

Referenz-Handbuch

Beschreibung der Menüpunkte	3.1.1
Status	3.1.3
Status/Verbindung	3.1.4
Status/Betriebszeit	3.1.5
Status/S0-Bus	3.1.5
Status/WAN-Statistik	3.1.5
Status/LAN-Statistik	3.1.7
Status/PPP-Statistik	3.1.7
Status/Bridge-Statistik	3.1.12
Status/IPX-Statistik	3.1.13
Status/TCP-IP-Statistik	3.1.17
Status/IP-Router-Statistik	3.1.20
Status/Config-Statistik	3.1.22
Status/Verb.-Statistik	3.1.22
Status/Info-Verbindung	3.1.23
Status/Layer-Verb.	3.1.24
Status/Ruf-Info-Tabelle	3.1.24
Status/Werte-löschen	3.1.25
Setup	3.1.26
Setup/WAN-Modul	3.1.27
Setup/Gebühren-Modul	3.1.37
Setup/LAN-Modul	3.1.39
Setup/Bridge-Modul	3.1.40
Setup/IPX-Modul	3.1.42
Setup/TCP-IP-Modul	3.1.51
Setup/IP-Router-Modul	3.1.54
Setup/SNMP-Modul	3.1.61
Setup/Config-Modul	3.1.61
Setup/Sonstiges	3.1.62
Firmware	3.1.64
Sonstiges	3.1.65
LANCOM intern	3.2.1
Script-Verarbeitung	3.2.2
Allgemeines	3.2.2
Die Script-Liste	3.2.2
Compuserve-Anwahl	3.2.3
Online Trace-Ausgaben	3.2.5
Allgemeines	3.2.5

Bedienung der Trace-Ausgaben.....	3.2.6
Beispiele zur Bedienung der Trace-Ausgaben.....	3.2.7
Unterstützte Protokolle und Funktionen.....	3.2.7
Policy Based Routing	3.2.18
Allgemeines	3.2.18
Beispiele.....	3.2.19
<hr/>	
Meldungen, Nummern, Ports	3.3.1
Fehlermeldungen	3.3.2
LANCOM-interne Fehlermeldungen.....	3.3.2
ISDN-Fehlermeldungen.....	3.3.2
V42bis Fehler.....	3.3.4
PPP-Fehlermeldungen	3.3.6
Modem-Fehlermeldungen.....	3.3.8
Status-Anzeigen.....	3.3.9
Novell SAP-Nummern.....	3.3.10
TCP/IP-Ports	3.3.14
<hr/>	
Häufig gestellte Fragen und Antworten	3.4.1
Allgemein	3.4.2
IP-RIP	3.4.6
PPP	3.4.8
Bridge.....	3.4.11
IPX-Router	3.4.13
IP-Router	3.4.18

Beschreibung der Menüpunkte

Der Menübaum der *LANCOM*-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 vollständige 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' auf Seite 1.3.1).






















Die Konfiguration mit *LANconfig* ist vergleichbar mit den Möglichkeiten aus dem Setup-Zweig dieser Menüstruktur.

Status.....	3
Setup.....	25
Firmware	61
Sonstiges	62

Symbole

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

Menü-Übersicht

















	Setup		Status
	Name		Verbindung
	WAN-Modul		Betriebszeit
	Gebühren-Modul		S0-Bus
	LAN-Modul		WAN-Statistik
	Bridge-Modul		LAN-Statistik
	IPX-Modul		PPP-Statistik
	TCP-IP-Modul		Bridge-Statistik
	IP-Router-Modul		IPX-Statistik
	SNMP-Modul		TCP-IP-Statistik
	Config-Modul		IP-Router-Statistik
	Sonstiges		Config-Statistik
	Firmware		Verbindungs-Statistik
	Versions-Tabelle		Info-Verbindung
	Firmware-Upload		Layer-Verbindung
	Sonstiges		Ruf-Info-Tabelle
	Manuelle Wahl		Werte-löschen
	System-Reset		
	System-Boot		
	System-Upload		

Status

Das Menü Status enthält Informationen zum aktuellen Status und über interne Abläufe im LAN und im WAN, die sich auf die Datenübertragungs-Strecke (z.B. Anwahl bzw. Verbindung) oder Statistiken (z.B. Anzahl empfangener bzw. gesendeter Datenblöcke) beziehen können. Die statistischen Anzeigen bieten eine leistungsfähige Hilfstellung 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 auf dem Display des *LANCOM MPR* bzw. im Statusmenü der Konfiguration aller *LANCOM*-Typen, werden laufend aktualisiert und können mit einer im jeweiligen Menü enthaltenen **Werte-löschen**-Aktion auf 0 gesetzt werden.

Das Menü besitzt den folgenden Aufbau:

Status		Fortlaufende Statusanzeigen
Verbindung		Zustand der WAN-Strecke
Betriebszeit		Betriebszeit des Gerätes seit dem letzten Einschalten
S0-Bus		Zustand der S0-Schnittstelle
WAN-Statistik		Anzeige der WAN-Statistiken
LAN-Statistik		Statistiken des Netzwerk-Bereichs
PPP-Statistik		Statistiken des Netzwerk-Bereichs
Bridge-Statistik		Statistiken des Bridge-Bereiches
IPX-Statistik		Statistiken aus dem IPX- und IPX-Router-Bereich
TCP-IP-Statistik		Statistiken aus dem TCP/IP-Bereich
IP-Router-Statistik		Statistiken aus dem IP-Router
Config-Statistik		Statistiken der Remote-Konfiguration
Verb.-Statistik		Verbindungs-Informationen für jedes Interface
Info-Verbindung		Informationen zur letzten Verbindung für jedes Interface
Layer-Verbindung		Informationen über das verwendete B-Kanal-Protokoll für jedes Interface
Ruf-Info-Tabelle		Informationen über die letzten 10 angekommenen Rufe
Werte-löschen		Alle Werte außer Tabellen der untergeordnet. Statistik löschen

Status/Verbindung

Der Menüpunkt **Status/Verbindung** gibt die Statusmeldungen der einzelnen Kanäle wieder, die bei *LANCOM* auch im Display erscheinen:

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

Folgende Zustände werden unterschieden:

Ch01: Bereit Ch02: Bereit	Daten werden nicht übertragen.
Ch01: xxxxxx-> Ch02: Bereit	Die Rufnummer xxxxxx... wird über den ersten B-Kanal ausgewählt.
Ch01: Anliegender Ruf Ch02: Bereit	Ein Ruf liegt auf dem ersten B-Kanal an.
Ch01: Protokoll Ch02: Bereit	Das Verbindungsprotokoll wird auf dem ersten B-Kanal ausgetauscht.
Ch01: GegenstellenName Ch02: Bereit	Aktive Verbindung mit der Gegenstelle "GegenstellenName" auf dem ersten B-Kanal.
Ch01: GegenstellenNa/2 Ch02: Bündelung	Aktive Verbindung mit Kanalbündelung zur Gegenstelle "GegenstellenName".
Ch01: Abbau Ch02: Bereit	Die Verbindung auf dem ersten B-Kanal wird beendet.
Ch01: Rückruf Ch02: Bereit	Die Gegenstelle wird zurückgerufen.
Ch01: Aufbau D64S Ch02: Reserviert	Aufbau einer Standleitung Gruppe 0.
Ch01: Aufbau S01/02 Ch02: Bündelung	Aufbau einer Standleitung Gruppe 2.

Zusätzlich werden bei dieser Einstellung Fehler, die bei einem Verbindungsversuch auftreten können, angezeigt. Bisher sind folgende Anzeigen festgelegt:

Ch01: Kein Protokoll Ch02: Bereit	Die Protokollverhandlung konnte nicht durchgeführt werden.
Ch01: Fehlermeldung Ch02: Bereit	Ein Fehler im ISDN-Netz ist aufgetreten und wird möglichst im Klartext angezeigt.







Manchmal erfolgt eine Fehlermeldung in Form von zwei dreistelligen Zahlen, die z.B. von Ihrer Nebenstellenanlage erzeugt werden und als interne Fehlercodes der Anlage vom LANCOM nicht in Klartext übersetzt werden können.

Status/Betriebszeit

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

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	
Spannung		Spannung des S ₀ -Bus ('Ja' oder 'Nein')
Aktiviert		Zustandsanzeige der Aktivierung ('Ja' oder 'Nein')
TEI		TEI zugewiesen ('Ja' oder 'Nein')
Layer-2		Aktivierung der Schicht 2 des D-Kanals ('Ja' oder 'Nein')

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 ISDN-Anschlusses, aufgetretene Fehler und im aktuellen Betriebszustand vorhandene interne Ressourcen des *LANCOM*.

Die WAN-Statistik wird interfacebezogen geführt, d.h. 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-Übertr.-Statistik		Statistik für übertragene Bytes
Paket-Übertr.-Statistik		Statistik für übertragene Daten-Pakete
Fehler Statistik		Statistik über aufgetretene Übertragungsfehler
WAN-Tx-verworfen		Anzahl durch Fehler/Ressourcenmangel verworfener Pakete
WAN-Heap-Blöcke		Anzahl belegter Puffer
WAN-Que-Blöcke		Anzahl verfügbarer Puffer
WAN-Que-Fehler		Anzahl durch Puffermangel verworfener Datenpakete
Werte-löschen		WAN-Statistik löschen

*Byte-Übertr.-
Statistik*

Der Menüpunkt **Status/WAN-Statistik/Byte-uebertr.-Stat** 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
Ser1	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	(Kurzform von Interface) bezeichnet den zugehörigen B-Kanal. Mögliche Werte sind: Ch01 (1. B-Kanal), Ch02 (2. B-Kanal) und Ser1 (Verbindung über die serielle Schnittstelle).
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-Übertr.-
Statistik*

Der Menüpunkt **Status/WAN-Statistik/Pkt.-uebertr.-Stat** 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
Ser1	0	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	(Kurzform von Interface) bezeichnet den zugehörigen B-Kanal. Mögliche Werte sind: Ch01 (1. B-Kanal), Ch02 (2. B-Kanal) und Ser1 (Verbindung über die serielle Schnittstelle).
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-L3-F.	Rx-L2-F.	Rx-L1-F.	Tx-Fehler	Stack-F.
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0
Ser1	0	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	Bezeichnet den zugehörigen B-Kanal (siehe auch Status/WAN-Statistik)
Rx-L3-F.	Anzahl Layer-3 Fehler bei empfangenen Daten (d.h. der Protokoll-Header der Layer-3 ist nicht korrekt; z.B. CISCO-, WaidNet- oder CONWARE-Header)
Rx-L2-F.	Anzahl Layer 2 Fehler bei empfangenen Daten (d.h. analog zu den Layer-3 Fehlern z.B. defekter PPP-, X75UI- oder X75BUI-Header).
Rx-L1-F.	Anzahl Layer 1 Fehler bei empfangenen Daten (d.h. analog zu Layer-3 Fehlern ein Fehler im HDLC-Header)
Tx-Fehler	Anzahl Übertragungsfehler beim Senden
Stack-F.	Anzahl Stack-Fehler bei empfangenen Daten. Stack-Fehler entstehen durch empfangene Frames, die keinem internen Verarbeitungsprozess (IP/IPX Router bzw. Bridge) zugeordnet werden können. (Dies können z.B. AppleTalk- DECNet- oder NetBEUI-Frames sein).

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		Statistik für übertragene Daten
Fehler Statistik		Statistik über aufgetretene Übertragungsfehler
WAN-Tx-verworfen		Anzahl durch Fehler/Ressourcenmangel verworfener Pakete
WAN-Heap-Blöcke		Anzahl belegter Puffer
WAN-Que-Blöcke		Anzahl verfügbarer Puffer
WAN-Que-Fehler		Anzahl durch Puffermangel verworfener Datenpakete
Werte-löschen		WAN-Statistik löschen

Status/PPP-Statistik

Innerhalb der PPP-Statistik werden die Zustände einzelner Sub-Protokolle des PPP für jedes Interface separat verwaltet. Die Statistiken der übertragenen Frames einzelner Sub-

Protokolle werden dagegen nur innerhalb einer gemeinsamen Statistik mitgeführt. Das Menü **Status/PPP-Statistik** besitzt daher folgenden Aufbau:

/PPP-Statistik	Fortlaufende Statusanzeigen	
Zustände		Statistik über Zustand der PPP-Protokollverhandlung für jedes Interface
LCP-Statistik		Anzeige der PPP/LCP-Statistiken
PAP-Statistik		Anzeige der PPP/PAP-Statistik
CHAP-Statistik		Anzeige der PPP/CHAP-Statistik
IPXCP-Statistik		Anzeige der PPP/IPXCP-Statistik
IPCP-Statistik		Anzeige der PPP/IPCP-Statistik
Werte-löschen		Löschen der PPP-Statistiken

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

Zustände

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

lfc	Phase	LCP	IPXCP	IPCP
Ch01	DEAD	Initial	Initial	Initial
Ch02	DEAD	Initial	Initial	Initial
Ser1	DEAD	Initial	Initial	Initial

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	Bezeichnet den zugehörigen B-Kanal (siehe auch " Status/WAN-Statistik ")
Phase	Enthält die Phase, in der sich das PPP befindet. Mögliche Werte sind DEAD , ESTABLISH , TERMINATE , AUTHENTIC und NETWORK .
LCP	Zustand des Unterprotokolls "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 Unterprotokolls "IP-Control-Protocol" angezeigt.
IPXCP	Analog zu "LCP" wird hier der Zustand des Unterprotokolls "IPX-Control-Protocol" angezeigt.

Unter „Zustände“ wird die jeweilige Phase des PPP aktuell angezeigt. Diese Zustände sind, wie oben angegeben, Ruhezustand (Dead), Bereitschaftszustand (Establish), Überprüfung der Zugangsparameter (Authenticate) und Netzwerkphase (Network). In den Un-

terstatistiken 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-Req	Anzahl empfangener Configure Request-Pakete für LCP
Rx-Config-Ack	Anzahl empfangener Configure Acknowledge-Pakete für LCP
Rx-Config-NAK	Anzahl empfangener Configure Negative Acknowledge-Pakete
Rx-Config-Rej	Anzahl empfangener Configure Reject-Pakete für LCP
Rx-Term-Req	Anzahl empfangener Terminate Request-Pakete für LCP
Rx-Term-Ack	Anzahl empfangener Terminate Acknowledge-Pakete für LCP
Rx-Code-Rej	Anzahl empfangener Code Reject-Pakete für PPP
Rx-Protocol-Rej	Anzahl empfangener Protocol Reject-Pakete für PPP
Rx-Echo-Req	Anzahl empfangener Echo Request-Pakete für LCP
Rx-Echo-Rep	Anzahl empfangener Echo Response-Pakete für LCP
Rx-Discard-Req	Anzahl empfangener Discard Request-Pakete für LCP
Tx-Config-Req	Anzahl gesendeter Configure Request-Pakete für LCP
Tx-Config-Ack	Anzahl gesendeter Configure Acknowledge-Pakete für LCP
Tx-Config-NAK	Anzahl gesendeter Configure Negative Acknowledge-Pakete
Tx-Config-Rej	Anzahl gesendeter Configure Reject-Pakete für LCP
Tx-Term-Req	Anzahl gesendeter Terminate Request-Pakete für LCP
Tx-Term-Ack	Anzahl gesendeter Terminate Acknowledge-Pakete für LCP
Tx-Code-Rej	Anzahl gesendeter Code Reject-Pakete für PPP
Tx-Protocol-Rej	Anzahl gesendeter Protocol Reject-Pakete für PPP
Tx-Echo-Req	Anzahl gesendeter Echo Request-Pakete für LCP
Tx-Echo-Rep	Anzahl gesendeter Echo Response-Pakete für LCP
Tx-Discard-Req	Anzahl gesendeter Discard Request-Pakete für LCP
Werte-löschen	LCP-Statistik löschen

Status/PPP-Statistik/PAP-Statistik

Das **PAP** (Password Authentication Protocol) ist eines von zwei üblichen Verfahren zur Überprüfung von Gegenstellen im PPP. Es überprüft beim Verbindungsaufbau einmalig das Passwort der Gegenstelle und läßt die Verbindung nur nach erfolgreichem Passwort-austausch zu (siehe auch Kapitel 'Point-to-Point Protocol' auf Seite 1.6.1). 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' auf Seite 1.6.1). 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/IPXCP-Statistik

Das **IPXCP** (Internet Exchange Protocol Control Protocol) zeigt bei Verwendung von IPX den Zustand des Protokolls und die zur Verhandlung ausgetauschten Pakete. Die Parameter in dieser Statistik bedeuten im einzelnen:

Rx-verworfen	Anzahl verworfener IPXCP-Pakete
Rx-Config-Req	Anzahl empfangener Configure Request-Pakete für IPXCP
Rx-Config-Ack	Anzahl empfangener Configure Acknowledge-Pakete für IPXCP
Rx-Config-NAK	Anzahl empfangener Configure Negative Acknowledge-Pakete
Rx-Config-Rej	Anzahl empfangener Configure Reject-Pakete für IPXCP
Rx-Term-Req	Anzahl empfangener Terminate Request-Pakete für IPXCP
Rx-Term-Ack	Anzahl empfangener Terminate Acknowledge-Pakete für IPXCP
Rx-Code-Rej	Anzahl empfangener Code Reject-Pakete für IPXCP
Tx-Config-Req	Anzahl gesendeter Configure Request-Pakete für IPXCP
Tx-Config-Ack	Anzahl gesendeter Configure Acknowledge-Pakete für IPXCP
Tx-Config-NAK	Anzahl gesendeter Configure Negative Acknowledge-Pakete
Tx-Config-Rej	Anzahl gesendeter Configure Reject-Pakete für IPXCP
Tx-Term-Req	Anzahl gesendeter Terminate Request-Pakete für IPXCP
Tx-Term-Ack	Anzahl gesendeter Terminate Acknowledge-Pakete für IPXCP
Tx-Code-Rej	Anzahl gesendeter Code Reject-Pakete für IPXCP
Werte-löschen	IPXCP-Statistik löschen

Status/PPP-Statistik/IPCP-Statistik

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

Rx-verworfen	Anzahl verworfener IPCP-Pakete
Rx-Config-Req	Anzahl empfangener Configure Request-Pakete für IPCP
Rx-Config-Ack	Anzahl empfangener Configure Acknowledge-Pakete für IPCP
Rx-Config-NAK	Anzahl empfangener Configure Negative Acknowledge-Pakete
Rx-Config-Rej	Anzahl empfangener Configure Reject-Pakete für IPCP
Rx-Term-Req	Anzahl empfangener Terminate Request-Pakete für IPCP
Rx-Term-Ack	Anzahl empfangener Terminate Acknowledge-Pakete für IPCP
Rx-Code-Rej	Anzahl empfangener Code Reject-Pakete für IPCP
Tx-Config-Req	Anzahl gesendeter Configure Request-Pakete für IPCP
Tx-Config-Ack	Anzahl gesendeter Configure Acknowledge-Pakete für IPCP
Tx-Config-NAK	Anzahl gesendeter Configure Negative Acknowledge-Pakete
Tx-Config-Rej	Anzahl gesendeter Configure Reject-Pakete für IPCP

Tx-Term-Req	Anzahl gesendeter Terminate Request-Pakete für IPCP
Tx-Term-Ack	Anzahl gesendeter Terminate Acknowledge-Pakete für IPCP
Tx-Code-Rej	Anzahl gesendeter Code Reject-Pakete für IPCP
Werte-löschen	IPCP-Statistik löschen

Status/Bridge-Statistik

Hier können die für die Bridge relevanten statistischen Informationen abgefragt werden. In der Bridge-Statistik finden Sie die folgenden Parameter:















/Bridge-Statistik	Fortlaufende Statusanzeigen	
BRG-LAN-Rx		Anzahl vom LAN empfangener Datenpakete
BRG-LAN-Tx		Anzahl zum LAN gesendeter Datenpakete
BRG-LAN-Filter		Anzahl vom LAN gefilterter Datenpakete
BRG-LAN-BCast		Anzahl vom LAN empfangener Broadcasts
BRG-LAN-MCast		Anzahl vom LAN empfangener Multicasts
BRG-WAN-Rx		Anzahl vom WAN empfangener Datenpakete
BRG-WAN-Tx		Anzahl zum WAN gesendeter Datenpakete
BRG-WAN-Filter		Anzahl vom WAN gefilterter Datenpakete
BRG-WAN-BCast		Anzahl vom WAN empfangener Broadcasts
BRG-WAN-MCast		Anzahl vom WAN empfangener Multicasts
BRG-Adressen		Anzahl der momentan bekannten Adressen
Werte-löschen		Bridge-Statistik löschen
Tabelle-BRG		Anzeige der Bridge-Filtertabelle
Aufbau-Tabelle		Tabelle der letzten 20 Pakete, die eine Verbindung erforderten

Tabelle-BRG

Die **BRG-Tabelle** (Bridge-Tabelle) gibt Auskunft über die von der Bridge erkannten MAC-Adressen, den Zeitpunkt in TICS, an dem das letzte Paket von diesem Gerät empfangen wurde und ob das entsprechende Gerät lokal oder remote vorhanden ist. Diese Tabelle dient nur zur internen Verwendung des Bridge-Moduls und kann manuell nicht verändert werden.

Node-ID	Letzter-Zugriff	Forward-Flag
00a0570308e1	396442 tics	lokal
00a0570308e2	29442 tics	remote

Aufbau-Tabelle In der **Aufbau-Tabelle** sind die letzten 20 Einträge, die Informationen über die Systemzeit, Zieladresse und Quelladresse der Datenpakete enthalten, die zu einem Verbindungsaufbau führen sollten.








Eine Bridge-Aufbau-Tabelle kann wie folgt aussehen:

Systemzeit	Ziel-Adresse	Quell-Adresse
1T; 16:45:01	ffffffffffff	0000c0057891
1T; 10:45:10	080000785734	0000c0057891

Die Systemzeit wird in Tagen, Stunden, Minuten und Sekunden seit Einschaltzeitpunkt angezeigt und belegt den Zeitpunkt des Verbindungsaufbaus. Die Zieladresse ffffffff deutet z.B. auf ein Broadcast-Paket hin.

Status/IPX-Statistik

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

/IPX-Statistik	Statistiken aus dem IPX- und IPX-Router-Bereich	
MAC-Statistik		Statistiken aus dem Media Access Control von IPX-Paketen
Watchdog-Stat.		Statistiken für Watchdog-Pakete
Prop.-Statistik		Statistiken für IPX-Propagated-Pakete (IPX-Typ 20)
RIP-Statistik		Statistiken für NetWare-RIP
SAP-Statistik		Statistiken für NetWare-SAP
Router-Statistik		Statistiken des Remote-IPX-Routers
Werte-löschen		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-BCast	Anzahl vom LAN empfangener Broadcast-IPX-Pakete
IPX-LAN-Rx-MCast	Anzahl vom LAN empfangener Multicast-IPX-Pakete
IPX-LAN-Rx-UCast	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-BCast	Anzahl vom WAN empfangener Broadcasts
IPX-WAN-Rx-MCast	Anzahl vom WAN empfangener Multicasts
IPX-WAN-Rx-UCast	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-WD-LAN-Rx	Anzahl vom LAN empfangener IPX-Watchdog-Pakete
IPX-WD-LAN-Tx	Anzahl zum LAN gesendeter IPX-Watchdog-Pakete
IPX-WD-WAN-Rx	Anzahl vom WAN empfangener IPX-Watchdog-Pakete
IPX-WD-WAN-Tx	Anzahl zum WAN gesendeter IPX-Watchdog-Pakete
SPX-WD-LAN-Rx	Anzahl vom LAN empfangener SPX-Watchdog-Pakete
SPX-WD-LAN-Tx	Anzahl zum LAN gesendeter SPX-Watchdog-Pakete
SPX-WD-WAN-Rx	Anzahl vom WAN empfangener SPX-Watchdog-Pakete
SPX-WD-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:

Prop-LAN-Rx	Anzahl vom LAN empfangener IPX-Propagated-Pakete
Prop-LAN-Filter	Anzahl vom LAN empfangener/gefilterter IPX-Propagated-Pak.
Prop-LAN-Tx	Anzahl zum LAN gesendeter IPX-Propagated-Pakete
Prop-LAN-Socketf	Anzahl vom LAN über Socketfilter gefiltert. IPX-Propagated-Pak.
Prop-LAN-Hopf.	Anzahl vom LAN über Hop Count gefiltert. IPX-Propagated Pak.
Prop-LAN-Backrf.	Anzahl vom LAN zurückzuroutender IPX-Propagated-Pak.
Prop-LAN-Cont.	Anzahl vom LAN zu routend. Pak. während einer falschen Verb.
Prop-WAN-Rx	Anzahl vom WAN empfangener IPX-Propagated-Pakete
Prop-WAN-Filter	Anzahl vom WAN empfangener/gefilterter IPX-Propagated-Pak.
Prop-WAN-Tx	Anzahl zum WAN gesendeter IPX-Watchdog-Pakete
Prop-WAN-Socketf	Anzahl vom WAN über Socketfilter gefiltert. PX-Propagated-Pak.
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 empf. 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 empf. 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

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 empf. 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 empf. 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

Status/IPX-Statistik/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-Hopf.	Anzahl vom LAN zu routender über Hop Count gefilterter IPX-Pak.
IPXR-LAN-Socketf	Anzahl vom LAN zu routender über Socketfilter gefilterter IPX-Pak.
IPXR-LAN-Netzwf.	Anzahl vom LAN zu routender Pakete zu falschen Netzwerken
IPXR-LAN-Backrf.	Anzahl vom LAN zurückzuroutender IPX-Pakete
IPXR-LAN-Cont.	Anzahl vom LAN zu routender Pak. während einer falschen Verb.
IPXR-LAN-Downf.	Anzahl vom LAN zu routender IPX-Pak. zu abgemeldeten Netzen
IPXR-WAN-Rx	Anzahl vom WAN zu routender IPX-Pakete
IPXR-WAN-Tx	Anzahl zum WAN gerouteter IPX-Pakete
IPXR-WAN-Hopf.	Anzahl vom WAN zu routender Über Hop Count gefilterter IPX-Pak.

IPXR-WAN-Socketf	Anzahl vom WAN zu routender Über Socketfilter gefilterter IPX-Pak.
IPXR-WAN-Netzwf.	Anzahl vom WAN zu routender Pakete zu falschen Netzwerken
IPXR-WAN-Backrf.	Anzahl vom WAN zurückzuroutender IPX-Pakete
IPXR-WAN-Downf.	Anzahl vom WAN zu routender IPX-Pak. zu abgemeldeten Netzen
IPXR-Int-Rx	Anzahl 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-Zieladresse, die IPX-Quelladresse der Datenpakete, die zu einem Verbindungsaufbau führen sollten.

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

Die Systemzeit wird in Tagen, Stunden, Minuten und Sekunden seit Einschaltzeitpunkt angezeigt und belegt den Zeitpunkt des Verbindungsaufbaus. Die Zieladresse ffffffff deutet z.B. auf ein Broadcast-Paket hin. Die Ziel- und Quelladressen 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 <i>LANCOMs</i> eingetragen.

Status/TCP-IP-Statistik

Hier werden die Statistiken aus dem TCP/IP-Bereich, gegliedert nach ARP-, IP-, ICMP-, TCP- und TFTP-Pakettypen, dargestellt. In der TCP-IP-Statistik finden Sie die folgenden Parameter:

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

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

Status/TCP-IP-Statistik/ARP-Statistik

In dieser Statistik werden die folgenden Werte angezeigt:

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

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-Chkf.	Anzahl vom LAN fehlerhaft empfangener IP-Pakete
IP-LAN-Serf.	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-Chkf.	Anzahl vom WAN fehlerhaft empfangener IP-Pakete
IP-WAN-Serf.	Anzahl vom WAN empfangener IP-Pakete für falschen Dienst
IP-WAN-Rx-verw.	Anzahl vom WAN durch Timeout-Management verworf. 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-Chkf.	Anzahl vom LAN fehlerhaft empfangener ICMP-Pakete
ICMP-LAN-Serf.	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-Chkf.	Anzahl vom WAN fehlerhaft empfangener ICMP-Pakete
ICMP-WAN-Serf.	Anzahl vom WAN empfangener nicht unterstützter ICMP-Pak.
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-Chkf.	Anzahl vom LAN fehlerhaft empfangener TCP-Pakete
TCP-LAN-Serf.	Anzahl vom LAN empfangener TCP-Pakete für falschen Port
TCP-LAN-Verb.	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-Wdh.	Anzahl zum WAN wiederholt gesendeter TCP-Pakete
TCP-WAN-Chkf.	Anzahl vom WAN fehlerhaft empfangener TCP-Pakete
TCP-WAN-Serf.	Anzahl vom WAN empfangener TCP-Pakete für falschen Port
TCP-WAN-Verb.	Anzahl der aktuellen 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 der vom LAN empfangenen TFTP-Pakete
TFTP-LAN-Rx-RReq	Anzahl der vom LAN empfangenen TFTP-Read-Requests
TFTP-LAN-Rx-WReq	Anzahl der vom LAN empfangenen TFTP-Write-Requests
TFTP-LAN-Rx-Data	Anzahl der vom LAN empfangenen TFTP-Daten-Pakete
TFTP-LAN-Rx-Ack	Anzahl der vom LAN empfangenen TFTP-Acknowledges
TFTP-LAN-Rx-OAck	Anzahl der vom LAN empfangenen TFTP-Option-Acknowledges
TFTP-LAN-Rx-Err	Anzahl der vom LAN empfangenen TFTP-Error-Pakete
TFTP-LAN-Rx-Bad	Anzahl der vom LAN empfangenen, unbekannten TFTP-Pakete
TFTP-LAN-Tx	Anzahl der auf das LAN gesendeten TFTP-Pakete
TFTP-LAN-Tx-Data	Anzahl der auf das LAN gesendeten TFTP-Daten-Pakete
TFTP-LAN-Tx-Ack	Anzahl der auf das LAN gesendeten TFTP-Acknowledges
TFTP-LAN-Tx-OAck	Anzahl der auf das LAN gesendeten TFTP-Option-Ack
TFTP-LAN-Tx-Err	Anzahl der auf das LAN gesendeten TFTP-Error-Pakete
TFTP-LAN-Tx-Rep.	Anzahl der wiederholt auf's LAN gesendeten TFTP-Paket
TFTP-LAN-Conn.	Anzahl der zum LAN aufgebauten TFTP-Verbindungen
TFTP-WAN-Rx	Anzahl der vom WAN empfangenen TFTP-Pakete
TFTP-WAN-Rx-RReq	Anzahl der vom WAN empfangenen TFTP-Read-Requests
TFTP-WAN-Rx-WReq	Anzahl der vom WAN empfangenen TFTP-Write-Requests

TFTP-WAN-Rx-Data	Anzahl der vom WAN empfangenen TFTP-Daten-Pakete
TFTP-WAN-Rx-Ack	Anzahl der vom WAN empfangenen TFTP-Acknowledges
TFTP-WAN-Rx-OAck	Anzahl der vom WAN empfangenen TFTP-Option-Acknowledges
TFTP-WAN-Rx-Err	Anzahl der vom WAN empfangenen TFTP-Error-Pakete
TFTP-WAN-Rx-Bad	Anzahl der vom WAN empfangenen, unbekannten TFTP-Pakete
TFTP-WAN-Tx	Anzahl der auf das WAN gesendeten TFTP-Pakete
TFTP-WAN-Tx-Data	Anzahl der auf das WAN gesendeten TFTP-Daten-Pakete
TFTP-WAN-Tx-Ack	Anzahl der auf das WAN gesendeten TFTP-Acknowledges
TFTP-WAN-Tx-OAck	Anzahl der auf das WAN gesendeten TFTP-Option-Ack
TFTP-WAN-Tx-Err	Anzahl der auf das WAN gesendeten TFTP-Error-Pakete
TFTP-WAN-Tx-Rep.	Anzahl der wiederholt auf's WAN gesendeten TFTP-Paket
TFTP-WAN-Conn.	Anzahl der zum WAN aufgebauten TFTP-Verbindungen

Status/IP-Router-Statistik

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

/IP-Router-Statistik		Statistiken aus dem IP-Router-Bereich
IPR-LAN-Rx		Anzahl vom LAN zu routender Datenpakete
IPR-LAN-Tx		Anzahl zum LAN gerouteter Datenpakete
IPR-LAN-lokal-R		Anzahl vom LAN empfangener und zum LAN gerouteter Pakete
IPR LAN-Netzwf.		Anzahl LAN-Pakete, die nicht geroutet wurden
IPR-LAN-Routef.		Anzahl LAN-Pakete, die zu einem anderen Router müssen
IPR-LAN-TTL-F.		Anzahl LAN-Pakete mit einem abgelaufenen time-to-live Wert
IPR-LAN-Filter		Anzahl der über die Filtertabelle gefilterten LAN-Pakete
IPR-LAN-verwrf.		Anzahl der verworfenen LAN-Pakete
IPR-WAN-Rx		Anzahl vom WAN zu routender Datenpakete
IPR-WAN-Tx		Anzahl zum WAN gerouteter Datenpakete
IPR-WAN-Netzwf.		Anzahl WAN-Pakete, die nicht geroutet wurden
IPR-WAN-TTL-F.		Anzahl WAN-Pak. mit einem abgelaufenem time-to-live Wert
IPR-WAN-Filter		Anzahl der über die Filtertabelle gefilterten WAN-Pakete
IPR-WAN-verwrf.		Anzahl der verworfenen WAN-Pakete
IPR-WAN-Typf.		Anzahl der Pakete vom WAN ohne IP-Router-Kennung
IPR-ARP-Fehler		Anzahl der nicht erfolgreichen Zugriffe auf den ARP-Cache

/IP-Router-Statistik	Statistiken aus dem IP-Router-Bereich	
Werte-löschen		IP-Router-Statistik löschen
Aufbau-Tabelle		Tabelle der letzten 20 Pakete, die eine Verbindung erforderten
Protokoll-Tab.		Tabelle über geroutete Pakete, protokollabhängig aufgestellt
RIP-Statistik	MENU	Statistiken aus dem IP/RIP-Bereich

Aufbau-Tabelle In der **Aufbau-Tabelle** sind die letzten 20 Einträge, die Informationen über die Systemzeit, Zieladresse und Quelladresse, IP-Protokoll, Zielport und Quellport 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

Die Systemzeit wird in Tagen, Stunden, Minuten und Sekunden seit Einschaltzeitpunkt angezeigt und belegt den Zeitpunkt den Verbindungsaufbaus. Die Ziel- und Quelladressen sind jeweils IP-Adressen, das Protokoll kann zum Beispiel auf tcp, udp oder ähnliches hinweisen und die Ziel- und Quellports definieren näher die betroffenen Dienste (Telnet z.B. über TCP und Z-Port. 23, Nameserver über UDP und Z-Port 53).

Protokoll-Tab. 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 *LANCOM* 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-F.	Anzahl fehlerhafter Einträge in IP-RIP-Paketen
RIP-Tx	Anzahl gesendeter IP-RIP-Pakete
Tabelle-RIP	Routing-Tabelle der durch RIP-Broadcast gelernten Routen

Tabelle-RIP









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

Eine IP-RIP-Tabelle kann wie folgt aussehen:

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

Status/Config-Statistik

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

/Config-Statistik	Statistiken der Remote-Konfiguration	
C-LAN-Akt. Verb.		Anzahl aktueller Konfigurationsverbindungen vom LAN
C-LAN-Ges. Verb.		Anzahl bisheriger Konfigurationsverbindungen vom LAN
C-WAN-Akt. Verb.		Anzahl aktueller Konfigurationsverbindungen vom WAN
C-WAN-Ges. Verb.		Anzahl bisheriger Konfigurationsverbindungen vom WAN
Outband-Akt. Verb.		Anzahl aktueller Outband-Konfigurationsverbindungen
Outband-Ges. Verb.		Anzahl bisheriger Outband-Konfigurationsverbindungen
OUTBAND-Bitrate		Bitrate der letzten Outband Konfigurationssitzung
Werte-löschen		Config-Statistik löschen

Status/Verb.-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/Verb.-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	Verb.-Zeit	Gebuehren
Ch01	0	0	0	0	Keine Verb.	0
Ch02	0	0	0	0	Keine Verb.	0
Ser1	0	0	0	0	Keine Verb.	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

lfc	Bezeichnet den zugehörigen B-Kanal (siehe auch "/Status/WAN-Statistik")
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
Verb.-Zeit	Gibt die Zeit an, seit der die aktuelle Verbindung besteht. Besteht keine Verbindung, so wird "Keine Verb." ausgegeben
Gebuehren	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-Verb."** enthält für jedes verfügbare Interface weitere Informationen über dessen aktuellen Verbindungszustand (logische Gegenstelle, deren Auswahl etc.). Die dort aufgeführte Tabelle hat folgendes Aussehen:

lfc	Status	Anw.	Rufnummer	Gerätename	B1-HZ	B2-HZ
Ch01	Bereit				0	0
Ch02	Bereit				0	0
Ser1	Bereit				0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	Bezeichnet den zugehörigen B-Kanal (siehe auch " Status/WAN-Statistik ")
Status	Gibt den Zustand der jeweiligen Verbindung an. Mögliche Werte sind: Initialisierung , Setup-WAN , Bereit , Anwahl , Anliegender-Ruf , Protokoll , Verbindung , Rückruf , sowie Bündelung und Reserviert . Der Status Bündelung wird im Display 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.
Anw.	Gibt die Art des Aufbaus wieder. Möglich sind: Akt. (aktiver Verbindungs-aufbau = Anwahl), Pas. (passiver Verbindungsaufbau = Anruf) und RR (Aufbau durch Rückruf).
Rufnummer	Gibt die Rufnummer der Gegenstelle an. Bei einer aktiv aufgebauten Verbindung steht hier die Rufnummer der Gegenstelle aus der Namenliste; bei passiv aufgebauten Verbindungen ebenfalls.
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 Short-Hold-Zeit der Verbindung an.
B2-HZ	Gibt die Short-Hold-Zeit für gebündelte Kanäle dieser Verbindung an.

Status/Layer-Verb.

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

Ifc	Layername	Encaps	Lay-3	Lay-2	L2-Opt.	Lay-1
Ch01	DEFAULT	ETHER	ELSA	X.75ELSA	compr.	HDLC64K
Ch02	PPPHDLC	TRANS	TRANS	PPP	Keine	HDLC64K
Ser1	V.24_DEF	ETHER	ELSA	X.75ELSA	compr.	HDLC64K

Status/Ruf-Info-Tabelle

In dieser Tabelle werden die letzten zehn angekommenen Rufe angezeigt; und zwar unabhängig davon, ob das *LANCOM* den Ruf angenommen hat oder nicht.

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

Systemzeit	Ifc	CLIP-Anrufer	Wahl-Anrufer	Dienst	B-Kanal
OT; 00:20:57	S0	5678	1234	HDLC64K	2
OT; 00:20:46	S0	4321	1234	HDLC64K	1
OT; 00:19:47	S0	4321	1234	HDLC64K	1
OT; 00:11:33	S0	5678	1234	HDLC64K	1
OT; 00:01:13	S0	4321	1234	HDLC64K	2
OT; 00:01:02	S0	4321	1234	HDLC64K	1
OT; 00:00:06	S0	5678	1234	HDLC64K	1

Die Einträge haben die folgende Bedeutung:

Systemzeit	Zeitpunkt, zu dem der Ruf ankam
Ifc	Interface, auf dem der Ruf ankam. Mögliche Werte sind S0 für den internen S0-Bus und Ser1 für die externe Schnittstelle.
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 unbek.. Ein analoger Ruf wird hier also als unbek. angezeigt.
B-Kanal	Hier wird der benutzte B-Kanal eingetragen. Ein Wert von 0 bedeutet, daß beide Kanäle bereits belegt sind, es sich also um ein anklopfen handelt.

Ein Tip für den Fall, daß ein LANCOM 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 LANCOM an der Stelle /SETUP/WAN-MODUL/S0-INTERFACE/MSN-AN eingetragen werden muß, damit ein Ruf von Außen korrekt angenommen werden kann.












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 des *LANCOM* notwendig sind, abgefragt und geändert werden.

/Setup	Konfiguration des Systems	
Name		Eingabe des <i>LANCOM</i> -Gerätenamens
WAN-Modul		Einstellungen für das WAN
Gebühren-Modul		Einstellungen für die Gebührenverwaltung
LAN-Modul		Einstellungen für das LAN
Bridge-Modul		Einstellungen für die Remote Bridge
IPX-Modul		Einstellungen für das IPX-Modul (IPX-Router)
TCP-IP-Modul		Einstellungen für das TCP/IP-Modul
IP-Router-Modul		Einstellungen für das IP-Router-Modul
SNMP-Modul		Einstellungen für die Konfiguration über SNMP
Config-Modul		Einstellungen für das Konfigurationsmodul
Sonstiges		Einstellungen für Display-Anzeige und Tastatur

Name

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

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

anzeigen lassen. Standardmäßig ist kein Name eingetragen.

Der Geräte name wird zur Identifikation benötigt und ist Voraussetzung für eine mögliche Verbindung über die IPX- oder IP-Router-Module, da die Router nur mit bekannten Gegenstellen Daten austauschen, sowie für die eindeutige Identifizierung einer Bridge-Gegenstelle.















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

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

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

Setup/WAN-Modul

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

/WAN-Modul		Einstellungen für das WAN
Interface		Einstellungen für das WAN-Interface
Namenliste		Einstellungen für die Gegenstellen
RoundRobin-Liste		Einstellungen verschiedener Gegenstellen-Nummern
Layerliste		Einstellungen der verwendeten Layer-Kombinationen
PPP-Liste		Einstellung der Parameter für PPP-Verbindungen
Nummernliste		Einstellung der zugangsberechtigten Rufnummern
Script-Liste		Einstellung der Anwahl-Scripte
Anwahl-Praefix		Anfangsnummern für den aktiven Verbindungsaufbau
ext. -Anw. -Praefix		Anfangsnummern für den aktiven Verbindungsaufbau
Manuelle-Wahl		Einstellungen für die manuelle Verbindungssteuerung
Schutz		keiner
RR-Versuche		3
V.24-Max.-Bps		
Backup-St.-Sek		

Interface

Die Interface-Tabelle enthält die Setup-Einträge für jedes verfügbare WAN-Interface. Alle Einstellungen werden gleichzeitig angezeigt. Im Betrieb werden jedoch nur die Einstellungen berücksichtigt, die zum jeweils eingestellten D-Kanal-Protokoll gehören (EAZ bei 1TR6 bzw. MSN bei DSS1, Master/Slave bei Festverbindungen). Die dort aufgeführte Tabelle hat folgendes Aussehen:

lfc	Protokoll	EAZ	MSN-an	MSN-ab	FV-Mode	B-Kanal	YV.
S0	DSS1	1			Master	1	Ein
Ser1	DSS1	0			Master	1	Ein

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	Bezeichnet den zugehörigen D-Kanal. Mögliche Werte sind: S0 (Einstellung der internen Schnittstelle) und Ser1 (serieller Port)
Protokoll	Einstellung des D-Kanal-Protokolls. Mögliche Werte sind: DSS1 : Euro-ISDN 1TR6 : nationales ISDN GRP0 : Festverbindung Gruppe 0 GRP2 : Festverbindung Gruppe 2
EAZ	Endgeräte-Auswahl-Ziffer des LANCOMs. Nur gültig, wenn als D-Kanal-Protokoll 1TR6 eingestellt ist.
MSN-an	Mehrfachrufnummer, auf die das <i>LANCOM</i> bei einem ankommenden Ruf reagieren soll. Nur gültig, wenn als Protokoll DSS1 eingestellt ist. Wenn keine MSNs eingegeben werden, reagiert das <i>LANCOM</i> auf alle eingehenden Rufe mit der Dienstekennung D-64S.
MSN-ab	Mehrfachrufnummer, die das <i>LANCOM</i> bei einem aktiven Verbindungsaufbau an die Vermittlungsstelle meldet. Nur gültig, wenn als Protokoll DSS1 eingestellt ist.
FV-Mode	Identifizierung des <i>LANCOM</i> bei einer Festverbindung. Mögliche Werte sind Master und Slave . Bei einer Festverbindung muß immer ein Gerät als Master und das andere als Slave konfiguriert sein. Nur gültig, wenn als D-Kanal-Protokoll GRP0 oder GRP2 eingestellt ist.
B-Kanal	B-Kanal, der für eine Festverbindung genutzt werden soll. Nur gültig, wenn als D-Kanal-Protokoll GRP0 eingestellt ist. Diese Einstellung muß bei beiden beteiligten Routern identisch sein.
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). Aus Y-Verbindung wird nicht unterstützt, es kann nur eine Verbindungen aufgebaut werden. Die zweite Verbindung wird blockiert. Nutzbar, um die Möglichkeit einer Kanalbündelung zu garantieren.

Namenliste

Die in der Namenliste eingetragenen Gerätenamen werden vom *LANCOM* benötigt, um die anzurufende Rufnummer und das einzustellende B-Kanal-Protokoll (Layername) zu ermitteln. Zusätzlich wird die Namenliste für die Rückruffunktion verwendet.

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

Geraetenname	Rufnummer	B1-HZ	B2-HZ	Layername	Rückruf
AACHEN	875463	180	0	X75COMPR	ein
BERLIN	040785647	20	20	RAWHDLCL	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 (Standard: Default).
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).
B2-HZ	In dieser Spalte können entsprechende Verbindungshaltezeiten für den zweiten B-Kanal festgelegt werden (analog B1-HZ, Standard: 20).
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 B-Kanal-Protokolls nach einer bestimmten ISDN-Layer-Kombination festgelegt (Standard: kein Layer, ELSA-Default).
Rückruf	In dieser Spalte können Sie festlegen, ob ein Rückruf für die entsprechende Gegenstelle erfolgen soll (Aus/Name/Auto/Looser; Standard: Aus).

■ Rückrufoptionen

Aus	Es erfolgt kein Rückruf
Looser	Das <i>LANCOM</i> bricht eigene Aufbauversuche ab, wenn ein Ruf von dieser Gegenstelle anliegt. (gegenseitiger Verbindungsaufbau)
Auto (nicht Windows 95 oder Windows NT, s.u.)	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 werden und zusätzlich über die Protokollverhandlung ein Rückruf gestartet werden. Dabei fällt eine Gebühr von einer Einheit an.

- Die Wahlsonderzeichen der folgenden Tabelle können mit den Rufnummern in der Namen- oder Round-Robin-Liste oder im logischen Anwahlpräfix eingegeben werden. Sie steuern die Amtsholung, die Verwendung einer semipermanenten Festverbindung oder bestimmen das für die Verbindung zu verwendende Interface:

#		Amtsholung (nur bei einigen TK-Anlagen)
S		Die semipermanente Verbindung (SPV) wird bei Verbindungen für den ersten B-Kanal verwendet
S2		Die semipermanente Verbindung (SPV) wird bei Verbindungen für beide B-Kanäle verwendet (Kanalbündelung)
I	Interner S0-Bus (ISDN)	Die Gegenstelle kann nur über den internen S0-Bus erreicht werden

E	Externe Schnittstelle	Die Gegenstelle kann nur über die externe Schnittstelle erreicht werden
B	Backup für Wählverbindung	Die Gegenstelle kann nur über die externe Schnittstelle erreicht werden. Wenn auf der externen Schnittstelle bereits eine Verbindung besteht, dann wird diese in jedem Fall abgebaut.
F	Backup für Festverbindung	Die Gegenstelle wird über die Festverbindung erreicht. Dies kann nur in der Namenliste eingegeben werden! Wenn auf das F eine Rufnummer folgt, so kennzeichnet diese die Backup-Rufnummer. Diese Rufnummer setzt sich zusammen wie im Abschnitt Round-Robin beschrieben.

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.*

RoundRobin-Liste

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

Geraetenname	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 zur Geräten

anderer Hersteller, die unterschiedliche B-Kanal-Protokolle verwenden, hergestellt werden.

Die folgende Tabelle dient als Beispiel und zeigt gleichzeitig die Standardeinstellungen:

Layer-Name	Encaps	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	ETHER	ELSA	X.75ELSA	compr.	HDLC64K
V.24_DEF	ETHER	ELSA	X.75ELSA	keine	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	keine	HDLC64K
RAWHDLCL	TRANS	TRANS	TRANS	keine	HDLC64K
X75	TRANS	TRANS	X.75LAPB	keine	HDLC64K
X75COMPR	TRANS	TRANS	X.75LAPB	compr.	HDLC64K
X75BUNDLE	TRANS	TRANS	X.75LAPB	bündeln	HDLC64K
X75B._C.	TRANS	TRANS	X.75LAPB	bnd+cmpr	HDLC64K
BRIDGE_BC	ETHER	TRANS	X.75LAPB	bnd+cmpr	HDLC64K
BRIDGE_B	ETHER	TRANS	X.75LAPB	bündeln	HDLC64K

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Layer-Name	<p>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 B-Kanal-Protokoll einzustellen.</p> <p>Ist in dieser Spalte ein Eintrag mit der Bezeichnung DEFAULT festgelegt, werden die dort abgelegten Einstellungen immer verwendet, wenn kein Layername zugeordnet werden kann, oder 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 löscht- oder veränderbar..</p>	
Encaps	<p>In der Spalte Encaps können zusätzliche Informationen zu den übertragenden Daten festgelegt werden. Folgende Eintragungen sind möglich</p>	
	ETHER	Die Daten werden mit einem Ethernet-Header versehen. Diese Einstellung ist zur Kommunikation mit älteren <i>LANCOM</i> -Geräten, den ELSA-Workstation-Treibern oder im Bridge-Betrieb notwendig.
	TRANS	B dieser Einstellung wird kein Ethernet Header ausgegeben. Es werden „reine“ IPX- oder IP-Datenpakete übertragen. Diese Einstellung sorgt für den größtmöglichen effektiven Datendurchsatz.
Lay-3	<p>In der Spalte Lay-3 können zusätzliche Header für die Datenübertragung im ISDN definiert werden. Folgende Einstellungen sind wählbar:</p>	
	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).
	CISCO	Bei dieser Einstellung wird ein Header nach dem CISCO-Standard eingefügt.

	CONWARE	Bei dieser Einstellung wird ein Header nach dem CONWARE-Standard eingefügt.
	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>LANCOM</i> -Geräten oder den ELSA-Workstation-Treibern notwendig.
	PPP	Es wird eine Verhandlung nach dem Point-To-Point-Protokoll durchgeführt. Eine Datenkompression bzw. eine Kanalbündelung ist mit dieser Einstellung nicht möglich.
	APPP	Es wird eine Verhandlung nach dem asynchronen PPP durchgeführt. APPP wird dann verwendet, wenn PPP nicht möglich ist, weil die Verbindung keine Synchronisation 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. Eine Datenkompression bzw. eine Kanalbündelung ist mit dieser Einstellung nicht möglich.
	X.75UI	Den Daten wird ein X.75UI-Header (Unnumbered Information Header) vorangestellt. Eine Datenkompression bzw. eine Kanalbündelung ist mit dieser Einstellung nicht möglich.
	X.75BUI	Die Daten wird ein X.75BUI-Header (Broadcast Unnumbered Information Header) vorangestellt. Eine Datenkompression bzw. eine Kanalbündelung ist mit dieser Einstellung nicht möglich.
	X.75ELSA	Der Datenaustausch erfolgt im X.75-ELSA-Format. Dieses Format läßt eine Komprimierung der Daten zu. Diese Einstellung ist zur Kommunikation mit älteren <i>LANCOM</i> -Geräten oder den ELSA-Workstation-Treibern notwendig. Die Kommunikation mit Geräten anderer Hersteller ist mit dieser Einstellung nicht möglich.
	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. Dieses Format läßt eine Datenkompression zu.
L2-Opt.	Die Spalte L2-Opt. Ermöglicht die Einstellung einer Option für die Datenübertragungseinstellung unter Lay-2 mit einem weiteren <i>LANCOM</i> .	
	keine	Es erfolgt keine Datenkompression oder Kanalbündelung.
	compr.	Es erfolgt eine Datenkompression nach V.42bis. Die Datenkompression ist nur für die Lay-2-Einstellungen X.75ELSA oder X.75LAPB möglich. Die Kompression kann nicht zur Kommunikation mit Geräten anderer Hersteller verwendet werden.

	buendeln	Es erfolgt eine Kanalbündelung über zwei B-Kanäle. Die Kanalbündelung ist nur für die Lay-2- Einstellungen X.75ELSA oder X.75LAPB möglich. Die statische bzw. dynamische Kanalbündelung ist abhängig von der B2-Verbindungshaltezeit.
	bnd+cmpr	Erfolgt eine Kanalbündelung und Datenkompression nach V.42bis über zwei B-Kanäle. Die Datenkompression und Kanalbündelung sind nur für die Lay-2- Einstellungen X.75ELSA oder X.75LAPB möglich.
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 das LANCOM als Router eingesetzt, ist der Eintrag frei wählbar und passend zur Gegenstelle einzustellen.

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

Wir empfehlen zur Netzzwerkkopplung das ELSA-Protokoll mit Komprimierung und evtl. Kanalbündelung.

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

PPP-Liste

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Gerätename	In der Spalte Gerätename können Sie den symbolischen Namen der PPP-Gegenstelle eintragen.	
Authentifizierung	In dieser Spalte können Sie das Sicherungsverfahren, mit dem die Gegenstelle überprüft werden soll, eintragen. Standardwert: PAP	
	Keine	LANCOM handelt beim Verbindungsaufbau keine Authentifizierung mit der Gegenstelle aus. Diese kann selbst jedoch eine Authentifizierung vom LANCOM verlangen (z.B. Anwahl an ISP).
	PAP	Die Gegenstelle wird nach dem Password-Authentication-Protokoll überprüft.
	CHAP	Die Gegenstelle wird nach dem Challenge-Handshake-Authentication-Protokoll überprüft.

Paßwort	In dieser Spalte kann ein Schlüssel eingetragen werden, dessen Vorhandensein durch das Symbol * dargestellt wird und der zur Überprüfung der Gegenstelle dient. Er kann aus 95 Zeichen (7-Bit ASCII) bestehen. Standardwert: keiner
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	Hier 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 mit dem Konfigurationsprogramm <i>LANconfig</i> verändert werden!
Username	Benutzername (max. 28 Zeichen) , der der Gegenstelle während der PPP-Verhandlung übermittelt wird. Wird kein Username eingetragen, gilt der Gerätenamen als Benutzername.

In der PPP-Liste können maximal 64 Einträge verwaltet werden.

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 LANCOM01 und LANCOM02 wie folgt aussehen, damit über die mitgeteilte Rufnummer deren Name erkannt und gegebenenfalls ein Rückruf (wenn gewünscht) über die Namenliste durchgeführt werden kann:

Rufnummer	Geraetenname
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).



Dieser Mechanismus ist bei Einsatz von analogen Modems an der seriellen Schnittstelle des LANCOM nicht einsetzbar, da bei analogen Leitungen normalerweise keine CLIP-Übertragung möglich ist.

Script-Liste

Einige Internetprovider (z.B. CompuServe) führen vor einer PPP-Verhandlung einen script-gesteuerten Anmeldevorgang durch. Um auch solche Verbindung aufbauen zu können, ist im LANCOM eine einfache Scriptverarbeitung implementiert (siehe 'Script-Verarbeitung' auf Seite 3.2.2).

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

Geraetenname	Script
Geraetenname	Script
Cserve	<>[Host]<CIS>[User]\$U[Password]\$P[PPP]\$C

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

- Gerätename: Name der logischen Gegenstelle
- Script: Alle auszuführenden Befehle - Maximal 58 Zeichen stehen pro Zeile zur Verfügung. Sollte die notwendige Befehlsfolge länger sein, so kann ähnlich wie in der RoundRobin-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.

Anwahl-Präfix Hier kann aus allen erlaubten Rufnummernzeichen eine konstante Anfangsnummer für die eigene Anwahl definiert werden. Für die Anwahl über eine Nebenstellenanlage kann hier z.B. eine Amtsholungsziffer eingegeben werden. Das Anwahl-Präfix wird grundsätzlich vor jede zu wählende Rufnummer gestellt.

ext.-Anw.-Präfix Durch den Menüpunkt 'ext.-Anw.-Präfix' kann ein Anwahl-Präfix für alle abgehenden Rufe über die serielle V.24-Schnittstelle definiert werden. Für Anwahlen auf dem internen SO-Interface wird weiterhin der unter 'Anwahl-Präfix' eingetragene verwendet.

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 bei Verwendung des ELSA-Layers oder PPP ein zusätzlicher Schutz gewährleistet.
- Bei der Einstellung 'Nummer' werden nur solche Gegenstellen akzeptiert, die in der Nummernliste als berechnigte Gegenstellen eingetragen sind.
- Auch ein Kombinationsschutz aus Namenliste oder Nummernliste ist mit 'Nr./Name' einstellbar. Damit werden nur Rufe von Gegenstellen akzeptiert, für die ein Eintrag in der Namenliste oder in der Nummernliste vorhanden ist.

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 Rückruffunktionalität zu optimieren. Der Standardwert beträgt 1.

V.24-Max.-Bps Der Menüpunkt 'V.24-Max.-Bps' dient dazu, die maximale Übertragungsrate der externen Schnittstelle einstellen zu können. Es sind die folgenden Einstellungen möglich:

- 115200 Die maximale Übertragungsrate beträgt 115200 Bits/s
- 230400 Die maximale Übertragungsrate beträgt 230400 Bits/s




Diese Einstellung ist nötig, da es bestimmte Kombinationen von LANCOMs und externen Endgeräten gibt, bei denen nur die niedrigere Übertragungsrate verwendet werden kann. Die Default-Einstellung ist 115200 und funktioniert mit jeder Hardwarekombination.

Backup-St.-Sek Mit dem Menüpunkt 'Backup-St.-Sek' kann die Zeit eingestellt werden, nach der bei einem Zusammenbruch der Festverbindung eine Backup-Verbindung über die externe Schnittstelle aufgebaut wird. Mögliche Werte sind 10 bis 999 Sek. Die Default-Einstellung ist 15 Sek.

Wird eine Zeit von Null Sekunden eingegeben, so wird der aktive Teil des Backup-Mechanismus abgeschaltet, d.h. es wird keine Backup-Verbindung mehr aktiv aufgebaut.

Setup/WAN-Modul/Manuelle-Wahl

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

/Manuelle Wahl	Einstellungen für die manuelle Verbindungssteuerung	
Aufbau		Aufbau einer Verbindung
Abbau		Abbau der aktuellen Verbindung
Zustand		Zeigt den aktuellen Verbindungszustand an

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

Mit dem Befehl

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

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






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

Abbau

Über diesen Befehl kann eine bestehende Verbindung abgebaut werden. Bei einem manuellen Verbindungsabbau kann in der remoten Konfiguration zusätzlich der Name einer Gegenstelle angegeben werden. Es wird dann nur die Verbindung zur angegebenen Gegenstelle gelöst. Besteht keine Verbindung zur angegebenen Gegenstelle, erfolgt keine weitere Reaktion. Wird dagegen kein Gegenstellename angegeben (entspricht der Aktivierung der Funktion über die Tastatur des *LANCOM*) so werden alle bestehenden Verbindungen abgebaut.

Setup/Gebühren-Modul

Über diesen Menüpunkt werden notwendige Einstellungen für den Gebührenschatz vorgenommen. Standardmäßig ist der Gebührenschatz auf 830 Einheiten für einen Zeitraum von sieben Tagen festgelegt. Somit können in sieben Tagen maximal ca. 100,- DM Gebühren anfallen. Das Menü hat folgendes Aussehen:

/Gebühren-Modul	Einstellungen für die Gebührenverwaltung	
Budget-Gebuehren		Einheiten, die pro Periodendauer zur Verfügung stehen
Tage / Periode		Länge einer Periode in Tagen
Rest-Budget		Einheiten, die noch zur Verfügung stehen
Gesamt-Einheiten		Verbrauchte Einheiten in allen Interfaces
Tabelle-Budget		Einstellungen für die lokalen Budgets der einzelnen Interfaces

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

Eine einwandfreie Benutzung des Gebührenschatzes ist nur möglich, wenn die Gebühreninformationen während der Verbindung (nach AOCD) übermittelt werden. Bitte beachten sie dies bei der Beantragung Ihres ISDN-Anschlusses.

*Im europäischen Ausland funktioniert der Gebührenschatz nicht, da noch keine europa-
weite Normung existiert.*

Budget- Gebühren

Über diesen Menüpunkt legen Sie fest, wieviele Einheiten der Gebührenüberwachung als globales Budget für alle Interfaces zusammen zur Verfügung stehen. Diese Einheiten können nur in Zehnerschritten bis maximal 2550 Einheiten eingegeben werden. Der Standardwert beträgt 830 Einheiten (ca. 100,- DM). Die durch die Gebühreninformationen übertragenen Gebühreneinheiten werden während des Betriebs addiert.

Wird der Wert 0 eingegeben, werden nur die lokalen Budget beachtet (s.u.). Bei Überschreitung des Gebührenbudgets, kann aktiv keine Verbindung mehr aufgebaut werden. Auf dem Display des *LANCOM MPR* erscheint die Meldung:

Gebührensperre
Ch02: Bereit

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

Tage / Periode

Über diesen Menüpunkt kann der Zeitraum in Tagen (von 0 bis 255) festgelegt werden, in dem die Gebühreninformationen addiert und mit dem Budget verglichen werden. Der Standardwert beträgt 7 Tage. Ist dieser Zeitraum abgelaufen, beginnt die Addition der Gebühreninformation neu.

Wird der Wert 0 eingegeben, kann nach Verbrauch des Gebührenbudget keine Verbindung aufgebaut werden.

Tabelle-Budget

Zusätzlich zum globalen Gebühren-Budget können für jedes Interface getrennt lokale Budgets definiert werden. Läuft ein lokales Budget ab, ohne daß gleichzeitig das globale Budget abgelaufen ist, wird nur das zugehörige Interface bis zum Ablauf der Gebühren-Periode gesperrt. Alle restlichen Interfaces können bis zum Ablauf der lokalen oder des globalen Budgets weiterhin aktiv Verbindungen aufbauen. So wird eine beliebige Verteilung der Gebühren auf einzelne Interfaces realisiert.

Die Tabelle zur Einstellung der lokalen Gebühren-Budgets besitzt folgenden Aufbau

lfc	Budget-Einheiten	Rest-Budget	Gesamt-Einheiten
S0	0	0	0
Ser1	0	0	0

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




Eine Eingabe von Null Budget-Einheiten deaktiviert die Gebührenüberwachung für das jeweilige Interface. Haben alle Budgets den Wert Null, so wird keine Gebührenüberwachung durchgeführt.

Werden keine oder für das *LANCOM* nicht auswertbare Gebühren-Informationen übermittelt, meldet der Router nach jeder Verbindung 'keine Geb.-Info'.

Für diese Funktionen muß das Telekommunikationsdienst-Merkmal „Gebühreninformation während der Verbindung“ für den ISDN-Anschluß freigeschaltet sein. Wenn die „Gebühreninformation“ nur nach der Verbindung mitgeteilt wird, kann eine Überwachung während der Verbindung nicht garantiert werden. In diesem Fall wird der Gebührenschatz nur vor dem nächsten Verbindungsaufbau wirksam. Verbindungen, die unendlich lange bestehen bleiben, können somit nicht kontrolliert werden und unterlaufen damit den Gebührenschatz.

Setup/LAN-Modul

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

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

Anschluß

Hier kann einer der folgenden Netzwerkanschlüsse ausgewählt werden:

- 10BASE-T (10B-T)
- 10BASE-2 (10B-2)
- 10BASE-5 (10B-5, nur LANCOM MPR)

Die Einstellung 'Auto' (Standardeinstellung ab Hardware-Release F) aktiviert die Auto-sense-Funktion des Netzwerk-Chips für die Anschlüsse 10BASE-2 und 10BASE-T. Dadurch stellt sich das *LANCOM* automatisch auf den verwendeten Anschluß ein, ohne das dieser Punkt manuell konfiguriert werden muß. Dies gilt nicht für den 10BASE-5-Anschluß, der in jedem Fall manuell konfiguriert werden muß.

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

Node-ID

Unter diesem Menüpunkt wird die eigene Ethernet-Adresse des Routers angezeigt. Der hier angezeigte Wert wurde von ELSA festgelegt und kann nicht verändert werden. Die

Anzeige der Ethernet-Adresse erfolgt als zwölfstellige Hexadezimalzahl, wobei die ersten sechs Stellen konstant sind.







Node-ID
00A057xxxxxx

Anzeige der Ethernet-Adresse

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 alle vier möglichen Telnet-Sitzungen jederzeit über das lokale Netzwerk aktiviert werden können.

Setup/Bridge-Modul

Hier können die für den Bridge-Betrieb notwendigen Einstellungen vorgenommen werden. Das Menü hat folgenden Aufbau:

/Bridge-Modul		Einstellungen für die Remote Bridge
Zustand		Remote Bridge aktiv oder inaktiv
Gegenstelle		Gegenstellename für eigenen Verbindungsaufbau
Bridge-Tabelle		Anzeige der Bridge-Tabelle
Bridge-Aging		Verweilzeit von MAC-Adressen in der Bridge-Tabelle
LAN-Einstellung		Einstellungen für die LAN-Seite
WAN-Einstellung		Einstellungen für die WAN-Seite

Zustand Hier kann die Remote Bridge aktiviert bzw. deaktiviert werden. Standardmäßig ist die Remote Bridge ausgeschaltet.

Wird das Gerät für eine reine IP-Router- oder IPX-Router-Verbindung eingesetzt, sollte die Remote Bridge ausgeschaltet werden.

Gegenstelle Hier wird der Name der anzurufenden Gegenstelle hinterlegt (als Zeichenketten aus maximal 16 Zeichen). Für die aktive Anwahl ist ein passender Eintrag in der Namenliste notwendig.

Bridge-Tabelle Über diesen Menüpunkt werden die Einträge der aktuellen Bridge-Tabelle angezeigt. Die Tabelle wird automatisch aufgebaut und nach einem Hash-Verfahren verwaltet. Sie umfaßt maximal 512 Einträge.

Einträge in der Bridge-Tabelle könnten wie folgt aussehen, wenn die Bridge lokale und remote MAC-Adressen im Laufe der Zeit erlernt hat:

Node-ID	Letzter Zugriff	Forward-Flag
00a05702000a	4 tics	lokal
0800096483d4	105073354 tics	lokal
00001b157de0	105079059 tics	remote

Die letzte Zugriffszeit wird in einem Vielfachen von 9ms (tics) seit Einschaltzeitpunkt abgelegt. Das Forward-Flag spiegelt die Lokalität der MAC-Adresse wider. Ein Eintrag der Form 00a057XXXXXX ist die eigene MAC-Adresse des LANCOM.





Die Spalte Forward-Flag wird nur bei der Remote-Konfiguration ausgegeben. Bei der Display-Anzeige fehlt diese Spalte.

Bridge-Aging

Hier kann eine Zeit (von 1 bis 60 Minuten) eingegeben werden, nach der die Bridgetabelle automatisch aktualisiert wird, d.h. alle nicht angesprochenen MAC-Adressen seit der letzten automatischen Aktualisierung werden entfernt. Der Standardwert beträgt 30 Minuten.

Setup/Bridge-Modul/LAN-Einstellung

Hier können die für die Datenpakete des LANs erforderlichen Übertragungsprofile eingestellt werden. Das Menü hat folgenden Aufbau:

/LAN-Einstellung	Einstellungen für die LAN-Seite	
Broadcast		Filterverhalten von Broadcast-Datenpaketen
Multicast		Filterverhalten von Multicast-Datenpaketen
Ziel-Adressen		Filterung von Zieladressen
Quell-Adressen		Filterung von Quelladressen

Broadcast

Unter diesem Menüpunkt kann eingestellt werden, ob Broadcast-Datenpakete immer (**pos**, Standard), nie (**neg**) oder nur bei bestehender Verbindung (**sem**) übertragen werden sollen.



Multicast

Hier kann eingestellt werden, ob Multicast-Datenpakete immer (**pos**, Standard), nie (**neg**) oder nur bei bestehender Verbindung (**sem**) übertragen werden sollen.

Die Einstellung pos bei Multicast oder Broadcast können zu hohen Gebühren führen, da sehr oft Verbindungen aufgebaut werden.

Setup/Bridge-Modul/LAN-Einstellung/Zieladressen

Unter diesem Menüpunkt können alle Einstellungen vorgenommen werden, die für die Filterung von Zieladressen erforderlich sind.

/Ziel-Adressen	Filterung von Zieladressen	
Filter-Typ		Positiver oder negativer Filter
Filter-Tabelle		Bearbeitung der Adreßfiltertabelle

Filtertyp

Der für die Zieladreßliste zu verwendende Filtertyp kann hier festgelegt werden. Möglich sind die Einstellungen (**pos**), so daß nur die Datenpakete übertragen werden, deren Zieladresse in der Zieladreß-Filtertabelle enthalten sind. Bei der Einstellung (**neg**, Standardwert) werden alle Frames übertragen, deren Zieladresse nicht in der Zieladreß-Filtertabelle enthalten sind.

Filtertabelle

In dieser Tabelle können die Zieladressen verwaltet werden. Der Eintrag besteht lediglich aus dem Feld **MAC-Adresse**.

Ziel-Adresse

0000c051d266

Setup/Bridge-Modul/LAN-Einstellung/Quelladressen







Die Einstellungen für Quelladressen erfolgen analog zu den Einstellungen für die Zieladressen.

Setup/Bridge-Modul/WAN-Einstellung

Einstellungen für WAN-Datenpakete. Die Einstellungen unter diesem Menü erfolgen völlig analog zu den Einstellungen im Menü **LAN-Einstellung**, filtern im Gegensatz dazu aber die vom WAN hereinkommenden Datenpakete.

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		IPX-Modul ein- oder ausgeschaltet
IPX-Router		IPX-Router ein- oder ausgeschaltet
LAN-Einstellung		Einstellungen für die LAN-Seite
WAN-Einstellung		Einstellungen für die WAN-Seite
RIP-Einstellung		Einstellungen für RIP
SAP-Einstellung		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 das IPX-Router-Modul aktiviert bzw. deaktiviert werden. Standardmäßig ist das IPX-Router-Modul ausgeschaltet.

Beim Einschalten des IPX-Router-Moduls 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		Logische IPX-Netzwerknummer des LAN-Anschlusses
Binding		Einstellung der Ethernet-Frame-Typen für den LAN-Anschluß
IPX-Watch		Einstellungen für IPX-Watchdog-Verwaltung
SPX-Watch		Einstellungen für SPX-Watchdog-Verwaltung
NetBios-Watch		Einstellungen für NetBIOS-Watchdog-Verwaltung
Socket-Filter		Filtertabelle für Zielsocketfilterung
Lok.-Routing		Lokales Routing aktiviert oder deaktiviert
RIP-SAP-Skal.		RIP-SAP-Skalierung aktiviert oder deaktiviert
LOOP-propagieren		Propagieren von redundanten Routen aktiviert oder deaktiviert

Netzwerk Hier wird die NetWare-Netzwerknummer des Netzes (8-stellig, hexadezimal) eingetragen, die an den LAN-Anschluß unter dem Binding (siehe unten) angeschlossen wird. Ist im lokalen Netzwerk ein NetWare-Server vorhanden, so können Sie diese Nummer mit Hilfe des Befehls `node` an einer angeschlossenen Workstation ermitteln.

Der Standardwert beträgt '00000000'.

Binding Das Ethernet-Paketformat (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 '802.3'.

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.

Propagat Hiermit wird eingestellt, ob IPX-Propagated-Typen geroutet (**Route**, Standard) oder nicht geroutet (**Filt**) werden sollen. Propagated-Typen werden häufig zu Broadcast-Funktionen über das IPX-Protokoll eingesetzt.

Damit die Remote-Konfiguration über DOS/IPX auch eine Remote-Gerät über die WAN-Verbindung erreichen kann, muß die Übertragung von Propagated-Typen eingeschaltet sein (Route).

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' auf Seite 3.4.13).

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 trotz-

dem 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. Das LANCOM 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 Realität entspricht. Hierdurch werden alle Clients ihre Pakete für diese Routen an das LANCOM schicken, daß die Verbindung hat. Weiterhin können in dem Fall, daß 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 wird (durch den sich andere Router zu weiteren Broadcasts veranlaßt sehen könnten und somit eine hohe Netzlast entstehen kann), ist diese 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		Router-Tabelle für die Zuordnung von IPX-Netzwerk und Gegenstelle
Socket-Filter		Filtertabelle für Zielsocketfilterung

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 zwei bzw. bei Verwendung der externen Schnittstelle als dritte Wahlleitung maximal drei Gegenstellen propagated Frames erhalten. Dies ist insbesondere bei einer WAN-Konfiguration mittels LC_CONF.EXE zu berücksichtigen, da dieses von „propagated frames“ Gebrauch macht. Die Default-Einstellung ist „Filter“.
- **Backoff:** Der IPX-Router benutzt einen speziellen Algorithmus (Exponential Backoff) um bei Fehlkonfigurationen die anfallenden Verbindungskosten so gering wie möglich zu halten (siehe unten).

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

Tabelle-RIP

Über diesen Menüpunkt werden die Einträge der aktuellen RIP-Tabelle angezeigt. Die Tabelle umfaßt maximal 64 Einträge.

Die Einträge in der RIP-Tabelle können wie folgt aussehen, wenn es zum Beispiel die Netzwerke 00000001, 00000081, 00000002, 00000010 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 remote Netz ist. **DOWN** weist auf ein Netz hin, das bekannt, aber momentan nicht erreichbar ist.

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

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 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, nach der 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		Anzeigen der SAP-Tabelle
LAN-Filtertab.		Filterbereiche für IPX-Serviceadressen (LAN)
WAN-Filtertab.		Filterbereiche für IPX-Serviceadressen (WAN)
Routen/Frm		Max. # SAP-Einträge pro gesendeten SAP-Frame
Aging		Aging-Zeitraum in Update-Einheiten
Spoofing		SAP-Spoofing-Verfahren einstellen
WAN-Update-Zeit		SAP-Update-Zeitraum, je nach Spoofing wirksam

Tabelle-SAP

Über diesen Menüpunkt werden die Einträge der aktuellen SAP-Tabelle angezeigt. Die Tabelle umfaßt maximal 128 Einträge. Eine beispielhafte SAP-Tabelle könnte wie folgt aussehen:

Typ	Server-Name	Netzwerk	Node-Id	Socket	Hops	Zeit	Flags
0047	X	00000001	0000c0123456	8060	1	0	lokal
0004	Y	000000c1	000000000001	0451	1	1	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 Socketnummer und Informationen über die Lokalität des Servers.

LAN-Filtertab.

Durch Einträge in der LAN-Filtertabelle ist es möglich bestimmte Bereiche der Serviceinformationen 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 daher 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' auf Seite 3.3.10.

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 filtert.

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 aufgebaut.
- Die **Trig**-Einstellung bewirkt eine Verschiebung der SAP-Daten zur Remote-Seite immer dann, wenn Änderungen anfallen.
- Die **Zeit**-Einstellung bewirkt eine Verschiebung 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, nach der 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		TCP/IP-Modul ein- oder ausgeschaltet
IP-Adresse		Eigene IP-Adresse
IP-Netz-Maske		Passende IP-Netzmaske des lokalen Netzes
Intranet-Adresse		Eigene Intranet-Adresse
Intranet-Maske		Passende Intranet-Netzmaske des lokalen Netzes
Zugangsliste		Einschränkung des Zugriffs auf interne Funktionen über TCP/IP
DNS-Default		Domain Name Server
DNS-Backup		Backup Domain Name Server
NBNS-Default		Net Bios Name Server
NBNS-Backup		Backup Net Bios Name Server
Tabelle-ARP		ARP-Tabelle für Abb. einer IP-Adresse auf eine MAC-Adresse
ARP-Aging-Min		Verweildauer für Einträge in der ARP-Tabelle
TCP-Aging-Min		Zeitbeschränkung für Konfigurations-Verbindungen, die inaktiv sind
TCP-Max.-Verb.		Max. Anzahl gleichzeitiger Konfigurations-Verbindungen zum LANCOM

Zustand Hier kann das TCP/IP-Modul des LANCOM 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 das LANCOM eingegeben werden. Die Standardadresse bei der Auslieferung ist die '0.0.0.0'. Die IP-Adresse ist im lokalen Netz und nach außen hin gültig.

IP-Netz-Maske Hier kann die IP-Netzmaske des LANCOM eingegeben werden.

Intranet-Adresse Hier kann die Intranet-Adresse, die für die Remote-Konfiguration und den IP-Router erforderlich ist, für das LANCOM eingegeben werden. Die Intranet-Adresse ist nur im lokalen Netz gültig. Die Standardadresse bei der Auslieferung ist die '0.0.0.0'. Bei dieser Einstellung 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 eine andere Adresse eingegeben oder das TCP/IP-Modul ausgeschaltet werden.

Intranet-Maske Hier kann die Intranet-Netzmaske des *LANCOM* eingegeben werden, die für die Remote-Konfiguration und den IP-Router erforderlich ist.

Zugangsliste Der Zugang zu „internen Funktionen“ des *LANCOM* kann in TCP/IP-Anwendungen durch eine Zugangs-Liste gesteuert werden.

Diese Einschränkung des Zugriffs ist speziell bei Protokollen angebracht, die keine eigenen Zugriffsbeschränkungen (z.B. Passwortüberprüfungen) enthalten, wie etwa das 'Trivial-File-Transfer-Protocol', das zum Laden und Speichern von Konfigurationen verwendet wird.

Die Zugangs-Kontrolle bezieht sich aus Konsistenzgründen auf alle „internen Funktionen“ des *LANCOMs*. Unter dem Begriff „interne Funktionen“ sind folgende zu verstehen:

- Telnet-Server: die bekannte Konfigurations-Schnittstelle auf Basis des Telnet-Protokolls.
- TFTP-Server: die neue Konfigurations-Schnittstelle auf Basis des TFTP-Protokolls.

Jeder der maximal 16 Einträge in der Zugangs-Liste 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 des *LANCOM* zugegriffen werden. Alle Anforderungen von Geräten mit anderen IP-Adressen bleiben unbeantwortet.

Soll einem kompletten Netzwerk der Zugang zu einem *LANCOM* ermöglicht werden, kann dies für ein Klasse C Netzwerk 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 *LANCOM* zu benutzen.

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

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

Im *LANCOM* wird als Adresse des DNS-Servers die '0.0.0.0' eingetragen. Dann können alle Rechner im lokalen Netz den DNS-Server des Providers nutzen.

Die eigene IP-Adresse des *LANCOMs* wird als DNS-Server eingetragen. Dann nutzt das *LANCOM* 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 beim *LANCOM* einwählen, können dann auch auf den DNS-Server des Providers zugreifen.

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

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

NBNS-Backup Durch den Eintrag **NBNS-Backup** kann ein zweiter Net Bios Name 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, 192.168.139.30) mit dem *LANCOM* kommuniziert haben:

IP-Adresse	Node-ID	Letzter Zugriff	Anschluß
192.168.139.20	0000c0717860	6780443 tics	lokal
192.168.139.30	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 *LANCOM* keine Übertragung mehr, wenn z.B. während der Remote-Konfiguration keine Daten mehr vom Benutzer eingegeben werden, baut das *LANCOM* die TCP-Verbindung automatisch nach der hier angegebenen Zeit ab. Gültige Werte sind 1 bis 99 Minuten. Der Standardwert beträgt 15 Minuten.

TCP-Max.-Verb. Hier kann die maximale Anzahl der TCP-Verbindungen, die gleichzeitig zum *LANCOM* bestehen, abgelesen werden. Standardmäßig können vier Verbindungen gleichzeitig zum

Router bestehen. Dieser Wert kann nicht verändert werden. Das betrifft nur die Konfigurationssitzungen. Die Anzahl der TCP-Verbindungen über den Router ist nicht limitiert.

Setup/IP-Router-Modul

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

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

Zustand

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

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

IP-Routing-Tab

In der Router-Tabelle können maximal 64 Einträge von Zielnetzwerkadressen oder direkten IP-Adressen mit dazugehörigen Netzwerkmasken und Namen der Gegenstellen 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.

Zur Identifizierung der anzurufenden Gegenstelle durchsucht der Router anhand der empfangenen Ziel-IP-Adresse die Router-Tabelle von oben nach unten. Wurde ein passender Eintrag in der Router-Tabelle gefunden, wird der gefundene Router-Name für den Verbindungsaufbau 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
10.0.0.0	255.0.0.0	0.0.0.0	0	Aus
172.16.0.0	255.240.0.0	0.0.0.0	0	Aus
192.168.0.0	255.255.0.0	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 ein *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 Zielnetze 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

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 vorher nicht übertragen kann und nicht verwerfen soll bzw. was von einem WAN-Anschluß kommt und nicht lokal ist, an den Router beim Provider.

LAN-Filtertab. Mit dieser Tabelle können bestimmte Ziel-Port-Bereiche gefiltert werden. Darüber hinaus kann bestimmt werden, wie diese Pakete gefiltert werden. Treffen von der LAN-Seite Pakete mit diesen 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	53	53	137	137	0.0.0.0	0.0.0.0	alle	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-Portbereich, der gefiltert werden soll. Ein Bereich von 0 bis 0 bedeutet, daß kein Zielpport von diesem Filter beeinflusst wird.
- **Q-von, Q-bis**
Quell-Portbereich, der gefiltert werden soll. Ein Bereich von 0 bis 0 bedeutet, daß kein Quellport von diesem Filter beeinflusst wird.
- **Quell-Adresse, Quell-Netzmaske**
Hiermit kann ein Subnetz des lokalen Netzes angegeben werden, für daß der Filter gelten soll. Ist die Quell-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).
- **Prot**
Protokoll, daß gefiltert werden soll. Möglich sind TCP, UDP, ICMP und alle
- **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 obigen Tabelle ist der Filter eingetragen, der den unerwünschten Verbindungsaufbau bei Windows-Netzen auf IP unterbindet.

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

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	Typ
WIN	53	53	137	137	0.0.0.0	0.0.0.0	alle	Immer

Die Felder der Tabelle haben die gleiche Bedeutung wie bei den LAN-Filtern, mit folgendem Unterschied:

■ Ziel-Adresse, Ziel-Netzmaske

Hiermit kann ein Subnetz des lokalen Netzes angegeben werden, für daß der Filter gelten soll. Ist 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).



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 (siehe auch 'Proxy-ARP' auf Seite 1.4.11).

Lok.-Routing Das lokale Routing ermöglicht es dem *LANCOM*, Datenpakete über das lokale Netz weiterzuleiten. Das lokale Routing wird dann nötig, wenn das *LANCOM* als Standard-Gateway der Arbeitsplatzrechner Pakete für Zielnetze empfängt, zu denen es selbst keine Verbindung aufbauen kann. Wenn das *LANCOM* die Adresse des zuständigen Routers nicht über IMCP an die Arbeitsplatzrechner zurückmelden kann, leitet es die Daten selbst zu dem entsprechenden Router weiter (siehe auch 'Lokales Routing' auf Seite 1.4.11). Da diese Einstellung zu einer erhöhten Netzlast führt, ist die Standardeinstellung 'aus'.

Setup/IP-Router-Modul/Routing-Methode

Das *LANCOM* 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 'Type-of-Service' Feldes innerhalb des IP-Headers auf.

Das Menü hat den folgenden Aufbau:

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

IP

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

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

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

Setup/IP-Router-Modul/RIP-Einstellungen

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

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

Typ

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

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

R1-Maske

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

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

Tabelle-RIP






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

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

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

Setup/IP-Router-Modul/Masquerading

In diesem Menü werden die Einstellungen für die Maskierungs-Funktion vorgenommen. Das Menü hat den folgenden Aufbau:

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

Service-Tab.

Bei der Verwendung des inversen Masquerading 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 un-

sichtbar bleiben (siehe auch 'IP-Masquerading (Single User Access, NAT, PAT)' auf Seite 1.4.15). 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 *LANCOM*s ein und hängen Sie die Port-Nr., durch Doppelpunkt getrennt, an die Adresse an.

Mit dem Befehl

```
telnet 192.38.50.100:27
```

verbinden Sie sich direkt zu einem News-Server, der über ein *LANCOM* mit der IP-Adresse 192.38.50.100 zu erreichen ist.

Tab.-Masquerade

Beim IP-Masquerading werden die IP-Adressen von Rechnern im lokalen Netz durch eine Umsetzung der Adressen und Ports im *LANCOM* nach außen hin unsichtbar gemacht. In der dynamischen Masquerading-Tabelle werden die IP-Adressen aus dem lokalen Netz angezeigt, die aktuell vom *LANCOM* maskiert werden. Die dynamische Masquerading-Tabelle hat max 512 Einträge nach folgendem Aufbau:





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

Hierbei bedeuten:

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

Setup/SNMP-Modul

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

/SNMP-Modul	Einstellungen für das Konfigurationsmodul	
Traps-senden		Schalter für die Ausgabe von SNMP-Traps
Trap-IP		Ziel-Adresse für Trap-Nachrichten
Administrator		Geräte-Administrator
Standort		Geräte-Standort

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

Trap-IP Gibt die IP-Adresse 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.

Setup/Config-Modul

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

/Config-Modul	Einstellungen für das Konfigurationsmodul	
LAN-Config		Schalter für Konfiguration von der LAN-Seite
WAN-Config		Schalter für Konfiguration von der WAN-Seite
Passw.Zwang		Passwortzwang ein/aus, wenn kein Passwort vorhanden ist
Maximale-Verb.		Maximale Anzahl gleichzeitiger Verbindungen
Conf.-Haltezeit		Zeitbeschränkung für Remote-Konfigurations-Verbindungen

LAN-Config Mit dieser Einstellung kann festgelegt werden, ob eine Remote-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 Remote-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.

Soll Ihr Router auf jeden Fall zuerst von der WAN-Seite konfiguriert werden, muß die Option 'Ein' aktiviert werden.

- Passw.Zwang** Hier wird festgelegt, ob bei nicht vorhandenem Passwort bei jedem Remote-Konfigurationsbeginn nach einem neuen Passwort gefragt werden soll (**Ein**), oder ob die Passwortabfrage unterdrückt werden soll (**Aus**). Standardmäßig ist die Option **Ein** aktiviert.
- Maximale-Verb.** Hier kann die maximale Anzahl der gleichzeitigen Remote-Konfigurationssitzungen zum Gerät abgelesen werden. Gleichzeitig können vier Konfigurations-Verbindungen zu einem Router bestehen. Dieser Wert kann nicht verändert werden.
- Conf.-Haltezeit** Erfolgt während einer Remote-Konfiguration keine Übertragung mehr, wenn z. B. keine Daten mehr vom Benutzer eingegeben werden, baut das Gerät die Verbindung automatisch nach der hier angegebenen Zeit ab. Gültige Werte sind 1 bis 99 Minuten. Der Standardwert beträgt 5 Minuten.

Setup/Sonstiges

Über dieses Menü können Sie die Optionen für das Display und die Tastatur einstellen. Das Menü hat den folgenden Aufbau:

/Sonstiges		Einstellungen für Display-Anzeige und Tastatur
LCD-Kontrast		LCD-Kontrast einstellen
Key-Passwort		Tastatur-Passwort vergeben
Key-Lock		Tastatur sperren

- LCD-Kontrast** Eingabe des LCD-Kontrastes: Gültige Werte sind 1 bis 8. Der Standardwert beträgt 3.
- Key-Passwort** Eingabe des Tastatur-Paßwortes. Die Länge des Paßwortes darf maximal 8 Zeichen betragen. Das Key-Passwort kann nur über die Tastatur eingegeben werden.
- Key-Lock** Sperren der Tastatur. Ist die Tastatur gesperrt, wird bei Betätigen einer Taste die Eingabe des Paßwortes verlangt. Nach Eingabe des richtigen Paßwortes ist die Tastatur wieder freigegeben. Bei Eingabe eines falschen Paßwortes bleibt die Tastatur gesperrt.

Die Tastatur kann nur bei vorhandenem Passwort gesperrt werden.

Die Sperrung der Tastatur kann über die Remote-Konfiguration sowohl vorgenommen als auch aufgehoben werden (siehe auch Kapitel „Häufig gestellte Fragen und Antworten“, Seite 164).

Wenn sowohl das Key-Paßwort als auch das Paßwort zum Schutz der Konfiguration nicht mehr bekannt sein, gibt es keine Möglichkeit mehr, den Router ohne Verlust aller Einstellungen zu konfigurieren!

Firmware

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

/Firmware	Einstellungen für Display-Anzeige und Tastatur	
Versions-Tabelle		Anzeige der Hardware-Releases und Seriennummern von <i>LANCOM</i> und dem Gerät an der seriellen Schnittstelle.
Firmware-Upload		Starten eines Firmware-Uploads über die serielle Schnittstelle mit X-Modem.

Versions-Tabelle





In der Versions-Tabelle werden sowohl die Versionen des Gerätes selbst als auch die des Gerätes an der seriellen Schnittstelle angezeigt.

lfc	Modul	Version	Seriennummer	Online-Bps
S0	LANCOM MPR	v1.39C 28.03.97	0317.000.005	
Ser1	ELSA ISDN/TLV.34	v1.57J 08.05.96	0326.003.908	230400

Der Eintrag Online-Bps zeigt bei externen Modulen an, mit welcher Übertragungsrate das *LANCOM* die Daten an das Modul übergibt. Die maximal mögliche Rate wird während der Initialisierung des externen Moduls bestimmt.

Sonstiges

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

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

Sonstiges/Manuelle-Wahl

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

System-Boot Über diesen Menüpunkt kann das Gerät neu gestartet werden.

System-Reset Über diesen Menüpunkt werden alle vorgenommenen Einstellungen rückgängig gemacht. Das Gerät wird in den Auslieferungszustand zurückversetzt und folgende Anzeige wird beim *LANCOM* kurz eingeblendet:

System-Reset
Bitte warten ...

Reset wird durchgeführt.

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

System-Upload Über diesen Menüpunkt kann ein Firmware-Upload gestartet werden (siehe Kapitel 'So spielen Sie eine neue Software ein' auf Seite 1.3.16).

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.

LANCOM intern

In diesem Kapitel finden Sie Informationen über die internen Funktionen des *LANCOMs*, die bei der täglichen Arbeit mit den ISDN-Routern nicht immer benötigt werden, die Spezialisten in besonderen Situationen jedoch gut unterstützen können.

Script-Verarbeitung.....	2
Online Trace-Ausgaben	5
Policy Based Routing	18

Script-Verarbeitung

Allgemeines

Einige Internetprovider (z.B. Compuserve) führen vor einer PPP-Verhandlung einen script-gesteuerten Anmeldevorgang durch. Um auch solche Verbindung aufbauen zu können, wurde im *LANCOM* eine einfache Scriptverarbeitung implementiert.

Ein Script kann aus den folgenden Elementen bestehen:

Element	Beschreibung
<>	Sende den eingeschlossenen Text mit einem abschließenden Carriage-Return.
[]	Warte auf den Empfang des eingeschlossenen Textes. Dabei wird die Groß-/Kleinschreibung ignoriert. Es genügt die Angabe eines eindeutigen Subtextes
\$U	Sende den User-Namen (aus der PPP-Tabelle) mit einem abschließenden Carriage-Return.
\$P	Sende das Paßwort (aus der PPP-Tabelle) mit einem abschließenden Carriage-Return.
\$C	Ende des Scripts

Wie bereits aus der Übersicht hervorgeht, werden Username und Paßwort aus der PPP-Tabelle entnommen, wenn sich dort ein passender Eintrag befindet. Gibt es den User-Namen in der PPP-Tabelle nicht, so wird der Gerätenamen des *LANCOMs* als Username übermittelt.

Nach Abschluß des Scripts wird eine PPP-Verhandlung gestartet, bzw. der Login-Vorgang abgeschlossen.

Zur Festlegung, ob nach der Script-Bearbeitung eine PPP-Verhandlung gestartet wird, dient der Layer-3-Eintrag in der Layerliste. Es existieren drei mögliche Einträge:

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 logische Verbindung zur Gegenstelle. Es erfolgt keine weitere Protokollverhandlung.

Die Script-Liste

Scripte werden in einer dafür vorgesehenen Tabelle der Script-Liste eingegeben. Diese Tabelle befindet sich unter /Setup/WAN-Modul und hat den folgenden Aufbau:

Geraetenname	Script
CSEVERE	<>[Host]<CIS>[User]\$U[Password]\$P[PPP]\$C

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

Geraetenname:	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 RoundRobin-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.

Beispiel:

Geraetenname	Script
CSERVE#1	<>[Host]<CIS>[User]
CSERVE#2	\$U[Password]\$P[PPP]\$C

Im *LANconfig* ist die Script-Liste auf der Registerkarte 'Kommunikation' zu finden.

Compuserve-Anwahl

Im folgenden werden an einem Beispiel die nötigen Einstellungen für die Anwahl an das Compuserve-Netzwerk über X.75, asynchronem PPP und Script-Steuerung vorgestellt.

Layerliste:

Layername	CSERVE	Encaps.	TRANS	Lay-3	SCAPPP
Lay-2	X.75LAPB	L2-Opt.	keine	Lay-1	HDLC64K

Namenliste:

Geraetenname	Rufnummer	B1-HZ	B2-HZ	Layername	Rueckruf
CSERVE	0021194260	60	60	CSERVE	Aus

PPP-Liste:

Geraetenname	Authent.	Passwort	Zeit	Wdh.	Username
CSERVE	keine	*	0	0	xxxxxx,xxxx/PPP:CISPPP

Für xxxxxx,xxxx ist der Compuserve-Account einzutragen.

Script-Liste:

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

Wobei die Elemente des Skripts folgende Bedeutung haben:

Element	Bedeutung
<>	Starte Script auf der Gegenstelle durch senden von Carriage-Return
[Host]	Warte auf die Antwort vom Compuserve-Einwahlknoten In der Antwort taucht irgendwann „Host Name“ auf
<CIS>	Sende „CIS“ gefolgt von Carriage return
[User]	Warte auf die Antwort. Compuserve fragt nach der „User ID“
\$U	Sende den Usernamen. Bei Compuserve besteht dieser aus der Compuserve-User-ID mit angehängtem „/PPP:CISPPP“. Der Username wird aus der PPP-Tabelle geholt und mit einem abschließenden Carriage-Return an die Gegenstelle gesendet
[Password]	Warte auf die Abfrage des Paßworts
\$P	Sende das Paßwort mit einem abschließenden Carriage-Return. Das Paßwort wird aus der PPP-Tabelle geholt.
[PPP]	Warte auf die Connect-Meldung der Gegenstelle
\$C	Das Script ist vollständig bearbeitet. Es wird die in der Layerliste eingestellte Asynchrone PPP-Verhandlung (SCAPPP) gestartet

Online Trace-Ausgaben

Allgemeines

Durch sogenannte 'Online Trace-Ausgaben' (Kontrollausgaben) kann der Anwender Informationen über interne Vorgänge eines arbeitenden *LANCOM* erhalten. Mit Hilfe solcher Informationen können Fehlkonfigurationen, sowohl von *LANCOM* als auch von anderen mit einem *LANCOM* verbundenen Geräten, einfach und sicher aufgespürt werden.

Die Online Trace-Ausgaben können dabei flexibel für einzelne Protokolle bzw. Funktionen innerhalb der Firmware und einzelne Konfigurations-Sitzungen verwaltet werden. Durch Sitzungsbezogene „Trace-Profile“ werden jeweils nur die innerhalb einer Sitzung aktivierten Trace-Informationen angezeigt.

Die Steuerung der Online Trace-Ausgaben erfolgt über ein neu implementiertes Kommando der Remote-Konfiguration, welches vom Kommando-Interpreter ausgewertet wird und dem Benutzer eine direkte Rückmeldung der vorgenommenen Einstellungen gibt. Änderungen dieser Einstellungen werden sofort wirksam und erzeugen bzw. unterdrücken direkt die entsprechenden Ausgaben.

Die Anzeige der Online Trace-Ausgaben erfolgt dabei zeitverzögert zum eigentlichen Ereignis durch die Fern-Konfiguration. Der optional anzuzeigende Zeitstempel spiegelt dabei den Zeitpunkt der Ausgabe, nicht jedoch den Zeitpunkt des tatsächlichen Ereignisses wieder. Im Regelfall differieren diese Zeiten nicht wesentlich, bei einer Analyse der Ausgaben sollte dieser Punkt dennoch immer berücksichtigt werden.

Alle Anzeigen innerhalb der Online Trace-Ausgaben erfolgen soweit möglich im Klartext. Da die Analyse von Netzwerkprotokollen nicht vollständig auf die Darstellung von numerischen Parametern verzichten kann und ein Trace-System nur dann sinnvoll anwendbar ist, wenn die angezeigte Information auch verstanden wird, werden im folgenden für alle Protokolle und Funktionen genaue Beschreibungen der Trace-Informationen nachgereicht.

Sind Anzeigen für ein Protokoll aktiviert, so überschreibt die nächste Ausgabe den aktuellen System-Prompt; jeder weiteren Ausgabe wird ein <Return> <LineFeed> vorangestellt. Betätigt der Anwender eine Taste, wird die gesamte gepufferte Eingabe zusammen mit dem aktuellen System-Prompt erneut dargestellt. Der Anwender erhält so einen visuellen Feedback und Eingaben müssen nicht „blind“ vorgenommen werden.

Bedienung der Trace-Ausgaben

Die Bedienung der Trace-Ausgaben erfolgt in gewohnter Weise kommandozeilen-orientiert. Dazu wurde die Remote-Konfiguration um den Befehl `trace` erweitert; dieser besitzt folgende Befehlssyntax

<code>trace [Schlüssel] [Parameter] ...[Parameter]</code>	Zeigt, oder beeinflusst, den Zustand der Trace-Ausgaben einzelner Protokolle oder Funktionen.
Schlüssel	<code>'?</code> Anzeige einer Hilfeseite <code>'+</code> Einschalten der Trace-Ausgaben <code>'-</code> Ausschalten der Trace-Ausgaben <code>'#</code> Umschalten der Trace-Ausgaben (toggle) (kein) Anzeige des Zustands
Parameter	Symbolischer Name des Protokoll bzw. der Funktion.

Schlüssel und Parameter sind durch Leerzeichen voneinander zu trennen. Die Schlüssel werden vom Kommando-Interpreter nur erkannt, wenn sie eindeutig sind, d.h. sie bestehen aus einem der oben aufgeführten Zeichen ohne Prä- oder Postfix. Für die Eingabe der symbolischen Namen von Protokollen oder Funktionen genügt wie üblich die Eingabe eines eindeutigen Präfixes.

Es können in einer Kommandozeile beliebig viele Schlüssel und Parameter angegeben werden, maßgebend als Obergrenze ist lediglich die Größe des Zeileneingabepuffers. Die Parameter werden entsprechend des letzten vorhergehenden Schlüssels bearbeitet. Ist vor Parametern kein Schlüssel angegeben, so wird der Zustand der jeweiligen Trace-Funktion (ON oder OFF) ausgegeben.

Zu beachten ist außerdem, daß die Kommandozeile von links nach rechts abgearbeitet wird. So kann die Trace-Ausgabe eines Parameters durchaus innerhalb einer Zeile mehrfach ein- und ausgeschaltet werden, da die Umschaltung während des Einlesens der Token aus dem Eingabepuffer erfolgt (siehe auch Beispiele).

Zusätzlich zur Aktivierung von Online Trace-Ausgaben kann über die Schlüsselwörter „Time“ und „Source“ die vorangestellte Ausgabe der Systemzeit und des Protokoll-Namen ein- bzw. ausgeschaltet werden. Ohne diese beiden Anzeigen wird jede Trace-Ausgabe um 21 Zeichen verkürzt.

Beispiele zur Bedienung der Trace-Ausgaben

Die folgende Tabelle soll einige praktische Beispiele aufzeigen, wie das Kommando für die Trace-Ausgaben genutzt werden kann:

Eingabe	Wirkung
trace	Ausgabe aller Protokolle, die in der Konfigurationssitzung Trace-Ausgaben erzeugen können, und des Zustandes der Ausgaben (ON, OFF).
trace + all	Schaltet alle Trace-Ausgaben in der jeweiligen Sitzung ein.
trace + protocol display	Schaltet alle Verbindungs-Aufbauprotokolle und die Anzeige der Display-Ausgaben ein.
trace + all - icmp	Schaltet alle Trace-Ausgaben ein, jedoch Ausgaben des ICMP-Protokolls aus.
trace ppp elsa	Zeigt den Zustand der PPP- und ELSA Trace-Ausgaben an.
trace # ipx-rt display	Schaltet die Trace-Ausgaben des IPX-Routers und der Display-Ausgaben um.
trace - time	Schaltet die Angabe der Betriebszeit vor der eigentlichen Ausgabe aus.

Unterstützte Protokolle und Funktionen

Folgende symbolische Namen für Protokoll-Stacks werden unterstützt:

Status	Anzeige von Status-Meldungen über Verbindungen
Error	Anzeige von Fehlermeldungen über Verbindungen
ELSA	Anzeige der ELSA Protokoll-Verhandlung
PPP	Anzeige der PPP Protokoll-Verhandlungen
SCRPT	Anzeige der Script-Verhandlung
IPX-Rt.	Anzeige des IPX-Routings
RIP	Anzeige des IPX Routing-Information-Protokolls
SAP	Anzeige des IPX Service-Advertising-Protokolls
IPX-Wd.	Anzeige des IPX Watchdog-Spoofings
SPX-Wd.	Anzeige des SPX Watchdog-Spoofings
NetBIOS	Anzeige der IPX NetBIOS-Verwaltung
IP-Rt.	Anzeige des IP-Routings
IP-RIP	Anzeige des IP Routing-Information-Protokolls
ICMP	Anzeige des Internet-Control-Message-Protokolls
IP-MASQ	Anzeige der Vorgänge im Masquerading Modul
ARP	Anzeige des Address-Resolution-Protocols

Außer diesen Parametern existieren noch folgende „Sammelparameter“ (das sind Parameter für eine bestimmte Protokoll-Art), mit deren Hilfe die Online Trace-Ausgaben für eine komplette, logisch zusammenhängende, Protokoll-Familie aktiviert bzw. deaktiviert werden können:

All	Anzeige aller Online Trace-Ausgaben
Display	Anzeige von "Status" und "Error"
Protocol	Anzeige von "ELSA" und "PPP" und "SCRPT"
TCP-IP	Anzeige von "IP-Rt.", "IP-RIP", "ICMP", "ARP" und "IP-MASQ"
IPX-SPX	Anzeige von "IPX-Rt.", "RIP", "SAP", "IPX-Wd.", "SPX-Wd." und "NetBIOS"

Schließlich werden noch weitere Parameter erkannt, über welche das Darstellungsformat der Trace-Ausgaben beeinflusst werden kann

Time	Anzeige der Systemzeit als Präfix
Source	Anzeige des erzeugenden Protokolls als Präfix

Durch Abschalten der Präfix-Ausgaben „Time“ und „Source“ wird jede Trace-Ausgabe um 21 Zeichen verkürzt. Standardmäßig ist die Ausgabe der Präfixe aktiviert.

Präfix-Ausgabe „Time“

Durch Aktivierung der Präfix-Ausgabe „Time“ wird jeder Trace-Ausgabe die Systemzeit (zum Zeitpunkt der Erzeugung der Ausgabe!) in folgender Form vorangestellt

■ Format: [Tage]t; _[Stunden]:[Minuten]:[Sekunden]_

■ Beispiel:

12t; 07:23:15

entspricht der Systemzeit von zwölf Tagen, sieben Stunden, dreiundzwanzig Minuten und fünfzehn Sekunden.

Präfix-Ausgabe „Source“

Durch Aktivierung der Präfix-Ausgabe „Source“ wird jeder Trace-Ausgabe der symbolische Name des Protokolls vorangestellt, welches diese Trace Ausgabe verursacht hat. Die Anzeige erfolgt dabei immer 9-stellig (wenn notwendig durch Auffüllen von Leerzeichen).

■ Beispiel: ICMP

d.h. die folgende Trace-Ausgabe wurde vom ICMP-Protokoll verursacht.

Online-Trace „Status“

Die Ausgaben unter „Status“ beschreiben Zustandsänderungen auf einem WAN-Interface (momentan nur der interne S₀-Anschluß). Sie werden in folgendem Format angezeigt

- Format: [Interface] [Zustand]

- Beispiel:

```
Ch01: Anwahl 8700
```

Auf dem ersten B-Kanal des internen S₀-Anschlusses wird die Rufnummer 8700 angewählt.

Online-Trace „Error“

Die Ausgaben unter „Error“ beschreiben Fehler, die auf einem WAN-Interface aufgetreten sind. Sie werden in folgendem Format angezeigt

- Format: [Interface] [Fehler]

- Beispiel:

```
Ch01: Keine Antwort
```

Die angewählte Gegenstelle hat auf den Ruf nicht reagiert.

Online-Trace „ELSA“

Die Ausgaben unter „ELSA“ beschreiben den Verlauf einer Protokoll-Verhandlung im ELSA-Format; durch Anzeige von empfangenen und gesendeten Protokoll-Frames, deren Inhalt und daraus folgenden Aktionen. Sie werden wie folgt angezeigt

- Format: [Interface] [Richtung] [Frametyp] [Parameter] [Aktion]

- Beispiel: (Passiver Verbindungsaufbau ohne CLIP-Auswertung)

```
Ch01: Rx Protokoll-Request ELSA.SUP.TEST Accept
```

```
Ch01: Tx Protokoll-Response ELSA.SUP.1
```

```
Ch01: Rx Protokoll-Response ELSA.SUP.TEST Connect
```

Auf dem ersten B-Kanal wird ein Protokoll-Request mit Geräte-ID „ELSA.SUP.TEST“ empfangen. Da dies ein zulässiger Peer (Gegenstelle oder Partner) ist, wird die ID übernommen und ein Protokoll-Response mit der eigenen ID „ELSA.SUP.1“ zurückgesendet. Durch einen weiteren Protokoll-Response zeigt „ELSA.SUP.TEST“ den Empfang des Protokoll-Responses an, der drei Wege Handshake ist komplett und die logische Verbindung ist aufgebaut.

Online-Trace „PPP“

Das Point-to-Point-Protocol besteht aus einer Sammlung von Subprotokollen, von denen *LANCOM* folgende erkennt und verwaltet

LCP	Das Link-Control-Protocol
PAP	Das Password-Authentication-Protocol
CHAP	Das Challenge-Handshake-Protocol
IPXCP	Das IPX Control-Protocol
IPCP	Das IP-Protocol

Diese Subprotokolle des PPP werden gezielt in einzelnen Phasen während einer Protokollverhandlung angesprochen. Innerhalb der ESTABLISH-Phase wird das Link-Control-Protocol ausgehandelt; zu diesem Zeitpunkt sind nur LCP-Pakete innerhalb des PPP zulässig. Wurde durch das LCP eine Authentifizierung ausgehandelt, geht PPP in die AUTHENTICATE-Phase über; ab diesem Zeitpunkt dürfen LCP-, PAP- und CHAP-Pakete übertragen werden. Nach Abschluß der (optionalen) Authentifizierung wechselt PPP in die NETWORK-Phase; ab sofort dürfen LCP-, Authentifizierungs- und Network-Control-Protocol-Pakete (wie IPXCP und IPCP) beliebig gemischt übertragen werden. Zum Abbau einer PPP-Verbindung wird in die TERMINATE-Phase gewechselt, in der wieder nur LCP-Pakete zulässig sind. Nach Abbau der Verbindung befindet sich PPP in der DEAD-Phase, aus der es nur durch einen erneuten Verbindungsaufbau in die ESTABLISH-Phase übergeht. Jeder Phasenwechsel des PPP wird in der Form

```
Change Phase to [Neue Phase]
```

etwa wie folgt angezeigt

```
Change Phase to AUTHENTICAT
```

Für alle oben aufgeführten Subprotokolle des PPP werden empfangene und gesendete Pakete, wichtige Parameter und Optionen sowie durchgeführte Aktionen angezeigt. Ein empfangener Frame wird immer in folgendem Format angezeigt

- Format: [Interface] Rx [Protokoll] [Pakettyp] [Pakettyp] [Länge des Pakets]
- Beispiel:

```
Ch01: Rx IPXCP ConfReq ID=00 Length=22
```

In obigem Beispiel wurde also auf dem ersten B-Kanal ein Configure-Request für das IPX Control-Protokoll mit der ID 00 und einer Länge von 22 Byte empfangen. Kann ein Paket keinem der fünf Subprotokolle zugeordnet werden erscheint die Meldung

- Format: [Interface] Rx Unknown Protocol [Protokoll-ID]
- Beispiel:

```
Ch01: Rx Unknown Protocol 8029
```

Ein Paket mit der Protokoll-ID 8029 (= Appletalk Control-Protocol) wurde empfangen.

Online-Trace „IPX-Rt.“

Die Ausgaben unter „IPX-Rt.“ beschreiben die Verarbeitung von IPX-Frames durch den IPX-Router. Sie werden in folgendem Format angezeigt

- Format: [Quell-Interface] [IPX-Zieladresse] [IPX-Quelladresse] [Ziel / Aktion]

- Beispiel:

Intern-Rx

DstAddr: 00000002 ffffffff 0453

SrcAddr: 00000002 00a057123456 0453

WAN-Tx Peer: ELSA.SUP.TEST

Der IPX-Router hat von einem internen Prozeß (hier von der Instanz des Routing-Information-Protokolls) einen Frame empfangen, dessen Zieladresse einer logischen Gegenstellen (ELSA.SUP.TEST) zugeordnet ist und daher auf ein WAN-Interface gesendet wird.

LAN-Rx

DstAddr: 00000001 ffffffff 0455

SrcAddr: 00000001 0123456789ab 0455

Filter

Der IPX-Router hat vom lokalen Netzwerk einen NetBIOS-Frame (IPX-Socket 455) empfangen, der als Broadcast ffffffff an alle Stationen im Netz 00000001 weitergeleitet werden soll. Da auf den Socket ein Filter gelegt wurde, wird der Frame vom Router verworfen.

Online-Trace „RIP“

Die Ausgaben unter „RIP“ beschreiben die Verarbeitung von IPX Routing-Information-Protocol-Frames durch den RIP-Prozess des IPX-Routers. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format

- Format: [Quell-Interface] [Receive/Transmitt/Aktion] [Quell-Node-Adresse] [Frame-typ] [Para.] [Netzwerkadresse] [Hops] [Tics] [Aktion] ... [Netzwerkadresse] [Hops] [Tics] [Aktion]

- Beispiel:

LAN-Rx Node: 0000c0123456 Req: 00000002

Vom lokalen Netzwerk wurde ein RIP-Request für das IPX-Netzwerk 00000002 empfangen. Der RIP-Request wurde vom IPX-Node 0000c0123456 gesendet.

- Beispiel:

LAN-Rx Node: 00a057123456 Resp

Route: 00000002 Hops: 0001 Tics: 0002 Up

Vom lokalen Netzwerk (erzeugt vom IPX-Node 00a057123456) wurde ein RIP-Response (Routing Information Protocol-Response) empfangen. Durch diesen Response wird die Route 00000002, mit einer Hop-Distanz (Anzahl der Zwischenstationen) von 1 und einer Tic-Distanz von 2, als weiterhin verfügbar in der RIP-Tabelle eingetragen.

LAN-Update

Der RIP-Prozess sendet alle notwendigen Routing-Informationen auf das lokale Netzwerk

Online-Trace „SAP“

Die Ausgaben unter „SAP“ beschreiben die Verarbeitung von IPX Service-Advertising-Protocol-Frames durch den SAP-Prozess des IPX-Routers. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format

- Format: [Quell-Interface] [Receive/Transmitt/Aktion] [Quell-Node-Adresse] [Frame-typ] [Para.] [Service-Typ] [Server-Name] [Aktion] ... [Service-Typ] [Server-Name] [Aktion]
- Beispiel:

```
LAN-Rx Node: 00a057123456 Response
```

```
0004 FS_Entwicklung Up
```

```
0107 FS_Entwicklung Up
```

```
023f FS_Entwicklung Up
```

```
0511 FS_Entwicklung Up Change
```

```
030c 08000912345678CGNP-Entwicklung Filtered
```

Vom lokalen Netzwerk wurde ein SAP-Response empfangen (ausgesendet vom IPX-Node 00a057123456). Durch diesen Response werden die Server „FS_Entwicklung“ (File-Server), „FS_Entwicklung“ (NetWare-386-Server), „FS_Entwicklung“ (DNS-Server) und „FS_Entwicklung“ (Time-Sync-Server) als weiterhin verfügbar in die SAP-Tabelle aufgenommen. Dabei hat sich der Zustand des Time-Sync-Servers „FS_Entwicklung“ innerhalb der SAP-Tabelle geändert (d.h. der Server war vorher nicht verfügbar). Der letzte angezeigte Server ist ein Printer-Server; da dieser Server-Typ mit einem SAP-Filter belegt ist wird er nicht in die SAP-Tabelle aufgenommen, sondern verworfen.

LAN-Trigger

Durch einen empfangenen SAP-Response ist eine Zustandsänderung innerhalb der SAP-Tabelle aufgetreten, die vom SAP-Prozess unmittelbar ins lokale Netzwerk gemeldet wird; die Änderung kann also nur durch die Auswertung eines SAP-Responses vom WAN eingetreten sein.

LAN-Age

Der SAP-Prozess des Routers „alert“ alle vom lokalen Netzwerk ermittelten Server/Services im Minutentakt. Nach einer einstellbaren Zeit wird ein SAP-Eintrag gelöscht (Setup/IPX-Modul/SAP-Einstellungen/Aging-Minuten)

Online-Trace „IPX-Watchdogs“

Die Ausgaben unter 'IPX-Wd.' beschreiben die Verarbeitung sogenannter „IPX-Watchdog“-Pakete. Dies sind Pakete, welche in regelmäßigen Abständen von einem Novell-Server zu einer Workstation gesendet werden, um die Verbindung zu dieser Workstation zu verifizieren. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format:

■ Format: [Quell-Interface] [Receive/Transmitt] [Quell-Adresse] [Ziel-Adresse] [Aktion]

■ Beispiel:

LAN-Rx

DstAddr: 12345678 00a057654321 0451

SrcAddr: 00000002 00a057123456 0451

Spoof

Das LANCOM hat vom Node 00a057123456 einen IPX-Watchdog empfangen, der zur Überprüfung einer remoten Workstation gedacht war. Da das remote Netzwerk, in welchem sich die Workstation befindet aktiv ist, wird der IPX-Watchdog von LANCOM lokal beantwortet, um einen unnötigen Verbindungsaufbau zu vermeiden. Alternativ können noch folgende Anzeigen für Aktionen erscheinen:

- **Route:** Der IPX-Watchdog wird weitergeleitet (Verbindungsaufbau)
- **Filter:** Der IPX-Watchdog wird verworfen und nicht beantwortet
- **Dst Net DOWN Error:** Das Zielnetz des IPX-Watchdogs ist nicht verfügbar

Online-Trace „SPX-Watchdogs“

Analog zu den Trace-Ausgaben für IPX-Watchdogs wird durch die Ausgaben unter SPX-Wd. die Verarbeitung von „SPX-Watchdog“-Paketen beschrieben. Dies sind Pakete, die von einem Novell-Server zur Überprüfung einer SPX-Verbindung (z.B. R-Console) in regelmäßigen Abständen zur beteiligten Workstation gesendet werden. Die Anzeige der Trace-Ausgaben geschieht in folgender Weise:

■ Format: [Quell-Interface] [Receive/Transmitt] [Quell-Adresse] [Ziel-Adresse] [Aktion]

also völlig analog zu den Anzeigen der IPX-Watchdog-Pakete.

Online-Trace „IPX-NetBIOS“

Die Ausgaben unter NetBIOS beschreiben die Verarbeitung von IPX-NetBIOS- und IPX-Propagated-Paketen. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format

■ Format: [Quell-Interface] [Receive/Transmitt] [Quell-Adresse] [Ziel-Adresse] [Aktion]

■ Beispiel:

LAN-Rx

DstAddr: 12345678 00a057654321 0455

SrcAddr: 00000002 00a057123456 0455

Route

Online-Trace „IP-Rt.“

Die Ausgaben unter „IP-Rt.“ beschreiben die Verarbeitung von IP-Frames durch den IP-Router. Sie werden in folgendem Format angezeigt

- Format: [Quell-Interface] [IP-Zieladresse] [IP-Quelladresse] [Protokoll] [Ziel-Port] [Quell-Port] [Type of Service] [Aktion][Ziel]
- Beispiel:

LAN-Rx

DstIP: 195.162.38.161, SrcIP: 194.162.38.162

Prot.: TCP, DstPort: 23, SrcPort: 1197, TOS: ----

Route: WAN-Tx Peer: R1

Der IP-Router hat vom Rechner mit der IP-Adresse 194.162.38.162 ein TCP-Paket erhalten, daß an der Rechner 195.162.38.161 gesendet werden soll.

Der Quellport ist 1197, der Ziel-Port 23 (Telnet), es ist kein Bit im TOS gesetzt. Das Feld TOS kann die folgenden Werte (bzw. Eine Kombination hiervon) annehmen:

D---	Low Delay
-T--	High Troughput
--R-	High Reliability
---C	Low Costs

Das Paket wird geroutet und der Zielrechner ist unter der logischen Gegenstelle **R1** erreichbar. Daher wird das Paket auf ein WAN-Interface gesendet.

LAN-Rx

DstIP: 195.162.38.161, SrcIP: 194.162.38.162

Prot.: ICMP, DstPort: ---, SrcPort: ---, TOS: --R-

Route: WAN-Tx Peer: R1

Der IP-Router hat vom Rechner mit der IP-Adresse 194.162.38.162 ein ICMP-Paket erhalten, daß an der Rechner 195.162.38.161 gesendet werden soll.

Da ICMP keine Ports kennt, wird als Ziel- bzw. Quellport --- ausgegeben. Im TOS ist das Feld **High Reliability** gesetzt.

Online-Trace „IP-RIP“

Die Ausgaben unter „IP-RIP“ beschreiben die Verarbeitung von IP Routing-Information-Protocol-Frames durch den RIP-Prozess des IP-Routers. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format

- Format: [Quell-Interface] [Receive/Transmitt/Aktion] [Quell-Adresse] [RIP-Version] [Routing-Domain] [Netzwerkadresse] [Netzmaske] [Beste Route] [Distanz] [Aktion] ... [Netzwerkadresse] [Netzmaske] [Beste Route] [Distanz] [Aktion]

- Beispiel:

```
LAN-Rx Src: 194.162.38.252
```

```
Vers.: RIP-1      Routg.Dom.: 0000
```

```
190.254.0.0      255.255.0.0      194.162.38.1623 Store
```

```
195.126.38.0     255.255.255.0     194.162.38.1623 update
```

```
255.255.255.255 0.0.0.0          194.162.38.1622 Discard
```

```
194.162.38.0     255.255.255.0     194.162.38.1622 Discard
```

Vom lokalen Netz wurde ein RIP-1 Frame empfangen. Dieser Frame enthält die Routen zu den Netzen 190.254.0.0, 195.126.38.0, 255.255.255.255 (DEFAULT-Route) und 194.162.38.0. Mit diesen Routen wurde wie folgt verfahren:

Die Route 190.254.0.0 wird gespeichert, da sie entweder besser als die bisherige oder noch unbekannt ist.

Die Route 195.126.38.0 wird überarbeitet, d.h. die Route ist unverändert, nur die Distanz kann sich geändert haben. In jedem Fall wird der Aging-Timer zurückgesetzt.

Die DEFAULT-Route wurde verworfen, da eine bessere Route bekannt ist.

Die Route zum Netz 194.162.38.0 wird verworfen, da es sich um eine Route zum lokalen Netz handelt (split horizon).

Die Trace-Ausgabe empfangener RIP-Frames erfolgt immer nachdem sie vom RIP-Prozess ausgewertet und dadurch Netzmasken (RIP-1) sowie beste Route bestimmt wurden. Bei gesendeten RIP-Frames werden die Pakete so angezeigt, wie sie gesendet wurden. Dies bedeutet, daß z.B. bei RIP-1 Frames die Netzmaske immer als 0.0.0.0 ausgegeben wird.

Online-Trace „ARP“

Die Ausgaben unter „ARP“ beschreiben die Verarbeitung Adress-Resolution-Protocol-Frames durch das TCP-IP-Modul. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format

- Format: [Quell-Interface] [Receive/Transmitt/Aktion] [Quell-Adresse] [Ziel-Adresse] [Ziel / Aktion]

- Beispiel:

```
LAN-Rx Request
```

SrcIP: 194.162.38.162, DstIP: 194.162.38.171

Cache-Update: 194.162.38.162 : 0000c0717860

Response LAN-Tx

Es wurde ein ARP-Request für die IP-Adresse 194.162.38.171 vom Rechner 194.162.38.162 empfangen. Die MAC-Adresse des Quell-Rechners wird in der ARP-Tabelle gespeichert. Weiterhin ist das *LANCOM* der nachgefragte Rechner. Daher wird ein ARP-Response auf das LAN-Interface zurückgeschickt.

Online-Trace „ICMP“

Die Ausgaben unter „ICMP“ beschreiben die Verarbeitung Internet-Control-Message-Protocol-Frames durch das TCP-IP-Modul. Die Anzeige der Trace-Ausgaben geschieht in folgendem Format

- Format [Quell-/Ziel-Interface] [Receive/Transmitt] [Quell-/Ziel.Adresse] [Message] [Aktion]

- Beispiel:

LAN-Rx

SrcIP: 194.162.38.162: Echo Request

LAN-Tx

DstIP: 194.162.38.162: Echo Reply

Auf dem LAN-Interface wurde ein ICMP Echo-Request (**ping**) vom Rechner 194.162.38.162 empfangen. Das *LANCOM* beantwortet dies mit einem ICMP Echo-Reply.

Online-Trace „IP-MASQ“

Die Ausgaben unter „IP-MASQ“ beschreiben die Vorgänge im Masquerading-Modul. Es wird das Öffnen sowie das Schließen einer maskierten Verbindung ausgegeben. Die Anzeige erfolgt in folgendem Format:

- Format: [Open/Close]: [Protokoll] [IP-Quelladresse] [Quell-Port] [Mapped-Port] [Grund]

Als Protokoll kommt TCP, UDP oder ICMP in Frage. Wenn das Protokoll ICMP ist, so gibt der Quell-Port den Identifier des Request-Pakets an. Das Feld Mapped-Port gibt an wie der Quell-Port ersetzt wurde. Im Feld Grund wird die Ursache eines Close angegeben. Mögliche Gründe sind:

Timeout	Der eingestellte Protokoll-Timeout ist abgelaufen
TCP finish	Eine TCP-Verbindung wurde normal beendet
TCP reset	Eine TCP-Verbindung wurde aufgrund eines Fehlers von einer der beteiligten Maschinen abgebrochen
Port assigned	Einer „passiven“ TCP-Verbindung wurde ein Quellport zugewiesen. Beispiel: FTP im passive Mode

■ Beispiele:

```
Open: TCP SrcIP: 10.0.0.44, 1121 -> 64107
```

```
Open: TCP SrcIP: 10.0.0.44, 1122 -> 64104
```

```
Open: TCP SrcIP: 10.0.0.44, 1123 -> 64105
```

```
Close: TCP SrcIP: 10.0.0.44, 1121 -> 64107 TCP reset
```

Online-Trace „SCRPT“

Die Ausgaben unter „SCRPT“ beschreiben den Fortschritt einer Script-Verhandlung. Die Ausgaben erfolgt in folgendem Format:

■ Format: [Quell-Interface] [Receive/Transmit/Error] [Text] [Aktion]

■ Beispiel:

```
CH01: Rx: Password -> Tx: * \r
```

In obigem Beispiel wird von der Gegenstelle das Paßwort erfragt. Dieses wird an die Gegenstelle zurückgeschickt (verborgen unter einem '*').

Policy Based Routing

Allgemeines

Der Begriff „Policy-Based-Routing“ beschreibt die Möglichkeit, zusätzlich zum Standard-Routing-Verfahren für IP-Pakete, weitere Routing-Methoden (eben diese „Policies“) zu verwenden.

Um die Inband-Konfiguration über Weitverkehrsnetzwerke bei starker Datenübertragung zu erleichtern und die Zusammenarbeit von *LANCOM* mit 'ping' und 'traceroute'-Mechanismen zu verbessern, wurden zwei Methoden für das IP-Routing eingeführt. Beide Methoden setzen auf der Auswertung des 'Type-of-Service' Feldes innerhalb des IP-Headers auf.

Das 'Type-of-Service' Feld (kurz TOS) beschreibt, wie IP-Pakete vorzugsweise behandelt werden sollen (aber nicht müssen). D.h. es spiegelt die gewünschte Verarbeitungsweise wieder, die der Erzeuger diesem IP-Paket zugedacht hat. TOS besitzt dabei folgenden Aufbau

Bit 7, 6	Bit 5	Bit 4	Bit 3	Bit 2, 1, 0
Unbenutzt	Reliable-Transmission	High-Throughput	Low-Delay	Precedence

Durch die Routing-Methoden werden das **R**- und das **D**-Bit ausgewertet und das Verhalten an deren Zustände angepaßt.

Ein gesetztes **R**-Bit fordert eine gesicherte Übertragung des zugehörigen IP-Pakets an. Derart gekennzeichnete Pakete werden entsprechend ihrer Empfangsreihenfolge über eine „gesicherte“ Queue immer übertragen. Im Extremfall kann dies dazu führen, daß ein bereits in einer Sende-Queue befindliches „normales“ Paket wieder aus dieser entnommen und in den Heap zurückgestellt wird, um Platz für das zu sendende Paket zu schaffen. Dies geschieht, wenn die maximale Anzahl an Pufferspeichern für die zugehörige Verbindung bereits verbraucht ist. Die Übertragungsreihenfolge zwischen Paketen mit gesetztem **R**-Bit und „normalen“ Bits wird durch diesen Mechanismus jedoch nicht verändert.

Die gesicherte Übertragung kann für alle ICMP-Pakete unabhängig vom Eintrag im 'Type-of-Service'-Feld aktiviert werden. Da ein derart gekennzeichnetes ICMP-Paket ohne Änderung der Übertragungsreihenfolge gesendet wird, können weiterhin durch 'ping' oder 'traceroute' die Durchlaufverzögerungen eines *LANCOM* ermittelt werden.

Durch ein gesetztes **D**-Bit fordert der Erzeuger eines IP-Pakets dessen schnellstmögliche Übermittlung an. Derart gekennzeichnete IP-Pakete werden entsprechend ihrer Empfangsreihenfolge über eine „Urgent“-Queue vor den Paketen der Sende-Queue übertragen. Dies führt zu Veränderungen in der Übertragungsreihenfolge, da ein so gekennzeichnetes IP-Paket als letztes empfangen aber als erstes gesendet wird. Zum anderen besteht ebenfalls die Möglichkeit, daß ein bereits in der Sende-Queue befindliches

Paket wieder aus dieser entnommen wird, um Platz für das zu sendende IP-Paket zu schaffen (s.o.).

Pakete, die sich bereits in der gesicherten oder der Urgent-Queue befinden, werden nicht verworfen. Befindet sich kein Paket mehr in der normalen Sende-, der gesicherten oder der Urgent-Queue, können keine Pakete mehr gesendet werden. Empfangene IP-Pakete werden daher auch mit gesetztem **D**- oder **R**-Bit verworfen.

Beispiele

Durch die Einstellung

`Setup/IP-Router-Modul/Routing-Methode/IP TOS`

wird das 'Type-of-Service-Feld' des IP-Headers eines empfangenen Pakets wie oben beschrieben ausgewertet, d.h. daß IP-Pakete mit gesetztem **D**-Bit in die Urgent-Queue und Pakete mit gesetztem **R**-Bit in die gesicherte Queue gestellt werden. Alle anderen Pakete werden in der normalen Sende-Queue abgelegt.

Dies bedeutet gleichzeitig, daß evtl. „normale„ IP-Pakete von „gesicherten„ oder „Urgent„-Paketen verdrängt werden können (bei maximaler Füllung der Sende-Queue dieser Verbindung) oder es zu Veränderungen in Paketreihenfolgen kommen kann!

Durch die Einstellung 'normal' werden alle IP-Pakete gleich behandelt, entsprechend den Routing-Vorschriften des Internet-Protocols.

Durch die Einstellung

`Setup/IP-Router-Modul/Routing-Methode/ICMP gesichert`

werden alle empfangenen ICMP-Pakete so übertragen, als hätten sie das **R**-Bit im Type-of-Service-Feld des IP-Headers gesetzt. (s.o.).

Das bedeutet, daß die gesicherte Übertragung von ICMP-Paketen evtl. zu Störungen in anderen Datenflüssen führen kann! Die Latenzzeit des Routers wird jedoch nicht beeinflusst, da das ICMP-Paket trotzdem als letztes in die Sende-Queue aufgenommen wird.

Durch die Einstellung 'normal' werden ICMP-Pakete wie alle anderen IP-Pakete behandelt, entsprechend den Routing-Vorschriften des Internet-Protocols.

Meldungen, Nummern, Ports

In diesem Kapitel finden Sie die Fehlermeldungen, die beim Betrieb eines *LANCOMs* ausgegeben werden sowie umfangreiche Listen mit SAP-Nummern von Novell und TCP/IP-Ports.

Auf eine Auflistung der IPX/SPX-Sockets wurde verzichtet, da diese Liste den Rahmen dieser Dokumentation sprengen würde.

Aktuelle Listen finden Sie z.B. im Internet bei Novell oder Microsoft sowie in den entsprechenden Dokumentationen zu Ihrem Netzwerkbetriebssystem.

Fehlermeldungen	2
Novell SAP-Nummern.....	10
TCP/IP-Ports	14

Fehlermeldungen

LANCOM-interne Fehlermeldungen

Fehlermeldung	Ursache	Behebung
Keine Rufnummer	Für die Gegenstelle wurde keine Rufnummer eingetragen.	Tragen Sie, falls gewünscht, unter SETUP/WAN/NAMENSLISTE der zugehörigen Gegenstelle eine Rufnummer ein.
Keine Gegenst.	Im IP- oder IPX-Router wurde ein Gegenstellename angeführt, der nicht in der Namensliste vorhanden ist.	Überprüfen Sie die Routingtabellen und vergleichen Sie die dort vergebenen Namen mit denen der Namensliste.
Gegenst. doppelt	Der Router hat versucht auf mehreren Kanälen die selbe Gegenstelle an zu rufen.	Führen Sie die Anwahl erneut durch
Gegenst gesperrt	Es wurde durch ein weiteres zu routendes Paket versucht eine Gegenstelle zu rufen, auf deren Rückruf bereits gewartet wird.	In der Regel kein Problem. Bleibt die Meldung längere Zeit bestehen, überprüfen Sie die Gegenstelle bzgl. des ausbleibenden Rückrufes.
DÜ-Modul falsch	Es wurde ein nicht unterstütztes Gerät an die serielle Schnittstelle angeschlossen.	Vergewissern Sie sich, daß das angeschlossenen Gerät in der Kompatibilitätsliste aufgeführt wird und korrekt arbeitet.
kein DÜ-Gerät	Es wurde kein Modem/ Terminaladapter am seriellen Interface gefunden.	Überprüfen Sie die Kabel und die Funktion des angeschlossenen Gerätes.

ISDN-Fehlermeldungen

Fehlermeldung	Ursache	Behebung
Wahlabbruch	Ein unvorhergesehener Fehler ist aufgetreten.	Bitte setzen Sie sich mit dem Support in Verbindung.
Abbruch S37 ung.	Die eingestellte Bitrate kann für das externe serielle Gerät nicht verwendet werden.	Überprüfen Sie das angeschlossene Gerät.
ATA/O ohne Ruf	Entweder hat die Gegenstelle schon aufgelegt oder ein anderes Gerät am selben Bus hat den bereits Ruf entgegen genommen.	Überprüfen Sie, ob ein anderes Gerät am gleichen Bus auf die selbe MSN hört.
Abbruch ATZ	An das angeschlossene Modem wurde während des Verbindungsaufbaus ein Zeichen gesendet.	
Gebührensperre	Die voreingestellten Gebühren in SETUP/GEBÜHREN-MODUL sind abgelaufen	Versuchen Sie durch Filterung unnötige Aufbauten des LANCOM zu verhindern, ändern Sie die Anzahl der Gebühren oder verringern Sie den Zeitraum

Fehlermeldung	Ursache	Behebung
Fehler Aufb. D 1	Es konnte keine oder nur eine gestörte Verbindung zum ISDN-Netz aufgebaut werden.	Überprüfen Sie die Kabel und Steckverbindungen vom Endgerät bis zu Ihrem ISDN-S0-Anschluß. Entfernen Sie zudem andere Geräte von Bus, um diese als Fehlerquelle auszuschließen.
Fehler Aufb. D 2	siehe Fehler Aufb. D1	siehe Fehler Aufb. D1
Fehler Aufb. B 1	Es ist das falsche B-Kanal-Protokoll eingestellt.	Korrigieren Sie die Einstellung unter SETUP/WAN-MODUL/INTERFACE
Fehler Aufb. B 2	siehe Fehler Aufb. B1	siehe Fehler Aufb. B1
Abbruch D-Kan. 2	siehe Fehler Aufb. D1	siehe Fehler Aufb. D1
Abbruch D-Kan. 3	Es ist das falsche B-Kanal-Protokoll eingestellt.	Korrigieren Sie die Einstellung unter SETUP/WAN-MODUL/INTERFACE
Abbruch B-Kan. 2	Die Gegenstelle hat die Verbindung unterbrochen	Lassen Sie einen erneuten Anwahlversuch durchführen.

V42bis Fehler

Fehlermeldung	Ursache	Behebung
Dienst n. verf.	Der Dienst 'Datenübertragung digital' ist nicht freigegeben.	Überprüfen Sie die Zielrufnummer und die Freischaltung des Dienstes 'Datenübertragung digital'. Dies gilt auch für TK-Anlagen.
Eig. Ltg.besetzt	Andere Geräte belegen bereits die verfügbaren B-Kanäle.	Trennen sie ggf. bestehende Verbindungen.
FAC n. unterst.	Die gewählte Betriebsart 'semi-permanente Verbindung' wird vom aktuellen Anschluß nicht unterstützt.	Prüfen Sie ob dieser Dienst für ihren S0-Bus freigeschaltet worden ist.
FAC n. einger.	Die gewählte Betriebsart 'semi-permanente Verbindung' wird vom aktuellen Anschluß nicht unterstützt.	Prüfen Sie ob dieser Dienst für ihren S0-Bus freigeschaltet worden ist.
Eig.Ltg.gesperrt	Die mit dem <i>LANCOM</i> verbundenen Busse sind bereits anderweitig belegt oder für eingehende Gespräche gesperrt.	Führen Sie die Anwahl zu einem späteren Zeitpunkt noch einmal aus und prüfen Sie ob abgehende Gespräche auf dem am <i>LANCOM</i> angeschlossenen Bus erlaubt sind.
Ziel-Ltg.besetzt	Der Anschluß der Gegenstelle ist belegt.	Führen Sie die Anwahl zu einem späteren Zeitpunkt erneut aus.
FAC n. erlaubt	Die gewählte Betriebsart 'semi-permanente Verbindung' wird vom aktuellen Anschluß nicht unterstützt.	Prüfen Sie ob dieser Dienst für ihren S0-Bus freigeschaltet worden ist.
Rufnummer falsch	Die Telefonnummer ist unvollständig oder ungültig.	Überprüfen Sie die in Setup/Wan/Nummernliste zugeordnete Telefonnummer.
Rufnr. Geändert	Die Rufnummer der Gegenstelle hat sich geändert.	Überprüfen Sie die in Setup/Wan/Nummernliste zugeordnete Telefonnummer.
Ziel n. bereit	Die Gegenstelle ist nicht betriebsbereit.	Überprüfen Sie die Gegenstelle.
Keine Antwort	Der Ruf wurde nicht entgegengenommen.	Überprüfen Sie die Gegenstelle.
Ziel besetzt	Die Gegenstelle ist besetzt.	Da auch andere am gleichen Bus der Gegenstelle installierte Geräte zu deren Bus belegen können, sollte die Gegenstelle ggf. einen eigenen Bus erhalten.
Ziel gesperrt	Die Gegenstelle wurde gegenüber einkommenden Rufen gesperrt.	Überprüfen Sie die Gegenstelle und ggf. die Einstellungen einer vorh. TK-Anlage.
Verb. Abgelehnt	Die Gegenstelle hat den herein-kommenden Ruf abgelehnt.	Dies ist korrekt, wenn die Gegenstelle auf Rückruf programmiert wurde, andernfalls überprüfen Sie die Gegenstelle.
Engpass im Netz	Eine vorgeschaltete TK-Anlage hat keine Leitung mehr frei um die Gegenstelle zu erreichen.	Führen Sie den Anwahlversuch zu einem späteren Zeitpunkt erneut aus.
Ausl.Gegenstelle		

Fehlermeldung	Ursache	Behebung
SEL: EAZ-Reject		
Lokaler Fehler	Es trat eine Störung im Protokoll auf	Anwahl wiederholen.
Ferner Fehler	Es trat eine Störung im Protokoll auf	Anwahl wiederholen.
MLP-Blockfehler	Die Gegenstelle ist nicht ELSA-MLP-konform.	Eine Verbindung ist nur ohne Kanalbündelung möglich.
MLP-Verb.-Abbau	Die Kanalbündelung wurde durch die Nebenverbindung beendet.	Mögliches Fehlverhalten der Gegenstelle.

PPP-Fehlermeldungen

Fehlermeldung	Ursache	Behebung
LCP abgelehnt	Die Gegenstelle hat das Link-Control-Protocol des PPP zurückgewiesen.	Überprüfen Sie die PPP-Einstellungen der Gegenstelle.
Auth. Falsch	Die Gegenstelle unterstützt das eingestellte Überprüfungsprotokoll nicht.	Gleichen Sie die Einstellungen zwischen dem <i>LANCOM</i> und der Gegenstelle ab, oder verzichten Sie auf die Überprüfung.
Auth. Abgelehnt,	Die Gegenstelle hat jegliche Überprüfung abgelehnt.	Schalten Sie die Überprüfung im <i>LANCOM</i> ab. Setup/WAN/PPP/Sicherung keine
PAP abgelehnt	Obwohl in der LCP-Verhandlung akzeptiert, hat die Gegenstelle das Password-Authentication-Protocol abgelehnt.	Überprüfen Sie den PPP-Stack der Gegenstelle und weichen sie ggf. auf das Challenge-Handshake-Authentication-Protocol (CHAP) aus.
PAP Rx-Timeout	Die Gegenstelle hat nicht innerhalb der eingestellten Zeit mit der Aussendung von PAP-Requests begonnen.	Durch Erhöhung der Wartezeit im <i>LANCOM</i> kann dieses Problem in der Regel behoben werden.
PAP Tx-Timeout	Die Gegenstelle hat nicht innerhalb der eingestellten Zeit auf ein PAP-Request vom <i>LANCOM</i> reagiert.	Erhöhen Sie die Wiederholungszahl im PPP-Setup des <i>LANCOM</i> .
PAP-Req falsch	Das von der Gegenstelle verwendete Passwort wurde als falsch vom <i>LANCOM</i> abgelehnt.	Überprüfen Sie die Passwörter. Überschreiben Sie ggf. das Passwort in der PPP-Liste des <i>LANCOM</i> .
PAP-NAK empf.	Der PAP-Request vom <i>LANCOM</i> wurde von der Gegenstelle abgelehnt, da die für beide Seiten verwendete Kombination aus Peer-ID (Name) und Passwort nicht übereinstimmte.	Überprüfen Sie die Kombination aus Name und Schlüsseleintrag im <i>LANCOM</i> .
CHAP abgelehnt,	Obwohl in der LCP-Verhandlung akzeptiert, hat die Gegenstelle das CHAP abgelehnt.	Überprüfen Sie den PPP-Stack der Gegenstelle und weichen sie ggf. auf PPP aus.
CHAP Rx-Timeout	Die Gegenstelle hat nicht innerhalb der eingestellten Zeit auf ein CHAP-Challenge mit einem CHAP-Response geantwortet.	Durch Erhöhung der Wartezeit im <i>LANCOM</i> kann dieses Problem in der Regel behoben werden.
CHAP Tx-Timeout	Die Gegenstelle hat nicht innerhalb der eingestellten Zeit auf ein CHAP-Response vom <i>LANCOM</i> reagiert.	Erhöhen Sie die Wiederholungszahl im PPP-Setup des <i>LANCOM</i> .
CHAP-Resp falsch	Der von der Gegenstelle übermittelte Response stimmt nicht mit dem erwarteten Wert überein.	Überprüfen Sie die Kombination aus Name und Passwort der Gegenstelle in der <i>LANCOM</i> Konfiguration.
CHAP-Fail empf.	Die Gegenstelle hat den CHAP-Response vom <i>LANCOM</i> zurückgewiesen.	Überprüfen Sie die Kombination aus Name und Passwort für die Gegenstelle im <i>LANCOM</i> .

Fehlermeldung	Ursache	Behebung
CHAP PeerID unb.	Von der Gegenstelle wurde im CHAP-Requeset eine Peer-ID angegeben, die vom <i>LANCOM</i> in der PPP-Tabelle nicht aufgelöst werden kann.	Fügen Sie ggf. den Namen und das nötige Passwort der PPP-Tabelle hinzu.
IPXCP abgelehnt	Die Gegenstelle hat das IPX-Control-Protocol zur Aushandlung der IPX-Parameter zurückgewiesen.	Überprüfen Sie, ob für diese Verbindung IPX-Routing auf der Gegenstelle zugelassen wurde oder ob es überhaupt möglich ist.
IPXCP-Net falsch	Die von beiden Seiten für das ISDN verwendeten IPX-Netzwerkadressen stimmen nicht überein.	Entweder ist der IPX-Router im <i>LANCOM</i> oder in der Gegenstelle falsch konfiguriert.
IPXCP-Net abgel.	Die Gegenstelle hat die Aushandlung ein IPX-Adresse für das ISDN abgelehnt.	Entweder muß die Gegenstelle rekonfiguriert werden oder sie unterstützt diese Funktion nicht.
IPXCP-Route unb.	Die Gegenstelle verwendet ein anderes Routing-Protokoll für IPX als RIP/SAP.	Überprüfen Sie die Einstellungen der Gegenstelle.
IPCP abgelehnt	Die Gegenstelle hat das IP-Control-Protocol zur Aushandlung der IP-Parameter zurückgewiesen.	Überprüfen Sie, ob für diese Verbindung IP-Routing auf der Gegenstelle zugelassen wurde oder ob es überhaupt möglich ist.
Kein NCP bereit	Für diese Verbindung konnte weder IPXCP noch IPCP aktiviert werden.	Vergleichen Sie den vom <i>LANCOM</i> ermittelten Namen der Gegenstelle unter Staus/Info-Verbindung/Kennung-Ggst. Mit dem Gegenstellennamen des IPX-Routers oder/und den Einträgen in der IP-Router-Tabelle.

Modem-Fehlermeldungen

Fehlermeldung	Ursache	Behebung
Trägerverlust	Das angeschlossene Modem hat den Kontakt zur Gegenstelle verloren.	Überprüfen Sie die Telefonleitung, stellen Sie ggf. Verbindung zu anderen Gegenstellen her um die Funktion des Modems und Ihrer Telefoninstallation sicher zu stellen.
Fehlerkor. fehlt	Es konnte keine Fehlerkorrektur mit der Gegenstelle ausgehandelt werden.	Überprüfen Sie die Gegenstelle auf Kompatibilität nach LAPB
Prot.-Ant. fehlt	Es konnte kein Protokoll mit der gegenstelle ausgehandelt werden.	Prüfen Sie die Gegenstelle auf Kompatibilität.
GGSt. ist sync	Die Gegenstelle versucht eine synchrone Verbindung auf zu bauen.	Prüfen Sie die Konfiguration der Gegenstelle.
Kein Framing,	Es konnte kein Protokoll mit der Gegenstelle ausgehandelt werden.	Prüfen Sie die Konfiguration der Gegenstelle.
Kein Protokoll	Es konnte keine Einigung über ein Protokoll nach V.42, MNP oder LAPB ausgehandelt werden.	Prüfen Sie die Konfiguration der Gegenstelle.
V42bis Fehler	Bei der DatenkoMPRimierung nach V24bis ist ein Fehler aufgetreten.	Prüfen Sie die Konfiguration der Gegenstelle.
Inaktiv.-Timer	Die Leitung wurde nach zu langer Inaktivität getrennt.	Prüfen Sie die Konfiguration der Gegenstelle.
Kein Schl.-Strom	Ein anderes Gerät benutzt z.Zt. die Telefonleitung oder die Anschlußdose ist falsch beschaltet.	Vergewissern Sie sich, daß gerade keinen anderen Endgeräte, wie z.B. Fax oder Telefon ihre Leitung benutzen.
Ziel besetzt	Die Gegenstelle führt bereits ein Gespräch und ist deshalb belegt.	Führen Sie die Anwahl zu einem späteren Zeitpunkt erneut aus.
Kein Amtston	Es konnte kein Freizeichen festgestellt werden. TK-Anlage (haben eigenes Freizeichen) oder Leitungsdefekt.	Korrigieren sie ggf. die Einstellungen im Setup/WAN-Modul für die Verwendung des Modems an einer TK-Anlage oder prüfen Sie den Telefonanschluß.
Kein Antwortton	Auf der Gegenseite hat kein Modem den Anruf entgegengenommen.	Prüfen Sie die Rufnummer der Gegenstelle.
Timeout	Es konnte keine Einigung über ein gemeinsames Protokoll innerhalb der eingestellten Zeit getroffen werden.	Prüfen Sie die Konfiguration der Gegenstelle.
Kein Rückfall L2	Die Modems konnten sich nicht auf eine gemeinsame Übertragungs-Geschwindigkeit einigen.	Prüfen Sie die Konfiguration der Gegenstelle.
Kein Zielmodem	Unter der Gegenstellenummer meldet sich kein Modem.	Prüfen Sie die Rufnummer und ggf. die Konfiguration der Gegenstelle.

Status-Anzeigen

Meldung	Ursache	Behebung
Init	Das <i>LANCOM</i> initialisiert sich und führt einen Selbsttest durch. Diese Meldung ist meist nicht sichtbar.	Bleibt diese Meldung über einen längeren Zeitraum sichtbar, setzen Sie sich bitte mit dem Support in Verbindung
Setup WAN	Das <i>LANCOM</i> initialisiert und testen die ISDN und seriellen Module. Diese Meldung ist meist nicht sichtbar.	Bleibt diese Meldung über einen längeren Zeitraum sichtbar, ist beim Selbsttest ein Defekt des entsprechenden Interfaces festgestellt worden. Versuchen Sie ein Firmware-Update einzuspielen oder/und setzen Sie sich mit dem Support in Verbindung.
Bereit	Das <i>LANCOM</i> ist inaktiv.	
Rufnummer	Das <i>LANCOM</i> wählt eine Gegenstelle an	Das Display zeigt bei längeren Nummern nur die letzten Stellen an.
Anliegender Ruf	Es liegt ein Ruf auf dem dem <i>LANCOM</i> zugeordneten Bus an.	
Protokoll	Das <i>LANCOM</i> versucht mit der Gegenstelle ein Protokoll auszuhandeln.	
Gegenstellenname	Der Router hat eine Verbindung zur angezeigten Gegenstelle. Das Feld kann auch leer sein, wenn die Gegenstelle keinen Namen zugewiesen bekommen hat.	
Abbau	Das <i>LANCOM</i> versucht eine Wählverbindung herzustellen.	
Rückruf	Das <i>LANCOM</i> versucht eine Gegenstelle zurück zu rufen.	
reserviert	Die Y-Verbindungsfähigkeit wurde deaktiviert. Der 2. B-Kanal kann nur noch für die Bündelung verwendet werden.	
Bündelung	Der 2. B-Kanal wird für die Bündelung verwendet.	
Aufbau D64S	Das <i>LANCOM</i> versucht eine Standleitungsverbindung nach D64S (Grp0) aufzubauen.	
Aufbau S01/S02	Das <i>LANCOM</i> versucht eine Standleitungsverbindung nach TS01/TS02 (Grp2) aufzubauen.	
n. verfügb.	Bei Standleitungsbetrieb mit nur einem B-Kanal ist der 2. Kanal nicht mehr nutzbar.	
kein Gerät	An der Seriellen Schnittstelle ist kein Gerät angeschlossen, oder es funktioniert nicht.	Überprüfen Sie ein eventuell angeschlossenes Gerät auf seine ordnungsgemäße Funktion.

Novell SAP-Nummern

Dezimal	Hexa-Dezimal	SAP-Beschreibung
1	0001	User
2	0002	User Group
3	0003	Print Queue or Print Group
4	0004	File Server (SLIST source)
5	0005	Job Server
6	0006	Gateway
7	0007	Print Server or Silent Print Server
8	0008	Archive Queue
9	0009	Archive Server
10	000a	Job Queue
11	000b	Administration
15	000F	Novell TI-RPC
23	0017	Diagnostics
32	0020	NetBIOS
33	0021	NAS SNA Gateway
35	0023	NACS Async Gateway or Asynchronous Gateway
36	0024	Remote Bridge or Routing Service
38	0026	Bridge Server or Asynchronous Bridge Server
39	0027	TCP/IP Gateway Server
40	0028	Point to Point (Eicon) X.25 Bridge Server
41	0029	Eicon 3270 Gateway
42	002a	CHI Corp
44	002c	PC Chalkboard
45	002d	Time Synchronization Server or Asynchronous Timer
46	002e	ARCserve 5.0 / Palindrome Backup Director 4.x (PDB4)
69	0045	DI3270 Gateway
71	0047	Advertising Print Server
74	004a	NetBlazer Modems
75	004b	Btrieve VAP/NLM 5.0

Dezimal	Hexa-Dezimal	SAP-Beschreibung
76	004c	Netware SQL VAP/NLM Server
77	004d	Xtree Network Version Netware XTree
80	0050	Btrieve VAP 4.11
82	0052	QuickLink (Cubix)
83	0053	Print Queue User
88	0058	Multipoint X.25 Eicon Router
96	0060	STLB/NLM
100	0064	ARCserve
102	0066	ARCserve 3.0
114	0072	WAN Copy Utility
122	007a	TES-Netware for VMS
146	0092	WATCOM Debugger or Emerald Tape Backup Server
149	0095	DDA OBGYN
152	0098	Netware Access Server (Asynchronous gateway)
154	009a	Netware for VMS II or Named Pipe Server
155	009b	Netware Access Server
158	009e	Portable Netware Server or SunLink NVT161
161	00a1	Powerchute APC UPS NLM
170	00aa	LAWserve
172	00ac	Compaq IDA Status Monitor
256	0100	PIPE STAIL
258	0102	LAN Protect Bindery
259	0103	Oracle DataBase Server
263	0107	Netware 386 or RSPX Remote Console
271	010f	Novell SNA Gateway
273	0111	Test Server
274	0112	Print Server (HP)
276	0114	CSA MUX (f/Communications Executive)
277	0115	CSA LCA (f/Communications Executive)
278	0116	CSA CM (f/Communications Executive)

Dezimal	Hexa-Dezimal	SAP-Beschreibung
279	0117	CSA SMA (f/Communications Executive)
280	0118	CSA DBA (f/Communications Executive)
281	0119	CSA NMA (f/Communications Executive)
282	011a	CSA SSA (f/Communications Executive)
283	011b	CSA STATUS (f/Communications Executive)
286	011e	CSA APPC (f/Communications Executive)
294	0126	SNA TEST SSA Profile
298	012a	CSA TRACE(f/Communications Executive)
299	012b	Netware for SAA
301	012e	IKARUS virus scan utility
304	0130	Communications Executive
307	0133	NNS Domain Server or Netware Naming Services Domain
309	0135	Netware Naming Services Profile
311	0137	Netware 386 Print Queue or NNS Print Queue
321	0141	LAN Spool Server (Vap, Intel)
338	0152	IRMAILAN Gateway
340	0154	Named Pipe Server
358	0166	NetWare Management
360	0168	Intel PICKIT Comm Server or Intel CAS Talk Server
371	0173	Compaq
372	0174	Compaq SNMP Agent
373	0175	Compaq
384	0180	XTree Server or XTree Tools
394	018A	NASl services broadcast server (Novell)
432	01b0	GARP Gateway (net research)
433	01b1	Binview (Lan Support Group)
447	01bf	Intel LanDesk Manager
458	01ca	AXTEC

Dezimal	Hexa-Dezimal	SAP-Beschreibung
459	01cb	Shiva NetModem/E
460	01cc	Shiva LanRover/E
461	01cd	Shiva LanRover/T
462	01ce	Shiva Universal
472	01d8	Castelle FAXPress Server
474	01da	Castelle LANPress Print Server
476	01dc	Castille FAX/Xerox 7033 Fax Server/Excel Lan Fax
496	01f0	LEGATO
501	01f5	LEGATO
563	0233	NMS Agent or Netware Management Agent
567	0237	NMS IPX Discovery or LANtern Read/Write Channel
568	0238	NMS IP Discovery or LANtern Trap/Alarm Channel
570	023a	LABtern
572	023c	MAVERICK
575	023f	Used by eleven various Novell Servers / Novell SMDR
590	024e	Netware Connect
591	024f	NASl server broadcast (Cisco)
618	026a	Network Management (NMS) Service Console
619	026b	Time Synchronization Server (Netware 4.x)
632	0278	Directory Server (Netware 4.x)
640	0280	Novell File and Printer Sharing Service for PC
989	03dd	Banyan ENS for Netware Client NLM
772	0304	Novell SAA Gateway
776	0308	COM or VERMED 1
778	030a	Galacticomm's Worldgroup Server
780	030c	Intel Netport 2 or HP JetDirect or HP Quicksilver
800	0320	Attachmate Gateway

Dezimal	Hexa-Dezimal	SAP-Beschreibung
807	0327	Microsoft Diagnostiocs
808	0328	WATCOM SQL server
821	0335	MultiTech Systems Multi-synch Comm Server
835	0343	Xylogics Remote Access Server or LAN Modem
853	0355	Arcada Backup Exec
858	0358	MSLCD1
865	0361	NETINELO
894	037e	Twelve Novell file servers in the PC3M family
895	037f	VirusSafe Notify
902	0386	HP Bridge
903	0387	HP Hub
916	0394	NetWare SAA Gateway
923	039b	Lotus Notes
951	03b7	Certus Anti Virus NLM
964	03c4	ARCserve 4.0 (Cheyenne)
967	03c7	LANspool 3.5 (Intel)
983	03d7	lexmark printer server (type 4033-011)
984	03d8	lexmark XLE printer server (type 4033-301)
990	03de	Gupta Sequel Base Server or NetWare SQL
993	03e1	Univel Unixware
996	03e4	Univel Unixware
1020	03fc	Intel Netport
1021	03fd	Print SErver Queue
1196	04ac	On-Time Scheduler NLM
1034	040A	ipnServer Running on a Novell Server
1037	040D	LVERRMAN Running on a Novell Server
1038	040E	LVLIC Running on a Novell Server
1044	0414	Kyocera
1065	0429	Site Lock Virus (Brightworks)
1074	0432	UFHELP R

Dezimal	Hexa-Dezimal	SAP-Beschreibung
1075	0433	Synoptics 281x Advanced SNMP Agent
1092	0444	Microsoft NT SNA Server
1096	0448	Oracle
1100	044c	ARCserve 5.01
1111	0457	Canon GP55 Running on a Canon GP55 network printer
1114	045a	QMS Printers
1115	045b	Dell SCSI Array (DSA) Monitor
1169	0491	NetBlazer Modems
1200	04b0	CD-Net (Meridian)
1299	0513	Emulux NQA Something from Emulex
1312	0520	Site Lock Checks
1321	0529	Site Lock Checks (Brightworks)
1325	052d	Citrix OS/2 App Server
1343	0535	Tektronix
1344	0536	Milan
1387	056b	IBM 8235 modem server
1388	056c	Shiva LanRover/E PLUS
1389	056d	Shiva LanRover/T PLUS
1408	0580	McAfee's NetShield anti-virus
1466	05BA	Compatible Systems Routers
	05B8	NLM to workstation communication (Revelation Software)
	0606	JCWatermark Imaging
1569	0621	IBM AntiVirus NLM
1600	0640	Microsoft Gateway Services for NetWare
1614	064e	Microsoft Internet Information Server
1900	076C	Xerox
1947	079b	Shiva LanRover/E 115
1958	079c	Shiva LanRover/T 115
1972	07B4	Cubix WorldDesk

Dezimal	Hexa-Dezimal	SAP-Beschreibung
	07c2	Quarterdeck IWare Connect V2.x NLM
	07c1	Quarterdeck IWare Connect V3.x NLM
2084	0824	Shiva LanRover Access Switch/E
2154	086a	ISSC collector NLMs
2175	087f	ISSC DAS agent for AIX
2857	0b29	Site Lock
3113	0c29	Site Lock Applications
3116	0c2c	Licensing Server
9088	2380	LAI Site Lock
9100	238c	Meeting Maker
18440	4808	Site Lock Server or Site Lock Metering VAP/NLM
21845	5555	Site Lock User
25362	6312	Tapeware
28416	6f00	Rabbit Gateway (3270)
30467	7703	MODEM??
32770	8002	NetPort Printers (Intel) or LANport
32776	8008	WordPerfect Network Version
34238	85BE	Cisco Enhanced Interior Routing Protocol (EIGRP)
34952	8888	WordPerfect Network Version or Quick Network Management
36864	9000	McAfee's NetShield anti-virus
38404	9604	?? CSA-NT_MON
46760	b6a8	Ocean Isle Reachout Remote Control
61727	f11f	Site Lock Metering VAP/NLM
61951	f1ff	Site Lock
62723	f503	Microsoft SQL Server
63749	f905	IBM Time and Place/2 application
64507	fbfb	TopCall III fax server
65535	ffff	Any Service or Wildcard

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
nbdatalogram	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
who	513	udp

Dienst	Port-Nr.	Protokoll
shell	514	tcp
syslog	514	udp
printer	515	tcp
talk	517	udp
ntalk	518	udp
efs	520	tcp
route	520	udp
timed	525	udp
tempo	526	tcp
courier	530	tcp
conference	531	tcp
rvd-control	531	udp
netnews	532	tcp
netwall	533	udp
uucp	540	tcp
klogin	543	tcp
kshell	544	tcp
new-rwho	550	udp
remotefs	556	tcp
rmonitor	560	udp
monitor	561	udp
garcon	600	tcp
maitrd	601	tcp
busboy	602	tcp
acctmaster	700	udp
acctslave	701	udp
acct	702	udp
acctlogin	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctslave2	706	udp
acctdisk	707	udp
kerberos	750	tcp
kerberos	750	udp
kerberos_master	751	tcp
kerberos_master	751	udp

Dienst	Port-Nr.	Protokoll
passwd_server	752	udp
userreg_server	753	udp
krb_prop	754	tcp
erlogin	888	tcp
kpop	1109	tcp
phone	1167	udp
ingreslock	1524	tcp
maze	1666	udp
nfs	2049	udp
knetd	2053	tcp
eklogin	2105	tcp
rmt	5555	tcp
mtb	5556	tcp
man	9535	tcp
w	9536	tcp
mantst	9537	tcp
bnews	10000	tcp
rscs0	10000	udp
queue	10001	tcp
rscs1	10001	udp
poker	10002	tcp
rscs2	10002	udp
gateway	10003	tcp
rscs3	10003	udp
remp	10004	tcp
rscs4	10004	udp
rscs5	10005	udp
rscs6	10006	udp
rscs7	10007	udp
rscs8	10008	udp
rscs9	10009	udp
rscsa	10010	udp
rscsb	10011	udp
qmaster	10012	tcp
qmaster	10012	udp

Häufig gestellte Fragen und Antworten

In diesem Kapitel finden Sie Hilfe bei Problemen beim Betrieb eines *LANCOMs*, die andere Anwender vor Ihnen schon mit der Hilfe unseres Supports gelöst haben.

Wenn Sie also Schwierigkeiten bei der Konfiguration eines *LANCOMs* haben oder eine Fehlfunktion vermuten, schauen Sie bitte zunächst hier nach, ob die Lösung vielleicht schon dokumentiert ist.

Um Ihnen die Suche zu erleichtern, sind die einzelnen Fragen nach Themengebieten geordnet.

Außerdem können Sie die Antworten zu den Fragen auch über den Index am Ende dieses Anhangs aufspüren ...

Allgemein.....	2
IP-RIP	7
PPP	9
Bridge.....	12
IPX-Router	14
IP-Router	19

Allgemein



Warum dauert das Starten von Programmen verhältnismäßig lange?

Der Durchsatz über eine ISDN-Leitung ist im Verhältnis zu einem lokalen Netzwerkstrang klein (ca. 20 bis 1000 mal geringer). Aus diesem Grund ist es nicht sinnvoll, Programme von einem Netzwerk über den Router zum Arbeitsplatzrechner zu übertragen. Statt dessen sollten alle häufig benutzten Programme auf einer lokalen Festplatte gespeichert sein und nur die Nutzdaten, die von diesen Programmen verarbeitet werden, über den Router übertragen werden.

Erreichbare Datendurchsätze bei Verbindungen über zwei Router liegen bei IPX zwischen 4,5 kByte/s (mit einem B-Kanal ohne Datenkompression und ohne PBURST.NLM) und 40 kByte/s (mit zwei B-Kanälen, Datenkompression und PBURST.NLM). Bei TCP/IP-Verbindungen können Datendurchsätze von 6 kByte/s (mit einem B-Kanal ohne Datenkompression) bis 32,5 kByte/s (mit zwei B-Kanälen und Datenkompression) erreicht werden.



Der Einsatz von Datenbanken im Remote-Mode-Betrieb ist über ISDN nur bei SQL-Datenbanken sinnvoll möglich. Ist der Einsatz einer Nicht-SQL-Datenbank aufgrund der Rahmenbedingungen absolut notwendig, so hilft häufig der Einsatz netzwerkfähiger Fernsteuerungssoftware (z.B. PC Anywhere) um im Remote-Control-Betrieb akzeptable Antwortzeiten zu erreichen.



Was ist zu tun, wenn das **LANCOM** nach erfolgter Anwahl die Meldung „Abbruch D-Kanal“ ausgibt?

- Überprüfen Sie den ISDN-Anschluß, um eine Leitungsstörung auszuschließen.
- Überprüfen Sie im Menü Setup/WAN-Modul/D-Kanal, ob das richtige D-Kanal-Protokoll eingestellt ist. Bei Verwendung des nationalen Protokolls wählen Sie die Einstellung 1TR6 und bei Euro-ISDN die Einstellung DSS1.



Warum meldet das **LANCOM** „keine Antwort“?

- Die Gegenstelle ist nicht betriebsbereit.
- Es wurde eine falsche Rufnummer eingegeben.



Warum erhalte ich häufig in der Statusmeldung (Display bei **LANCOM MPR**) die Meldung „Gegenstelle gesperrt“?

- Wird eine Verbindung vom **LANCOM** der Gegenseite aktiv abgelehnt, um z.B. einen Rückruf zu initiieren, muß das anrufende **LANCOM** warten, bis dieser Rückruf erfolgt. Werden in dieser Zeit weitere Daten für die gleiche Gegenstelle zum **LANCOM** gesendet, wird kein erneuter Verbindungsaufbau initiiert, sondern die Meldung „Gegenstelle gesperrt“ ausgegeben.

- Wird während einer PPP-Verhandlung die Authentifizierung von der Gegenstelle abgelehnt oder tritt ein anderer Fehler in der PPP-Verhandlung auf, wird ebenfalls eine weitere Anwahl, unter Ausgabe der Meldung Gegenstelle gesperrt, verzögert.

Nach einer zufälligen Wartezeit von 20-40 Sekunden wird die Gegenstellensperre aufgehoben und die gleiche Gegenstelle kann erneut angewählt werden.

Warum meldet das **LANCOM** „Kein Protokoll“?

- Das anrufende **LANCOM** benutzt den Layer ELSA-DEFAULT und das angerufene z.B. RAWHDLC. Dann versucht das anrufende **LANCOM** eine Protokoll-Verhandlung nach ELSA-Standard, auf die das angerufene Gerät nicht antwortet. Abhilfe schafft hier die Verwendung des gleichen Layers auf beiden Seiten.
- Bei Rückruf über Name, wird während der Protokoll-Verhandlung, direkt nach Übertragung des Namens, vom angerufenen Gerät die Verbindung abgebrochen. Dieses Verhalten ist für den Anrufer vom oben beschriebenen nicht zu unterscheiden. Deshalb erscheint die gleiche Fehlermeldung, bis der Rückruf des angerufenen Geräts erfolgt.

Trotz Eintrag in der Nummernliste wird das falsche Layer und/oder die falsche Gegenstelle erkannt.

- Auch innerhalb des Ortsnetzes wird die Vorwahl mit übermittelt. Bitte fügen Sie vor der Rufnummer also auf jeden Fall die entsprechende Ortsnetzkennzahl ein.
- In Deutschland gibt es zwei Arten von Vermittlungsstellen, die die Telekom einsetzt. Die eine übermittelt die Ortskennzahlen mit, die andere ohne die führende „0“.

Beispiel:

Aachen: 0241...

München: 89...

Lösung 1: Tragen Sie beide Varianten in die Nummernliste ein.

Lösung 2: Schauen Sie unter /Status/Info.-Verb./Rufnummer nach, welche CLIP übermittelt wird. Diese übernehmen Sie dann in die Nummernliste.

- TK-Anlagen neigen dazu ihrerseits zusätzliche Zeichen vor die CLIP zu setzen. So sind Fälle bekannt in denen aus z.B. 0241... eine 00241... oder eine #0241... wurde. Stellen Sie dies bitte auf dem unter Lösung 2 beschriebenen Weg fest und korrigieren Sie die Nummernliste entsprechend.
- Situation: Sie benutzen zwei **LANCOM** innerhalb einer TK-Anlage und erhalten o.g. Problem.

Lösung: TK-Anlage identifizieren ihre Anschlüsse oft nicht mit der kompletten Nummer sondern nur mit der internen Durchwahl.

Beispiel: **LANCOM** 1 wählt #705

LANCOM 2 erhält 705 als CLIP



Warum bricht das **LANCOM** die ISDN-Verbindung sofort nach dem **CONNECT** wieder ab?

Der Zugangsschutz ist im Menü Setup/WAN-Modul/Schutz aktiviert, jedoch ist der Eintrag in der Nummern- bzw. Namenliste nicht vorhanden oder falsch.



Wodurch können hohe Gebühren entstehen?

Die Konfiguration des Gerätes ist nicht optimal. Überprüfen Sie bitte die Einstellungen des Bridge-Moduls bzw. der Router-Module.



Einige Server in Ihrem Netzwerk übertragen Daten zum Remote-Netzwerk. Mit Hilfe der Aufbautabellen der Bridge- oder Router-Module können Sie leicht die MAC-Adressen der Geräte herausfinden, die an einem Verbindungsaufbau beteiligt sind (siehe Kapitel 'Status/Verb.-Statistik' auf Seite 3.1.22).



Wie kann ich überhöhte Verbindungsgebühren vermeiden?

Durch Fehlkonfiguration der Router oder durch häufige Nutzung der WAN-Verbindung kann eine hohe Gebührenrechnung entstehen. Das **LANCOM** bietet Ihnen hierzu einen wirksamen Schutz vor ungewollt hohen Verbindungsgebühren. Über den Menüpunkt Setup/Gebühren-Modul können alle notwendigen Einstellungen für den Gebührenschatz vorgenommen werden. Standardmäßig ist der Gebührenschatz auf 830 Einheiten für einen Zeitraum von sieben Tagen festgelegt. Somit können in 7 Tagen maximal für ca. 100,- DM Gebühren anfallen (siehe auch 'Setup/Gebühren-Modul' auf Seite 3.1.37).

Über den Menüpunkt Budget-Gebühren legen Sie fest, wieviele Einheiten der Gebührenüberwachung als Budget zur Verfügung stehen. Diese Einheiten können nur in Zehnerschritten bis maximal 2550 Einheiten (Standardwert 830 = ca. 100,- DM) eingegeben werden. Mit dieser Funktion können Sie die anfallenden Verbindungskosten selbst bestimmen und werden im Fehlerfall auf unnötig anfallende Verbindungsaufbauten aufmerksam gemacht. Nach Verbrauch des Budgets stellt das **LANCOM** dann selbst den Dienst ein.



Warum entstehen trotz lokal vorhandener Programme immer noch unerklärliche Wartezeiten, in denen der Arbeitsplatzrechner nicht zu arbeiten scheint?

Es kann sein, daß bei einem Login-Vorgang Programme gestartet werden, die sich auf Netzwerklaufwerken befinden. Überprüfen Sie bitte daher alle Pfadangaben und ändern sie diese auf lokale Einstellungen. Zusätzlich müssen Sie natürlich auch die gewünschten Programme in die entsprechende lokale Umgebung kopieren.



Woran kann es liegen, daß die Verbindung nicht mehr abgebaut wird?

- Die dieser Verbindung zugeordnete Verbindungshaltezeit (eventuell in der Namenliste) ist auf den Wert 0 gestellt (0 = unendlich lange die Verbindung halten).

- Ständige Übertragungen verhindern einen Verbindungsabbau. Sie können die Verbindung manuell abbauen und warten, bis die Verbindung wieder automatisch aufgebaut wird. Die Ursache des Wiederaufbaus können Sie in den jeweiligen Aufbautabellen (siehe 'Status/Verb.-Statistik' auf Seite 3.1.22) nachlesen. Durch eine Anpassung der Workstation-/Server-Konfiguration oder einen verbesserten Einsatz der Filter am *LANCOM*, können Sie das Problem beheben.
- Datenpakete, die in Novell-Netzwerken periodisch versendet werden, können den Verbindungsabbau verhindern. Sollten Frames dieser Art in Ihrem Netz vorkommen, sollten Sie diese in Ihre Socket-Filter-Tabelle (siehe 'Socket-Filter' auf Seite 3.1.44) aufnehmen.



Woran kann es liegen, daß nach einem passiven Verbindungsaufbau keine Daten ausgetauscht werden?

Kontrollieren Sie, ob in der Nummernliste ein Verweis auf die anrufende Gegenstelle eingetragen ist. Zusätzlich muß in der Namenliste ein Verweis von der anrufenden Gegenstelle auf das gewünschte WAN-Layer vorhanden sein.



Was mache ich, wenn ich nicht mehr weiß, mit welchen Paßwörtern das System geschützt ist?

Für den Fall, daß Sie Ihre Passwörter, die Sie für die Tastatur und die Remote-Konfiguration vergeben haben, nicht mehr kennen, können Sie das Gerät über die Outband-Schnittstelle zurücksetzen. Dazu gehen Sie wie folgt vor:

- ① Bauen Sie zuerst eine Outband-Konfigurationsverbindung auf (siehe 'Der direkte Weg: Outband' auf Seite 1.3.5).
- ② Sobald Sie nach dem Passwort gefragt werden, geben Sie die Seriennummer Ihres *LANCOM* ein. Die Seriennummer befindet sich an der Geräteunterseite. Daraufhin wird automatisch ein Firmware-Upload gestartet.
- ③ Führen Sie den Firmware-Upload durch wie im Kapitel 'So spielen Sie eine neue Software ein' auf Seite 1.3.16 beschrieben. Danach sind die Passwörter für die Remote-Konfiguration und die Tastatur gelöscht. Die Tastatur ist somit entsperrt.



Wenn ich mit Telix für DOS aus einer DOS-Box unter Windows 95 versuche, eine neue Firmware in das *MicroLink LANCOM* zu laden, wird der FlashROM-Upload jedesmal mit der Meldung "FlashROM defekt" abgebrochen. Muß ich mein Gerät zur Reparatur einsenden ?

Falls Sie ein Flash-ROM-Update mit Telix für DOS aus einer DOS-Box von Windows 95 heraus durchführen, ist darauf zu achten, daß das Update nicht durch den Start anderer Programme (z.B. Bildschirmschoner von Windows 95) unterbrochen wird. Sie müssen Ihr Gerät nicht zur Reparatur einsenden, sondern können den Upload erneut durchführen.

IP-RIP



Ich setze die *LANCOM*-Geräte sowohl mit als auch ohne IP-RIP-Unterstützung am gleichen Netz an. Wenn ich IP-RIP eingeschaltet habe, bauen die Geräte ohne IP-RIP ständig Verbindungen auf. Wie kann ich das verhindern?

RIP-Datagramme werden als IP-Broadcast bzw. RIP-2 Multicast versendet. Da das *LANCOM* ohne RIP-Unterstützung diese Datagramme nicht erkennen kann, besteht die Gefahr, daß die RIP-Pakete in das WAN verschickt werden, wenn die in diesem *LANCOM* eingetragene Standard-Route ein Remote-Gerät ist. Um hier einen unnötigen Verbindungsaufbau (und die damit verbundene Gebührenbelastung) zu vermeiden, sollte IP-RIP bei diesem *LANCOM* sowohl in der LAN- als auch in der WAN-Filtertabelle eingetragen werden:

LAN-Filtertabelle zur Unterdrückung von RIP:

Anfangs-Port	End-Port	Protokoll	Typ
520	520	UDP	Immer-Filter

WAN-Filtertabelle zur Unterdrückung von IP-RIP:

Anfangs-Port	End-Port	Protokoll
520	520	UDP



Warum werden bei einer bestehenden Verbindung (nicht Standard-Route) IP-Pakete, die an die Standard-Route versendet werden sollen, nicht mit Fehlermeldungen wie "Destination Network unreachable", sondern mit "Connection timed out" oder "Time to live exceeded" quittiert?

- Sie haben einen weiteren Router (kein *LANCOM*) in Ihrem Netzwerk, der RIP-Pakete versendet. In der (statischen) Routing-Tabelle dieses Routers ist das *LANCOM* als Standard-Route eingetragen. In diesem Fall werden die IP-Pakete ständig zwischen Router und *LANCOM* hin- und hergeschickt. Abhilfe schafft das Entfernen des statischen Eintrags der Standard-Route.
- Auf einer oder mehreren Workstations in Ihrem Netz ist der "Routing-Dämon" routed falsch installiert. Diese Workstations verhalten sich so, als wären sie Router und geben ihre Standard-Route (*LANCOM*, s.o.) bekannt. Installieren Sie den "Routing-Dämon" beim nächsten Systemstart (Reboot) wie folgt:

```
routed -q
```



Wegen der IP-RIP-Unterstützung durch *LANCOM* habe ich an allen Workstations die Standard-Route entfernt und stattdessen den "Routing-Dämon" *routed* gestartet. Warum kann keine Internet-Verbindung mehr aufgebaut werden?

- Die RIP-Unterstützung des *LANCOM* ist nicht eingeschaltet (Menü: Setup/IP-Router-Modul/RIP-Einstellung/Zustand steht auf Aus)
- Der "Routing-Dämon" *routed* ihres UNIX-Systems versteht nur RIP-1, im *LANCOM* ist jedoch R1-komp. oder RIP-2 eingestellt (Menü Setup/IP-Router-Modul/RIP-Einstellung/Typ).



Ich habe mehrere *LANCOM*-Geräte "parallelgeschaltet", d.h., diese besitzen die gleiche Routing-Tabelle und sollen Verbindungen über das jeweils "freie" *LANCOM* aufbauen. Der Verbindungsaufbau im ISDN funktioniert zwar korrekt, jedoch kommt eine TCP/IP-Verbindung nur Zustande, wenn ein bestimmtes *LANCOM* die Verbindung aufbaut.

- Sie haben unter dem Menü Setup/WAN-Modul/Layerliste als Layer-3-Protokoll das ELSA-Protokoll für die Gegenstellen eingetragen. In diesem Fall müssen alle parallelgeschalteten Geräte den gleichen Namen besitzen.
- Bei den Gegenstellen muß für die zugehörigen Routen dieser gemeinsame Name als Router-Name in der Routing-Tabelle (Menü: Setup/IP-Router-Modul/IP-Routing-Tab.) eingetragen sein
- Sie haben ein anderes Layer-3-Protokoll eingestellt. In diesem Fall ist die Namensvergabe der parallelgeschalteten *LANCOM* beliebig.
Bei den Gegenstellen müssen in der Nummernliste (Menü: Setup/WAN-Modul/Nummernliste) die Rufnummern aller parallelgeschalteten *LANCOM* mit demselben Namen versehen werden. Dieser Name muß dem in der Namenliste (Menü: Setup/WAN-Modul/Namenliste) entsprechen, über den die Gegenstelle eine Verbindung zu einem der parallelgeschalteten *LANCOM* aufbaut.



Ich habe mehrere *LANCOM*-Geräte "parallelgeschaltet", d.h., sie besitzen die gleiche Routing-Tabelle und sollen Verbindungen über das jeweils "freie" *LANCOM* aufbauen. Bei einem ankommenden Ruf auf einem der *LANCOM*, versucht ein anderes *LANCOM* eine Verbindung zum Anrufer aufzubauen.

In diesem Fall ist das *LANCOM*, das versucht, die Verbindung aufzubauen, als Standard-Router für den Empfänger des eingehenden IP-Pakets eingetragen. Weiterhin ist die RIP-Unterstützung bei diesem *LANCOM* entweder nicht eingeschaltet oder falsch konfiguriert. Stellen Sie für die Einträge Typ und R1-Maske im Menü Setup/IP-Router-Modul/RIP-Einstellung in allen parallelgeschalteten *LANCOM* die gleichen Werte ein.



PPP

Ich kann eine PPP-Verbindung zu einer PPP-fähigen Gegenstelle nicht aufbauen. Bei jedem Versuch wird die Protokoll-Verhandlung abgebrochen. Was kann ich tun, um den Fehler zu beheben?

Durch Auswerten der Fehlermeldungen kann in den meisten Fällen die Ursache für das Fehlschlagen der PPP-Verhandlung ermittelt werden. Die vom *LANCOM* angezeigten Fehlermeldungen können folgende Ursachen haben:

Fehler	Mögliche Ursache
LCP abgelehnt	Die Gegenstelle hat das Link-Control-Protokoll des PPP zurückgewiesen. Es liegt eine schwere Funktionsstörung im PPP-Stacks der Gegenstelle vor.
Auth. Falsch	Die Gegenstelle unterstützt das eingestellte Überprüfungsprotokoll nicht. Die Einstellungen müssen zwischen dem <i>LANCOM</i> und der Gegenstelle abgeglichen werden. Evtl. kann eine Verbindung nur aufgebaut werden, wenn die Überprüfung abgeschaltet wird.
Auth. Abgelehnt	Die Gegenstelle hat jegliche Überprüfung abgelehnt. Eine Verbindung kann nur nach Abschalten der Überprüfung in der PPP-Liste aufgebaut werden.
PAP abgelehnt	Obwohl in der LCP-Verhandlung akzeptiert, hat die Gegenstelle das Password-Authentication-Protokoll zur Überprüfung zurückgewiesen. Es liegt eine schwere Funktionsstörung im PPP-Stack der Gegenstelle vor. Evtl. kann die Verbindung durch Aktivieren des Challenge-Handshake-Authentication-Protokolls (CHAP) in der PPP-Liste dennoch gesichert aufgebaut werden.
PAP Rx-Timeout	Die Gegenstelle hat nicht innerhalb der eingestellten Zeit mit der Aussendung von PAP-Requests zum <i>LANCOM</i> begonnen. Durch Erhöhen der Wiederholungszahl kann in den meisten Fällen dieses Problem behoben werden.
PAP Tx-Timeout	Die Gegenstelle hat nicht innerhalb der eingestellten Zeit auf einen PAP-Request vom <i>LANCOM</i> geantwortet. Durch Erhöhen der Wiederholungszahl kann dies meist behoben werden.
PAP-Req falsch	Das von der Gegenstelle verwendete Passwort paßt nicht zum Passwort in der PPP-Liste.
PAP-NAK empfangen	Der PAP-Request vom <i>LANCOM</i> wurde von der Gegenstelle zurückgewiesen. Die für beide Seiten verwendete Kombination aus Peer-ID (Gerätename) und Passwort stimmt nicht überein. Im <i>LANCOM</i> muß entweder der Geräteiname oder der Schlüssel-Eintrag in der PPP-Liste angepaßt werden.
CHAP abgelehnt	Obwohl in der LCP-Verhandlung akzeptiert, hat die Gegenstelle das Challenge-Handshake-Authentication-Protokoll zur Überprüfung zurückgewiesen. Es liegt eine schwere Funktionsstörung im PPP-Stack der Gegenstelle vor. Evtl. kann die Verbindung, durch Aktivieren des Password-Authentication-Protokolls (PAP) in der PPP-Liste dennoch gesichert aufgebaut werden.
CHAP Rx-Timeout	Die Gegenstelle hat nicht innerhalb der eingestellten Zeit auf einen CHAP-Challenge mit einem CHAP-Response reagiert. Durch Erhöhen der Wiederholungszahl kann in den meisten Fällen dieses Problem behoben werden.
CHAP Tx-Timeout	Die Gegenstelle hat nicht innerhalb der eingestellten Zeit auf einen CHAP-Response vom <i>LANCOM</i> reagiert. Durch Erhöhen der Wiederholungszahl kann dies meist behoben werden.

Fehler	Mögliche Ursache
CHAP-Resp falsch	Der von der Gegenstelle empfangene Response-Wert paßt nicht zu dem erwarteten Wert. Die für beide Seiten verwendete Kombination aus Name und Passwort stimmt nicht überein. Im <i>LANCOM</i> muß entweder der Gerätenamen oder der Schlüsseleintrag in der PPP-Liste angepaßt werden.
CHAP-Fail empf.	Die Gegenstelle hat den CHAP-Response von <i>LANCOM</i> zurückgewiesen. Es liegt der gleiche Fehler wie bei CHAP-Resp falsch vor.
CHAP Peer ID unb.	Von der Gegenstelle wurde im CHAP-Request eine Peer ID angegeben, die vom <i>LANCOM</i> in der PPP-Tabelle nicht aufgelöst werden kann. Es liegt womöglich der gleiche Fehler wie bei CHAP-Resp falsch vor.
IPXCP abgelehnt	Die Gegenstelle hat das IPX-Control-Protokoll zur Aushandlung der IPX-Parameter zurückgewiesen. Entweder unterstützt die Gegenstelle kein IPX-Routing unter PPP, oder IPX ist in der Gegenstelle für diese Verbindung nicht aktiviert. Die Konfiguration der Gegenstelle muß überprüft werden.
IPXCP-Net falsch	Die von beiden Seiten für das ISDN verwendeten IPX-Netzwerkadressen stimmen nicht überein. Entweder ist der IPX-Router vom <i>LANCOM</i> oder der IPX-Router der Gegenstelle falsch konfiguriert.
IPXCP-Net abgel.	Die Gegenstelle hat die Aushandlung der IPX-Netzwerkadresse für das ISDN abgelehnt. Die Konfiguration der Gegenstelle muß überprüft werden.
IPXCP-Route unb.	Die Gegenstelle verwendet ein anderes Routing-Protokoll für IPX als RIP/SAP. Die Konfiguration der Gegenstelle muß überprüft werden.
IPCP abgelehnt	Die Gegenstelle hat das IP-Control-Protokoll zur Aushandlung der IP-Parameter zurückgewiesen. Entweder unterstützt die Gegenstelle kein IP-Routing unter PPP, oder IP ist in der Gegenstelle für diese Verbindung nicht aktiviert. Die Konfiguration der Gegenstelle muß angepaßt werden.
Kein NCP bereit	Für die Verbindung konnte weder das IPXCP noch das IPCP aktiviert werden. Sowohl der IPX-Router als auch der IP-Router besitzen keinen Verweis auf die Gegenstelle in ihrer Konfiguration. Vergleichen Sie den vom <i>LANCOM</i> für die Verbindung ermittelten Namen der Gegenstelle (unter dem Menü: Status/Info-Verbindung/Kennung-Ggst. mit dem Gegenstellennamen des IPX-Routers (unter dem Menü: Setup/IPX-Modul/WAN-Einstellung/Gegenstelle) bzw. den Einträgen in der Routingtabelle des IP-Routers (unter dem Menü: Setup/IP-Router/IP-Routing-Tab.) und passen Sie diese an.



Mein Provider hat mir für die Internet Anbindung einen User-Namen, ein Passwort und das Authentifizierungsprotokoll PAP genannt. Obwohl ich in der PPP-Liste User-Namen, Passwort und Authentifizierung nach PAP korrekt eingetragen habe, bricht die Verbindung sofort wieder ab und das *LANCOM* meldet „Aut. abgelehnt“.

Da ein Internet-Provider meist mehrere Kunden über die gleiche Wählleitung bedient, wird häufig auf eine Authentifizierung des Providers gegenüber dem Kunden verzichtet und nur der Kunde-Router zur Authentifizierung nach PAP oder CHAP aufgefordert. Bei eingestelltem Authentifizierungs-Protokoll fordert jedoch das *LANCOM* aktiv eine Authentifizierung der Gegenstelle mit Name und Passwort. Wird dieser Request nicht beantwortet wird die Verbindung sofort abgebrochen. Deshalb wählen Sie unter Setup/WAN-Modul/PPP-Liste unter Sicherung „keine“. Dann beantwortet das *LANCOM* zwar automatisch

den PAP- oder CHAP-Request des Providers, fordert die Gegenseite jedoch nicht aktiv zur Authentifizierung auf. So kann die PPP-Verhandlung erfolgreich durchgeführt werden.

Bridge



Die Verbindung kommt zustande, aber die Bridge arbeitet nicht. Woran liegt das?

- Da eine Remote Bridge auf ETHERNET-Adressen arbeitet, darf auf dem B-Kanal nur mit Protokollen gearbeitet werden, die über einen ETHERNET-Vorspann verfügen. Achten Sie bitte darauf, daß Sie aus der Layerliste nur Einträge verwenden, die in der Spalte Encaps die Einstellung ETHER haben. Über den Menüpunkt Sonstiges/Info.-Verb./Encaps können Sie die aktuelle Einstellung kontrollieren.
- Kontrollieren Sie die Filtereinstellungen der Bridge, besonders die WAN-Filtereinstellungen im Menü Setup/Bridge-Modul/WAN-Einstellung.



Warum wird häufig eine Verbindung aufgebaut?

Dieses Verhalten existiert sehr häufig im Zusammenhang mit einer Netzwerkkopplung über eine Bridge. Bedingt durch die regelmäßige Verbreitung von Broadcast-Datenpaketen von einigen Servern aus, die in den meisten Fällen auf die Remote-Seite übertragen werden müssen, muß eine Bridge eine Verbindung aufbauen. In bestimmten Fällen können Broadcasts von der Übertragung auf die Gegenseite ausgeschlossen werden (Setup/Bridge-Modul/LAN-Einstellung/Broadcast auf neg konfigurieren).

Zum Beispiel bei der ARP-Problematik unter TCP/IP erfolgt die Umwandlung einer IP-Adresse in die MAC-Layer-Adresse der zugehörigen Netzwerkkarte mittels ARP. Das Address Resolution Protocol arbeitet mit Broadcast-Datenpaketen, die die Bridge dazu veranlassen, eine Verbindung aufzubauen.

Dieses unerwünschte Aufbauen einer Verbindung kann durch die Einrichtung eines lokalen ARP-Servers vermieden werden. Auf dem Server wird dazu eine statische ARP-Tabelle eingerichtet, in der zumindest für alle fernen Arbeitsplatzrechner die Zuordnung von IP-Adresse und MAC-Layer-Adresse eingetragen ist. Auf dem lokalen LANCOM können dann alle Broadcasts vom LAN gefiltert werden. Analog zu dieser Vorgehensweise kann auch ein RARP-Server eingerichtet werden.



Warum wird ein NetWare-Arbeitsplatzrechner nach einer gewissen Zeit vom Server abgemeldet?

Ein NetWare-Server erwartet Rückmeldungen von angeschlossenen Arbeitsplatzrechnern. Bleiben diese Rückmeldungen aus, wird die logische Verbindung nach einer einstellbaren Zeit für ungültig erklärt und die Meldung *Connection no longer valid* ausgegeben, falls der Arbeitsplatzrechner versucht, Daten mit dem Server auszutauschen.

Dieser Zustand tritt beim Einsatz der Bridge nur dann auf, wenn durch den Short-Hold-Modus die WAN-Verbindung zum Server für eine längere Zeit unterbrochen wurde und das LANCOM auf der Serverseite keine Rufnummer eingestellt hat, also selbst die Ver-

bindung nicht aufbauen kann. Die Zeiteinstellung, die der Server benötigt, um eine logische Verbindung abzubauen, sollte erhöht werden. Dazu dienen die folgenden Server-Parameter, die durch das SET-Kommando auf der Server-Console bzw. in der START-UP.NCF beeinflußt werden können:

NUMBER OF WATCHDOG PACKETS:	<Anzahl>
DELAY BETWEEN WATCHDOG PACKETS:	<Zeitmaß>
DELAY BEFORE FIRST WATCHDOG PACKET:	<Zeitmaß>

IPX-Router



Warum läßt sich unter Setup/IPX-Modul der IPX-Router nicht einschalten?

Im Menü Setup/IPX-Modul/Netzwerk wurde noch keine logische IPX-Netzwerknummer für den LAN- bzw. WAN-Anschluß eingetragen. Für die Funktion eines IPX-Routers ist die Zuweisung beider Netzwerknummern unbedingt erforderlich. Erst dann ist IPX-Routing möglich und das Modul einschaltbar.



Warum wird ein NetWare-Arbeitsplatzrechner nach einer gewissen Zeit vom Server abgemeldet?

Ein NetWare-Server erwartet Rückmeldungen von angeschlossenen Arbeitsplatzrechnern. Bleiben diese Rückmeldungen aus, wird die logische Verbindung nach einer einstellbaren Zeit für ungültig erklärt und die Meldung *Connection no longer valid* ausgegeben, falls der Arbeitsplatzrechner versucht, Daten mit dem Server auszutauschen.

Unter Setup/IPX-Modul/LAN-Einstellung/IPX-Watchdog ist Filt ausgewählt. IPX-Watchdog-Pakete werden demnach nicht beantwortet. Verwenden Sie die Einstellung Spoof (gebührensparend) oder Route (Watchdog-Pakete werden geroutet).



Warum baut das LANCOM keine Verbindung zur Gegenstelle auf?

- Die unter den Parametern Setup/IPX-Modul/LAN-Einstellung/Binding bzw. Setup/IPX-Modul/LAN-Einstellung/Netzwerk eingestellten Werte stimmen nicht mit den Werten des lokalen Netzwerkes überein. Kontrollieren Sie diese Einstellungen anhand der NetWare-Server-Konfiguration.
- Der Gegenstellename ist nicht eingetragen.
- Die Gegenstelle ist nicht vorhanden.
- Ihr Workstation-Netware-Requester hat einen falschen Frame eingestellt, wodurch ein Verbindungsaufbau seitens des LANCOM nicht durchgeführt werden kann.

Kontrollieren Sie, ob der im LANCOM unter Setup/IPX-Modul/LAN-Einstellungen/Binding eingestellte Typ (z.B. 802.2) mit dem in der vom Netware-Requester benutzten NET.CFG übereinstimmt.



Warum baut der Router eine Verbindung zur Gegenstelle auf, überträgt aber keine Datenpakete?

Der unter dem Parameter Setup/IPX-Modul/WAN-Einstellung/Gegenstelle eingestellte Name stimmt nicht mit dem Namen des angewählten LANCOM-Gerätes auf der Remote-Seite überein.



Warum baut der Router eine Verbindung zur Gegenstelle auf und überträgt Daten, die von dem IPX-Router der Gegenseite aber nicht empfangen werden?

- Der unter dem Parameter Setup/IPX-Modul/WAN-Einstellung/Binding eingestellte Wert ist nicht bei beiden LANCOM-Geräten gleich.
- Der IPX-Router der Gegenseite ist nicht eingeschaltet.



Warum werden bei der Inbetriebnahme des LANCOM die Fehlermeldung *Router configuration ERROR detected, Router at node xxx claims Network xxx should be xxx* auf dem File-Server ausgegeben?

Die unter den Parametern Setup/IPX-Modul/LAN-Einstellung/Netzwerk oder Setup/IPX-Modul/ WAN-Einstellung/Netzwerk eingestellte Netzwerknummer wurde bereits an anderer Stelle vergeben oder paßt nicht zum verwendeten Netzwerk-Strang.



Warum baut der Router scheinbar grundlos Verbindungen auf?

Folgende Gründe führen zu einem Verbindungsaufbau:

- Spoofing für RIP und/oder SAP steht auf:
 - Ohne, also Novell-konform
 - Zeit in Verbindung mit einer kurzen WAN-Update-Zeit.

Die Einstellungen trig (nur Änderungen werden übertragen) oder pBack (RIP/SAP-Informationen werden nur bei bestehender Verbindung aktualisiert) sind hier gebührensparend.
- Setup/IPX-Modul/LAN-Einstellung/IPX-Watchdog steht auf Route, besser auf Spoof stellen.
- Setup/IPX-Modul/LAN-Einstellung/SPX-Watchdog steht auf Route, besser auf Spoof stellen.
- Server im lokalen Netzwerk verschicken Datenpakete zu Remote-Servern.

Stellt eine remote verbundene Arbeitsstation per Netware-Befehl CASTOFF ALL den Empfang von Nachrichten ab, so ergibt sich bei älteren Requestern eine permanente Kommunikation zwischen Server und Remote-Server/Remote-Workstation über die ISDN-Strecke (alle 2 Sekunden versucht der Server, die Nachricht erneut zuzustellen). Dieses Problem ist durch Einsatz einer Novell-VLM-Shell ab der Version 1.20a zu beheben, bei der dieser Spezialfall anders verwaltet wird.
- Anhand der Statistik unter Status/IPX-Statistik/Router-Statistik/Aufbau-Tabelle können Sie Informationen über die letzten 20 Datenpakete erhalten, die zu einem Verbindungsaufbau führten. Dadurch können Rückschlüsse auf die Ursachen gezogen und gegebenenfalls Abhilfe geschaffen werden. Eine Lösungsmöglichkeit kann eine gezielte Filterung bestimmter Sockets für die LAN-Filter (Setup/IPX-Modul/LAN-Einstellung/Socket-Filter) des Routers sein. Sie sollten jedoch zunächst versu-

chen, bei den lokalen Servern die Versendung zu unterbinden. Sockets, die häufig zu Problemen führen, sind defaultmäßig ausgeblendet:

Socket	Bedeutung
0455h:	Novell Netware, NetBIOS-Pakete
0456h:	Novell Netware, Diagnostik-Pakete (alle 8 Minuten)
0457h:	Novell Netware, Serialization-Pakete (jede Minute oder alle 5 Minuten)
0550h - 0555h:	Microsoft-NetBIOS-Pakete (Win95/NT)
1401h - 1402h:	Periphery File Services (CD-ROM-Clients)
1480h - 1481h:	HP-"Keep alive"-Pakete (Drucker-Server)
83BAh:	Ferrari Fax-Server-Client-Abfrage
900fh - 9010h:	SNMP über IPX, Protokoll und Traps

Es können jedoch weitere Applikationen ein ähnliches Verhalten zeigen.



Durch welche Einstellungen kann der Router-Betrieb unter Novell NetWare optimiert werden?

■ SHELL.CFG

In dieser Datei sind Parameter für den Betrieb der Treiber IPX.COM und NETX.COM enthalten. Durch Änderung dieser Parameter (z.B. mit einem Editor-Programm) können bestimmte Funktionen im Novell-Betrieb unmittelbar beeinflusst werden. Für Arbeitsplatzrechner, die über den Router arbeiten, sind folgende Parameter von Bedeutung:

– IPX RETRY COUNT

Mit diesem Parameter kann die Arbeitsweise des Treibers IPX.COM beeinflusst werden. Er definiert, wie oft ein Datenpaket wiederholt werden soll, bevor der Treiber einen Netzwerkfehler meldet. Der Standardwert für diesen Zähler ist 20. Darüber hinaus wird für ISDN-Verbindungen folgende Einstellung empfohlen:

```
IPX RETRY COUNT=100
```

– SPX ABORT TIMEOUT

Mit diesem Parameter wird ebenfalls die Arbeitsweise des Treibers IPX.COM beeinflusst. Er definiert, wie lange (gemessen in 1/18 Sekunden) SPX auf die Beantwortung eines Datenpaketes wartet, bevor SPX die zugehörige Sitzung beendet. Der Standardwert beträgt 540 (ca. 30 Sekunden). Darüber hinaus wird für ISDN-Verbindungen folgende Einstellung empfohlen:

```
SPX ABORT TIMEOUT=1100 (entspricht ca. 1 Minute)
```

■ NET.CFG

In der Datei NET.CFG sind Parameter für den Betrieb des DOS-Requesters, bestehend aus LSL, einem kartenspezifischen Treiber, IPXODI und den VLMs, enthalten.

Durch Änderungen dieser Parameter können verschiedene Funktionen für den Betrieb mit dem Router optimiert werden.

– AUTO RECONNECT

Ist dieser Parameter auf **ON** gesetzt, versucht der DOS-Requester, eine abgelaufene Verbindung ("Connection no longer valid") neu aufzunehmen. Diese Einstellung ist besonders sinnvoll bei der Kopplung eines Arbeitsplatzrechners an ein Netzwerk, wenn die Verbindung durch das Leitungsmanagement des Routers unterbrochen werden kann.

Zusätzlich zu dieser Einstellung muß noch das **AUTO.VLM** geladen werden. Dies geschieht durch den Parameter:

```
vlm auto.vlm
```

oder durch den Eintrag dieses Moduls in der NET.CFG

– BIND RECONNECT

Durch diesen Parameter wird der DOS-Requester veranlaßt, verlorene Bindery-Verbindungen, Laufwerk-Mappings und Druckerverbindungen wiederherzustellen. Der Parameter ist nur im Zusammenhang mit dem Parameter **AUTO RECONNECT** wirksam.

– BROADCAST RETRIES

Dieser Parameter legt fest, wie oft der Requester eine Anforderung mittels Broadcast wiederholt. Wird dieser Wert erhöht (Standardeinstellung = 3), verlängert sich die Zeitspanne, bevor der Requester einen Netzwerkfehler meldet. Währenddessen kann das *LANCOM* gegebenenfalls die Verbindung neu aufbauen.

– BROADCAST SEND DELAY

Durch diesen Parameter wird die Zeit (in Tics) festgelegt, die der DOS-Requester zwischen dem Aussenden des Broadcast und der Bearbeitung des entsprechenden Requests wartet. Dieser Parameter kann benutzt werden, um Laufzeiten von langsamen Verbindungen auszugleichen.

– BROADCAST TIMEOUT

Durch diesen Parameter kann die Zeit eingestellt werden, die der DOS-Requester zwischen der Aussendung von zwei Broadcast-Anforderungen wartet.

– MINIMUM TIME TO NET

Bei Netzwerken, die durch Remote Bridges oder Satellitenstrecken verbunden sind, kann die TIME TO NET-Vorgabe des lokalen Routers zu klein sein. Da der Router nichts von der zwischengeschalteten Bridge "weiß", wäre es einem fernen Arbeitsplatzrechner nicht möglich, mit dem Router eine Verbindung aufzubauen.

Unter folgenden Bedingungen kann mit diesem Parameter das Fehlverhalten korrigiert werden:

- Der ferne Arbeitsplatzrechner ist ein NetWare 3.x-Typ oder älter.
- Die Datendurchsatzrate auf einer der WAN-Strecken ist kleiner als 2400 bit/s.



Was muß für den Burst-Modus berücksichtigt werden?

Dies ist ein spezieller Modus zur Verwaltung von Datenübertragungen, mit dem die Anzahl der Netzwerk-Datenpakete deutlich reduziert werden kann. Wird der Burst-Modus auf dem Server und auf dem Arbeitsplatzrechner aktiviert, werden große Dateien in direkt aufeinanderfolgenden Netzwerk-Datenpaketen übertragen. Dabei wird nicht mehr nach jedem Datenpaket auf die Bestätigung durch die Gegenseite gewartet.

Der Burst-Modus kann auf dem Server durch Laden des Moduls PBURST.NLM und auf dem Arbeitsplatzrechner durch Verwendung des Treibers BNETX.COM aktiviert werden.

Für die Installation des PBURST.NLM-Moduls auf dem File-Server sollte mindestens die Version 2.02 vom 10.7.93 verwendet werden. Dieses Modul kann unter Novell NetWare 3.11 verwendet werden; für spätere Versionen von Novell NetWare existieren entsprechende Patches.

Zusätzlich zur Installation des PBURST.NLM-Moduls müssen eventuell die Dateien LOGIN.EXE und ATTACH.EXE durch eine angepaßte Version ersetzt werden.

Bei Nutzung der VLM-Shell ist in der NET.CFG folgender Eintrag nötig:

```
PB BUFFERS = xx ( 2-255 , z.B. 10 )
```

IP-Router



Warum treten auf TCP/IP-Servern Fehlermeldungen der Art *Destination Network unreachable* auf?

- Bei dem jeweiligen Server wurde vergessen, den *LANCOM*-Router durch einen geeigneten Eintrag bekanntzumachen (bei vielen UNIX-Systemen z.B. mit Eintragungen in */etc* oder durch das Kommando *route add...*).
- Das *LANCOM* besitzt in der Router-Tabelle keinen Eintrag für die Ziel-IP-Adresse.
- Durch Zustandekommen von "Timeout-Schranken" wurde die Kommunikation eingestellt, da eventuell die Gegenstelle nicht erreicht wurde, gerade eine Verbindung zu einer anderen Gegenstelle vorhanden war oder der jeweilige TCP/IP-Zielserver nicht antwortet.



Warum baut der Router keine Verbindung zur gewünschten Gegenstelle auf?

- Die notwendigen Einträge in der Router-Tabelle unter Setup/IP-Router-Modul/IP-Routing-Tabelle sind nicht vorhanden oder fehlerhaft (IP-Adresse, Netzmaske oder Routername falsch).
- Der Routername ist nicht in der Namenliste unter Setup/WAN-Modul/Namenliste vorhanden oder besitzt keine oder die falsche Rufnummer.



Warum baut der Router eine Verbindung zur Gegenstelle auf, überträgt aber keine Datenpakete?

Der in der Tabelle Setup/IP-Router-Modul/IP-Routing-Tabelle eingestellte Router-Name stimmt nicht mit dem Namen des angewählten *LANCOM*-Gerätes auf der Remote-Seite überein.



Warum baut der Router eine Verbindung zur Gegenstelle auf und überträgt Daten, die von dem IP-Router der Gegenseite aber nicht empfangen werden?

Der IP-Router der Gegenseite ist nicht eingeschaltet bzw. nicht korrekt installiert. Überprüfen Sie, ob der IP-Router eingeschaltet ist (Setup/IP-Router-Modul/Zustand/Ein).



Wie können einzelne Stationen an ein lokales Netzwerk gekoppelt werden, ohne eine logische IP-Netzadresse zu vergeben und damit mehrere IP-Netzwerke einrichten zu müssen?

Hierfür kann Proxy-ARP benutzt werden. Dazu müssen auf der Netzwerkseite (*LANCOM 1*) in der Routertabelle alle kompletten IP-Adressen der remote aufzustellenden Geräte mit komplett besetzter IP-Netzmaske (255.255.255.255) und zugehörigem Gegenstellennamen (*LANCOM 2*) angelegt werden. Diese IP-Adressen müssen Adressen des lokalen Netzes sein. Weiterhin ist an beiden Geräten unter SETUP/IP-Router-Modul/Proxy-ARP einzuschalten.

Die Router-Tabelle könnte auf der Netzwerkseite bei Anbindung zweier IP-Maschinen wie folgt aussehen:

IP-Adresse	IP-Netz-Maske	Router-Name
193.41.22.17	255.255.255.255	LANCOM 2
193.41.22.18	255.255.255.255	LANCOM 2

In der Routertabelle des Remote-Gerätes wird dann die eigentliche IP-Netzadresse mit passender Netzmaske (255.255.255.0) und dem *LANCOM*-Namen auf der Netzwerkseite aufgenommen. Sollen die einzelnen Remote-Server auch untereinander kommunizieren, müssen Sie zur Vermeidung von Problemen wieder deren komplette IP-Adressen, Netzmasken und einen Routername 0.0.0.0 angeben. Dadurch werden für solche Adressen ARP-Broadcasts nicht beantwortet.

IP-Adresse	IP-Netz-Maske	Router-Name
193.41.22.17	255.255.255.255	0.0.0.0
193.41.22.18	255.255.255.255	0.0.0.0
193.41.22.0	255.255.255.0	LANCOM 1

Für die Proxy-ARP-Technik ist es nicht notwendig, den einzelnen Servern das *LANCOM* als Router bekanntzumachen, da durch die ARP-Auflösung die Kommunikation automatisch funktioniert.



Warum enthalten ARP-Caches lokaler Maschinen mehrmals die MAC-Adresse des LANCOM?

Durch den Proxy-ARP-Mechanismus antwortet das *LANCOM* bei allen ARP-Broadcasts mit seiner eigenen MAC-Adresse, wenn die nachgefragte IP-Adresse in der Routing-Tabelle eingetragen ist. Wenn Sie den Proxy-ARP-Mechanismus nicht benötigen, schalten Sie ihn im Menü Setup/IP-Router-Modul/Proxy-ARP aus. Dies können Sie immer bei einer klassischen IP-Router-Verbindung durchführen.



Warum steht unter Setup/TCP-IP-Modul/TCP-Max.-Verb. die Info, daß nur vier Verbindungen erlaubt sind. Können nur vier Anwender gleichzeitig den Router benutzen ?

Diese Info bezieht sich ausschließlich auf TCP-/IP-Konfigurationssitzungen zum *LANCOM* selbst. Das bedeutet, daß maximal vier Benutzer gleichzeitig eine Konfigurationssitzung zum *LANCOM* aufbauen können, wovon immer nur der Erste schreibberechtigt ist.

Eine Limitierung der maximal aufbaubaren logischen TCP-/IP-Verbindungen über das *LANCOM* gibt es nicht!

**Warum können bei Verbindungen zu Fremdgeräten (z.B. netGW von der Firma NetCS) Probleme bei der Erreichbarkeit verschiedener IP-Adressen auftreten?**

Viele Fremdgeräte definieren für das ISDN ein eigenes IP-Netzwerk und versehen die ISDN-Anschlüsse mit eigenen IP-Adressen aus diesem Netzwerk. Um diese IP-Adressen zu erreichen, muß das ISDN-IP-Netzwerk in der Routing-Tabelle des *LANCOM* ebenfalls eingetragen werden. Dies gilt besonders beim Zugriff von einer UNIX-Maschine, in der ein NetGW-Router installiert ist, auf ein entferntes Netzwerk. Die UNIX-Maschine hinterläßt als Absender-IP-Adresse eine Adresse aus dem ISDN-IP-Netzwerk.

**Warum gibt es beim IP-Routing kein Spoofing?**

Eine Kommunikation über das IP-Protokoll ist nicht auf periodisch versandte Pakete angewiesen. Deshalb ist es möglich, die IP-Maschinen in einem lokalen Netzwerk so zu konfigurieren, daß nur reine Nutzdaten über einen Router an ein WAN verschickt werden.