

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.

Dieser Referenzteil beschreibt die folgenden Geräte:

- *ELSA LANCOM Wireless IL-11*
- *ELSA LANCOM Wireless L-11*
- *ELSA LANCOM Wireless* Geräte mit DSL-Firmware

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 vorhandenen IEEE-Normen für LANs dar, von denen IEEE 802.3 für Ethernet der bekannteste ist. In der Tat lassen sich nach 802.11 arbeitende Funknetze sehr leicht mit vorhandenen Ethernet-Netzen verbinden, und dies ist die wichtigste Funktion der *ELSA LANCOM Wireless*-Geräte. Nach 802.11 arbeitende Funkkarten stellen sich bis auf ein paar Zusatzparameter einem Rechner 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, Net-BIOS,...); der einzige Unterschied ist, daß Sie keine Kabel zwischen den Rechnern verlegen müssen!

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

Ad-hoc-Modus

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

Ein Funk-LAN im Ad-hoc-Modus besteht aus einer einzelnen abgeschlossenen Funkzelle, die aus Ethernet-Sicht 'abgeschlossen' ist, d.h. eine Verbindung nach außen ist lediglich über das Routing höherwertiger Protokolle möglich; ein Beispiel für ein solches Element wäre ein *ELSA LANCOM Wireless IL-11*, 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 physisch, weil ja immer nur eine Station senden kann, d.h. keine der Funkzellen würde im Überlappungsfalle die volle Bandbreite erreichen. Das können Sie verhindern, indem Sie den einzelnen Netzen nicht nur verschiedene Domain-Namen, sondern auch verschiedene 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 eigentlich Stärke von IEEE 802.1-basierten Funknetzen ist aber die einfache Koppelbarkeit mit bestehender (Ethernet-)Vernetzung. Ein Funknetz kann genutzt werden, um mobile Station mit an ein bestehendes, Kabelbasiertes 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 Basisstation, die auch als Access Point oder Distribution System bezeichnet wird. Die *ELSA LANCOM Wireless*-Geräte wurden dazu entwickelt, die Funktion einer Basisstation zu übernehmen. Im Infrastrukturmodus übernimmt die Basisstation 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 Basisstation aufgespannt, und jede Station muß sich bei der Basisstation anmelden, bevor sie Daten in der Funkzelle austauschen darf. Der Basisstation kommt dabei üblicherweise auch die Funktion einer 'Relaisstation' für Daten zu; dies reduziert zwar die erreichbare Datenrate, kann bei geschickter Aufstellung der Basisstation aber die Größe einer Funkzelle erhöhen. Die eigentliche Aufgabe der Basisstation ist aber die Verbindung der Funkzelle mit einem kabelgebundenen Ethernet: Erhält die Basisstation 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 Basisstation 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 macht also nur dann Sinn, wenn Sie die Ethernet-Schnittstelle nicht benutzen wollen!

Wie bereits erwähnt, kann ein Ethernet-Backbone auch dazu genutzt werden, die Reichweite eines Funk-LANs zu vergrößern: Dazu schließt man mehrere Basisstationen 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 Basisstationen die mit dem stärksten Signal und meldet sich bei dieser an; zwei an unterschiedlichen Basisstationen angemeldete Mobilstationen können so auch miteinander kommunizieren, wenn sie nicht in direkter Funkreichweite sind; das Ethernet, über das alle Basisstationen 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 Basisstation 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 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 z.T. 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,
Übertragungs-
medium,
Schnittstellen*

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



Wenn im folgenden der Begriff Netzworkkabel (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 Host. 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.

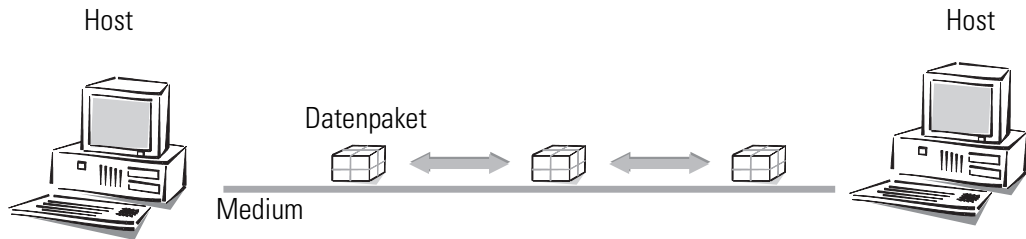
Router

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 kann und an einen Empfänger weiterleiten kann. Ein Router hat neben der Vermittlungsfunktion auch immer die Eigenschaften eines Hosts, damit er selbst das Ziel von Datenpaketen sein kann, z.B. zum Zweck der Konfiguration.

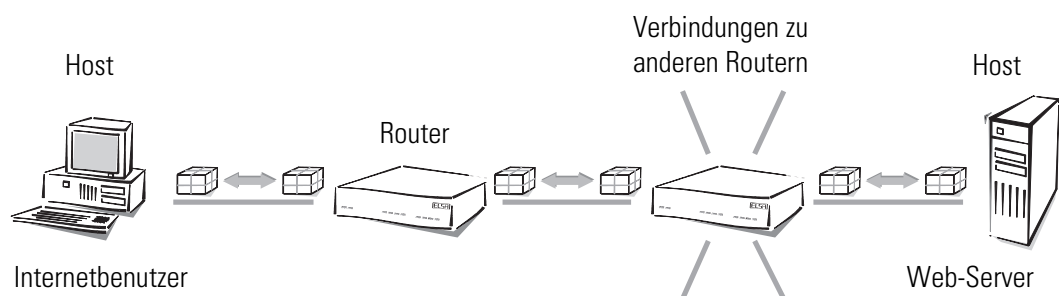
Verbindungsarten

*Punkt-zu-Punkt-
Verbindung*

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



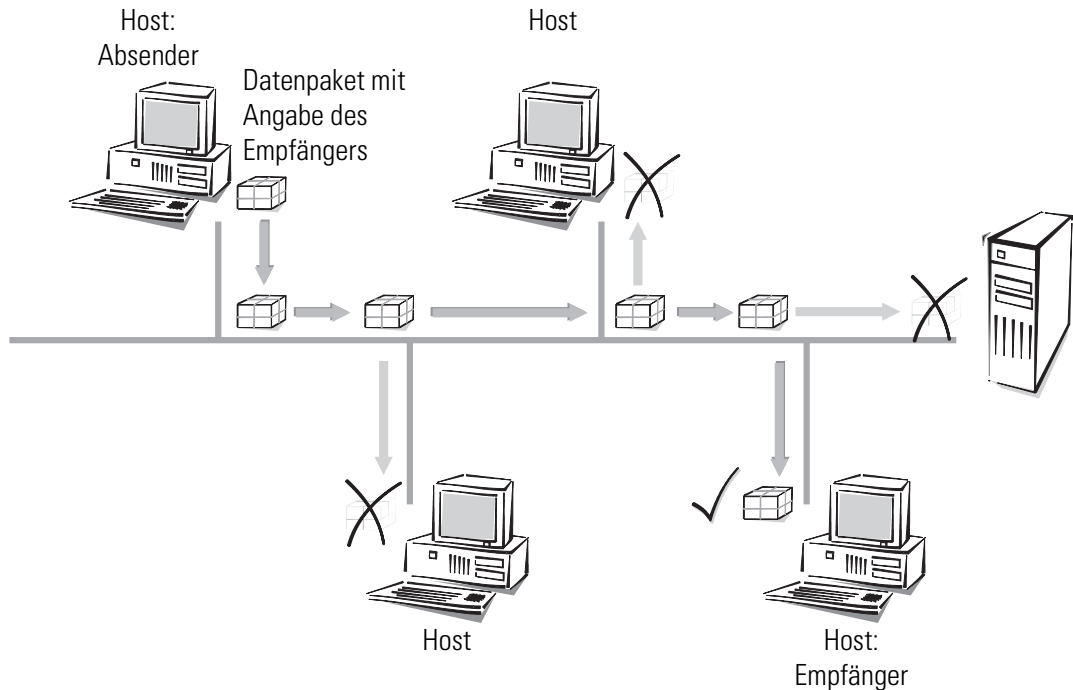
Auch bei einem Zugriff auf das Internet handelt es sich um eine Punkt-zu-Punkt-Verbindung. Die Datenpakete werden zwar vom Host beim Internetbenutzer über mehrere Router zum Host (Server) beim Internet-Provider gesendet, jedes Datenpaket hat jedoch ein ganz bestimmtes Ziel. Die Router geben die Datenpakete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



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

Punkt-zu-Mehrpunkt-Verbindung

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



Netzwerk-Arten

Protokoll

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

TCP/IP

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

IP-Netz

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

Internetwork Internet

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

Lokales Netz- werk (LAN)

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

IP-Adressierung

Paketorientierte Übertragung

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

IP-Adresse

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



Exakt betrachtet bezeichnet eine IP-Adresse nicht den Host, sondern seine Schnittstelle. Hat ein Endgerät im Netzwerk mehrere Schnittstellen (wie z.B. Router), so muß er für jede Schnittstelle eine eigene IP-Adresse besitzen. Deshalb haben ISDN-Router von ELSA 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.

Netzwerkadresse

In einer IP-Adresse ist sowohl die Adresse des Netzwerks enthalten als auch die des Hosts. Die Netzwerkadresse 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 Netzwerkadresse 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 $254 \times 254 = 64516$ verschiedene Adressen! Die erste und die letzte Ziffer eines Adreßraums sind jeweils reserviert für die Netzwerkadresse und die Broadcastadresse (Adresse für Pakete an alle Hosts in einem IP-Netz). Bei der Netzmaske 255.255.255.0 sind das die '0' für die Netzwerkadresse und die '255' als Broadcastadresse.

Eine neuere Schreibweise der Netzmaske hängt einfach die Anzahl der Bits, die für die Netzwerkadresse stehen, an die IP-Adresse an: 137.226.4.101/24. Die Zahl hinter dem Schrägstrich zeigt an, daß die ersten 24 Bits die Netzwerkadresse 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) bekannt gemacht werden. Nur **die** Geräte in einem Netzwerk, die Verbindung mit öffentlichen Netzwerken haben (z.B. Router an der Schnittstelle zum Internet), müssen eine registrierte IP-Adresse haben.

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

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

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

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

IP-Routing und hierarchische IP-Adressierung

Routing

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

Routingtabelle

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

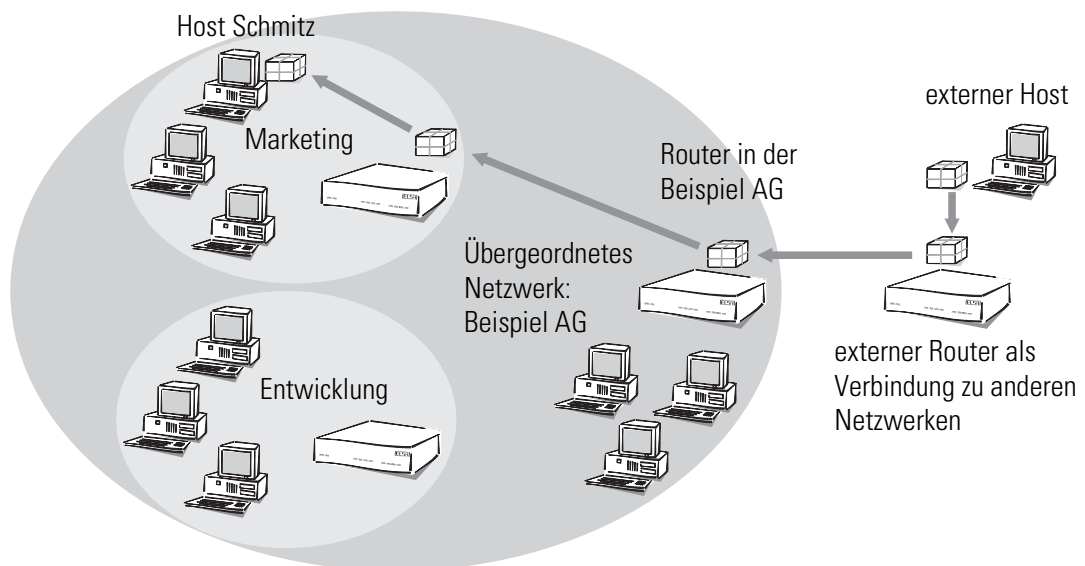
hierarchische IP-Adressen

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

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

Die Konsequenzen dieser hierarchischen IP-Adressierung:

- Da die Netzwerkadresse 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 Netzwerkadresse und der '255' als Broadcastadresse.

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 Netzwerkadresse. Dabei führt er ein logisches UND mit der Netzmaske aus und vergleicht das Ergebnis mit der Netzwerkadresse: '192.168.100.4' UND '255.255.255.0' ergibt '192.168.100.0'. Dies ist die Netzwerkadresse 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. Zum Vermeiden und Auflösen derartiger Kollisionen wird ein Zugriffsprotokoll (engl. **Medium Access Control**, MAC) eingesetzt.

LAN und IP-Netz Der Verbund aller Rechner, die mittels eines MAC-Protokolls über ein Shared-Medium kommunizieren, wird als LAN bezeichnet. Ein LAN bildet ein eigenständiges Netz und ist dem IP-Netz logisch untergeordnet, d.h., IP-Netze können die physikalischen Verbindungen eines LANs verwenden, um Verbindungen zwischen Hosts und Routern herzustellen. Ein LAN ist in der Regel räumlich und von der Anzahl der Netzteilnehmer auf wenige 10 bis 100 Hosts begrenzt, während ein IP-Netz theoretisch beliebig viele Hosts und Router verbinden kann (z.B. Internet).

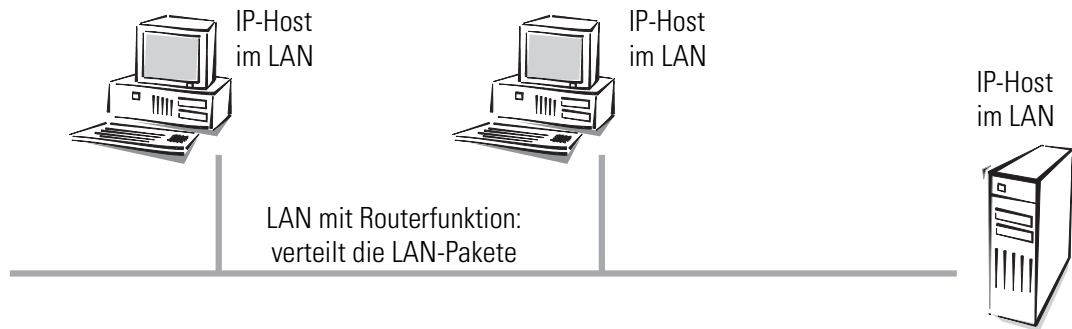
MAC-Adresse Zur Organisation der Übertragung im LAN werden spezifische LAN-Adressen verwendet, die vom Hersteller der Schnittstellenhardware fest einprogrammiert werden. Da die LAN-Adressen für die Kommunikation über das MAC-Protokoll verwendet werden, heißen Sie auch MAC-Adressen. Man kann sie sich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

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

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

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

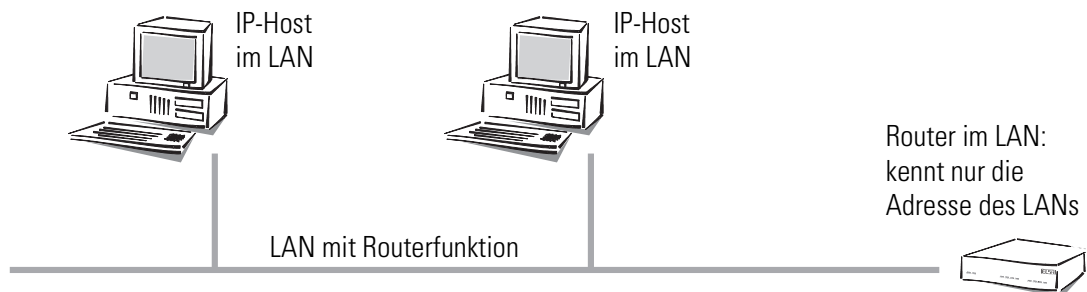
Für einen IP-Host verhält sich ein LAN so, also ob es ein eigenes Netzwerk mit einem Router wäre. Die Hosts geben die Pakete an das LAN ab, das die weitere Verteilung der Datenpakete übernimmt. Für die Kommunikation der Hosts untereinander über das IP-Protokoll dürfen in einem LAN somit nur IP-Adressen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



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

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

kennen muß, muß er sich also nur die Netzwerkadresse 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

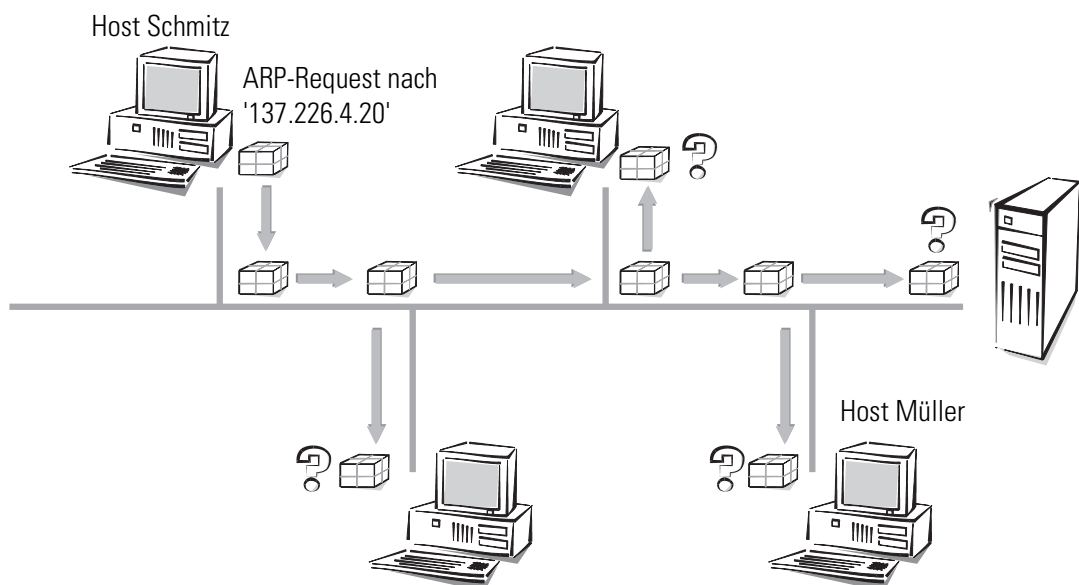
Veranschaulichen wir uns das an einem Beispiel. Stellen wir uns vor, daß die Hosts des Teilnetzes im Marketing über ein LAN verkabelt sind. Die Hosts haben IP-Adressen aus dem Nummernraum '137.226.4.1' bis '137.226.4.254' (die Adressen '137.226.4.0' und '137.226.4.255' sind reserviert), die Netzwerkadresse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

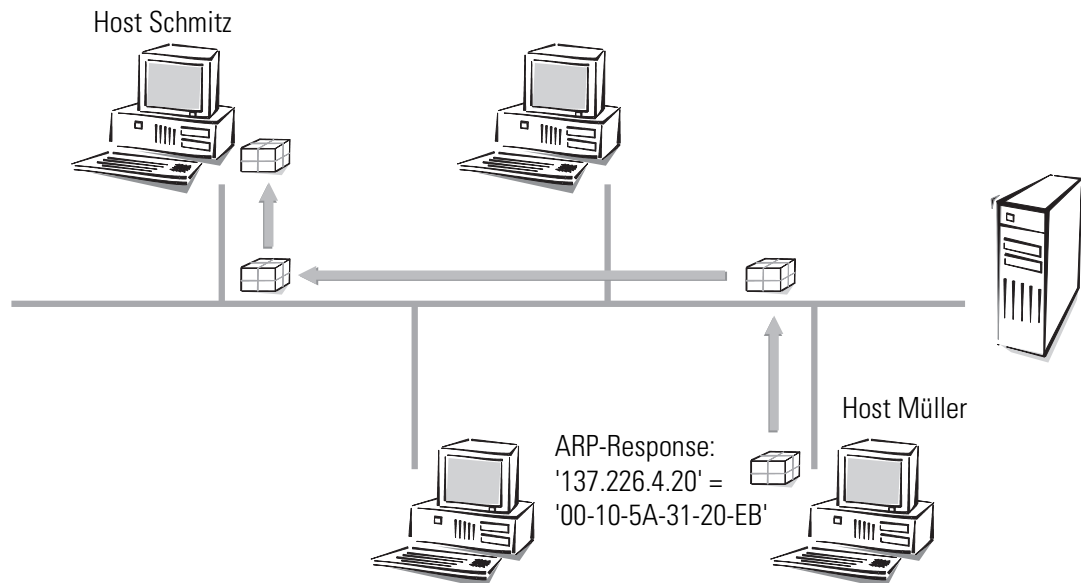
ARP

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 IP-Adresse 151.189.12.43 zu übertragen. Host Schmitz vergleicht die IP-Adresse mit seiner Netzwerkadresse 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 Netzwerkadresse von diesem Host und findet so die Schnittstelle, über die er das IP-Paket weiterleiten muß.

LAN-Kopplung auf MAC-Basis

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

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

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

Somit hat man wieder das Problem, das man bei Routern vor der Einführung von Teilnetzen hatte: Mit wachsender LAN-Größe werden die Adreßtabellen der Bridges irgendwann gesprengt. Man kann also nicht beliebig viele 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.

Erläuterung zu den Tabellen

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

MENU	Setup
WERT	Name
MENU	WAN-Modul
MENU	Accounting-Modul
MENU	Gebühren-Modul
MENU	LAN-Modul
MENU	IPX-Modul
MENU	TCP-IP-Modul
MENU	IP-Router-Modul
MENU	SNMP-Modul
MENU	DHCP-Modul
MENU	DNS-Modul
MENU	NetBIOS-Modul
MENU	Config-Modul
MENU	WLAN-Modul
MENU	LANCAPI-Modul
MENU	LCR-Modul
MENU	Zeit-Modul

MENU	Firmware
INFO-TABELLE	Versions-Tabelle
INFO-TABELLE	Tabelle-Firmsafe
WERT	Modus-Firmsafe
WERT	Timeout-Firmsafe
AKTION	Test-Firmware
AKTION	Firmware-Upload

MENU	Status
INFO	Verbindung
INFO	Aktuelle-Zeit
INFO	Betriebszeit
MENU	WLAN-Statistik
MENU	WAN-Statistik
MENU	LAN-Statistik
MENU	PPP-Statistik

MENU	IPX-Statistik
MENU	TCP-IP-Statistik
MENU	IP-Router-Statistik
MENU	Config-Statistik
MENU	Queue-Statistik
INFO-TABELLE	Verbindungs-Statistik
INFO-TABELLE	Info-Verbindung
INFO-TABELLE	Layer-Verbindung
INFO-TABELLE	Ruf-Info-Tabelle
INFO-TABELLE	Gegenstellen-Statistik
MENU	S ₀ -Bus
INFO-TABELLE	Kanal-Statistik
MENU	Zeit-Statistik
MENU	LCR-Statistik
INFO-TABELLE	Gebühren-Statistik
MENU	PCMCIA-Status
AKTION	Werte löschen
MENU	LAN-Management-Statistiken

MENU Sonstiges

MENU	Manuelle Wahl
AKTION	System-Boot
AKTION	System-Reset
AKTION	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	INFO	Zustand der WAN-Strecke
Aktuelle-Zeit	INFO	Aktuelle Zeit im Gerät
Betriebszeit	INFO	Betriebszeit des Gerätes seit dem letzten Einschalten
WAN-Statistik	MENU	Anzeige der WAN-Statistiken
LAN-Statistik	MENU	Statistiken des Netzwerk-Bereichs
WLAN-Statistik	MENU	Statistiken des Funk-Netzwerk-Bereichs
PPP-Statistik	MENU	Statistiken des Point-to-Point-Protokolls
IPX-Statistik	MENU	Statistiken aus dem IPX-Bereich
Bridge-Statistik	MENU	Statistiken des Bridge-Bereichs
TCP-IP-Statistik	MENU	Statistiken aus dem TCP/IP-Bereich
IP-Router-Statistik	MENU	Statistiken aus dem IP-Router
Config-Statistik	MENU	Statistiken der Remote-Konfiguration
Queue-Statistik	MENU	Statistiken über die Pakete in den Queues der einzelnen Module
Verbindungs-Statistik	INFO-TABELLE	Verbindungs-Informationen für jedes Interface
Info-Verbindung	INFO-TABELLE	Informationen zur letzten Verbindung für jedes Interface
Layer-Verbindung	INFO-TABELLE	Informationen über das verwendete B-Kanal-Protokoll für jedes Interface
Ruf-Info-Tabelle	INFO-TABELLE	Informationen über die letzten 100 angekommenen Rufe
Gegenstellen-Statistik	INFO-TABELLE	Statistik über die letzten 100 Verbindungen
S ₀ -Bus	MENU	Zustand der S ₀ -Schnittstelle
Kanal-Statistik	INFO-TABELLE	Informationen über den Zustand der einzelnen Kanäle.
Zeit-Statistik	MENU	Informationen aus dem Zeit-Modul
LCR-Statistik	MENU	Informationen aus dem Least-Cost-Router

Status	Fortlaufende Statusanzeigen	
PCMCIA-Status	INFO-TABELLE	Informationen zum PCMCIA-Status
Gebühren-Statistik	MENU	Informationen aus dem Gebühren-Modul
Werte löschen	AKTION	Alle Werte außer Tabellen der untergeordnet. Statistik löschen
LAN_Management-Statistiken	MENU	Adreßtabelle für das lokale Netzwerk

Status/Verbindung

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

/Verbindung	Fortlaufende Statusanzeigen	
Verbindung	INFO	DSL1: Bereit; 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/WLAN-Statistik

Hier wird der momentane Status des WLAN-Interfaces beschrieben.

LAN-Rx-Pakete	INFO	Anzahl empfangener Datenpakete
LAN-Tx-Pakete	INFO	Anzahl gesendeter Datenpakete
LAN-Rx-Fehler	INFO	Anzahl fehlerhaft empfangener Datenpakete
LAN-Tx-Fehler	INFO	Anzahl fehlerhaft gesendeter Datenpakete
LAN-Stack-Fehler	INFO	Anzahl Pakete ohne passendes Empfangsmodul (Bridge/Router)
LAN-Queue-Pakete	INFO	Anzahl belegter Puffer
LAN-Queue-Fehler	INFO	Anzahl durch Puffermangel verworfener Pakete
LAN-Rx-Bytes	INFO	Anzahl vom LAN empfangener Zeichen
LAN-Tx-Bytes	INFO	Anzahl zum LAN gesendeter Zeichen

LAN-Rx-Broadcasts	INFO	Anzahl vom LAN empfangener Broadcast-Pakete
LAN-Rx-Multicasts	INFO	Anzahl vom LAN empfangener Multicast-Pakete
LAN-Rx-Unicasts	INFO	Anzahl vom LAN empfangener direkt adressierter Pakete
LAN-Tx-Broadcasts	INFO	Anzahl vom WAN empfangener Broadcasts
LAN-Tx-Multicasts	INFO	Anzahl vom WAN empfangener Multicasts
LAN-Tx-Unicasts	INFO	Anzahl vom WAN empfangener Unicasts
LAN-Tx-Verworfen	INFO	Anzahl vom LAN verworfener Pakete
LAN-Wiederholungen	INFO	Anzahl der Pakete, die erst nach einer Wiederholung zugestellt werden konnten
LAN-Mehrfachwiederholungen	INFO	Anzahl der Pakete, die erst nach mehreren Wiederholungen zugestellt werden konnten
LAN-bereit	INFO	Erfolgreich Initialisierung der Funk-Netzwerkkarte
Stationstabelle	INFO-TABELLE	Anzeige der momentan angemeldeten Mobil-Stationen.
WLAN-Parameter	MENU	Parameter des Funk-Netzwerks
Interpoint-Statistiken	MENU	Hier werden die Punkt-zu-Punkt-Statustabellen gesammelt. Die Kopplung von Netzen mit zwei oder mehr Basis-Stationen.
IAPP-Tabelle	INFO-TABELLE	Zeigt alle Basis-Stationen an, die über das IAP-Protokoll gefunden wurden. IAPP wird sowohl für Punkt-zu-Punkt-Verbindungen als auch für das Roaming zwischen den Basis-Stationen verwendet.

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	Zeigt die momentan verwendete Kennung für die Funkzelle. Im Infrastruktur-Modus ist das immer die MAC-Adresse der Basis-Station, im Ad-hoc-Modus eine zufällig zwischen den Stationen bestimmte Zahl. Darin sind die folgenden Punkte enthalten:
	<i>Accesspoint-Liste</i> – alle momentan bekannten gegenstellen mit Adresse, Signalstärke und Datenrate des letzten empfangenen Paketes.
	<i>Routing-Liste</i> – in den gegenüberliegenden LANs bekannten Rechner mit MAC-Adresse, Transfer-Statistik und der Nummer der Basis-Station, über den sie erreicht werden. Diese Nummer korrespondiert mit der Position in der Accesspoint-Liste, nur beginnen hier die Nummern bei 0.
	<i>Broadcast</i> – Anzahl von Broadcasts über die Funkbrücke und die damit übertragene Datenmenge. Weil Broadcasts nicht an eine bestimmte Station gerichtet sind und daher nicht in der Routing-Liste gezählt werden, gibt es zwei Extrazähler.
PHY-Kanal	Der aktuell benutzte Kanal. Im Infrastruktur-Modus durch den Basisport, im Ad-hoc-Modus durch die Station gegeben.
Regulatory-Domain	Der Zulassungsbereich der eingesetzten Funk-Netzwerkkarte.
PHY-Typ	Das von der WLAN-Karte verwendete Modulationsverfahren DSSS (D irect S equences S pread S pectrum).
WEP-Unterstützung	Zeigt an, ob die eingesetzte Funk-Netzwerkkarte die WEP-Verschlüsselung unterstützt. Nur wenn dies gegeben ist, haben die WEP-Punkte im WLAN-Setup eine Wirkung.

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	INFO-TABELLE	Statistik für übertragene Bytes
Paket-Transport-Statistik	INFO-TABELLE	Statistik für übertragene Daten-Pakete
Fehler-Statistik	INFO-TABELLE	Statistik über aufgetretene Übertragungsfehler
WAN-Tx-Verworfen	INFO	Anzahl durch Fehler/Ressourcenmangel verworfener Pakete
WAN-Heap-Pakete	INFO	Anzahl belegter Puffer
WAN-Queue-Pakete	INFO	Anzahl verfügbarer Puffer

/WAN-Statistik	Fortlaufende Statusanzeigen	
WAN-Queue-Fehler	INFO	Anzahl durch Puffermangel verworfener Datenpakete
Durchsatz-Statistik	INFO-TABELLE	Statistik für die auf jedem Kanal übertragenen Bytes
Werte löschen	AKTION	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:

lfc	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:

lfc	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:

lfc	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:

lfc	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:

lfc	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:

lfc	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:

lfc	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:

lfc	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	INFO	Anzahl empfangener Datenpakete
LAN-Tx-Pakete	INFO	Anzahl gesendeter Datenpakete
LAN-Rx-Fehler	INFO	Anzahl fehlerhaft empfangener Datenpakete
LAN-Tx-Fehler	INFO	Anzahl fehlerhaft gesendeter Datenpakete
LAN-Stack-Fehler	INFO	Anzahl Pakete ohne passendes Empfangsmodul (Bridge/Router)
LAN-NIC-Fehler	INFO	Anzahl vom NIC verworfener Datenpakete
LAN-Heap-Pakete	INFO	Anzahl verfügbarer Puffer
LAN-Queue-Pakete	INFO	Anzahl belegter Puffer
LAN-Queue-Fehler	INFO	Anzahl durch Puffermangel verworfener Pakete
LAN-Kollisionen	INFO	Anzahl Kollisionen während des Sendevorgangs
Verbindung-aufgebaut	INFO	Anzeige der korrekten Verbindung auf dem Ethernet (Datenübertragung möglich). Entspricht der 'Link'-LED am Gerät.
Verhandlung-abgeschlossen	INFO	
Anschluß	INFO	
LAN-Rx-Bytes	INFO	Anzahl vom LAN empfangener Zeichen
LAN-Tx-Bytes	INFO	Anzahl zum LAN gesendeter Zeichen
LAN-Rx-Broadcasts	INFO	Anzahl vom LAN empfangener Broadcast-Pakete
LAN-Rx-Multicasts	INFO	Anzahl vom LAN empfangener Multicast-Pakete
LAN-Rx-Unicasts	INFO	Anzahl vom LAN empfangener direkt adressierter Pakete
WAN-Rx-Broadcasts	INFO	Anzahl vom WAN empfangener Broadcasts
WAN-Rx-Multicasts	INFO	Anzahl vom WAN empfangener Multicasts
WAN-Rx-Unicasts	INFO	Anzahl vom WAN empfangener Unicasts
Werte löschen	AKTION	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	INFO-TABELLE	Statistik über Zustand der PPP-Protokollverhandlung für jedes Interface
LCP-Statistik	MENU	Anzeige der PPP/LCP-Statistiken
PAP-Statistik	MENU	Anzeige der PPP/PAP-Statistik
CHAP-Statistik	MENU	Anzeige der PPP/CHAP-Statistik
CBCP-Statistik	MENU	Anzeige der PPP/CBCP-Statistik
IPXCP-Statistik	MENU	Anzeige der PPP/IPXCP-Statistik
IPCP-Statistik	MENU	Anzeige der PPP/IPCP-Statistik
CCP-Statistik	MENU	Anzeige der PPP/CCP-Statistik
ML-Statistik	MENU	Anzeige der PPP/ML-Statistik
BACP-Statistik	MENU	Anzeige der PPP/BACP-Statistik
Rx-Optionen	MENU	Anzeige der empfangenen LCP-, IPCP- und IPXCP-Informationen
Tx-Optionen	MENU	Anzeige der gesendeten LCP-, IPCP- und IPXCP-Informationen
Werte löschen	AKTION	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:

lfc	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:

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

Status/PPP-Statistik/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	INFO-TABELLE	Informationen über Paketgrößen, Steuerzeichen, Sicherungsverfahren und Rückruf
IPCP	INFO-TABELLE	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 <i>ELSA LANCOM</i> 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/IPX-Statistik

Hier werden die Statistiken aus dem IPX-Bereich gesammelt, gegliedert nach Typen-, Socket- und Router-Informationen. In der IPX-Statistik finden Sie die folgenden Parameter:

/IPX-Statistik	Statistiken aus dem IPX- und IPX-Router-Bereich	
MAC-Statistik	MENU	Statistiken aus dem Media Access Control von IPX-Paketen
Watchdog-Statistik	MENU	Statistiken für Watchdog-Pakete
Propagate-Statistik	MENU	Statistiken für IPX-Propagated-Pakete (IPX-Typ 20)
RIP-Statistik	MENU	Statistiken für NetWare-RIP
SAP-Statistik	MENU	Statistiken für NetWare-SAP
IPX-Router-Statistik	MENU	Statistiken des Remote-IPX-Routers
Werte löschen	AKTION	IPX-Statistiken löschen

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

Status/IPX-Statistik/MAC-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

IPX-LAN-Rx	Anzahl vom LAN empfangener IPX-Pakete
IPX-LAN-Rx-Broadcasts	Anzahl vom LAN empfangener Broadcast-IPX-Pakete
IPX-LAN-Rx-Multicasts	Anzahl vom LAN empfangener Multicast-IPX-Pakete
IPX-LAN-Rx-Unicasts	Anzahl vom LAN empfangener direkt adressierter IPX-Pakete

IPX-LAN-Tx	Anzahl zum LAN gesendeter IPX-Pakete
IPX-WAN-Rx	Anzahl vom WAN empfangener IPX-Pakete
IPX-WAN-Rx-Broadcasts	Anzahl vom WAN empfangener Broadcasts
IPX-WAN-Rx-Multicasts	Anzahl vom WAN empfangener Multicasts
IPX-WAN-Rx-Unicasts	Anzahl vom WAN empfangener direkt adressierter IPX-Pakete
IPX-WAN-Tx	Anzahl zum WAN gesendeter IPX-Pakete
Werte löschen	MAC-Statistik löschen

Status/IPX-Statistik/Watchdog-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

IPX-Watchdog-LAN-Rx	Anzahl vom LAN empfangener IPX-Watchdog-Pakete
IPX-Watchdog-LAN-Tx	Anzahl zum LAN gesendeter IPX-Watchdog-Pakete
IPX-Watchdog-WAN-Rx	Anzahl vom WAN empfangener IPX-Watchdog-Pakete
IPX-Watchdog-WAN-Tx	Anzahl zum WAN gesendeter IPX-Watchdog-Pakete
SPX-Watchdog-LAN-Rx	Anzahl vom LAN empfangener SPX-Watchdog-Pakete
SPX-Watchdog-LAN-Tx	Anzahl zum LAN gesendeter SPX-Watchdog-Pakete
SPX-Watchdog-WAN-Rx	Anzahl vom WAN empfangener SPX-Watchdog-Pakete
SPX-Watchdog-WAN-Tx	Anzahl zum WAN gesendeter SPX-Watchdog-Pakete
Werte löschen	Watchdog Statistik löschen

Status/IPX-Statistik/Propagate-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

Propagate-LAN-Rx	Anzahl vom LAN empfangener IPX-Propagated-Pakete
Propagate-LAN-Filter	Anzahl vom LAN empfangener/gefilterter IPX-Propagated-Pakete
Propagate-LAN-Tx	Anzahl zum LAN gesendeter IPX-Propagated-Pakete
Propagate-LAN-Socket-Fehler	Anzahl vom LAN über Socket-Filter gefilterter IPX-Propagated-Pakete
Propagate-LAN-Hop-Fehler	Anzahl vom LAN über Hop-Count gefilterter IPX-Propagated-Pakete
Propagate-LAN-Backroute-Fehler	Anzahl vom LAN zurückzuroutende IPX-Propagated-Pakete
Propagate-LAN-Contention	Anzahl vom LAN zu routende Pakete während einer falschen Verbindung
Propagate-WAN-Rx	Anzahl vom WAN empfangener IPX-Propagated-Pakete
Propagate-WAN-Filter	Anzahl vom WAN empfangener/gefilterter IPX-Propagated-Pakete

Propagate-WAN-Tx	Anzahl zum WAN gesendeter IPX-Watchdog-Pakete
Propagate-WAN-Socket-Fehler	Anzahl vom WAN über Socket-Filter gefilterter IPX-Propagated-Pakete
Werte löschen	IPX-Propagated-Paket-Statistik löschen

Status/IPX-Statistik/RIP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

RIP-LAN-Rx	Anzahl vom LAN empfangener RIP-Pakete
RIP-LAN-Fehler	Anzahl vom LAN empfangener RIP-Pakete mit fehlerhaftem Inhalt
RIP-LAN-Tx	Anzahl zum LAN gesendeter RIP-Pakete
RIP-WAN-Rx	Anzahl vom WAN empfangener RIP-Pakete
RIP-WAN-Fehler	Anzahl vom WAN empfangener RIP-Pakete mit fehlerhaftem Inhalt
RIP-WAN-Tx	Anzahl zum WAN gesendeter RIP-Pakete
Werte löschen	RIP-Statistik löschen
Tabelle-RIP	Anzeige der RIP-Tabelle

Tabelle-RIP

In der **RIP-Tabelle** finden Sie 256 Einträge mit RIP-Informationen. Sie hat den folgenden Aufbau:

Netzwerk	Hops	Tics	Node-ID	Zeit	Flags
Adresse des Netzwerks	Anzahl der zu passierenden Router auf dem Weg zum anderen Netz	Benötigte Zeit für diese Route in tics	MAC-Adresse des Servers	Anzahl der Aktualisierungen der Tabelle, bis der Eintrag entfernt wird	lokal, remote, loop oder down

Status/IPX-Statistik/SAP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

SAP-LAN-Rx	Anzahl vom LAN empfangener SAP-Pakete
SAP-LAN-Fehler	Anzahl vom LAN empfangener SAP-Pakete mit fehlerhaftem Inhalt
SAP-LAN-Tx	Anzahl zum LAN gesendeter SAP-Pakete
SAP-WAN-Rx	Anzahl vom WAN empfangener SAP-Pakete
SAP-WAN-Fehler	Anzahl vom WAN empfangener SAP-Pakete mit fehlerhaftem Inhalt
SAP-WAN-Tx	Anzahl zum WAN gesendeter SAP-Pakete
Werte löschen	SAP-Statistik löschen
Tabelle-SAP	Anzahl vom LAN empfangener SAP-Pakete

Tabelle-SAP

In der **SAP-Tabelle** finden Sie 512 Einträge mit SAP-Informationen. Sie hat den folgenden Aufbau:

Typ	Server-Name	Netzwerk	Node-ID	Socket	Hops	Zeit	Flags
SAP-Nr. des Dienstes	Rechnername des Servers	Adresse des Netzwerks	MAC-Adresse des Servers	Socket für den Dienst	Anzahl der Router bis zum Ziel-Netz	Anzahl der Aktualisierungen der Tabelle, bis der Eintrag entfernt wird	lokal, remote, loop oder down

Status/IPX-Statistik/IPX-Router-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

IPXr-LAN-Rx	Anzahl vom LAN zu routender IPX-Pakete
IPXr-LAN-Tx	Anzahl zum LAN gerouteter IPX-Pakete
IPXr-LAN-Hop-Fehler.	Anzahl vom LAN zu routender über Hop-Count gefilterter IPX-Pak.
IPXr-LAN-Socket-Fehler	Anzahl vom LAN zu routender über Socket-Filter gefilterter IPX-Pakete
IPXr-LAN-Netzwerk-Fehler	Anzahl vom LAN zu routende Pakete zu falschen Netzwerken
IPXr-LAN-Backroute-Fehler	Anzahl vom LAN zurückzuroutende IPX-Pakete
IPXr-LAN-Contention	Anzahl vom LAN zu routender Pakete während einer falschen Verbindung
IPXr-LAN-Down-Fehler	Anzahl vom LAN zu routender IPX-Pakete zu abgemeldeten Netzen
IPXr-WAN-Rx	Anzahl vom WAN zu routender IPX-Pakete
IPXr-WAN-Tx	Anzahl zum WAN gerouteter IPX-Pakete
IPXr-WAN-Hop-Fehler.	Anzahl vom WAN zu routender über Hop-Count gefilterter IPX-Pakete
IPXr-WAN-Socket-Fehler	Anzahl vom WAN zu routender über Socket-Filter gefilterter IPX-Pak.
IPXr-WAN-Netzwerk-Fehler	Anzahl vom WAN zu routender Pakete zu falschen Netzwerken
IPXr-WAN-Backroute-Fehler	Anzahl vom WAN zurückzuroutender IPX-Pakete
IPXr-WAN-Down-Fehler	Anzahl vom WAN zu routender IPX-Pakete zu abgemeldeten Netzen
IPXr-Int-Rx	Anzahl der Pakete von internen Modulen an den IPX-Router
Netzwerke	Tabelle der Netzwerke in der IPX-Routing-Tabelle mit Node-IDs
Werte löschen	IPX-Router-Statistik löschen
Aufbau-Tabelle	Tabelle der letzten 20 Pakete, die eine Verbindung erforderten

Aufbau-Tabelle

Die **Aufbau-Tabelle** ist ein weiterer Unterpunkt der Router-Statistik. Darin finden Sie die letzten 20 Einträge mit Informationen über die Systemzeit, die IPX-Ziel-Adresse, die IPX-Quell-Adresse der Datenpakete, die zu einem Verbindungsaufbau geführt haben.

Eine IPX-Aufbau-Tabelle kann wie folgt aussehen:

Systemzeit	Ziel-Adresse	Quell-Adresse
1T; 16:45:01	00000081 ffffffff 0453	00000001 00a05702000a 0453
1T; 10:45:10	00000081 ffffffff 0452	00000001 00a05702000a 0452

Als 'Systemzeit' wird entweder die Betriebszeit des Geräts angezeigt oder die Echtzeit des ISDN-Netzes (falls diese vom ISDN-Anschluß zur Verfügung gestellt wird). Die Ziela-dresse 'ffffffff' deutet z.B. auf ein Broadcast-Paket hin. Die Ziel- und Quell-Adressen besteht jeweils aus der Netzwerknummer, MAC-Adresse und der Socketnummer (alles hexadezimale Werte).

Netzwerke

Auch die **Netzwerk-Statistik** ist der IPX-Router-Statistik untergliedert. Diese Tabelle zeigt erweiterte Informationen zu einer statischen Route (Gegenstelle). Sie hat den folgenden Aufbau:

Gegenstelle	Netzwerk	Binding	Propagate	Backoff	Zeit	Node-ID
logische Gegenstelle	Netzwerk- Adresse	Binding	Route /Filter	Aufbau- Zähler	Restzeit bis zum nächsten Aufbau	Node-ID der Gegenstelle

Die Einträge haben die folgende Bedeutung:

Gegenstelle	Logischer Name der Gegenstelle, wie in der Routing-Tabelle eingetragen. Zusätzlich ist noch ein Eintrag für die LAN-Anbindung vorhanden. Dieser steht an erster Stelle der Tabelle und hat den Namen „LAN“.
Netzwerk	Adresse des Netzwerks in dem sich die Gegenstelle befindet. Für WAN-Gegenstellen entspricht dieser dem Eintrag in der Routing-Tabelle. Falls in der IPX-Routing-Tabelle (/SETUP/IPX-MODUL/LAN-EINSTELLUNG/NETZWERK) die Autodetect-Funktion eingestellt ist, kann an dieser Stelle abgelesen werden, welches Netzwerk erkannt wurde.
Binding	Ethernet-Binding, auf das die Gegenstelle gebunden ist. Für WAN-Gegenstellen entspricht dieses dem Eintrag in der Routing-Tabelle. Falls in der IPX-Routing-Tabelle (/SETUP/IPX-MODUL/LAN-EINSTELLUNG/NETZWERK) die Autodetect-Funktion eingestellt ist, kann an dieser Stelle abgelesen werden, welches Binding erkannt wurde.
Propagate	Filterflag für IPX Typ 20 (propagated) Frames. Für WAN-Gegenstellen entspricht dieses dem Eintrag in der Routing-Tabelle. Für das LAN ist hier immer Route eingetragen.
Backoff	Aufbau-Zähler für den Exponential-Backoff-Algorithmus. Wenn der Aufbau-Zähler den Wert 16 hat, so wird kein erneuter Versuch mehr durchgeführt, die Route ist damit inaktiv (auch für das LAN möglich).
Zeit	Restzeit bis zum nächsten Aufbauversuch des Exponential-Backoff-Algorithmus in Sekunden. War ein Aufbau erfolgreich, so wird die Restzeit auf Null gesetzt. Damit ist die Route aktiv.
Node-ID	Node-ID des zuständigen Routers im WAN-Netz. Für den LAN-Eintrag ist hier die Node-ID des Routers eingetragen.

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	MENU	Statistiken aus dem ARP-Bereich
IP-Statistik	MENU	Statistiken aus dem IP-Bereich
ICMP-Statistik	MENU	Statistiken für ICMP-Pakete
TCP-Statistik	MENU	Statistiken für TCP-Pakete von TCP-Sitzungen zum Router
TFTP-Statistik	MENU	Statistiken für TFTP-Operationen
DHCP-Statistik	MENU	Statistiken aus dem DHCP-Server
NetBIOS-Statistik	MENU	Statistiken aus dem NetBIOS-Modul
DNS-Statistik	MENU	Statistiken aus dem DNS-Server
Werte löschen	AKTION	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-Acknowledges
TFTP-LAN-Tx-Option-Ack.	Anzahl auf das LAN gesendeter TFTP-Option-Ack
TFTP-LAN-Tx-Fehler	Anzahl auf das LAN gesendeter TFTP-Error-Pakete
TFTP-LAN-Tx-Wiederholungen	Anzahl wiederholt aufs LAN gesendeter TFTP-Pakete
TFTP-LAN-Verbindungen	Anzahl zum LAN aufgebauter TFTP-Verbindungen
TFTP-WAN-Rx	Anzahl vom WAN empfangener TFTP-Pakete
TFTP-WAN-Rx-Read-Request	Anzahl vom WAN empfangener TFTP-Read-Requests
TFTP-WAN-Rx-Write-Request	Anzahl vom WAN empfangener TFTP-Write-Requests

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

Status/TCP-IP-Statistik/DHCP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

DHCP-LAN-Rx	Anzahl aus dem LAN empfangener DHCP-Pakete
DHCP-LAN-Tx	Anzahl in das LAN gesendeter DHCP-Pakete
DHCP-WAN-Rx	Anzahl aus dem WAN empfangener DHCP-Pakete
DHCP-Verworfen	Anzahl verworfener DHCP-Pakete
DHCP-Rx-Discover	Anzahl empfangener Discover-Messages
DHCP-Rx-Request	Anzahl empfangener Request-Messsges
DHCP-Rx-Dcline	Anzahl empfangener Decline-Messages
DHCP-Rx-Inform	Anzahl empfangener Inform-Messages
DHCP-Rx-Release	Anzahl empfangener Release-Messages
DHCP-Tx-Offer	Anzahl gesendeter Offer-Messages
DHCP-Tx-Ack.	Anzahl bestätigter DHCP-Pakete
DHCP-Tx-Nak	Anzahl nicht bestätigter DHCP-Pakete
DHCP-Server-Fehler	Anzahl empfangener DHCP-Pakete, die nicht für diesen Server bestimmt waren
DHCP-Zugewiesen	Anzahl aktuell zugewiesener Adressen
DHCP-MAC-Konflikte	Anzahl abgelehnter Zuweisungen aufgrund belegter IP-Adressen
Tabelle-DHCP	Tabelle mit den Zuweisungen von IP-Adressen zu MAC-Adressen
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	INFO	Anzahl der NetBIOS-Pakete, die vom LAN bzw. WAN empfangen wurden
LAN-Tx, WAN-Tx	INFO	Anzahl der NetBIOS-Pakete, die auf das LAN bzw. WAN gesendet wurden
Registrierungen	INFO	Anzahl der erfolgten Namenregistrierungen
Konflikte	INFO	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	INFO	Anzahl der erfolgten Namensfreigaben
Erneuerungen	INFO	Anzahl der erfolgten Namenserneuerungen (Refresh)
Timeouts	INFO	Anzahl der durch Alterung herausgefallenen Namen
B-Knoten	INFO	Anzahl der gerade aktiven B-Knoten (Broadcast) im Netz
P-Knoten	INFO	Anzahl der gerade aktiven P-Knoten (Peer-to-Peer) im Netz
M-Knoten	INFO	Anzahl der gerade aktiven M-Knoten (Mixed-Mode) im Netz
W-Knoten	INFO	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 Namenverhandlung 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	INFO	Anzahl der DNS-Pakete, die vom LAN empfangen wurden
LAN-Tx	INFO	Anzahl der DNS-Pakete, die zum LAN gesendet wurden
WAN-Rx	INFO	Anzahl der DNS-Pakete, die vom WAN empfangen wurden
WAN-Tx	INFO	Anzahl der DNS-Pakete, die zum WAN gesendet wurden
Forwarded	INFO	Anzahl der Anfragen, die nicht beantwortet werden konnten und daher über den Forwarding-Mechanismus weitergeleitet wurden
Fehler	INFO	Anzahl von ungültigen Anfragen
DNS-Zugriffe	INFO	Gibt an, wie viele Namen aus der DNS-Tabelle aufgelöst wurden
DHCP-Zugriffe	INFO	Gibt an, wie viele Namen aus der DHCP-Tabelle aufgelöst wurden
NetBIOS-Zugriffe	INFO	Gibt an, wie viele Namen aus den NetBIOS-Tabellen aufgelöst wurden
Filter	INFO-TABELLE	Anzahl der über die Filtertabelle gefilterten DNS-Pakete
Hit-Liste	INFO-TABELLE	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	INFO	Anzahl vom LAN zu routender Datenpakete
IPr-LAN-Tx	INFO	Anzahl zum LAN gerouteter Datenpakete
IPr-LAN-lokales-Routing	INFO	Anzahl vom LAN empfangener und zum LAN gerouteter Pakete
IPr LAN-Netzwerk-Fehler	INFO	Anzahl LAN-Pakete, die nicht geroutet wurden
IPr-LAN-Routing-Fehler	INFO	Anzahl LAN-Pakete, die zu einem anderen Router müssen
IPr-LAN-TTL-Fehler	INFO	Anzahl LAN-Pakete mit einem abgelaufenen Time-to-Live-Wert
IPr-LAN-Filter	INFO	Anzahl der über die Filtertabelle gefilterten LAN-Pakete
IPr-LAN-verworfen	INFO	Anzahl der verworfenen LAN-Pakete
IPr-WAN-Rx	INFO	Anzahl vom WAN zu routender Datenpakete
IPr-WAN-Tx	INFO	Anzahl zum WAN gerouteter Datenpakete
IPr-WAN-Netzwerk-Fehler	INFO	Anzahl WAN-Pakete, die nicht geroutet wurden
IPr-WAN-TTL-Fehler	INFO	Anzahl WAN-Pakete mit einem abgelaufenem Time-to-Live-Wert
IPr-WAN-Filter	INFO	Anzahl der über die Filtertabelle gefilterten WAN-Pakete
IPr-WAN-verworfen	INFO	Anzahl der verworfenen WAN-Pakete
IPr-WAN-Typ-Fehler	INFO	Anzahl der Pakete vom WAN ohne IP-Router-Kennung
IPr-ARP-Fehler	INFO	Anzahl der nicht erfolgreichen Zugriffe auf den ARP-Cache
Aufbau-Tabelle	INFO-TABELLE	Tabelle der letzten 20 Pakete, die eine Verbindung erforderten
Protokoll-Tabelle	INFO-TABELLE	Tabelle über geroutete Pakete, protokollabhängig aufgestellt
RIP-Statistik	MENU	Statistiken aus dem IP/RIP-Bereich
Werte löschen	AKTION	IP-Router-Statistik löschen

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 UDP und Z-Port 53).

Protokoll-Tabelle

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

Eine Protokoll-Tabelle kann wie folgt aussehen:

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

Status/IP-Router-Statistik/RIP-Statistik

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

RIP-Rx	Anzahl empfangener IP-RIP-Pakete
RIP-Request	Anzahl empfangener IP-RIP-Request-Pakete
RIP-Response	Anzahl empfangener IP-RIP-Response-Pakete
RIP-verworfen	Anzahl verworfener IP-RIP-Pakete
RIP-Fehler	Anzahl fehlerhafter IP-RIP-Pakete
RIP-Eintrag-Fehler	Anzahl fehlerhafter Einträge in IP-RIP-Paketen
RIP-Tx	Anzahl gesendeter IP-RIP-Pakete
Tabelle-RIP	Routing-Tabelle der durch RIP-Broadcast gelernten Routen
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	INFO	Anzahl aktueller Konfigurationsverbindungen vom LAN
LAN-Ges.-Verbindungen	INFO	Anzahl bisheriger Konfigurationsverbindungen vom LAN
WAN-Akt.-Verbindungen	INFO	Anzahl aktueller Konfigurationsverbindungen vom WAN
WAN-Ges.-Verbindungen	INFO	Anzahl bisheriger Konfigurationsverbindungen vom WAN
Outband-Akt.-Verbindungen	INFO	Anzahl aktueller Outband-Konfigurationsverbindungen
Outband-Ges.-Verbindungen	INFO	Anzahl bisheriger Outband-Konfigurationsverbindungen
Outband-Bitrate	INFO	Bitrate der letzten Outband Konfigurationssitzung
Login-Fehler	INFO	Gesamtzahl der fehlerhaften Logins
Login-Sperren	INFO	Anzahl der Login-Sperrungen
Login-Ablehnungen	INFO	Anzahl der Login-Versuche, während die Login-Sperre aktiv war
Werte löschen	AKTION	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	INFO	Anzahl verfügbarer Puffer
LAN-Queue-Pakete	INFO	Anzahl belegter Puffer
WAN-Heap-Pakete	INFO	Anzahl verfügbarer Puffer
WAN-Queue-Pakete	INFO	Anzahl belegter Puffer
ARP-Query-Queue-Pakete	INFO	Anzahl der ARP-Pakete in der Query-Queue
ARP-Queue-Pakete	INFO	Anzahl der ARP-Pakete in der normalen Queue
IP-Queue-Pakete	INFO	Anzahl der IP-Pakete in der normalen Queue
IP-Urgent-Queue-Pakete	INFO	Anzahl der IP-Pakete in der gesicherten Queue
ICMP-Queue-Pakete	INFO	Anzahl der ICMP-Pakete
TCP-Queue-Pakete	INFO	Anzahl der TCP-Pakete
TFTP-Queue-Pakete	INFO	Anzahl der TFTP-Pakete
SNMP-Queue-Pakete	INFO	Anzahl der SNMP-Pakete
Prot-Heap-Pakete	INFO	Anzahl der Prot-Heap-Pakete

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

lfc	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:

lfc	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:

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	bezeichnet den zugehörigen Kanal.
Status	gibt den Zustand der jeweiligen Verbindung an. Mögliche Werte sind: Initialisierung , Setup-WAN , Bereit , Anwahl , Anliegen-der-Ruf , Protokoll , Verbindung , Rückruf sowie Bündelung und Reserviert . Der Status Bündelung wird im Display (nur <i>ELSA LANCOM Wireless</i>) 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:

lfc	Layername	Encaps	Lay-3	Lay-2	L2-Opt.	Lay-1
Ch01 Ch02	DEFAULT PPPHDL	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	lfc	CLIP-Anrufer	Wahl-Anrufer	Dienst	B-Kanal
OT; 00:20:57	S ₀	5678	1234	HDLC64K	2
OT; 00:20:46	S ₀	4321	1234	HDLC64K	1
OT; 00:19:47	S ₀	4321	1234	HDLC64K	1
OT; 00:11:33	S ₀	5678	1234	HDLC64K	1
OT; 00:01:13	S ₀	4321	1234	HDLC64K	2
OT; 00:01:02	S ₀	4321	1234	HDLC64K	1
OT; 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).
lfc	Bezeichnet das zugehörige Interface.
CLIP-Anrufer	Die Rufnummer (CLIP) des Anrufers
Wahl-Anrufer	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. <i>LANCOM Office</i> -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 hundert Verbindungen mit Informationen über die Gegenstelle angezeigt.

Die Tabelle hat den folgenden Aufbau:

Verb.-Start	Gegenstelle	Anw.	Ifc	Verb.-Zeit	Gebühren
OT; 00:20:57	BERLIN	Akt.	Ch01	50	5
OT; 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 Gegenstellename
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/S₀-Bus

Unter diesem Menüpunkt wird der aktuelle Zustand der S₀-Schnittstelle angezeigt. Die Statistik hat den folgenden Aufbau:

/S ₀ -Bus	Fortlaufende Statusanzeigen	
D-Info	INFO-TABELLE	Übersicht über den Zustand eines D-Kanals.
D2-Statistik	INFO-TABELLE	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 dentifizier.
L2-Aktivierung	Aktivierung der Schicht 2 des D-Kanals ('Ja' oder 'Nein').
Verbindungen	Anzahl der Verbindungen, die über die angezeigte TEI abgewickelt wurden.

Status/Kanal-Statistik

Diese Tabelle zeigt Ihnen Informationen über den aktuellen Zustand der beiden B-Kanäle. Beim *ELSA LANCOM Wireless* werden auch Informationen über die a/b-Ports angezeigt. Die Informationen aus dieser Tabelle werden hauptsächlich zur Ausgabe über *ELSA LAN-monitor* 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 0	Router	akt.	0000	0241123456	00000000	3	0		
S ₀ -B1	00000000 0	a/b	akt.	0000	0241123457	00000000	2	20		
S ₀ -B2	00000000 0	Lancapi	pass.	0000	0241123458	00000000	4	180		

Kanal	Zustand	App	Mode	Cause	Rufnummer	Subadr.	Geb.	Verb.-Zeit	Extra
DSL-ERR	00000000	keine	akt.	0000	0241123456	00000000	3	0	
DSL-Line	00000000	Router	fest	0000	0241123456	00000000	2	20	
S ₀ -1-ERR	00000000	keine	unb.	0000	0241123456	00000000			
S ₀ -1-B1	00000000	keine	unb.	0000	0241123456	00000000			
S ₀ -1-B2	00000000	keine	unb.	0000	0241123456	00000000			

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Kanal	Kanal, für den der Eintrag gilt. Es wird immer nur der letzte Zustand eines Kanals angezeigt. Für Fehlermeldungen auf Kanälen wird ein eigener „Kanal“ geführt.
Zustand	Als Zustand eines Kanals wird hier z.B. 'bereit' angezeigt.
App	Applikation, die den Kanal belegt: Router <i>LANCAPI</i>
Mode	Art des letzten Verbindungsaufbaus: aktiv 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 <i>LANCAPI</i> 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	INFO	Aktuelle Zeit des Geräts
Quelle	INFO	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	INFO	Anzahl der bisher erfolgten Zeit-Übernahmen aus einer der vorher genannten Quellen
ISDN	MENU	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
Einheiten	

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

Status/PCMCIA-Status

Hier finden sich einige allgemeine Informationen zur eingesteckten Karte:

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

Status/Gebühren-Statistik

In diesem Menü werden die aktuellen Werte aus dem Gebührenmodul angezeigt:

Resttage/Per.	INFO	Anzahl der verbleibenden Tage bis zum Ablauf des Überwachungszeitraums.
Rest-Budget	INFO	Restbudget in der aktuellen Überwachungsperiode.
Router-Einheiten	INFO	Anzahl der von den Routermodulen in der aktuellen Überwachungsperiode verbrauchten Einheiten.
Gesamt-Einheiten	INFO	Anzahl der insgesamt in der aktuellen Überwachungsperiode verbrauchten Einheiten.
Tabelle-Budget	INFO-TABELLE	Genaue Auflistung der durch die einzelnen Module (Router/LAN-CAP/Zeit-Modul) auf dem ISDN angefallenen Gebühreneinheiten.
Rest-ISDN-Minuten	INFO	Restbudget in der aktuellen Überwachungsperiode.
Router-ISDN-Minuten	INFO	Gesamt-Onlinezeit auf dem ISDN-Interface seit Einschalten des Geräts.
Rest-DSL-Minuten	INFO	Restbudget in der aktuellen Überwachungsperiode.
Router-DSL-Minuten	INFO	Gesamt-Onlinezeit auf dem ISDN-Interface seit Einschalten des Geräts.
Zeit-Tabelle	INFO-TABELLE	Genaue Auflistung der durch die einzelnen Module (Router (ISDN) / Router (DSL) / LAN-CAP (ISDN) / Zeit-Modul (ISDN)) auf dem jeweiligen Interface angefallenen Onlinezeit.
Werte-Löschen	AKTION	Gebührenstatistik löschen

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	WERT	Eingabe des Gerätenamens
WAN-Modul	MENU	Einstellungen für das WAN
Accounting-Modul	MENU	Einstellungen für die Gebührenverwaltung
Gebühren-Modul	MENU	Einstellungen für die Gebührenverwaltung
LAN-Modul	MENU	Einstellungen für das LAN
WLAN-Modul	MENU	Einstellungen für das WLAN

/Setup	Konfiguration des Systems	
IPX-Modul	MENU	Einstellungen für das IPX-Modul
TCP-IP-Modul	MENU	Einstellungen für das TCP/IP-Modul
IP-Router-Modul	MENU	Einstellungen für das IP-Router-Modul
SNMP-Modul	MENU	Einstellungen für die Konfiguration über SNMP
DHCP-Modul	MENU	Einstellungen für den DHCP-Server
NetBIOS-Modul	MENU	Einstellungen für den NetBIOS-Proxy
Config-Modul	MENU	Einstellungen für das Konfigurationsmodul
DNS-Modul	MENU	Einstellungen für den DNS-Server
LANCAPi-Modul	MENU	Einstellungen für die <i>ELSA LANCAPI</i>
LCR-Modul	MENU	Einstellungen für den Least-Cost-Router
Zeit-Modul	MENU	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/Accounting-Modul

Im Accounting-Modul kann eingestellt werden, ob die Userdaten aufgezeichnet und im Flashrom abgespeichert werden sollen. Das Menü hat den folgenden Aufbau (incl. Default-Werten):

/Accounting-Modul	Einstellungen für die Gebührenverwaltung	
Zustand	WERT	Gibt an, ob die Accounting-Daten aufgezeichnet werden sollen oder nicht. Mögliche Werte sind Ein oder Aus.
Speichern-Flashrom	WERT	Gibt an, ob die Summen-Tabelle im Flashrom gespeichert werden soll oder nicht. Mögliche Werte sind Ja oder Nein.
Sortieren-nach	WERT	Gibt an wie die Summentabelle sortiert werden soll. Mögliche Werte sind Zeit (sortiert nach Onlinezeit) oder Daten (sortiert nach Transfervolumen).
Aktuelle User	INFO-TABELLE	In dieser Tabelle werden die Daten für alle aktuellen Verbindungen gehalten. Diese Tabelle ist halbdynamisch und beginnt mit zunächst 16 Einträgen. Ist die Tabelle voll, so wird sie um jeweils 16 weitere Einträge vergrößert.
Accounting-Liste	INFO-TABELLE	Hier wird die Summentabelle gespeichert. Diese Tabelle enthält die 512 Userinträge, die entweder die längste Onlinezeit belegt oder das größte Transfervolumen vorzuweisen haben
Loeschen-Accounting-Liste	AKTION	Löscht die Werte in der Accounting-Liste

Die Accounting-Liste hat folgenden Aufbau:

Username	Gegenstelle	Verb-Typ	Rx-KBytes	Tx-KBytes	Gesamt-Zeit	Verbindungen
User1	Internet	DSL-Verb.	234	45	43	4
User2	0	unbekannt	34	453	23	34

Die Summen-Tabelle und die Tabelle für die aktuelle Verbindung besitzen jeweils die gleichen Felder:

<i>Username</i>	Name des Users, bzw. falls dieser nicht aufgelöst werden kann, seine Layer-3-Adresse (IP-Adresse, IPX-Adresse oder Mac-Adresse).
<i>Gegenstelle</i>	Name der Gegenstelle zu der der User Daten übertragen hat bzw. von der Daten empfangen wurden.
<i>Verb.-Type</i>	Art der Verbindung, die zur Gegenstelle aufgebaut wurde. Mögliche Werte sind unbekannt, Wählverbindung, Festverbindung und DSL-Verbindung.
<i>Rx-, Tx-Bytes</i>	Datenvolumen auf dem Interface (als 64-bit-Zähler).
<i>Gesamt-Zeit</i>	Gesamte Onlinezeit für den User.
<i>Verbindungen</i>	Anzahl der für den User gezählten Verbindungsaufbauten.

Setup/Gebühren-Modul

Über diesen Menüpunkt werden notwendige Einstellungen für den Gebührenschatz vorgenommen.



Dabei haben die einzelnen Punkte die folgende Bedeutung:

Tage/Periode	Anzahl Tage in einem Überwachungszeitraum.
Budget-Einheiten	Budget an Gebühreneinheiten, das innerhalb des Überwachungszeitraums genutzt werden darf. Steht hier der Wert 0, so ist die Überwachung abgeschaltet.
Rest-Einheiten	Restbudget in der aktuellen Überwachungsperiode.
ISDN-Minuten-budget	Onlinezeit auf dem ISDN-Interface, die innerhalb des Überwachungszeitraums genutzt werden darf. Steht hier der Wert 0, so ist die Überwachung abgeschaltet
Rest-ISDN-Minuten	Restbudget in der aktuellen Überwachungsperiode.
Router-ISDN-Minuten	Gesamt-Onlinezeit auf dem ISDN-Interface seit Einschalten des Geräts.
DSL-Minuten-budget	Onlinezeit auf dem DSL-Interface, die innerhalb des Überwachungszeitraums genutzt werden darf. Steht hier der Wert 0, so ist die Überwachung abgeschaltet
Rest-DSL-Minuten	Restbudget in der aktuellen Überwachungsperiode.
Reserve-DSL-Budget	Zusätzliches Budget, daß auf dem DSL-Interface bis zum Ablauf des Überwachungszeitraums genutzt werden darf, wenn das normale DSL-Budget verbraucht wurde. Dieses Budget muß manuell freigeschaltet werden.
Router-DSL-Minuten	Gesamt-Onlinezeit auf dem ISDN-Interface seit Einschalten des Geräts.
Tabelle-Budget	Genaue Auflistung der durch die einzelnen Module (Router/LANCAPI/Zeit-Modul) auf dem ISDN angefallenen Gebühreneinheiten.
Zeit-Tabelle	Genaue Auflistung der durch die einzelnen Module (Router (ISDN) / Router (DSL) / LANCAPI (ISDN) / Zeit-Modul (ISDN)) auf dem jeweiligen Interface angefallenen Onlinezeit.
Aktivieren-Reserve	Mit dieser Aktion wird das Zusatzbudget freigeschaltet.

Wenn das jeweilige Budget abgelaufen ist baut das Gerät automatisch die Verbindung mit der Fehlermeldung 'Gebührensperre' ab. Ein weiterer Aufbau ist erst nach Ablauf des Überwachungszeitraums oder nach dem Aus- und wieder Einschalten des Geräts möglich. Zusätzlich kann ein neues Budget eingegeben werden. Hierdurch wird die Gebührensperre ebenfalls zurückgesetzt.

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	TABELLE	Einstellungen für das S ₀ -Interface
Router-Interface-Liste	TABELLE	Einstellungen für das Interface der Routermodule
ISDN-Namenliste	TABELLE	Einstellungen für die Gegenstellen
Round-Robin-Liste	TABELLE	Einstellungen verschiedener Gegenstellen-Nummern
Layerliste	TABELLE	Einstellungen der verwendeten Layer-Kombinationen
DSL-Namenliste	TABELLE	Einstellungen für die Gegenstellen
PPP-Liste	TABELLE	Einstellung der Parameter für PPP-Verbindungen
Nummernliste	TABELLE	Einstellung der zugangsberechtigten Rufnummern
Script-Liste	TABELLE	Einstellung der Anwahl-Scripte
Schutz	WERT	Schutz für die Annahme von eingehenden Rufen
RR-Versuche	WERT	Anzahl der Rückrufversuche, wenn die Gegenstelle besetzt ist
Manuelle-Wahl	MENU	Einstellungen für die manuelle Verbindungssteuerung

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

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

lfc	Protokoll	Anwahl-Prae	Max-pass-Verb.	Max-akt-Verb
S0	Auto	0	2	2

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
```

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 <i>ELSA LAN-COM Wireless</i> .
Anwahl-Præ	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.
Max-pass-Verb	Anzahl der maximal gleichzeitig möglichen passiven Verbindungen
Max-akt-Verb	Anzahl der maximal gleichzeitig möglichen aktiven Verbindungen

Router-Interface-Liste

Diese Tabelle enthält die Interface-Einstellungen, die für die Router-Module 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 <i>LANCAP</i> . 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 Kanalbündelung 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.

ISDN- 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 ISDN-Namenliste können 64 verschiedene Gerätenamen verwaltet werden, die z.B. so aussehen können:

Geraetenname	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 <i>ELSA LANCOM</i> 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 bestimmen 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). first: 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	bnd+compr.	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	keine	HDLC64K
MLPPP	TRANS	PPP	TRANS	bnd+compr.	HDLC64K
RAWHDLC	TRANS	TRANS	TRANS	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 <i>ELSA LANCOM</i> -Geräten oder im Bridge-Betrieb notwendig.
	ETHER	Die Daten werden mit einem Ethernet-Header versehen. Diese Einstellung ist zur Kommunikation mit älteren <i>ELSA LANCOM</i> -Geräten 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 <i>ELSA LANCOM</i> -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.
	SCTTRANS	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 <i>ELSA LANCOM</i> .	
	keine	Es erfolgt keine Datenkompression oder Kanalbündelung.
	compr.	Es erfolgt eine Datenkompression nach V.42bis (<i>ELSA LANCOM Wireless</i>) 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 Multi-link-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.

DSL-Namenliste Die in der DSL-Namenliste eingetragenen Gerätenamen werden vom Router benötigt, um die richtige Gegenstelle und den entsprechenden Layernamen zu ermitteln.

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

PPP-Liste

Die in der PPP-Liste eingetragenen Gerätenamen werden vom Router benötigt, um die zur Verbindung passenden Einstellungen für das Sicherungsverfahren und die PPP-Parameter zu ermitteln. Sie 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 <code>set ?</code> erhalten Sie eine Liste der erlaubten Zeichen.	
Zeit	In dieser Spalte kann der Zeitraum in Minuten zwischen zwei Überprüfungen der Gegenstelle eingetragen werden. Das Protokoll CHAP muß hierbei eingestellt sein. Standardwert: 0	
Wdh.	Hier kann die Anzahl der Wiederholungen von Überprüfungsversuchen eingestellt werden. Bei fehlgeschlagener Überprüfung wird die Verbindung sofort abgebrochen. Standardwert: 5	
Conf, Fail und Term	Durch diese Parameter kann die Arbeitsweise des PPP beeinflußt werden. Diese Parameter sind im RFC 1661 definiert und beschrieben. Die Standardwerte sind für die meisten Gegenstellen ausreichend. Wird hier nichts eingetragen, erscheinen diese Werte in der Anzeige als 0,0,0. In diesem Fall werden trotzdem die Standardwerte 10, 5, 2 benutzt. Diese Parameter können nur über SNMP oder TFTP (mit dem Konfigurationsprogramm <i>ELSA LANconfig</i>) verändert werden!	
Username	Benutzername (max. 64 Zeichen), der der Gegenstelle während der PPP-Verhandlung übermittelt wird. Damit meldet sich der Router bei der Gegenstelle an. Wird kein Username eingetragen, gilt der Gerätenamen 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	Gerätenamen
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 können, 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
CSEVERE	<>[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	AKTION	Aufbau einer Verbindung
Abbau	AKTION	Abbau von Verbindungen
Status	INFO	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.

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 Gegenstellennamen 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	WERT	Wahl des Netzwerkanschlusses
Node-ID	INFO	MAC-Layer-Adresse des Geräts
Heap-Reserve	WERT	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/IPX-Modul

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

/IPX-Modul	Einstellungen für das IPX-Modul (IPX-Router)	
Zustand	WERT	IPX-Modul ein- oder ausgeschaltet
IPX-Router	WERT	IPX-Router ein- oder ausgeschaltet
LAN-Einstellung	MENU	Einstellungen für die LAN-Seite
WAN-Einstellung	MENU	Einstellungen für die WAN-Seite
RIP-Einstellung	MENU	Einstellungen für RIP
SAP-Einstellung	MENU	Einstellungen für SAP

Zustand

Hier kann das IPX-Modul ein- bzw. ausgeschaltet werden. Standardmäßig ist das IPX-Modul eingeschaltet.



Die Remote-Konfiguration über DOS/IPX und der IPX-Router können nur benutzt werden, wenn das IPX-Modul eingeschaltet ist. Zur lokalen Konfiguration über LAN muß der Router nicht eingeschaltet sein.

IPX-Router

Hier kann der IPX-Router aktiviert bzw. deaktiviert werden. Standardmäßig ist der IPX-Router ausgeschaltet.



Beim Einschalten des IPX-Routers wird auch das IPX-Modul aktiviert. Der IPX-Router kann nur dann eingeschaltet werden, wenn unter LAN- und WAN-Einstellung unterschiedliche zulässige Netzwerkadressen eingetragen sind.

Setup/IPX-Modul/LAN-Einstellung

Hier können Einstellungen für die Datenpakete des LAN durchgeführt werden. Das Menü hat folgenden Aufbau:

/LAN-Einstellung	Einstellungen für die LAN-Seite	
Netzwerk	WERT	Logische IPX-Netzwerknummer des LAN-Anschlusses
Binding	WERT	Einstellung der Ethernet-Frame-Typen für den LAN-Anschluß
IPX-Watch	WERT	Einstellungen für IPX-Watchdog-Verwaltung
SPX-Watch	WERT	Einstellungen für SPX-Watchdog-Verwaltung
NetBIOS-Watch	WERT	Einstellungen für NetBIOS-Watchdog-Verwaltung
Socket-Filter	TABELLE	Filtertabelle für Zielsocketfilterung
Lok.-Routing	WERT	Lokales Routing aktiviert oder deaktiviert
RIP-SAP-Skal.	WERT	RIP-SAP-Skalierung aktiviert oder deaktiviert
LOOP-propagieren	WERT	Propagieren von redundanten Routen aktiviert oder deaktiviert

Netzwerk

Hier wird die IPX Netzwerknummer des Netware-Netzes (8stellig, hexadezimal) eingetragen, die an den LAN-Anschluß unter dem Binding (siehe unten) angeschlossen wird. Ist im lokalen Netzwerk ein NetWare-Server vorhanden, so kann der Router die Netzwerknummer und das Binding automatisch ermitteln.

Der Standardwert beträgt '00000000' und bedeutet, daß der Router die Netzwerknummer automatisch ermitteln soll.

Binding

Das Ethernet-Paketformat (Auto, II, 802.3, 802.2, SNAP) kann hiermit für den LAN-Anschluß eingestellt werden. Dieses Format muß zu dem im lokalen Netzwerk gebundenen Ethernetformat unter der eben beschriebenen Netzwerknummer passen.

Der Standardwert beträgt 'Auto' und bedeutet, daß der Router das Binding automatisch ermitteln soll (nur, wenn im lokalen Netzwerk ein NetWare-Server vorhanden ist).

IPX-Watch

Die Art der Verwaltung von IPX-Watchdog-Paketen wird hiermit festgelegt.

- **Filt.** bedeutet, daß IPX-Watchdog-Pakete weder lokal beantwortet noch übertragen werden. Dadurch wird ein Benutzer nach der im NetWare-Server eingestellten Zeit auf jeden Fall abgemeldet.

- **Route** bewirkt die Übertragung der Watchdog-Pakete und damit auch einen regelmäßigen Verbindungsaufbau durch Watchdog-Pakete des Servers.
- **Spoof** (Standard) sorgt dafür, daß IPX-Watchdog-Pakete lokal vom Router beantwortet werden, Benutzer also nicht mehr automatisch abgemeldet werden. Diese Einstellung ist besonders gebührenschonend, allerdings muß im Server eventuell dafür gesorgt werden, daß zu bestimmten Zeiten die Benutzer auf jeden Fall abgemeldet werden, um nicht zu viele Benutzerlizenzen zu belegen.

SPX-Watch Die Art der Verwaltung von SPX-Watchdog-Paketen wird hiermit festgelegt.

- **Route** bewirkt die Übertragung der SPX-Watchdog-Pakete und damit auch einen regelmäßigen Verbindungsaufbau durch SPX-Watchdog-Pakete des Servers.
- **Spoof** (Standard) sorgt dafür, daß SPX-Watchdog-Pakete lokal beantwortet werden. Diese Einstellung ist besonders gebührenschonend.

NetBIOS-Watch Dieser Punkt gibt an, wie mit NetBIOS-Watchdog-Paketen verfahren werden soll. NetBIOS-Watchdog-Pakete treten auf, wenn z.B. Windows-Netze auf IPX gebunden werden. Es sind die gleichen Optionen möglich wie bei IPX- oder SPX-Watchdog-Paketen (Filter, Route, Spoof).

Socket-Filter Die Socket-Filtertabelle ermöglicht die gezielte Filterung von LAN-Paketen zu bestimmten Ziel-Socket-Bereichen. Die Filterung erfolgt sowohl für einfache IPX-Pakete also auch für Propagated-IPX-Pakete. Folgende Sockets, die im Netzwerk periodisch versandt werden und deshalb zu häufigen Verbindungsaufbauten führen würden, sind bereits defaultmäßig in der LAN-Filter-Tabelle vorhanden (siehe dazu auch FAQs zum 'IPX-Router').

Anfangs-Socket	End-Socket
0455	0457
0550	0555
1401	1402
1480	1481
83ba	83ba
900f	9010

Lok.-Routing Mit dieser Einstellung wird die Skalierung von mehreren Routern in einem lokalen Netz unterstützt. Wenn bei einem Router schon alle Kanäle belegt sind, und es kommen trotzdem noch Pakete für andere Gegenstellen bei ihm an, haben möglicherweise andere Router in LAN noch freie Kanäle.

Ist die Option 'Lokales Routing' eingeschaltet, leitet der Router die Pakete auf dem lokalen Netz weiter zu einem Router, der eine Route zur angestrebten Gegenstelle propagiert hat. Der Router hat diese Route gespeichert, obwohl sie schlechter war als die eigene, und mit dem Flag 'Reserve' in der RIP-Tabelle markiert.

Die Default-Einstellung hierfür ist 'Aus', da ein IPX-Client nach einem Timeout einen RIP-Request für die gewünschte Route sendet und damit automatisch andere Router findet, über die das Zielnetz erreichbar ist.

RIP-SAP-Skal. Eine weitere Möglichkeit, die Skalierung zu unterstützen, ist, jede Route, zu der eine aktive Verbindung besteht, mit einem etwas besseren Tic-Count zu propagieren als der tatsächliche. Hierdurch werden alle Clients ihre Pakete für diese Routen an den Router schicken, der die Verbindung hat. Weiterhin können in dem Fall, in dem alle Kanäle belegt sind, die nicht mehr erreichbaren Routen als 'DOWN' propagiert werden. Da hierdurch bei jedem Verbindungsauf- und Abbau ein oder mehrere Broadcasts auf das LAN gesendet werden (durch die sich andere Router zu weiteren Broadcasts veranlaßt sehen könnten und somit eine hohe Netzlast entstehen kann), ist dieses Feature ein- und ausschaltbar. Die Default-Einstellung ist 'Aus'.

LOOP-propagieren Redundante Routen, d.h. Routen mit gleichem Tic- und Hopcount, werden nur den Gegenstellen mitgeteilt, von denen sie nicht empfangen wurden (Split Horizon). Mit dem Einschalten der Funktion 'LOOP-Propagieren' kann das Verbreiten dieser Routen trotzdem ermöglicht werden. Redundante Routen werden in der RIP-Tabelle mit dem Flag 'LOOP' gekennzeichnet.

Da die Verbreitung von redundanten Routen nach den Novell-Spezifikationen zwar nicht verboten ist, aber trotzdem möglichst unterlassen werden sollte, ist die Default-Einstellung 'Aus'.

Setup/IPX-Modul/WAN-Einstellung

Hier können Einstellungen der Datenpakete für den WAN-Anschluß durchgeführt werden. Das Menü hat folgenden Aufbau:

/WAN-Einstellung	Einstellungen für die WAN-Seite	
Routing-Tabelle	TABELLE	Router-Tabelle für die Zuordnung von IPX-Netzwerk und Gegenstelle
Socket-Filter	TABELLE	Filtertabelle für Ziel-Socketfilterung

Routing-Tabelle Die Routing-Tabelle kann bis zu 16 Gegenstellen und Zielnetze aufnehmen. Diese Tabelle hat folgende Einträge:

Gegenstelle	Netzwerk	Binding	Propagate	Backoff
Name der IPX Gegenstelle	Netzwerk-Adresse	802.3, II, 802.2, SNAP	Route / Filter	Ein /Aus

Hierbei bedeuten:

- **Gegenstelle:** Name der logischen Gegenstelle (wie in /Setup/WAN-Modul/ Namenliste angegeben).
- **Netzwerk:** Die Adresse des WAN-seitigen Netzwerk. Es muß ein eigenständiges Netzwerk verwendet werden, für die beiden beteiligten Router jedoch das gleiche!

- **Binding:** Zu verwendendes Ethernet-Binding auf der ISDN-Strecke. Diese Angabe wird nur berücksichtigt, wenn Ethernet-Encapsulation im verwendeten Layer eingestellt ist. Wird kein Binding eingegeben, so wird 802.3 angenommen.
- **Propagate:** Dieser Eintrag gibt an, wie mit IPX-Paketen vom Typ 20 (NetBIOS Propagated Frames) verfahren werden soll. Mögliche Einstellungen sind Route oder Filter. Hat dieses Feld den Eintrag **Filter** werden keine Propagated Frames an diese Gegenstelle weitergeleitet. Hat der Eintrag den Wert **Route**, so werden die Pakete an alle gerade erreichbaren Gegenstellen weitergeleitet, d.h., zu der Gegenstelle muß eine Verbindung bestehen, oder es ist mindestens ein Kanal für einen Verbindungsaufbau zur Gegenstelle verfügbar.

Besteht keine Verbindung und ist kein Kanal verfügbar, so wird das Paket verworfen. Daher können maximal maximal so viele Gegenstellen Propagated-Frames erhalten, wie gleichzeitige Verbindungen möglich sind. Die Default-Einstellung ist 'Filter'.

- **Backoff:** Der IPX-Router benutzt einen speziellen Algorithmus (Exponential Back-off), um bei Fehlkonfigurationen die anfallenden Verbindungskosten so gering wie möglich zu halten (siehe unten).

Wenn im entfernten Netz kein Server vorhanden ist (z.B. bei Remote-Access von einer Workstation), so kann der Router dies nicht erkennen und die entsprechende Gegenstelle wird nach spätestens einem Tag deaktiviert. Damit dies nicht geschieht kann der Exponential-Backoff-Algorithmus für diese Gegenstellen ausgeschaltet werden.

Die Default-Einstellung ist 'Ein'.

Socket-Filter

Die Socket-Filtertabelle ermöglicht die gezielte Filterung von WAN-Paketen zu bestimmten Ziel-Socket-Bereichen. Die Filterung erfolgt sowohl für einfache IPX-Pakete also auch für Propagated-IPX-Pakete.

Setup/IPX-Modul/RIP-Einstellung

Hier können Einstellungen für RIP-Datenpakete (Router-Informationen) hinterlegt werden. Das Menü hat folgenden Aufbau:

/RIP-Einstellung	Einstellungen für das RIP	
Tabelle-RIP	INFO-TABELLE	Anzeigen der RIP-Tabelle
LAN-Filtertab.	TABELLE	Filterbereiche für IPX-Netzwerkadressen (LAN)
WAN-Filtertab.	TABELLE	Filterbereiche für IPX-Netzwerkadressen (WAN)
Routen/Frm	WERT	Max. # RIP-Einträge pro gesendeten RIP-Frame
Aging	WERT	Aging-Zeitraum in Update-Einheiten
Spoofing	WERT	RIP-Spoofing-Verfahren einstellen
WAN-Update-Zeit	WERT	RIP-Update-Zeitraum, je nach Spoofing wirksam

Tabelle-RIP

Über diesen Menüpunkt werden die Einträge der aktuellen RIP-Tabelle angezeigt. Die Tabelle umfaßt maximal 256 Einträge.

Die Einträge in der RIP-Tabelle können wie folgt aussehen, wenn es zum Beispiel die Netzwerke 00000001, 00000002, 00000010, 00000081 gibt und diese über verschiedene Router erreicht werden können. Über die Flags kann ermittelt werden, wo diese Netzwerke, vom jeweiligen Router aus gesehen, liegen (**lokal** oder **remote**). Der Zusatz **direkt** gibt einen Hinweis darauf, daß dieses Netz direkt das lokale oder entfernte Netz ist. **DOWN** weist auf ein Netz hin, das bekannt, aber momentan nicht erreichbar ist. Die Tabelle ist nach den Netzwerknummern sortiert.

Netzwerk	Hops	Tics	Node-Id	Zeit	Flags
00000001	0	1	00a05702000a	0	lokal, direkt
00000002	1	2	00608c70ab56	1	lokal
00000010	2	7	00a057020014	1	lokal, DOWN
00000081	1	6	00a05702000b	0	remote, direkt

LAN-Filtertab.

Die LAN-Filtertabelle ermöglicht die gezielte Filterung von Routen, die über das lokale Netzwerk „gelernt“ werden. Gefilterte Routen erscheinen nicht in der IPX-RIP-Tabelle.

Eine LAN-Filtertabelle zur Filterung der Routen im Bereich 00001000 bis 00001fff sieht z.B. wie folgt aus:

Startnetz	Endnetz
00001000	00001fff

WAN-Filtertab.

Die WAN-Filtertabelle ermöglicht die gezielte Filterung von Routen, die über das Weitverkehrsnetzwerk „gelernt“ werden. Gefilterte Routen erscheinen nicht in der IPX-RIP-Tabelle.

Eine WAN-Filtertabelle zur Filterung der Routen im Bereich 00002000 bis 00002fff sieht z.B. wie folgt aus:

Startnetz	Endnetz
00002000	00002fff

Routen/FRM

Dieser Parameter setzt die maximale Anzahl von Routen, die in einem RIP-Frame enthalten sein können. Der ursprünglich von Novell definierte Vorgabewert ist 50. Heutzutage ist es jedoch üblich, eine höhere Anzahl von Routen in jeden Frame zu packen, da dies die Netzwerklast senkt. Falls alle beteiligten Geräte im Netzwerk eine höhere Anzahl unterstützen, kann dieser Wert auf bis zu 182 erhöht werden.

Aging

Hier kann die Anzahl der Updates (Aktualisierungsvorgänge der RIP-Tabelle) eingestellt werden, die durchgeführt werden, bis ein Eintrag in der RIP-Tabelle altert, d.h. die dort

vermerkte Route als „nicht erreichbar (down)“ markiert wird. Die Eingabemöglichkeiten reichen von 1 bis 60 bei einem Standardwert von 3.

Spoofing

Hiermit kann das Verhalten des Routers für RIP-Pakete eingestellt werden.

- Bei der Einstellung **Ohne** werden RIP-Pakete auf dem WAN genauso wie auf lokalen Netzwerken behandelt. Bei neuen Informationen und im Minutenabstand werden RIP-Daten zur Remote-Seite geschickt, also eine Verbindung wird aufgebaut.
- Die **Trig**-Einstellung bewirkt eine Verschiebung der RIP-Daten zur Remote-Seite immer dann, wenn Änderungen anfallen.
- Die **Zeit**-Einstellung bewirkt eine Verschiebung der RIP-Daten zur Remote-Seite in einem einzustellenden Zeitabstand (siehe unten).
- **pBack** (Standard) ist die gebührenschonendste Einstellung, wodurch RIP-Daten nur zur Gegenseite verschickt werden, wenn eine Verbindung aktiv ist.



Bei der Spoofing-Einstellung **pBack** altern Einträge aus der RIP-Tabelle nur dann, wenn eine Verbindung neu aufgebaut wird und gezielt ein Eintrag als „nicht erreichbar“ gekennzeichnet wurde.

WAN-Update-Zeit

Hier wird für eine Spoofing-Zeitsteuerung der zeitliche Übertragungsabstand angegeben, in dem RIP-Daten zur Gegenseite übertragen werden. Die Eingabemöglichkeiten reichen von 1 bis 60 Minuten bei einem Standardwert von 5.

Setup/IPX-Modul/SAP-Einstellung

Hier werden Einstellungen für SAP-Datenpakete (Server-Informationen) hinterlegt.

/SAP-Einstellung		Einstellungen für das SAP
Tabelle-SAP	INFO-TABELLE	Anzeigen der SAP-Tabelle
LAN-Filtertab.	TABELLE	Filterbereiche für IPX-Service-Adressen (LAN)
WAN-Filtertab.	TABELLE	Filterbereiche für IPX-Service-Adressen (WAN)
Server/Frm	WERT	Max. # SAP-Einträge pro gesendeten SAP-Frame
Aging	WERT	Aging-Zeitraum in Update-Einheiten
Spoofing	WERT	SAP-Spoofing-Verfahren einstellen
WAN-Update-Zeit	WERT	SAP-Update-Zeitraum, je nach Spoofing wirksam

Tabelle-SAP

Über diesen Menüpunkt werden die Einträge der aktuellen SAP-Tabelle angezeigt. Die Tabelle umfaßt maximal 512 Einträge. Die Tabelle ist nach dem Service-Typ und bei glei-

chem Typ nach Server-Namen sortiert. Eine beispielhafte SAP-Tabelle könnte wie folgt aussehen:

Typ	Server-Name	Netzwerk	Node-Id	Socket	Hops	Zeit	Flags
0004	Y	000000c1	000000000001	0451	1	1	lokal
0047	X	00000001	0000c0123456	8060	1	0	lokal
0107	Z	000000c1	000000000001	8104	2	1	lokal

Verschiedene SAP-Typen sind dort abgelegt. Nachzulesen ist der Server-Name, das zuständige Netzwerk, die MAC-Adresse des Servers (bei internen Server-Netzwerken 000000000001), die Socket-Nummer und Informationen über die Lokalität des Servers.

LAN-Filtertab.

Durch Einträge in der LAN-Filtertabelle ist es möglich, bestimmte Bereiche der Service-Informationen eines Novell-Netzwerks von der Aufnahme in die SAP-Tabelle auszuschließen und so die Ressourcen des IPX-Routers besser zu nutzen. Außerdem werden ungewünschte Verbindungsaufbauten durch diese SAPs (Dienste) verhindert.

Alle Service-Informationen, die sich innerhalb eines Filterbereiches der LAN-Filtertabelle befinden, werden nicht vom lokalen Netzwerk in die SAP-Tabelle des IPX-Routers übernommen. Sie werden ebenfalls nicht an die Gegenstelle des IPX-Routers übertragen und stehen daher dort auch nicht zur Verfügung.

Häufig sind z.B. die Service-Informationen der Printer-Server für die Gegenstelle des IPX-Routers nicht notwendig. Sollen diese Informationen durch die LAN-Filtertabelle von der Aufnahme in die SAP-Tabelle ausgeschlossen werden, ist folgender Eintrag notwendig:

Anfangsservice	Endservice
030c	030c

Eine Liste von SAP-Services mit Beschreibung finden Sie im Kapitel 'Novell-SAP-Nummern'.

WAN-Filtertab.

Analog zur LAN-Filtertabelle ist es durch die WAN-Filtertabelle möglich, Bereiche von Service-Informationen aus dem WAN von der Aufnahme in die SAP-Tabelle auszuschließen.

Die gesperrten Dienste haben damit allerdings auf der Gegenstelle schon zu einem Verbindungsaufbau geführt, bevor der Zielrouter sie WAN-seitig filtern konnte.

Aufbau und Funktion der WAN-Filtertabelle sind dabei völlig analog zur LAN-Filtertabelle. Eine WAN-Filtertabelle zur Filterung der File-Services sieht z.B. wie folgt aus:

Startservice	Endservice
0004	0004

Server/FRM

Dieser Parameter setzt die maximale Anzahl von Services, die in einem SAP-Frame enthalten sein können. Der ursprünglich von Novell definierte Vorgabewert ist 7. Heutzutage ist es jedoch üblich, eine höhere Anzahl von Services in jeden Frame zu packen, da dies die Netzwerklast senkt. Falls alle beteiligten Geräte im Netzwerk eine höhere Anzahl unterstützen, kann dieser Wert auf bis zu 22 erhöht werden.

Aging

Hier kann die Anzahl der Updates (Aktualisierungsvorgänge der SAP-Tabelle) eingestellt werden, die durchgeführt werden, bis ein Eintrag in der SAP-Tabelle altert, d.h. der dort vermerkte Service als „nicht erreichbar (down)“ markiert wird. Die Eingabemöglichkeiten reichen von 1 bis 60 bei einem Standardwert von 3.

Spoofing

Hiermit kann das Verhalten des Routers für SAP-Pakete eingestellt werden.

- Bei der Einstellung **Ohne** werden SAP-Pakete auf dem WAN genauso wie auf lokalen Netzwerken behandelt. Bei neuen Informationen und im Minutenabstand werden SAP-Daten zur Remote-Seite geschickt, also eine Verbindung wird aufgebaut.
- Die **Trig**-Einstellung bewirkt eine Verschickung der SAP-Daten zur Remote-Seite immer dann, wenn Änderungen anfallen.
- Die **Zeit**-Einstellung bewirkt eine Verschickung der SAP-Daten zur Remote-Seite in einem einzustellenden Zeitabstand (siehe unten).
- **pBack** (Standard) ist die gebührenschonendste Einstellung, wodurch SAP-Daten nur zur Gegenseite verschickt werden, wenn eine Verbindung aktiv ist.



*Bei der Spoofing-Einstellung **pBack** altern Einträge aus der RIP-Tabelle nur dann, wenn eine Verbindung neu aufgebaut wird und gezielt ein Eintrag als „nicht erreichbar“ gekennzeichnet wurde.*

WAN-Update-Zeit

Hier wird für eine Spoofing-Zeitsteuerung der zeitliche Übertragungsabstand eingegeben, in dem SAP-Daten zur Gegenseite übertragen werden. Die Eingabemöglichkeiten reichen von 1 bis 60 Minuten bei einem Standardwert von 5.

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	WERT	TCP/IP-Modul ein- oder ausgeschaltet
IP-Adresse	WERT	Eigene IP-Adresse
IP-Netz-Maske	WERT	Passende IP-Netzmaske des lokalen Netzes
Intranet-Adresse	WERT	Eigene Intranet-Adresse
Intranet-Maske	WERT	Passende Intranet-Netzmaske des lokalen Netzes
Zugangsliste	TABELLE	Einschränkung des Zugriffs auf interne Funktionen über TCP/IP
DNS-Default	WERT	Domain Name Server

/TCP-IP-Modul	Einstellungen für das TCP/IP-Modul	
DNS-Backup	WERT	Backup Domain Name Server
NBNS-Default	WERT	NetBIOS Name Server
NBNS-Backup	WERT	Backup NetBIOS Name Server
Tabelle-ARP	TABELLE	ARP-Tabelle für Abb. einer IP-Adresse auf eine MAC-Adresse
ARP-Aging-Min	WERT	Verweildauer für Einträge in der ARP-Tabelle
TCP-Aging-Min	WERT	Zeitbeschränkung für Konfigurations-Verbindungen, die inaktiv sind
TCP-Max.-Verbindungen.	INFO	Max. Anzahl gleichzeitiger Konfigurations-Verbindungen zum <i>ELSA LANCOM</i>

Zustand

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



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

IP-Adresse

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

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

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

IP-Netzmaske

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

Intranet-Adresse

Hier kann eine zweite IP-Adresse für 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 LAN-COM Wireless) 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 TFTP-Protokolls.
- SNMP: die Konfigurations-Schnittstelle auf Basis von SNMP.

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

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

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

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

IP-Adresse	IP-Netz-Maske
192.234.222.0	255.255.255.0

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

DNS-Default

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

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

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

DNS-Backup

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

NBNS-Default

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

NBNS-Backup

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

ARP-Tabelle

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

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

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

- ARP-Aging-Min* Hier kann eine Zeit (von 1 bis 99 Minuten) eingegeben werden, nach der die ARP-Tabelle automatisch aktualisiert wird, d.h., alle nicht angesprochenen IP-Adressen seit der letzten automatischen Aktualisierung werden entfernt. Der Standardwert beträgt 15 Minuten.
- TCP-Aging-Min* Erfolgt während einer TCP-Verbindung zum Router keine Übertragung mehr, wenn z.B. während der Remote-Konfiguration keine Daten mehr vom Benutzer eingegeben werden, baut er die TCP-Verbindung automatisch nach der hier angegebenen Zeit ab. Gültige Werte sind 1 bis 99 Minuten. Der Standardwert beträgt 15 Minuten.
- TCP-Max.-Verbindungen* Hier kann die Anzahl der maximal zulässigen, gleichzeitig möglichen Verbindungen eingestellt werden. DEFAULT-Einstellung ist '0', was gleichbedeutend ist mit „beliebig viele“.

Setup/IP-Router-Modul

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

/IP-Router-Modul	Einstellungen für das IP-Router-Modul	
Zustand	WERT	IP-Router-Modul ein- oder ausgeschaltet
IP-Routing-Tabelle	TABELLE	Router-Tabelle für Zuordnung IP-Netzwerk und Gegenstelle
Default-Zeittabelle	TABELLE	Router-Tabelle für Zuordnung IP-Netzwerk und Gegenstelle
Nutzung-Default-Listen	WERT	Router-Tabelle für Zuordnung IP-Netzwerk und Gegenstelle
LAN-Filtertabelle	TABELLE	Negativ/Aufb.-Filtertabelle für TCP/UDP-Zielports von LAN-Pak.
WAN-Filtertabelle	TABELLE	Negativ-Filtertabelle für TCP/UDP-Zielports von WAN-Paketen
Proxy-ARP	WERT	Aktivierung/Deaktivierung der Proxy-ARP-Funktion
Lok.-Routing	WERT	Ein- und Ausschalten des lokalen Routings
Routing-Methode	MENU	Routing-Verfahren für IP-Pakete
RIP-Einstellungen	MENU	Einstellungen für den Betrieb von IP-RIP
Masquerading	MENU	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 Gegenstelle (z.B. Ihr Internet-Provider) mit den Zugangsdaten eine feste IP-Adresse mitgeteilt hat. Dieses Verfahren funktioniert natürlich nur dann, wenn Sie diese Adresse auch als IP-Adresse im Router eingetragen haben.

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

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

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

Im Internet verbotene Adreßbereiche werden über voreingestellte Einträge in der IP-Routing-Tabelle von der Übertragung ausgeschlossen (Router-Name 0.0.0.0 bedeutet:

Pakete an diese Adressen nicht übertragen). Die folgende IP-Routing-Tabelle dient als Beispiel und zeigt gleichzeitig die Standardeinträge:

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

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

● Beispiel

- Die lokale Netzwerkadresse ist 192.120.130.0.
- 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.

*Default-Zeit-
tabelle*

Ähnlich dem Least-Cost-Routing (LCR) ist die Zeitsteuerung für die Default-Route eine Funktion, mit der automatisch je nach Uhrzeit der Provider mit dem günstigsten Tarif gewählt wird.

Sobald ein IP-Paket zu einer Verbindung über die Default-Route führen möchte, wird zuerst einmal nicht die in der Default-Route eingetragene Gegenstelle angewählt, sondern es wird vorher in der Zeitsteuerungstabelle geprüft, welche Gegenstelle zu benutzen ist.

In dieser Zeitsteuerungstabelle geben Sie an, an welchen Wochentagen und zu welcher Uhrzeit ein bestimmter Provider zu benutzen ist. Sobald nun ein IP-Paket einen Aufbau der Default-Route erfordert, wird zunächst geprüft, ob die Verwendung der Zeitsteuerungstabelle aktiviert ist. Anschließend wird in der Tabelle ein Eintrag gesucht, der den aktuellen Wochentag und die aktuelle Uhrzeit abdeckt. Wird ein solcher Eintrag gefunden, baut der Router eine Verbindung zu der dort eingetragenen Gegenstellen auf. Findet sich in der Zeitsteuerungstabelle kein passender Eintrag, kehrt der Router zurück in die IP-Routing-Tabelle und verwendet die dort eingetragene Gegenstelle.

*Nutzung-
Default-Listen*

Schaltet die Verwendung der Default-Liste ein oder aus.

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 spezifizierten Quell-Netz bzw. zum Ziel-Netz.
- **Typ**
Art des Filters. Möglich sind Immer, Aufbau und I-Net.
 - **Immer**-Filter: Das Paket wird verworfen.
 - **Aufbau**-Filter: Das Paket wird verworfen, wenn keine Verbindung zur Gegenstelle besteht.
 - **I-Net**-Filter: Das Paket wird verworfen, wenn sein Ziel nur über die DEFAULT-Route erreichbar ist.

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

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

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

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

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

- Ziel-Adresse, Ziel-Netzmaske

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

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

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

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

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

Proxy-ARP

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

Lok.-Routing

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

Setup/IP-Router-Modul/Routing-Methode

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

Das Menü hat den folgenden Aufbau:

/Routing-Methode	Einstellungen der Routing-Methode	
Routing-Methode	WERT	Routing-Methode für IP-Pakete
ICMP-Routing-Methode	WERT	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	WERT	RIP-Kompatibilitätsschalter
R1 Maske	WERT	Verwaltung von Netzwerkmasken
Tabelle-RIP	INFO-TABELLE	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	WERT	Zeit in Sekunden bis eine TCP-Maskierung ungültig wird
UDP-Aging	WERT	Zeit in Sekunden bis eine UDP-Maskierung ungültig wird
ICMP-Aging	WERT	Zeit in Sekunden bis eine ICMP-Maskierung ungültig wird
Service-Tabelle	TABELLE	statische Masquerading-Tabelle
Tabelle-Masquerade	INFO-TABELLE	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	WERT	Schalter für die Ausgabe von SNMP-Traps
IP-Trap-Tabelle	TABELLE	Tabelle mit 20 Ziel-Adressen für Trap-Nachrichten
Administrator	WERT	Geräte-Administrator
Standort	WERT	Geräte-Standort

/SNMP-Modul	Einstellungen für das SNMP-Modul	
Register-Monitor	AKTION	Befehl zum Anmelden einer Zieladresse, zu der Traps gesendet werden sollen
Loesche-Monitor	AKTION	Befehl zum Löschen einer Adresse, die mit 'Register-Monitor' gesetzt wurde
Monitor-Tabelle	INFO-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-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	WERT	Schalter für die Aktivierung des DHCP-Moduls
Start-Adreß-Pool	WERT	Start-Adresse für den Adreßpool
Ende-Adreß-Pool	WERT	End-Adresse für den Adreßpool
Netzmaske	WERT	Netzmaske für den Adreßpool
Broadcast-Adresse	WERT	Broadcast-Adresse für das LAN
Gateway-Adresse	WERT	Gateway-Adresse für das LAN
Max.-Gültigkeit-Minute(n)	WERT	Maximal-Gültigkeit der Adreßzuweisung über DHCP
Default-Gültigkeit-Minute(n)	WERT	Standard-Gültigkeit der Adreßzuweisung über DHCP
Tabelle-DHCP	INFO-TABELLE	Tabelle mit den aktuellen Zuweisungen über DHCP

Zustand

Ein: Das Gerät arbeitet als DHCP-Server

Aus: Das Gerät arbeitet nicht als DHCP-Server

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



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

Start-Adreß-Pool Ende-Adreß-Pool

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

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

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

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

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

Netzmaske Die Zuweisung der Netzmaske erfolgt analog zur Adreßzuweisung:

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

Broadcast Die Zuweisung der Broadcast-Adresse erfolgt analog zur Adreßzuweisung:

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

Max.-Gültigkeit-Minute(n) Hier kann die maximale Gültigkeitsdauer eingetragen werden, die der DHCP-Server einem Host zuweist.

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

Default-Gültigkeit-Minute(n) Hier kann die Gültigkeitsdauer eingetragen werden, die zugewiesen wird, wenn der Host überhaupt keine Gültigkeitsdauer anfordert.

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

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

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

- IP-Adresse: zugewiesene IP-Adresse
- MAC-Adresse: Ethernet-Adresse des Rechners
- Timeout: Restzeit bis die Zuweisung ungültig wird
- Rechnername: Klartextname des Rechners, wenn er diesen in der Anfrage übermittelt
- Typ: Dieses Feld enthält weitere Informationen zu der Zuweisung.
Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:

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

Setup/NetBIOS-Modul

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

Zustand	WERT	Ein oder aus
Scope-ID	WERT	NetBIOS-Scope, in dem sich der Router befindet.
NT-Domaene	WERT	Arbeitsgruppe/Domain, in dem sich der Router befindet.
Gegenstellen-Tab.	TABELLE	In der Gegenstellen-Tabelle werden alle Gegenstellen eingetragen, mit denen NetBIOS-Informationen ausgetauscht werden.
Gruppen-Liste	INFO-TABELLE	In der Gruppen-Liste werden alle über NetBIOS bekannten Arbeitsgruppen abgelegt.
Host-Liste	INFO-TABELLE	In der Host-Liste werden alle über NetBIOS bekannten Rechner-Namen abgelegt.
Server-Liste	INFO-TABELLE	In der Server-Liste werden alle Server abgelegt, die sich im Netz bekannt gemacht haben.
Watchdogs	INFO-TABELLE	Legt die Behandlung von Watchdog-Paketen fest.
Abgleich	INFO-TABELLE	Art des Abgleichs von Routing-Informationen.
WAN-Update-Min	INFO-TABELLE	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	WERT	Schalter für Konfiguration von der LAN-Seite
WAN-Config	WERT	Schalter für Konfiguration von der WAN-Seite
Passwort-Zwang	WERT	Paßwortzwang ein/aus, wenn kein Paßwort vorhanden ist
Maximale Verbindungen	WERT	Maximale Anzahl gleichzeitiger Verbindungen
Fernconfig-(EAZ-MSN)	WERT	Rufnummer für die Fernkonfiguration über PPP
Conf.-Haltezeit	WERT	Zeitbeschränkung für Remote-Konfigurationsverbindungen
Login-Fehler	WERT	Anzahl für Login-Fehlversuche, bevor die Login-Sperre greift
Sperr-Minuten	WERT	Dauer der Sperrung und Zeitraum, bis alte Login-Fehler vergessen sind
Sprache	WERT	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 <i>LANCAPI</i>	
Zugangsliste	TABELLE	Liste der Rechner, die die <i>LANCAPI</i> nutzen dürfen
LANCAPI-UDP-Port	WERT	UDP-Port für die Kommunikation zwischen <i>LANCAPI</i> -Server und -Clients
EAZ-MSN(s)	WERT	EAZ oder MSN, auf die die <i>LANCAPI</i> reagieren soll
Prio-ab	WERT	Priorität für die <i>LANCAPI</i> 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 Nebenchkanäle 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	WERT	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	WERT	Der Funkkanal, auf dem der Basisport arbeiten soll. Mögliche Werte sind 1 bis 14, die Kanäle überlappen sich aber durch das Spread-Spectrum-Verfahren, so daß sich im gesamten Funkband maximal 3 vollständig unabhängige Funkkanäle aufspannen lassen. <i>Nicht in jedem Land sind alle Kanäle erlaubt (siehe auch Tabelle mit Funkkanälen im Anhang).</i>
Paketgroesse	WERT	Ein Wert zwischen 600 und 1600, der die maximale Größe von Paketen im WLAN in Bytes angibt. Default: 1550.
Zugangs-Liste	TABELLE	Mit dieser Liste lassen sich Stationen in WLAN explizit vom Datenverkehr mit dem LAN/Basisport ausschließen bzw. es können die Stationen definiert werden, denen Verkehr erlaubt sein soll. In die Liste sind die MAC-Adressen von Stationen einzutragen, also die auf den Karten aufgedruckten 12-stelligen Hexadezimalzahlen, allerdings ohne die Trennzeichen, aus 00-60-B3-1F-02-11 wird also z.B. 0060B31F0211. <i>Hiermit wird nur Stationen der Zugriff zum LAN bzw. WAN verwehrt, der Datentransport zwischen Stationen im WLAN, bei dem der Basisport typischerweise Relais spielt, ist davon unbeeinflusst!</i>
Zugriffsmodus	WERT	Der Positiv/Negativ-Schalter bestimmt, ob es eine Ausschußliste oder Positivliste ist. Defaultmäßig steht der Modus auf Negativ und die Zugangs-Liste ist leer, d.h., keiner Station wird Datenverkehr verwehrt.
Protokoll-Liste	TABELLE	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 FOF0, E0E0 = IPX 809B und 80F3 = Appletalk 6001 bis 6007 = Decnet 80D5 und 0808 bis 0D0D = IBM SNA <i>Wiederum wird hier nur der Zugang von Stationen im WLAN zum LAN bzw. WAN gesperrt, nicht jedoch der Traffic zwischen WLAN-Stationen.</i>
Protokollmodus	WERT	Positiv/Negativ-Schalter für die Protokoll-Liste
Interpoint-Verkehr	WERT	Erlaubt die Verwendung der Basis-Station für die Punkt-zu-Punkt-Kommunikation, um zwei oder mehrere LANs drahtlos zu verbinden.
Accesspoint-Liste	TABELLE	Für Punkt-zu-Punkt-Verbindungen ist es erforderlich, hier die MAC-Adressen der gegenüberliegenden Basis-Stationen einzutragen. Dies können maximal sechs Stück sein.
WEP-Verschlüsselung	WERT	Aktiviert die Verschlüsselung von Datenpaketen auf dem WLAN. Sobald diese Option aktiviert ist, können keine Stationen mehr angemeldet werden, die keine gültigen Schlüssel besitzen.

WEP-Vorgabe-schlüssel	WERT	Der Schlüssel, der für die gesendeten Pakete verwendet wird.
WEP-Schlüssel	TABELLE	Der Schlüssel für die Kodierung. Intern ist ein solcher Schlüssel eine 40-Bit-Zahl, die entweder hexadezimal oder als 5-stelliger ASCII-String eingegeben werden kann.
Node-ID	INFO	MAC-Layer-Adresse des Geräts
Heap-Reserve	WERT	Pufferspeicher für die Aufnahme von Datenpaketen aus dem lokalen Netzwerk
IAPP-Protokoll	WERT	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	WERT	Zeitintervall, in dem sich eine Basis-Station beim Roaming bei allen anderen über das kabelgebundene LAN bekannt macht
IAPP-Handover-Timeout	WERT	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	WERT	LCR für die Routermodule aktivieren, Ein oder Aus
Lancapi-Nutzung	WERT	LCR für die <i>LANCAPI</i> aktivieren, Ein oder Aus
Zeittabelle	TABELLE	Tabelle der Rufumleitungen
Feiertagstabelle	TABELLE	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 Werkstage, '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	WERT	Ein (Default) oder aus
Domaene	WERT	Eigene Domain, optional, maximal 32 Zeichen
DHCP-verwenden	WERT	Ja (Default) oder nein
NetBIOS-verw.	WERT	Ja (Default) oder nein

DNS-Tabelle	TABELLE	Statische DNS-Tabelle zur manuellen Zuweisung von IP-Adressen und Namen, 64 Einträge
Filter-Liste	TABELLE	Filter-Liste zum Ausschließen verbotener Domains, 64 Einträge
Gültigkeit	WERT	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	WERT	Aktivierung des Moduls: Ein, Aus
Aktuelle-Zeit	INFO	Anzeige der aktuellen Zeit im Gerät
Time EAZ-MSN	WERT	Rufnummer, zu der eine Verbindung aufgebaut werden soll, um eine Zeitinformation aus dem ISDN-Netz zu erhalten
Anwahl-Versuche	WERT	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	INFO-TABELLE	Anzeige der Hardware-Releases und Seriennummern des Routers
Tabelle-Firmsafe	INFO-TABELLE	Informationen über die beiden im Gerät gespeicherten Firmware-Versionen und über den Bootloader.
Modus-Firmsafe	WERT	Modus der Firmware-Aktivierung
Timeout-Firmsafe	WERT	Zeit in Minuten für den Test einer neuen Firmware
Test-Firmware	AKTION	Testet die inaktive Firmware
Firmware-Upload	AKTION	Starten eines Firmware-Uploads

Versions-Tabelle

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

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	Große	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	AKTION	Test einer Verbindung
System-Boot	AKTION	Neustart des Gerätes
System-Reset	AKTION	Rücksetzen auf Werkseinstellung
System-Upload	AKTION	Neue Firmware laden

Sonstiges/Manuelle-Wahl

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

System-Boot

Über diesen Menüpunkt kann das Gerät neu gestartet werden.



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

System-Reset

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

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

System-Upload

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

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

TCP/IP-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

Dienst	Port-Nr.	Protokoll
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
nbssession	139	tcp
NeWS	144	tcp
sgmp	153	udp
tcprepo	158	tcp
snmp	161	udp
snmp-trap	162	udp
print-srv	170	tcp
vmnet	175	tcp
load	315	udp
vmnet0	400	tcp
sytek	500	udp
biff	512	udp
exec	512	tcp
login	513	tcp

Dienst	Port-Nr.	Protokoll
who	513	udp
shell	514	tcp
syslog	514	udp
printer	515	tcp
talk	517	udp
ntalk	518	udp
efs	520	tcp
route	520	udp
timed	525	udp
tempo	526	tcp
courier	530	tcp
conference	531	tcp
rxd-control	531	udp
netnews	532	tcp
netwall	533	udp
uucp	540	tcp
klogin	543	tcp
kshell	544	tcp
new-rwho	550	udp
remotefs	556	tcp
rmonitor	560	udp
monitor	561	udp
garcon	600	tcp
maitrd	601	tcp
busboy	602	tcp
acctmaster	700	udp
acctslave	701	udp
acct	702	udp
acctlogin	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctslave2	706	udp
acctdisk	707	udp
kerberos	750	tcp
kerberos	750	udp

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

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