimmte Ziel-Port-Bereiche gefiltert werden. Darüber hinaus kann bestimmt werden, wie diese Pakete gefiltert werden. Treffen von der LAN-Seite Pakete mit den eingetragenen Ports ein, so werden sie nicht weitergeroutet (Immer-Filter), nur, wenn die Verbindung gerade steht (Aufbau-Filter) oder nur, wenn sie über eine andere als die DEFAULT-Route gerouted werden können (I-Net-Filter).

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

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

Die Felder der Tabelle haben folgende Bedeutung:

- Idx.

  Eindeutiger Index. Dieser Eintrag ist nötig, um die Filter unterscheiden zu können. Der Index kann vier Zeichen lang sein und beliebig gewählt werden.

- Z-von, Z-bis

  Ziel-Port-Bereich, der gefiltert werden soll. Ein Bereich von 0 bis 0 bedeutet, daß kein Ziel-Port von diesem Filter beeinflußt wird.

- Q-von, Q-bis

  Quell-Port-Bereich, der gefiltert werden soll. Ein Bereich von 0 bis 0 bedeutet, daß kein Quell-Port von diesem Filter beeinflußt wird.

- Quell-Adresse, Quell-Netzmaske

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

- Prot

  Protokoll, das gefiltert werden soll. Möglich sind **TCP**, **UDP**, **ICMP** und **alle**.

  Die Einstellung **alle** filtert jedes Paket aus dem spezifierten Quell-Netz bzw. zum Ziel-Netz.

- Typ

  Art des Filters. Möglich sind Immer, Aufbau und I-Net.

  – **Immer**-Filter: Das Paket wird verworfen.
  – **Aufbau**-Filter: Das Paket wird verworfen, wenn keine Verbindung zur Gegenstelle besteht.
  – **I-Net**-Filter: Das Paket wird verworfen, wenn sein Ziel nur über die DEFAULT-Route erreichbar ist.

In der vorhergehenden Tabelle ist der Default-Filter eingetragen, der den unerwünschten und kostenintensiven Verbindungsaufbau bei Windows-Netzen auf IP unterbindet. Diese Netze senden regelmäßig z.B. DNS-Anfragen ins lokale Netz, die ohne diesen Filter ins Internet geleitet werden.

WAN-Filtertab.

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

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

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

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

- Ziel-Adresse, Ziel-Netzmaske

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

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

- Die längsten Netzmasken stehen oben.
- Bei gleicher Netzmaske steht die größte IP-Adresse oben.

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

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

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

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

Setup/IP-Router-Modul/Routing-Methode

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

Das Menü hat den folgenden Aufbau:

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

Routing-Methode

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

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

ICMP-Routing-Methode

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

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

Setup/IP-Router-Modul/RIP-Einstellungen

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

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

Typ

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

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

R1-Maske

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

- **Klasse** (Standard): Die im RIP-Paket verwendete Netzwerkmaske ergibt sich direkt aus der IP-Adresse-Klasse, d.h., für die Netzwerkklassen werden folgende Netzwerkmasken verwendet:
  - Klasse A: 255.0.0.0

- Klasse B: 255.255.0.0
- Klasse C: 255.255.255.0

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

Tabelle-RIP

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

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

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

Stellen Sie hier ein- bzw. aus, ob RIP-Pakete ins LAN bzw. Kabelnetz gesendet werden.

Setup/IP-Router-Modul/Masquerading

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

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

Service-Tabelle

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

Z-Port	Intranet-Adresse
20	10.1.1.10
21	10.1.1.10

Hierbei bedeuten:

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

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

Mit dem Befehl

```
telnet 192.38.50.100:27
```

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

Tabelle-Masquerade

Beim IP-Masquerading werden die IP-Adressen von Rechnern im lokalen Netz durch eine Umsetzung der Adressen und Ports im Router nach außen hin unsichtbar gemacht. In der dynamischen Masquerading-Tabelle werden die IP-Adressen aus dem lokalen Netz angezeigt, die aktuell vom Router maskiert werden. Die dynamische Masquerading-Tabelle hat maximal 2048 Einträge nach folgendem Aufbau:

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

Hierbei bedeuten:

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

Setup/SNMP-Modul

Über dieses Menü können Einstellungen 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

/SNMP-Modul		Einstellungen für das SNMP-Modul
Register-Monitor		Befehl zum Anmelden einer Zieladresse, zu der Traps gesendet werden sollen
Loesche-Monitor		Befehl zum Löschen einer Adresse, die mit 'Register-Monitor' gesetzt wurde
Monitor-Tabelle		Tabelle mit allen aktuell aktiven Zieladressen, die mit 'Register-Monitor' gesetzt wurden

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

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

Administrator Name des Administrators

Standort Standort des Gerätes

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

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

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

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

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

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

Monitor-Tabelle Die Monitor-Tabelle hat folgenden Aufbau:

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

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

Setup/DHCP-Server-Modul

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

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

Zustand

Ein: Das Gerät arbeitet als DHCP-Server

Aus: Das Gerät arbeitet nicht als DHCP-Server

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

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

Start-Adreß-Pool
Ende-Adreß-Pool

Die zugewiesene IP-Adresse wird aus dem eingestellten Adreß-Pool genommen ('Start-Adress-Pool' bis 'Ende-Adress-Pool'). Hier können beliebige im lokalen Netz gültige Adressen eingegeben werden.
Wird stattdessen '0.0.0.0' eingegeben, so ermittelt das Gerät die jeweiligen Adressen (Start bzw. Ende) aus den Einstellungen unter 'Setup/TCP-Modul'. Dabei wird wie folgt vorgegangen:

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

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

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

Netzmaske

Die Zuweisung der Netzmaske erfolg analog zur Adreßzuweisung:

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

Broadcast

Die Zuweisung der Broadcast-Adresse erfolg analog zur Adreßzuweisung:

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

Max.-Gültigkeit-Minute(n)

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

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

Default-Gültigkeit-Minute(n)

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

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

Tabelle-DHCP

Im DCHP-Modul kann über den Punkt 'Tabelle-DCHP' 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/NetBIOS

Im Menü Setup/NetBIOS werden die Einstellungen für das NetBIOS-Modul vorgenommen. Das Menü hat den folgenden Aufbau:

Zustand		Ein oder aus
Scope-ID		NetBIOS-Scope, in dem sich der Router befindet.
NT-Domaene		Arbeitsgruppe/Domain, in dem sich der Router befindet.
Gegenstellen-Tab.		In der Gegenstellen-Tabelle werden alle Gegenstellen eingetragen, mit denen NetBIOS-Informationen ausgetauscht werden.
Gruppen-Liste		In der Gruppen-Liste werden alle über NetBIOS bekannten Arbeitsgruppen abgelegt.
Host-Liste		In der Host-Liste werden alle über NetBIOS bekannten Rechner-Namen abgelegt.
Server-Liste		In der Server-Liste werden alle Server abgelegt, die sich im Netz bekannt gemacht haben.
Watchdogs		Legt die Behandlung von Watchdog-Paketen fest.
Abgleich		Art des Abgleichs von Routing-Informationen.
WAN-Update-Min		Intervall des Abgleichs in Minuten.

Scope-ID

Im Menüpunkt Scope-ID kann der NetBIOS-Scope angegeben werden, in dem sich das Gerät befindet. Es sieht dann nur noch NetBIOS-Pakete, die aus dem selben NetBIOS-Scope kommen. Alle anderen Pakete werden stillschweigend verworfen. Die Scope-ID wird nur in Verbindung mit Windows-Name-Servern (WINS) verwendet. Im allgemeinen kann dieser Eintrag frei bleiben.

NT-Domaene

Im Punkt NT-Domaene kann eine Arbeitsgruppe/Domain angegeben werden, um den Such-Vorgang beim Start des NetBIOS-Moduls anzustoßen. Dies ist notwendig, wenn sich im Netz keine Rechner mit Windows 95 oder Windows 98 befinden.

Gegenstellen-Tab.

In der Gegenstellen-Tabelle werden alle Gegenstellen eingetragen, die NetBIOS Informationen erhalten sollen, bzw. von denen NetBIOS-Information angenommen werden.

Wenn das NetBIOS-Modul eingeschaltet ist, werden NetBIOS-Pakete von anderen als den angegebenen Gegenstellen stillschweigend verworfen. Die Gegenstellen-Tabelle hat den folgenden Aufbau:

Name	Typ
AACHEN	Router oder Workstation

Wenn die Verbindung zur gewählten Gegenstelle über eine PPP-Verbindung realisiert wird, müssen in der PPP-Tabelle für den entsprechenden Eintrag die Rechte für NetBIOS aktiviert sein!

Typ

Das Feld 'Typ' gibt an, ob die Gegenstelle ein Router oder eine Workstation ist. Ist die Gegenstelle eine Workstation, so werden alle von dieser Gegenstelle bekannten Namen und Server im lokalen Netz und allen anderen verbundenen Routern abgemeldet und aus den jeweiligen Tabellen gelöscht, sobald die Verbindung zu der Gegenstelle abgebaut wird.

Host-Tabelle

Die Host-Tabelle hat den folgenden Aufbau:

Name	Typ	IP-Adresse	Gegenstelle	Timeout	Flags
REMOTE	00	10.0.1.100	AACHEN	5000	xx20
WORKSTATION	00	10.0.0.10		5000	xx00

Gruppentabelle

Die Gruppentabelle sieht entsprechend so aus:

Gruppe/ Domaene	Typ	IP-Adresse	Gegenstelle	Timeout	Flags
WORKGROUP	1e	10.0.0.10		5000	xx00
WORKGROUP	1e	10.0.1.100	AACHEN	5000	xx20

Die Felder der Tabellen haben dabei die folgende Bedeutung:

Name	Name des Hosts in der Host-Tabelle
Gruppe/ Domaene	Name der Gruppe bzw. Domain in der Gruppenliste. Gruppen und NT-Domains werden aus NetBIOS-Sicht gleich behandelt.
Typ	WINS-Typ des Host. Der Typ ist aus NetBIOS-Sicht uninteressant, jedoch ist ordnen Windows-Netze anhand des Typs dem Namen bestimmte Eigenschaften zu.
IP-Adresse	IP-Adresse des Besitzers des Namens. In der Gruppenliste können mehrere IP-Adressen dem gleichen Namen zugeordnet sein
Gegenstelle	Name der Gegenstelle, über die der Name bekannt wurde.
Timeout	Zeit bis der Name ungültig wird. Der Timeout ist zusätzlich mit einem Aging-Counter in den Flags verknüpft.
Flags	In den Flags werden bestimmte Zusatzinformationen zu dem Namen gehalten.

Flags

Die Flags haben folgende Bedeutung:

0x0003	Dieser Zähler wird nach jedem Ablauf der Gültigkeit erhöht. Wenn den Name nicht spätestens nach dem zweiten ablaufen erneuert wurde, so wird der Eintrag gelöscht.
0x0004	Dies kennzeichnet einen Eintrag, der noch übertragen werden muß.
0x0008	Dies kennzeichnet einen Eintrag, der zum Löschen ansteht, d.h., der Name wurde nach einem Verbindungsaufbau noch nicht erneuert.
0x0010	reserviert
0x0020	Dies kennzeichnet eine remote Gegenstelle.
0x0040	reserviert
0x0080	reserviert

Die Server-Liste hat den folgenden Aufbau:

Host	Gruppe/ Domaene	UPD	IP-Adresse	OS-Ver	SMB-Ver	Server-Typ	Gegen-stelle	Timeout	Flags
REMOTE	WORKGROUP	00	10.0.1.100	0400	010f	0004140b	AACHEN	13	0020
WORKSTATION	WORKGROUP	07	10.0.0.10	0400	0415	00452003		31	0000

Diese Tabelle füllt sich im Gegensatz zur Host- und Gruppen-Liste nur allmählich, da das NetBIOS-Modul darauf angewiesen ist, daß sich die Server von sich aus melden.

Dabei haben die einzelnen Felder die folgende Bedeutung:

Host	Name des Servers
Gruppe/ Domaene	Arbeitsgruppe bzw. Domain, in der sich der Server befindet
UPD	Update-Counter: gibt an wie oft der Server sich bereits propagiert hat
IP-Adresse	Adresse des Servers
OS-Ver	Versions-Nummer des Betriebssystems
SMB-Ver	Versions-Nummer des verwendeten SMB-Protokolls
Server-Typ	Bitmaske, in der die Dienste des Servers codiert sind
Gegenstelle	Name der Gegenstelle von der der Server bekannt gegeben wurde
Timeout	Zeit bis zum ungültig werden des Eintrags (bei Einträgen vom LAN) bzw. Zeit bis der Router einen Remote-Eintrag propagiert.
Flags	Entspricht den Flags in der Host- bzw. Gruppentabelle.

Setup/Config-Modul

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

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

LAN-Config

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

WAN-Config

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

Passw.Zwang

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

Fernconfig-(EAZ-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/*LANCAPI*-Modul

Bei der Einstellung der *LANCAPI* werden im Prinzip folgende Fragen geregelt:

- Auf welche Rufnummer aus dem Telefonnetz soll die *LANCAPI* reagieren?
- Welche der Rechner im lokalen Netz sollen über die *LANCAPI* Zugang zum Telefonnetz erhalten?
- Über welchen UDP-Port kommunizieren *LANCAPI*-Server und *LANCAPI*-Clients?

Das *LANCAPI*-Modul hat folgenden Aufbau:

/LANCAPI-Modul	Einstellungen für die *LANCAPI*	
Zugangsliste		Liste der Rechner, die die *LANCAPI* nutzen dürfen
LANCAPI-UDP-Port		UDP-Port für die Kommunikation zwischen *LANCAPI*-Server und -Clients
EAZ-MSN(s)		EAZ oder MSN, auf die die *LANCAPI* reagieren soll
Prio-ab		Priorität für die *LANCAPI* gegenüber Routerverbindungen

- **Zustand**: 'ein', 'aus' oder 'abgehend'. Bei letztgenannter Einstellung werden keine ankommenden Rufe von der *LANCAPI* angenommen.
- **Zugangsliste**: Grenzen Sie hier den Kreis der Rechner ein, die die *LANCAPI* nutzen dürfen. Diese Tabelle kann maximal 16 Einträge aufnehmen. Ist die Tabelle leer, können alle Rechner auf die *LANCAPI* zugreifen.
- **LANCAPI-UDP-Port**: Dieser Port steht in der Standardeinstellung auf '75'. Ändern Sie diesen Port nur dann, wenn andere Geräte in Ihrem Netz schon diesen Port verwenden.

Beim Umstellen des Ports gehen alle aktiven Verbindungen über die LANCAPI verloren!

- **EAZ/MSN(s)**: Geben Sie die Rufnummern ein, auf die die *LANCAPI* reagieren soll. Wenn Sie mehrere Nummern eingeben wollen, trennen Sie die einzelnen Nummern durch Semikola.
- **Prio-ab**: Mit der Priorität steuern Sie die Möglichkeit, für abgehende Verbindungen über die *LANCAPI* Routerverbindungen zu unterbrechen. Mit der Option '1' werden keine Routerverbindungen unterbrochen, mit der Einstellung '2' werden nur Nebenkanäle einer Routerverbindung mit Kanalbündelung unterbrochen, mit der Auswahl '3' werden auch Hauptkanäle einer Routerverbindung unterbrochen.

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. *Nicht in jedem Land sind alle Kanäle erlaubt (siehe auch Tabelle mit Funkkanälen im Anhang).*
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. *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!*
Zugriffsmodus		Der Positiv/Negativ-Schalter bestimmt, ob es eine Ausschlußliste 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 809B und 80F3 = Appletalk 6001 bis 6007 = Decnet 80D5 und 0808 bis 0D0D = IBM SNA *Wiederum wird hier nur der Zugang von Stationen im WLAN zum LAN bzw. WAN gesperrt, nicht jedoch der Traffic zwischen WLAN-Stationen.*
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

IAPP-Protokoll		Ein-/Aus-Schalter für Roaming. Beim Roaming müssen alle beteiligten Basis-Stationen die gleiche WLAN-Domain und den gleichen Funk-Kanal benutzen.
IAPP-Announce-Interval		Zeitinterval, in dem sich eine Basis-Station beim Roaming bei allen anderen über das kabelgebundene LAN bekannt macht
IAPP-Handover-Timeout		Maximale Dauer, in der die Basis-Station auf die Bestätigung der Mobil-Station wartet.

Setup/LCR-Modul

Bei der Einstellung des Least-Cost-Routers geben Sie folgende Informationen an:

- Für welche Module im Gerät sollen die Funktionen des LCR aktiv sein?
- Welche Vorwahlen sollen wann über welchen Call-by-Call-Provider umgeleitet werden?

Das LCR-Modul hat folgenden Aufbau:

/LCR-Modul		Einstellungen für den Least-Cost-Router
Router-Nutzung		LCR für die Routermodule aktivieren, **Ein** oder **Aus**
Lancapi-Nutzung		LCR für die *LANCAPI* aktivieren, **Ein** oder **Aus**
Zeittabelle		Tabelle der Rufumleitungen
Feiertagstabelle		Liste der Feiertage, die von der Zeittabelle berücksichtigt werden müssen.

Zeittabelle

Die Zeittabelle hat 256 Einträge mit folgendem Aufbau:

Index	Praefix	Tage	Start	Stop	Nummernliste	Rueckfall
1	0171	192	0:00	23:59	01013;01070	Ein

Die einzelnen Einträge haben die folgende Bedeutung:

Index	Durchlaufender Index für die Einträge in der Tabelle
Praefix	Vorwahl, die umgeleitet werden soll
Tage	Gültigkeit des Eintrags für Wochen- und Feiertage in Darstellung einer 8-bit-Maske: Bit 0 steht für Montag, Bit 7 für Feiertage. Der Eintrag '31' bezeichnet also alle Werktage, '192' die Sonn- und Feiertage
Start	Anfangszeit für die Gültigkeit des Eintrags an den definierten Tagen
Stop	Endzeit für die Gültigkeit des Eintrags an den definierten Tagen
Nummernliste	Netzkennzahl des Call-by-Call-Providers
Rueckfall	Automatischer Rückfall auf die eigene Telefongesellschaft, falls alle Call-by-Call-Nummern besetzt sind

Beispiel:

`set 1 02 31 1:00 11:59 01030;01090;01070 Ein` leitet alle Fernverbindungen in die Region '02' zwischen ein und zwölf Uhr um auf den Provider mit der Netzkennzahl '01030'. Falls da besetzt ist, werden die Netzkennzahlen '01090' und '01070' versucht. Sind die auch nicht verfügbar, wird die Verbindung über die normale Telefongesellschaft aufgebaut.

Feiertagstabelle

Die Feiertagstabelle hat 256 Einträge mit folgendem Aufbau:

Index	Datum
1	01010000
2	01050000
3	03100000
4	25120000
5	26120000
6	02041999
7	13051999

Die einzelnen Einträge haben die folgende Bedeutung:

Index	Durchlaufender Index für die Einträge in der Tabelle
Datum	Datum der einzelnen Feiertage Geben Sie den Index und das Datum vollständig ohne Trennzeichen ein, also z.B. 'set 8 13041999' für den 13. April 1999 als achten Listeneintrag. Geben Sie als Jahr '0000' für jährlich wiederkehrende Feiertage ein.

Setup/DNS-Modul

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

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

DNS-Tabelle

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

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

Rechnername	Ip-Adresse
HOST10	10.0.0.10

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

Filter-Liste

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

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

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

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

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

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

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

Setup/Zeit-Modul

Der Least-Cost-Router im Gerät benötigt korrekte Zeitinformationen für die Berechnung der Rufnummernumleitungen über Call-by-Call-Provider. Auch bei einigen Statistiken ist die Anzeige einer präzisen Zeitinformation wünschenswert.

Die Zeit kann entweder manuell gesetzt werden (mit dem Befehl 'time') oder automatisch aus dem ISDN-Netz abgelesen werden.

Für den automatischen Zeitabgleich wird beim Einschalten des Moduls direkt eine vorher bestimmte Gegenstelle angerufen und dabei die Zeitinformation aus dem ISDN-Netz übernommen. Solange das Zeit-Modul eingeschaltet ist, wird bei jeder Verbindung erneut die Zeit aus dem ISDN übernommen.

Das Zeit-Modul hat folgenden Aufbau:

/Zeit-Modul		Einstellungen für das Zeit-Modul
Zustand		Aktivierung des Moduls: **Ein**, **Aus**
Aktuelle-Zeit		Anzeige der aktuellen Zeit im Gerät
Time EAZ-MSN		Rufnummer, zu der eine Verbindung aufgebaut werden soll, um eine Zeitinformation aus dem ISDN-Netz zu erhalten
Anwahl-Versuche		Anzahl der möglichen Versuche, eine Zeitinformation zu erhalten.

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.

Ifc	Modul	Version	Seriennummer
Ifc	LANCOM Business 4100	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 Zustan-

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

Position	Status	Version	Datum	Groe	Index
1	inaktiv	1.60	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
Manuelle Wahl		Test einer Verbindung
System-Boot		Neustart des Gerätes
System-Reset		Rücksetzen auf Werkseinstellung
System-Upload		Neue Firmware laden

Sonstiges/Manuelle-Wahl

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

System-Boot Über diesen Menüpunkt kann das Gerät neu gestartet werden.

Vor der Ausführung des Befehls werden alle offenen Verbindungen (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 'So spielen Sie eine neue Software ein').

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

Ports und Protokolle

Ports

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
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
nbdatagram	138	udp
nbsession	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
sytek	500	udp
biff	512	udp

Dienst	Port-Nr.	Protokoll
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
rvd-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
acctdisk	707	udp
kerberos	750	tcp

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

Protokolle

Protokoll	Protokoll-Nr
apollo domain	8019
apple talk 1 & 2	809B
apple talk arp 1 & 2	80F3
banyan vines	0BAD
banyan vines echo	0BAF
decnet phase IV	6003
hp probe control	8005
ibm sna services	80D5
ip	0800
ip-arp	0806
novell (econfig e)	8137
rarp reverse arp	8035
snmp over ethernet	814c
xyplex	0888