

Inhalt

- 1 Status , 1
 - 1.1 Verbindung , 1
 - 1.2 Betriebszeit , 1
 - 1.3 WAN-Statistik , 1
 - 1.3.1 Byte-Transport-Statistik , 2
 - 1.3.2 Paket-Transport-Statistik , 2
 - 1.3.3 Fehler-Statistik , 3
 - 1.3.4 WAN-TX-verworfen , 3
 - 1.3.5 WAN-Heap-Pakete , 3
 - 1.3.6 WAN-Queue-Pakete , 3
 - 1.3.7 WAN-Queue-Fehler , 3
 - 1.3.8 Durchsatz-Statistik , 3
 - 1.3.9 Werte-loeschen , 4
 - 1.4 LAN-Statistik , 4
 - 1.4.1 LAN-Rx-Pakete , 5
 - 1.4.2 LAN-Tx-Pakete , 5
 - 1.4.3 LAN-Rx-Fehler , 5
 - 1.4.4 LAN-Tx-Fehler , 5
 - 1.4.5 LAN-Stack-Fehler , 5
 - 1.4.6 LAN-NIC-Fehler , 5
 - 1.4.7 LAN-Heap-Pakete , 5
 - 1.4.8 LAN-Queue-Pakete , 5
 - 1.4.9 LAN-Queue-Fehler , 5
 - 1.4.10 LAN-Kollisionen , 5
 - 1.4.11 Werte-loeschen , 5
 - 1.4.12 Verbindung-aufgebaut , 5
 - 1.4.13 Verhandlung-abgeschlossen , 6
 - 1.4.14 Anschluss , 6
 - 1.4.15 Kein Eintrag , 6
 - 1.4.16 Kein Eintrag , 6
 - 1.4.17 Kein Eintrag , 6
 - 1.4.18 LAN-Rx-Bytes , 6
 - 1.4.19 LAN-Tx-Bytes , 6
 - 1.4.20 LAN-Rx-Broadcasts , 6
 - 1.4.21 LAN-Rx-Multicasts , 6
 - 1.4.22 LAN-Rx-Unicasts , 6
 - 1.4.23 LAN-Tx-Broadcasts , 6
 - 1.4.24 LAN-Tx-Multicasts , 6
 - 1.4.25 LAN-Tx-Unicasts , 6
 - 1.4.26 LAN-RX-CRC-Fehler , 6
 - 1.4.27 LAN-RX-Align-Fehler , 7
 - 1.5 PPP-Statistik , 7
 - 1.5.1 **Zustände** , 7
 - 1.5.2 LCP-Statistik , 8
 - 1.5.2.1 Rx-Fehler , 8
 - 1.5.2.2 Rx-Verworfen , 8

- 1.5.2.3 Rx-Config-Request , 8
- 1.5.2.4 Rx-Config-Ack. , 8
- 1.5.2.5 Rx-Config-Nack. , 8
- 1.5.2.6 Rx-Config-Reject , 8
- 1.5.2.7 Rx-Termination-Request , 8
- 1.5.2.8 Rx-Termination-Ack , 9
- 1.5.2.9 Rx-Code-Reject , 9
- 1.5.2.10 Rx-Protocol-Reject , 9
- 1.5.2.11 Rx-Echo-Request , 9
- 1.5.2.12 Rx-Echo-Reply , 9
- 1.5.2.13 Rx-Discard-Request , 9
- 1.5.2.14 Tx-Config-Request , 9
- 1.5.2.15 Tx-Config-Ack. , 9
- 1.5.2.16 Tx-Config-Nak. , 9
- 1.5.2.17 Tx-Config-Reject , 9
- 1.5.2.18 Tx-Termination-Request , 9
- 1.5.2.19 Tx-Termination-Ack. , 9
- 1.5.2.20 Tx-Code-Reject , 9
- 1.5.2.21 Tx-Protocol-Reject , 9
- 1.5.2.22 Tx-Echo-Request , 9
- 1.5.2.23 Tx-Echo-Reply , 10
- 1.5.2.24 Tx-Discard-Request , 10
- 1.5.2.25 Werte-loeschen , 10
- 1.5.3 PAP-Statistik , 10
 - 1.5.3.1 Rx-verworfen , 10
 - 1.5.3.2 Rx-Request , 10
 - 1.5.3.3 Rx-Success , 10
 - 1.5.3.4 Rx-Failure , 10
 - 1.5.3.5 Tx-Retry , 10
 - 1.5.3.6 Tx-Request , 10
 - 1.5.3.7 Tx-Success , 10
 - 1.5.3.8 Tx-Failure , 10
 - 1.5.3.9 Werte-loeschen , 10
- 1.5.4 CHAP-Statistik , 11
 - 1.5.4.1 Rx-verworfen , 11
 - 1.5.4.2 Rx-Challenge , 11
 - 1.5.4.3 Rx-Response , 11
 - 1.5.4.4 Rx-Success , 11
 - 1.5.4.5 Rx-Failure , 11
 - 1.5.4.6 Tx-Retry , 11
 - 1.5.4.7 Tx-Challenge , 11
 - 1.5.4.8 Tx-Response , 11
 - 1.5.4.9 Tx-Success , 11
 - 1.5.4.10 Tx-Failure , 11
 - 1.5.4.11 Werte-loeschen , 11
- 1.5.5 IPXCP-Statistik , 11
 - 1.5.5.1 Rx-Rejected , 11
 - 1.5.5.2 Rx-Config-Request , 12
 - 1.5.5.3 Rx-Config-Ack. , 12

- 1.5.5.4 Rx-Config-Nak. , 12
- 1.5.5.5 Rx-Config-Reject , 12
- 1.5.5.6 Rx-Termination-Request , 12
- 1.5.5.7 Rx-Termination-Ack. , 12
- 1.5.5.8 Rx-Code-Reject , 12
- 1.5.5.9 Tx-Config-Request , 12
- 1.5.5.10 Tx-Config-Ack. , 12
- 1.5.5.11 Tx-Config-Nak. , 12
- 1.5.5.12 Tx-Config-Reject , 12
- 1.5.5.13 Tx-Termination-Request , 12
- 1.5.5.14 Tx-Termination-Ack. , 12
- 1.5.5.15 Tx-Code-Reject , 12
- 1.5.5.16 Werte-loeschen , 12
- 1.5.6 IPCP-Statistik , 13
 - 1.5.6.1 Rx-Rejected , 13
 - 1.5.6.2 Rx-Config-Request , 13
 - 1.5.6.3 Rx-Config-Ack. , 13
 - 1.5.6.4 Rx-Config-Nak. , 13
 - 1.5.6.5 Rx-Config-Reject , 13
 - 1.5.6.6 Rx-Termination-Request , 13
 - 1.5.6.7 Rx-Termination-Ack. , 13
 - 1.5.6.8 Rx-Code-Reject , 13
 - 1.5.6.9 Tx-Config-Request , 13
 - 1.5.6.10 Tx-Config-Ack. , 13
 - 1.5.6.11 Tx-Config-Nak. , 13
 - 1.5.6.12 Tx-Config-Reject , 13
 - 1.5.6.13 Tx-Termination-Request , 13
 - 1.5.6.14 Tx-Termination-Ack. , 14
 - 1.5.6.15 Tx-Code-Reject , 14
 - 1.5.6.16 Werte-loeschen , 14
- 1.5.7 CBCP-Statistik , 14
 - 1.5.7.1 Rx-verworfen , 14
 - 1.5.7.2 Rx-Request , 14
 - 1.5.7.3 Rx-Response , 14
 - 1.5.7.4 Rx-Acknowledge , 14
 - 1.5.7.5 Tx-Request , 14
 - 1.5.7.6 Tx-Response , 14
 - 1.5.7.7 Tx-Acknowledge , 14
 - 1.5.7.8 Werte-loeschen , 14
- 1.5.8 RX-Optionen , 14
 - 1.5.8.1 LCP , 15
 - 1.5.8.2 IPXCP , 15
 - 1.5.8.3 IPCP , 15
- 1.5.9 TX-Optionen , 15
 - 1.5.9.1 LCP , 15
 - 1.5.9.2 IPXCP , 15
 - 1.5.9.3 IPCP , 16
- 1.5.10 CCP-Statistik , 16
 - 1.5.10.1 Rx-verworfen , 16

- 1.5.10.2 Rx-Config-Request , 16
- 1.5.10.3 Rx-Config-Ack. , 16
- 1.5.10.4 Rx-Config-Nak. , 16
- 1.5.10.5 Rx-Config-Reject , 16
- 1.5.10.6 Rx-Termination-Request , 16
- 1.5.10.7 Rx-Termination-Ack. , 16
- 1.5.10.8 Rx-Code-Reject , 16
- 1.5.10.9 Rx-Reset-Request , 16
- 1.5.10.10 Rx-Reset-Ack , 16
- 1.5.10.11 Tx-Config-Request , 17
- 1.5.10.12 Tx-Config-Ack. , 17
- 1.5.10.13 Tx-Config-Nak. , 17
- 1.5.10.14 Tx-Config-Reject , 17
- 1.5.10.15 Tx-Termination-Request , 17
- 1.5.10.16 Tx-Termination-Ack. , 17
- 1.5.10.17 Tx-Code-Reject , 17
- 1.5.10.18 , 17
- 1.5.10.19 Tx-Reset-Request , 17
- 1.5.10.20 Tx-Reset-Ack , 17
- 1.5.10.21 Werte-loeschen , 17
- 1.5.10.22 Kompressionsfehler , 17
- 1.5.11 ML-Statistik , 17
 - 1.5.11.1 Buendel-Verb , 17
 - 1.5.11.2 Rx-Seq-Verlust , 18
 - 1.5.11.3 Rx-Seq-Wiederholung , 18
 - 1.5.11.4 Rx-Mrru-Ueberlauf , 18
 - 1.5.11.5 Rx-Header-Fehler , 18
 - 1.5.11.6 Rx-verworfen , 18
 - 1.5.11.7 Rx-Frag-Start , 18
 - 1.5.11.8 Rx-Frag-Mid , 18
 - 1.5.11.9 Rx-Frag-Ende , 18
 - 1.5.11.10 Rx-unfragmentiert , 18
 - 1.5.11.11 Werte-loeschen , 18
- 1.5.12 BACP-Statistik , 18
 - 1.5.12.1 Rx-Fehler , 18
 - 1.5.12.2 Rx-verworfen , 18
 - 1.5.12.3 Rx-Call-Request , 18
 - 1.5.12.4 Rx-Call-Response , 19
 - 1.5.12.5 Rx-Callback-Request , 19
 - 1.5.12.6 Rx-Callback-Response , 19
 - 1.5.12.7 Rx-Link-Drop-Request , 19
 - 1.5.12.8 Rx-Link-Drop-Response , 19
 - 1.5.12.9 Rx-Status-Indication , 19
 - 1.5.12.10 Rx-Status-Response , 19
 - 1.5.12.11 Tx-Call-Request , 19
 - 1.5.12.12 Tx-Call-Response , 19
 - 1.5.12.13 Tx-Callback-Request , 19
 - 1.5.12.14 Tx-Callback-Response , 19
 - 1.5.12.15 Tx-Link-Drop-Request , 19

- 1.5.12.16 Tx-Link-Drop-Response , 19
 - 1.5.12.17 Tx-Status-Indication , 19
 - 1.5.12.18 Tx-Status-Response , 20
 - 1.5.12.19 Werte-loeschen , 20
- 1.6 Bridge-Statistik , 20
 - 1.6.1 Brg-LAN-Rx , 20
 - 1.6.2 Brg-LAN-Tx , 20
 - 1.6.3 Brg-LAN-Filter , 20
 - 1.6.4 Brg-LAN-Broadcasts , 20
 - 1.6.5 Brg-LAN-Multicasts , 20
 - 1.6.6 Brg-WAN-Tx , 20
 - 1.6.7 Brg-WAN-Rx , 20
 - 1.6.8 Brg-WAN-Filter , 20
 - 1.6.9 Brg-WAN-Broadcasts , 20
 - 1.6.10 Brg-WAN-Multicasts , 20
 - 1.6.11 Brg-Adressen , 20
 - 1.6.12 Tabelle-Bridge , 21
 - 1.6.13 Aufbau-Tabelle , 21
 - 1.6.14 Werte-loeschen , 21
- 1.7 IPX-Statistik , 21
 - 1.7.1 MAC-Statistik , 21
 - 1.7.1.1 IPX-LAN-Rx , 21
 - 1.7.1.2 IPX-LAN-Rx-Broadcasts , 21
 - 1.7.1.3 IPX-LAN-Rx-Multicasts , 21
 - 1.7.1.4 IPX-LAN-Rx-Unicasts , 21
 - 1.7.1.5 IPX-LAN-Tx , 21
 - 1.7.1.6 IPX-WAN-Rx , 21
 - 1.7.1.7 IPX-WAN-Rx-Broadcasts , 21
 - 1.7.1.8 IPX-WAN-Rx-Multicasts , 21
 - 1.7.1.9 IPX-WAN-Rx-Unicasts , 21
 - 1.7.1.10 IPX-WAN-Tx , 22
 - 1.7.1.11 Werte-loeschen , 22
 - 1.7.2 Watchdog-Statistik , 22
 - 1.7.2.1 IPX-Watchdog-LAN-Rx , 22
 - 1.7.2.2 IPX-Watchdog-LAN-Tx , 22
 - 1.7.2.3 IPX-Watchdog-WAN-Rx , 22
 - 1.7.2.4 IPX-Watchdog-WAN-Tx , 22
 - 1.7.2.5 SPX-Watchdog-LAN-Rx , 22
 - 1.7.2.6 SPX-Watchdog-LAN-Tx , 22
 - 1.7.2.7 SPX-Watchdog-WAN-Rx , 22
 - 1.7.2.8 SPX-Watchdog-WAN-Tx , 22
 - 1.7.2.9 Werte-loeschen , 22
 - 1.7.3 Propagate-Statistik , 22
 - 1.7.3.1 Propagate-LAN-Rx , 22
 - 1.7.3.2 Propagate-LAN-Filter , 22
 - 1.7.3.3 Propagate-LAN-Tx , 23
 - 1.7.3.4 Propagate-LAN-Socket-Fehler , 23
 - 1.7.3.5 Propagate-LAN-Hop-Fehler , 23
 - 1.7.3.6 Propagate-LAN-Backroute-Fehler , 23

- 1.7.3.7 Propagate-LAN-Contention , 23
- 1.7.3.8 Propagate-WAN-Rx , 23
- 1.7.3.9 Propagate-WAN-Filter , 23
- 1.7.3.10 Propagate-WAN-Tx , 23
- 1.7.3.11 Propagate-WAN-Socket-Fehler , 23
- 1.7.3.12 Werte-loeschen , 23
- 1.7.4 RIP-Statistik , 23
 - 1.7.4.1 RIP-LAN-Rx , 23
 - 1.7.4.2 RIP-LAN-Fehler , 23
 - 1.7.4.3 RIP-LAN-Tx , 23
 - 1.7.4.4 RIP-WAN-Rx , 23
 - 1.7.4.5 RIP-WAN-Fehler , 24
 - 1.7.4.6 RIP-WAN-Tx , 24
 - 1.7.4.7 Tabelle-RIP , 24
 - 1.7.4.8 Werte-loeschen , 24
- 1.7.5 SAP-Statistik , 24
 - 1.7.5.1 SAP-LAN-Rx , 24
 - 1.7.5.2 SAP-LAN-Fehler , 24
 - 1.7.5.3 SAP-LAN-Tx , 24
 - 1.7.5.4 SAP-WAN-Rx , 24
 - 1.7.5.5 SAP-WAN-Fehler , 24
 - 1.7.5.6 SAP-WAN-Tx , 24
 - 1.7.5.7 Tabelle-SAP , 24
 - 1.7.5.8 Werte-loeschen , 25
- 1.7.6 IPX-Router-Statistik , 25
 - 1.7.6.1 IPXr-LAN-Rx , 25
 - 1.7.6.2 IPXr-LAN-Tx , 25
 - 1.7.6.3 IPXr-LAN-Hop-Fehler. , 25
 - 1.7.6.4 IPXr-LAN-Socket-Fehler , 25
 - 1.7.6.5 IPXr-LAN-Netzwerk-Fehler , 25
 - 1.7.6.6 IPXr-LAN-Backroute-Fehler , 25
 - 1.7.6.7 IPXr-LAN-Contention , 25
 - 1.7.6.8 IPXr-LAN-Down-Fehler , 25
 - 1.7.6.9 IPXr-WAN-Rx , 25
 - 1.7.6.10 IPXr-WAN-Tx , 25
 - 1.7.6.11 IPXr-WAN-Hop-Fehler. , 26
 - 1.7.6.12 IPXr-WAN-Socket-Fehler , 26
 - 1.7.6.13 IPXr-WAN-Netzwerk-Fehler , 26
 - 1.7.6.14 IPXr-WAN-Backroute-Fehler , 26
 - 1.7.6.15 IPXr-WAN-Down-Fehler , 26
 - 1.7.6.16 IPXr-Int-Rx , 26
 - 1.7.6.17 Netzwerke , 26
 - 1.7.6.18 Aufbau-Tabelle , 27
 - 1.7.6.19 Werte-loeschen , 27
- 1.8 TCP-IP-Statistik , 27
 - 1.8.1 ARP-Statistik , 27
 - 1.8.1.1 ARP-LAN-Rx , 27
 - 1.8.1.2 ARP-LAN-Tx , 27
 - 1.8.1.3 ARP-LAN-Fehler , 27

- 1.8.1.4 ARP-WAN-Rx , 28
- 1.8.1.5 ARP-WAN-Tx , 28
- 1.8.1.6 ARP-WAN-Fehler , 28
- 1.8.1.7 Tabelle-ARP , 28
- 1.8.1.8 Werte-loeschen , 28
- 1.8.2 IP-Statistik , 28
 - 1.8.2.1 IP-LAN-Rx , 28
 - 1.8.2.2 IP-LAN-Tx , 28
 - 1.8.2.3 IP-LAN-Checksummen-Fehler , 28
 - 1.8.2.4 IP-LAN-Service-Fehler , 28
 - 1.8.2.5 IP-WAN-Rx , 28
 - 1.8.2.6 IP-WAN-Tx , 28
 - 1.8.2.7 IP-WAN-Checksummen-Fehler , 28
 - 1.8.2.8 IP-WAN-Service-Fehler , 29
 - 1.8.2.9 IP-WAN-Rx-verworfen , 29
 - 1.8.2.10 IP-LAN-Fragmentierungs-Fehler , 29
 - 1.8.2.11 IP-WAN-Fragmentierungs-Fehler , 29
 - 1.8.2.12 Werte-loeschen , 29
 - 1.8.2.13 IP-LAN-Fragmentierungen , 29
 - 1.8.2.14 IP-LAN-Fragmentierung-erzwungen , 29
 - 1.8.2.15 IP-WAN-Fragmentierungen , 29
 - 1.8.2.16 IP-WAN-Fragmentierung-erzwungen , 29
- 1.8.3 ICMP-Statistik , 29
 - 1.8.3.1 ICMP-LAN-Rx , 29
 - 1.8.3.2 ICMP-LAN-Tx , 29
 - 1.8.3.3 ICMP-LAN-Checksummen-Fehler , 29
 - 1.8.3.4 ICMP-LAN-Service-Fehler , 29
 - 1.8.3.5 ICMP-WAN-Rx , 29
 - 1.8.3.6 ICMP-WAN-Tx , 30
 - 1.8.3.7 ICMP-WAN-Checksummen-Fehler , 30
 - 1.8.3.8 ICMP-WAN-Service-Fehler , 30
 - 1.8.3.9 Werte-loeschen , 30
- 1.8.4 TFTP-Statistik , 30
 - 1.8.4.1 TFTP-LAN-Rx , 30
 - 1.8.4.2 TFTP-LAN-Rx-Read-Request , 30
 - 1.8.4.3 TFTP-LAN-Rx-Write-Request , 30
 - 1.8.4.4 TFTP-LAN-Rx-Data , 30
 - 1.8.4.5 TFTP-LAN-Rx-Ack. , 30
 - 1.8.4.6 TFTP-LAN-Rx-Option-Ack. , 30
 - 1.8.4.7 TFTP-LAN-Rx-Fehler , 30
 - 1.8.4.8 TFTP-LAN-Rx-Unb. , 30
 - 1.8.4.9 TFTP-LAN-Tx , 30
 - 1.8.4.10 TFTP-LAN-Tx-Data , 30
 - 1.8.4.11 TFTP-LAN-Tx-Ack. , 31
 - 1.8.4.12 TFTP-LAN-Tx-Option-Ack. , 31
 - 1.8.4.13 TFTP-LAN-Tx-Fehler , 31
 - 1.8.4.14 TFTP-LAN-Tx-Wiederholungen , 31
 - 1.8.4.15 TFTP-LAN-Verbindungen , 31
 - 1.8.4.16 TFTP-WAN-Rx , 31

- 1.8.4.17 TFTP-WAN-Rx-Read-Request , 31
- 1.8.4.18 TFTP-WAN-Rx-Write-Request , 31
- 1.8.4.19 TFTP-WAN-Rx-Data , 31
- 1.8.4.20 TFTP-WAN-Rx-Ack. , 31
- 1.8.4.21 TFTP-WAN-Rx-Option-Ack. , 31
- 1.8.4.22 TFTP-WAN-Rx-Fehler , 31
- 1.8.4.23 TFTP-WAN-Rx-Unb. , 31
- 1.8.4.24 TFTP-WAN-Tx , 31
- 1.8.4.25 TFTP-WAN-Tx-Data , 31
- 1.8.4.26 TFTP-WAN-Tx-Ack. , 32
- 1.8.4.27 TFTP-WAN-Tx-Option-Ack. , 32
- 1.8.4.28 TFTP-WAN-Tx-Fehler , 32
- 1.8.4.29 TFTP-WAN-Tx-Wiederholungen , 32
- 1.8.4.30 TFTP-WAN-Verbindungen , 32
- 1.8.4.31 Werte-loeschen , 32
- 1.8.5 TCP-Statistik , 32
 - 1.8.5.1 TCP-LAN-Rx , 32
 - 1.8.5.2 TCP-LAN-Tx , 32
 - 1.8.5.3 TCP-LAN-Tx-Wdh. , 32
 - 1.8.5.4 TCP-LAN-Checksummen-Fehler , 32
 - 1.8.5.5 TCP-LAN-Service-Fehler , 32
 - 1.8.5.6 TCP-LAN-Verbindungen , 32
 - 1.8.5.7 TCP-WAN-Rx , 32
 - 1.8.5.8 TCP-WAN-Tx , 32
 - 1.8.5.9 TCP-WAN-Tx-Wiederholungen , 33
 - 1.8.5.10 TCP-WAN-Checksummen-Fehler , 33
 - 1.8.5.11 TCP-WAN-Service-Fehler , 33
 - 1.8.5.12 TCP-WAN-Verbindungen , 33
 - 1.8.5.13 Werte-loeschen , 33
- 1.8.6 DHCP-Statistik , 33
 - 1.8.6.1 DHCP-LAN-Rx , 33
 - 1.8.6.2 DHCP-LAN-Tx , 33
 - 1.8.6.3 DHCP-WAN-Rx , 33
 - 1.8.6.4 DHCP-Verworfen , 33
 - 1.8.6.5 DHCP-Rx-Discover , 33
 - 1.8.6.6 DHCP-Rx-Request , 33
 - 1.8.6.7 DHCP-Rx-Denial , 33
 - 1.8.6.8 DHCP-Rx-Inform , 33
 - 1.8.6.9 DHCP-Rx-Release , 33
 - 1.8.6.10 DHCP-Tx-Offer , 34
 - 1.8.6.11 DHCP-Tx-Ack. , 34
 - 1.8.6.12 DHCP-Tx-Nak , 34
 - 1.8.6.13 DHCP-Server-Fehler , 34
 - 1.8.6.14 DHCP-Zugewiesen , 34
 - 1.8.6.15 DHCP-MAC-Konflikte , 34
 - 1.8.6.16 Tabelle-DHCP , 34
 - 1.8.6.17 Server-Flags , 34
 - 1.8.6.18 Werte-loeschen , 34
- 1.8.7 Kein Eintrag , 34

- 1.8.8 NetBIOS-Statistik , 34
 - 1.8.8.1 LAN-Rx , 35
 - 1.8.8.2 LAN-Tx , 35
 - 1.8.8.3 WAN-Rx , 35
 - 1.8.8.4 WAN-Tx , 35
 - 1.8.8.5 Registrierungen , 35
 - 1.8.8.6 Konflikte , 35
 - 1.8.8.7 Freigaben , 35
 - 1.8.8.8 Erneuerungen , 35
 - 1.8.8.9 Timeouts , 35
 - 1.8.8.10 Hosts , 35
 - 1.8.8.11 Gruppen , 35
 - 1.8.8.12 B-Knoten , 35
 - 1.8.8.13 P-Knoten , 35
 - 1.8.8.14 M-Knoten , 36
 - 1.8.8.15 W-Knoten , 36
 - 1.8.8.16 Gegenstellen-Tab. , 36
 - 1.8.8.17 Werte-loeschen , 36
- 1.8.9 DNS-Statistik , 36
 - 1.8.9.1 LAN-Rx , 36
 - 1.8.9.2 LAN-Tx , 36
 - 1.8.9.3 WAN-Rx , 36
 - 1.8.9.4 WAN-Tx , 36
 - 1.8.9.5 Forwarded , 36
 - 1.8.9.6 Fehler , 36
 - 1.8.9.7 DNS-Zugriffe , 37
 - 1.8.9.8 DHCP-Zugriffe , 37
 - 1.8.9.9 NetBIOS-Zugriffe , 37
 - 1.8.9.10 Filter , 37
 - 1.8.9.11 Hit-Liste , 37
 - 1.8.9.12 Werte-loeschen , 37
- 1.8.10 HTTP-Statistik , 37
 - 1.8.10.1 HTTP-Zugriffe , 37
 - 1.8.10.2 HTTP-nichtgefunden-Fehler , 37
 - 1.8.10.3 HTTP-Authentisierungs-Fehler , 38
 - 1.8.10.4 HTTP-Protokoll-Fehler , 38
 - 1.8.10.5 Werte-loeschen , 38
- 1.9 IP-Router-Statistik , 38
 - 1.9.1 IPr-LAN-Rx , 38
 - 1.9.2 IPr-LAN-Tx , 38
 - 1.9.3 IPr-LAN-lokales-Routing , 38
 - 1.9.4 IPr LAN-Netzwerk-Fehler , 38
 - 1.9.5 IPr-LAN-Routing-Fehler , 38
 - 1.9.6 IPr-LAN-TTL-Fehler , 38
 - 1.9.7 IPr-LAN-Filter , 38
 - 1.9.8 IPr-LAN-verworfen , 38
 - 1.9.9 IPr-WAN-Rx , 38
 - 1.9.10 IPr-WAN-Tx , 39
 - 1.9.11 IPr-WAN-Netzwerk-Fehler , 39

- 1.9.12 IPr-WAN-TTL-Fehler , 39
- 1.9.13 IPr-WAN-Filter , 39
- 1.9.14 IPr-WAN-verworfen , 39
- 1.9.15 IPr-WAN-Typ-Fehler , 39
- 1.9.16 IPr-ARP-Fehler , 39
- 1.9.17 Aufbau-Tabelle , 39
- 1.9.18 Protokoll-Tabelle , 39
- 1.9.19 RIP-Statistik , 40
 - 1.9.19.1 RIP-Rx , 40
 - 1.9.19.2 RIP-Request , 40
 - 1.9.19.3 RIP-Response , 40
 - 1.9.19.4 RIP-verworfen , 40
 - 1.9.19.5 RIP-Fehler , 40
 - 1.9.19.6 RIP-Eintrag-Fehler , 40
 - 1.9.19.7 RIP-Tx , 40
 - 1.9.19.8 Tabelle-RIP , 40
 - 1.9.19.9 Werte-loeschen , 41
- 1.9.20 Werte-loeschen , 41
- 1.9.21 Service-Tabelle , 41
- 1.10 Config-Statistik , 41
 - 1.10.1 LAN-Akt.-Verbindungen , 41
 - 1.10.2 LAN-Ges.-Verbindungen , 41
 - 1.10.3 WAN-Akt.-Verbindungen , 41
 - 1.10.4 WAN-Ges.-Verbindungen , 42
 - 1.10.5 Outband-Akt.-Verbindungen , 42
 - 1.10.6 Outband-Ges.-Verbindungen , 42
 - 1.10.7 Outband-Bitrate , 42
 - 1.10.8 Login-Fehler , 42
 - 1.10.9 Login-Sperren , 42
 - 1.10.10 Login-Ablehnungen , 42
 - 1.10.11 Werte-loeschen , 42
- 1.11 Queue-Statistik , 42
 - 1.11.1 LAN-Heap-Pakete , 42
 - 1.11.2 LAN-Queue-Pakete , 42
 - 1.11.3 WAN-Heap-Pakete , 42
 - 1.11.4 WAN-Queue-Pakete , 42
 - 1.11.5 ARP-Query-Queue-Pakete , 42
 - 1.11.6 ARP-Queue-Pakete , 43
 - 1.11.7 IP-Queue-Pakete , 43
 - 1.11.8 IP-Urgent-Queue-Pakete , 43
 - 1.11.9 ICMP-Queue-Pakete , 43
 - 1.11.10 TCP-Queue-Pakete , 43
 - 1.11.11 TFTP-Queue-Pakete , 43
 - 1.11.12 SNMP-Queue-Pakete , 43
 - 1.11.13 Prot-Heap-Pakete , 43
 - 1.11.14 IPR-Queue-Pakete , 43
 - 1.11.15 DHCP-Server-Queue-Pakete , 43
 - 1.11.16 IPR-RIP-Queue-Pakete , 43
 - 1.11.17 DNS-Sende-Queue , 43

- 1.11.18 DNS-Empfangs-Queue , 43
- 1.11.19 IP-Masq. Sende-Queue , 43
- 1.11.20 IP-Masq. Empfangs-Queue , 44
- 1.11.21 WLAN-Management-Heap-Pakete , 44
- 1.11.22 PROT-Heap-Pakete , 44
- 1.11.23 Kein Eintrag , 44
- 1.11.24 IPR-Queue-Pakete , 44
- 1.11.25 Kein Eintrag , 44
- 1.11.26 Kein Eintrag , 44
- 1.11.27 DHCP-Server-Queue-Pakete , 44
- 1.11.28 DHCP-client-queue-packets , 44
- 1.11.29 IPR-RIP-Queue-Pakete , 44
- 1.11.30 DNS-Sende-Queue , 44
- 1.11.31 DNS-Empfangs-Queue , 44
- 1.11.32 IP-Masq. Sende-Queue , 44
- 1.11.33 IP-Masq. Empfangs-Queue , 44
- 1.12 Verbindungs-Statistik , 45
- 1.13 Info-Verbindung , 45
- 1.14 Layer-Verbindung , 46
- 1.15 Ruf-Info-Tabelle , 46
- 1.16 Gegenst.-Statistik , 47
- 1.17 Aktuelle-Zeit , 48
- 1.18 Kanal-Statistik , 48
- 1.19 Werte loeschen , 49
- 1.20 Zeit-Statistik , 49
 - 1.20.1 Aktuelle Zeit , 50
 - 1.20.2 Quelle , 50
 - 1.20.3 Übernahme , 50
 - 1.20.4 ISDN , 50
 - 1.20.4.1 Verbindungen , 50
 - 1.20.4.2 Informationen , 50
 - 1.20.4.3 Infofehler , 50
 - 1.20.4.4 Einheiten , 50
 - 1.20.4.5 Werte-loeschen , 50
- 1.21 LCR-Statistik , 50
 - 1.21.1 Gesamtaufrufe , 50
 - 1.21.2 Erfolge , 50
 - 1.21.3 nicht-gefunden-Fehler , 51
 - 1.21.4 fehlende-Zeit-Fehler , 51
 - 1.21.5 Kein Eintrag , 51
 - 1.21.6 Provider-Statistik , 51
 - 1.21.7 Werte-loeschen , 51
- 1.22 S0-Bus , 51
 - 1.22.1 D-Info , 51
 - 1.22.2 D2-Statistik , 51
- 1.23 Gebuehren-Stat. , 52
 - 1.23.1 Rest-Minuten , 52
 - 1.23.2 Zeit-Tabelle , 52
 - 1.23.3 Werte-loeschen , 52

- 1.23.4 Rest-Budget , 52
- 1.23.5 Tabelle-Budget , 52
- 1.23.6 Resttage/Per. , 52
- 1.23.7 Router-Einheiten , 52
- 1.23.8 Gesamt-Einheiten , 52
- 1.23.9 Router-Minuten-aktiv , 52
- 1.24 Kein Eintrag , 52
- 1.25 Kein Eintrag , 52
- 1.26 Kein Eintrag , 52
- 1.27 Kein Eintrag , 53
- 1.28 Kein Eintrag , 53
- 1.29 Kein Eintrag , 53
- 1.30 Kein Eintrag , 53
- 1.31 DHCP-Client-Status , 53
 - 1.31.1 Status , 53
 - 1.31.2 Lease-Zeit [Sekunden] , 53
 - 1.31.3 Zugewiesene-IP-Adresse , 53
 - 1.31.4 Zugewiesene-IP-Netzmaske , 53
 - 1.31.5 Gateway-IP-Adresse , 53
 - 1.31.6 Server-IP-Adresse , 53
 - 1.31.7 Security-Server , 53
 - 1.31.8 Zeit-Offset , 53
 - 1.31.9 Zeit-Server , 54
 - 1.31.10 Tabelle-Zeit-Server , 54
 - 1.31.11 Tabelle-Router , 54
 - 1.31.12 Tabelle-Name-Server , 54
 - 1.31.13 Tabelle-Domain-Name-Server , 54
 - 1.31.14 Tabelle-Log-Server , 54
 - 1.31.15 Konfigurations-Datei , 54
- 1.32 Kein Eintrag , 54
- 1.33 Kein Eintrag , 54
- 1.34 Kein Eintrag , 54
- 1.35 Kein Eintrag , 54
- 1.36 Kein Eintrag , 54
- 1.37 Kein Eintrag , 54
- 1.38 Kein Eintrag , 55
- 1.39 Kein Eintrag , 55
- 2 Setup , 56
 - 2.1 Name , 56
 - 2.2 WAN-Modul , 56
 - 2.2.1 Kein Eintrag , 56
 - 2.2.2 Namenliste , 56
 - 2.2.3 Round-Robin-Liste , 58
 - 2.2.4 Layerliste , 59
 - 2.2.5 PPP-Liste , 60
 - 2.2.6 Nummernliste , 61
 - 2.2.7 Kein Eintrag , 62
 - 2.2.8 Script-Liste , 62
 - 2.2.9 Schutz , 62

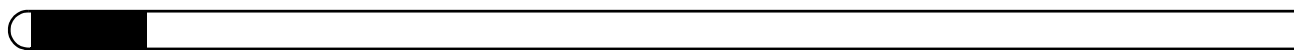
- 2.2.10 RR-Versuche , 63
- 2.2.11 Router-Interface-Liste , 63
- 2.2.12 Kein Eintrag , 63
- 2.2.13 Manuelle-Wahl , 64
 - 2.2.13.1 Aufbau , 64
 - 2.2.13.2 Abbau , 64
 - 2.2.13.3 Status , 64
- 2.2.14 Interface-Liste , 64
- 2.2.15 Festverbindung , 65
- 2.2.16 Kanal-Liste , 65
- 2.2.17 ISDN-Namenliste , 65
- 2.2.18 DSL-Namenliste , 67
- 2.2.19 Verkehrskontrakte , 68
- 2.3 Gebühren-Modul , 68
 - 2.3.1 Budget-Einheiten , 68
 - 2.3.2 Tage/Periode , 68
 - 2.3.3 Rest-Budget , 68
 - 2.3.4 Router-Einheiten , 68
 - 2.3.5 Tabelle-Budget , 68
 - 2.3.6 Gesamt-Einheiten , 68
 - 2.3.7 Zeit-Tabelle , 68
 - 2.3.8 Minuten-Budget , 68
 - 2.3.9 Rest-Minuten , 68
 - 2.3.10 Router-Minuten , 68
 - 2.3.11 Aktivieren-Reserve , 68
- 2.4 LAN-Modul , 69
 - 2.4.1 Anschluß , 69
 - 2.4.2 Node-ID , 69
 - 2.4.3 Heap-Reserve , 69
- 2.5 Bridge-Modul , 69
 - 2.5.1 Zustand , 69
 - 2.5.2 Gegenstelle , 69
 - 2.5.3 Bridge-Tabelle , 69
 - 2.5.4 Aging-Minute(n) , 69
 - 2.5.5 LAN-Einstellung , 69
 - 2.5.5.1 Broadcast , 70
 - 2.5.5.2 Multicast , 70
 - 2.5.5.3 Ziel-Adresse , 70
 - 2.5.5.4 Quell-Adresse , 70
 - 2.5.6 WAN-Einstellung , 70
 - 2.5.6.1 Broadcast , 70
 - 2.5.6.2 Multicast , 70
 - 2.5.6.3 Ziel-Adresse , 70
 - 2.5.6.4 Quell-Adresse , 71
- 2.6 IPX-Modul , 71
 - 2.6.1 Zustand , 71
 - 2.6.2 IPX-Router , 71
 - 2.6.3 LAN-Einstellung , 71
 - 2.6.3.1 Netzwerk , 71

- 2.6.3.2 Binding , 72
- 2.6.3.3 SPX-Watchdog , 72
- 2.6.3.4 IPX-Watchdog , 72
- 2.6.3.5 NetBIOS-Watch , 72
- 2.6.3.6 Socket-Filter , 72
- 2.6.3.7 Lok.-Routing , 73
- 2.6.3.8 2.6.3.8RIP-SAP-Skal. , 73
- 2.6.3.9 LOOP-propagieren , 73
- 2.6.4 WAN-Einstellung , 74
 - 2.6.4.1 Routing-Tabelle , 74
 - 2.6.4.2 Socket-Filter , 75
- 2.6.5 RIP-Einstellung , 75
 - 2.6.5.1 Tabelle-RIP , 75
 - 2.6.5.2 LAN-Filtertab. , 75
 - 2.6.5.3 WAN-Filtertab. , 75
 - 2.6.5.4 Routen/Frm , 76
 - 2.6.5.5 Aging-Minute(n) , 76
 - 2.6.5.6 Spoofing , 76
 - 2.6.5.7 WAN-Update-Min. , 76
- 2.6.6 SAP-Einstellung , 77
 - 2.6.6.1 Tabelle-SAP , 77
 - 2.6.6.2 LAN-Filtertab. , 77
 - 2.6.6.3 WAN-Filtertab. , 77
 - 2.6.6.4 Server/Frm , 78
 - 2.6.6.5 Aging-Minute(n) , 78
 - 2.6.6.6 Spoofing , 78
 - 2.6.6.7 WAN-Update-Min. , 78
- 2.7 TCP-IP-Modul , 79
 - 2.7.1 Zustand , 79
 - 2.7.2 IP-Adresse , 79
 - 2.7.3 IP-Netz-Maske , 80
 - 2.7.4 Intranet-Adr. , 80
 - 2.7.5 Intranet-Maske , 80
 - 2.7.6 Zugangsliste , 80
 - 2.7.7 DNS-Default , 81
 - 2.7.8 DNS-Backup , 81
 - 2.7.9 NBNS-Default , 81
 - 2.7.10 NBNS-Backup , 82
 - 2.7.11 ARP-Aging-Min , 82
 - 2.7.12 TCP-Aging-Min , 82
 - 2.7.13 TCP-Max.-Verb. , 82
 - 2.7.14 Cable-IP-Adresse , 82
 - 2.7.15 Cable-IP-Netz-Maske , 82
 - 2.7.16 Tabelle-ARP , 82
 - 2.7.17 LAN-IP-Adresse , 83
 - 2.7.18 LAN-IP-Maske , 83
- 2.8 IP-Router-Modul , 83
 - 2.8.1 Zustand , 83
 - 2.8.2 IP-Routing-Tabelle , 83

- 2.8.3 Kein Eintrag , 85
- 2.8.4 Kein Eintrag , 86
- 2.8.5 Proxy-ARP , 86
- 2.8.6 Lok.-Routing , 86
- 2.8.7 Routing-Methode , 86
 - 2.8.7.1 Routing-Methode , 86
 - 2.8.7.2 ICMP-Routing-Methode , 86
- 2.8.8 RIP-Einstellungen , 87
 - 2.8.8.1 RIP-Typ , 87
 - 2.8.8.2 R1-Maske , 87
 - 2.8.8.3 Tabelle-RIP , 87
- 2.8.9 Masquerading , 88
 - 2.8.9.1 TCP-Aging-Sekunde(n) , 88
 - 2.8.9.2 UDP-Aging-Sekunde(n) , 88
 - 2.8.9.3 ICMP-Aging-Sekunde(n) , 88
 - 2.8.9.4 Service-Tabelle , 88
 - 2.8.9.5 Tabelle-Masquerading , 89
- 2.8.10 Firewall , 89
 - 2.8.10.1 Objekt-Tabelle , 89
 - 2.8.10.2 Regel-Tabelle , 90
 - 2.8.10.3 Filter-Liste , 92
- 2.8.11 Kein Eintrag , 93
- 2.8.12 Kein Eintrag , 93
- 2.8.13 Default-Zeittabelle , 93
- 2.8.14 Nutzung-Default-Listen , 93
- 2.8.15 LAN-Filtertab. , 93
- 2.8.16 WAN-Filtertab. , 94
- 2.8.17 Start-Adreß-Pool , 95
- 2.8.18 Ende-Adreß-Pool , 95
- 2.9 SNMP-Modul , 95
 - 2.9.1 Traps-senden , 96
 - 2.9.2 IP-Trap-Tabelle , 96
 - 2.9.3 Administrator , 96
 - 2.9.4 Standort , 96
 - 2.9.5 Register-Monitor , 96
 - 2.9.6 Loesche-Monitor , 96
 - 2.9.7 Monitor-Tabelle , 96
 - 2.9.8 Kein Eintrag , 97
 - 2.9.9 Kein Eintrag , 97
 - 2.9.10 Passw.Zwang-fuer-SNMP-leszugriff , 97
- 2.10 DHCP-Modul , 97
 - 2.10.1 Zustand , 97
 - 2.10.2 Start-Adreß-Pool (Ende-Adreß-Pool) , 97
 - 2.10.3 (Start-Adreß-Pool) Ende-Adreß-Pool , 98
 - 2.10.4 Netz-Maske , 99
 - 2.10.5 Broadcast-Adresse , 99
 - 2.10.6 Max.-Gültigkeit-Minute(n) , 99
 - 2.10.7 Default-Gültigkeit-Minute(n) , 99
 - 2.10.8 Tabelle-DHCP , 99

- 2.10.9 Host-Tabelle , 100
- 2.10.10 Alias-Tabelle , 100
- 2.10.11 Kein Eintrag , 100
- 2.10.12 Master-Server , 100
- 2.10.13 Reply-Anpassung , 100
- 2.10.14 Gateway-Adresse , 100
- 2.10.15 Relay-Cache , 100
- 2.11 Config-Modul , 100
 - 2.11.1 LAN-Config , 101
 - 2.11.2 WAN-Config , 101
 - 2.11.3 Passw.Zwang , 101
 - 2.11.4 Maximale-Verb. , 101
 - 2.11.5 Conf.-Aging-Min. , 101
 - 2.11.6 Sprache , 101
 - 2.11.7 Login-Fehler , 101
 - 2.11.8 Sperr-Minuten , 102
 - 2.11.9 Fernconfig-(EAZ-MSN) , 102
- 2.12 ab-Modul , 102
 - 2.12.1 Port-Liste , 102
 - 2.12.2 Amtsholung-Liste , 102
 - 2.12.3 Amtsberechtigung-Liste , 102
 - 2.12.4 Prioritaeten-Liste , 102
 - 2.12.5 Klingelfolge , 102
 - 2.12.6 Land , 102
- 2.13 *LANCAPI*-Modul , 102
 - 2.13.1 **Zugangsliste** , 103
 - 2.13.2 **Kein Eintrag** , 103
 - 2.13.3 **UDP-Port** , 103
 - 2.13.4 **Kein Eintrag** , 103
 - 2.13.5 Kein Eintrag , 103
 - 2.13.6 **Interface-Tabelle** , 103
 - 2.13.7 **Prioritaeten-Tabelle** , 103
- 2.14 Zeit-Modul , 104
 - 2.14.1 Zustand , 104
 - 2.14.2 Aktuelle-Zeit , 104
 - 2.14.3 Zeit-Rufnummer , 104
 - 2.14.4 Kein Eintrag , 104
 - 2.14.5 Anwahl-Versuche , 104
- 2.15 LCR-Modul , 104
 - 2.15.1 Router-Nutzung , 105
 - 2.15.2 Lancapi-Nutzung , 105
 - 2.15.3 ab-Port-Nutzung , 105
 - 2.15.4 Zeittabelle , 105
 - 2.15.5 Feiertagstabelle , 106
- 2.16 NetBIOS-Modul , 106
 - 2.16.1 Zustand , 106
 - 2.16.2 Scope-ID , 107
 - 2.16.3 NT-Domaene , 107
 - 2.16.4 Gegenstellen-Tab. , 107

- 2.16.5 Host-Tabelle , 107
 - 2.16.6 Gruppentabelle , 108
- 2.17 DNS-Modul , 109
 - 2.17.1 Zustand , 109
 - 2.17.2 Domaene , 109
 - 2.17.3 DHCP-verwenden , 109
 - 2.17.4 NetBIOS-verw. , 110
 - 2.17.5 DNS-Tabelle , 110
 - 2.17.6 Filter-Liste , 110
 - 2.17.7 Gueltigkeit , 110
- 2.18 Accounting-Modul , 111
- 2.19 Kein Eintrag , 112
 - 2.19.1 Kein Eintrag , 112
 - 2.19.2 Kein Eintrag , 112
- 2.20 HTTP-Modul , 112
 - 2.20.1 Dokumentenwurzel , 112
- 2.21 SYSLOG-Modul , 112
 - 2.21.1 Zustand , 112
 - 2.21.2 Tabelle-SYSLOG , 112
 - 2.21.3 Facility-Mapper , 114
 - 2.21.4 Port , 114
- 3 Firmware , 115
 - 3.1 Versions-Tabelle , 115
 - 3.2 Tabelle-Firmsafe , 115
 - 3.3 Modus-Firmsafe , 115
 - 3.4 Timeout-Firmsafe , 116
- 4 Sonstiges , 117
 - 4.1 Manuelle Wahl , 117
 - 4.1.1 Aufbau , 117
 - 4.1.2 Abbau , 117
 - 4.1.3 Status , 117
 - 4.2 System-Boot , 117
 - 4.3 System-Reset , 117
 - 4.4 System-Upload , 117



1 Status

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

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

1.1 Verbindung

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

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

1.2 Betriebszeit

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

1.3 WAN-Statistik

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

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

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

1.3.1 Byte-Transport-Statistik

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

1.3.2 Paket-Transport-Statistik

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

1.3.3 Fehler-Statistik

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

1.3.4 WAN-TX-verworfen

Anzahl durch Fehler/Ressourcenmangel verworfener Pakete

1.3.5 WAN-Heap-Pakete

Anzahl belegter Puffer

1.3.6 WAN-Queue-Pakete

Anzahl verfügbarer Puffer

1.3.7 WAN-Queue-Fehler

Anzahl durch Puffermangel verworfener Datenpakete

1.3.8 Durchsatz-Statistik

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

lfc	Rx aktuell	Tx aktuell	Rx gemittelt	Tx gemittelt
Ch01	0	0	0	0
Ch02	0	0	0	0

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

1.3.9 Werte-loeschen

Löschen der WAN-Statistik

1.4 LAN-Statistik

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

/LAN-Statistik	Fortlaufende Statusanzeigen
LAN-Rx-Pakete	Anzahl empfangener Datenpakete
LAN-Tx-Pakete	Anzahl gesendeter Datenpakete
LAN-Rx-Fehler	Anzahl fehlerhaft empfangener Datenpakete
LAN-Tx-Fehler	Anzahl fehlerhaft gesendeter Datenpakete
LAN-Stack-Fehler	Anzahl Pakete ohne passendes Empfangsmodul (Bridge/Router)
LAN-NIC-Fehler	Anzahl vom NIC verworfener Datenpakete
LAN-Heap-Pakete	Anzahl verfügbarer Puffer
LAN-Queue-Pakete	Anzahl belegter Puffer
LAN-Queue-Fehler	Anzahl durch Puffermangel verworfener Pakete
LAN-Kollisionen	Anzahl Kollisionen während des Sendevorgangs
Verbindung-aufgebaut	Anzeige der korrekten Verbindung auf dem Ethernet (Datenübertragung möglich). Entspricht der 'Link'-LED am Gerät.
Verhandlung-abgeschlossen	Die Aushandlung der Übertragungsart zwischen Gerät und Gegenstelle ist abgeschlossen.
Anschluß	Anzeige des Netzwerkanschlusses
LAN-Rx-Bytes	Anzahl vom LAN empfangener Zeichen
LAN-Tx-Bytes	Anzahl zum LAN gesendeter Zeichen
LAN-Rx-Broadcasts	Anzahl vom LAN empfangener Broadcast-Pakete
LAN-Rx-Multicasts	Anzahl vom LAN empfangener Multicast-Pakete
LAN-Rx-Unicasts	Anzahl vom LAN empfangener direkt adressierter Pakete
WAN-Rx-Broadcasts	Anzahl vom WAN empfangener Broadcasts

/LAN-Statistik	Fortlaufende Statusanzeigen
WAN-Rx-Multicasts	Anzahl vom WAN empfangener Multicasts
WAN-Rx-Unicasts	Anzahl vom WAN empfangener Unicasts
Werte-loeschen	LAN-Statistik löschen

1.4.1 LAN-Rx-Pakete

Anzahl empfangener Datenpakete

1.4.2 LAN-Tx-Pakete

Anzahl gesendeter Datenpakete

1.4.3 LAN-Rx-Fehler

Anzahl fehlerhaft empfangener Datenpakete

1.4.4 LAN-Tx-Fehler

Anzahl fehlerhaft gesendeter Datenpakete

1.4.5 LAN-Stack-Fehler

Anzahl Pakete ohne passendes Empfangsmodul (Bridge/Router)

1.4.6 LAN-NIC-Fehler

Anzahl vom NIC verworfener Datenpakete

1.4.7 LAN-Heap-Pakete

Anzahl verfügbarer Puffer

1.4.8 LAN-Queue-Pakete

Anzahl belegter Puffer

1.4.9 LAN-Queue-Fehler

Anzahl durch Puffermangel verworfener Pakete

1.4.10 LAN-Kollisionen

Anzahl Kollisionen während des Sendevorgangs

1.4.11 Werte-loeschen

LAN-Statistik löschen

1.4.12 Verbindung-aufgebaut

Anzeige der korrekten Verbindung auf dem Ethernet (Datenübertragung möglich). Entspricht der 'Link'-LED am Gerät.

1.4.13 Verhandlung-abgeschlossen

Die Aushandlung der Übertragungsart zwischen Gerät und Gegenstelle ist abgeschlossen. Hat nur eine Bedeutung, wenn Setup/LAN-/Anschluss auf 'Auto' steht.

1.4.14 Anschluss

Anzeige des Netzwerkanschlusses (z.B. 10B-T oder 100B-T für 10 oder 100 MBit Ethernet-Anschluss)

1.4.15 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.4.16 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.4.17 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.4.18 LAN-Rx-Bytes

Anzahl vom LAN empfangener Zeichen

1.4.19 LAN-Tx-Bytes

Anzahl zum LAN gesendeter Zeichen

1.4.20 LAN-Rx-Broadcasts

Anzahl vom LAN empfangener Broadcast-Pakete

1.4.21 LAN-Rx-Multicasts

Anzahl vom LAN empfangener Multicast-Pakete

1.4.22 LAN-Rx-Unicasts

Anzahl vom LAN empfangener direkt adressierter Pakete

1.4.23 LAN-Tx-Broadcasts

Anzahl vom LAN gesendeter Broadcasts

1.4.24 LAN-Tx-Multicasts

Anzahl vom LAN gesendeter Multicasts

1.4.25 LAN-Tx-Unicasts

Anzahl vom LAN gesendeter Unicasts

1.4.26 LAN-RX-CRC-Fehler

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.4.27 LAN-RX-Align-Fehler

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5 PPP-Statistik

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

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

1.5.1 Zustände

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

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

lfc	Phase	LCP	IPCP	CCP
Ch01	DEAD	Initial	Initial	Initial
Ch02	DEAD	Initial	Initial	Initial

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

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

1.5.2 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:

1.5.2.1 Rx-Fehler

Anzahl fehlerhaft empfangener PPP-Pakete

1.5.2.2 Rx-Verworfen

Anzahl verworfener PPP-Pakete

1.5.2.3 Rx-Config-Request

Anzahl empfangener Configure-Request-Pakete für LCP

1.5.2.4 Rx-Config-Ack.

Anzahl empfangener Configure-Acknowledge-Pakete für LCP

1.5.2.5 Rx-Config-Nack.

Anzahl empfangener Configure-Negative Acknowledge-Pakete

1.5.2.6 Rx-Config-Reject

Anzahl empfangener Configure-Reject-Pakete für LCP

1.5.2.7 Rx-Termination-Request

Anzahl empfangener Terminate-Request-Pakete für LCP

1.5.2.8 Rx-Termination-Ack

Anzahl empfangener Terminate-Acknowledge-Pakete für LCP

1.5.2.9 Rx-Code-Reject

Anzahl empfangener Code-Reject-Pakete für PPP

1.5.2.10 Rx-Protocol-Reject

Anzahl empfangener Protocol-Reject-Pakete für PPP

1.5.2.11 Rx-Echo-Request

Anzahl empfangener Echo-Request-Pakete für LCP

1.5.2.12 Rx-Echo-Reply

Anzahl empfangener Echo-Response-Pakete für LCP

1.5.2.13 Rx-Discard-Request

Anzahl empfangener Discard-Request-Pakete für LCP

1.5.2.14 Tx-Config-Request

Anzahl gesendeter Configure-Request-Pakete für LCP

1.5.2.15 Tx-Config-Ack.

Anzahl gesendeter Configure-Acknowledge-Pakete für LCP

1.5.2.16 Tx-Config-Nak.

Anzahl gesendeter Configure-Negative-Acknowledge-Pakete

1.5.2.17 Tx-Config-Reject

Anzahl gesendeter Configure-Reject-Pakete für LCP

1.5.2.18 Tx-Termination-Request

Anzahl gesendeter Terminate-Request-Pakete für LCP

1.5.2.19 Tx-Termination-Ack.

Anzahl gesendeter Terminate-Acknowledge-Pakete für LCP

1.5.2.20 Tx-Code-Reject

Anzahl gesendeter Code-Reject-Pakete für PPP

1.5.2.21 Tx-Protocol-Reject

Anzahl gesendeter Protocol-Reject-Pakete für PPP

1.5.2.22 Tx-Echo-Request

Anzahl gesendeter Echo-Request-Pakete für LCP

1.5.2.23 Tx-Echo-Reply

Anzahl gesendeter Echo-Response-Pakete für LCP

1.5.2.24 Tx-Discard-Request

Anzahl gesendeter Discard-Request-Pakete für LCP

1.5.2.25 Werte-loeschen

LCP-Statistik löschen

1.5.3 PAP-Statistik

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

1.5.3.1 Rx-verworfen

Anzahl verworfener PAP-Pakete

1.5.3.2 Rx-Request

Anzahl empfangener PAP-Request-Pakete

1.5.3.3 Rx-Success

Anzahl empfangener PAP-Success-Pakete

1.5.3.4 Rx-Failure

Anzahl empfangener PAP-Failure-Pakete

1.5.3.5 Tx-Retry

Anzahl gesendeter Wiederholungen von PAP-Request-Paketen

1.5.3.6 Tx-Request

Anzahl gesendeter PAP-Request-Pakete

1.5.3.7 Tx-Success

Anzahl gesendeter PAP-Success-Pakete

1.5.3.8 Tx-Failure

Anzahl gesendeter PAP-Failure-Pakete

1.5.3.9 Werte-loeschen

PAP-Statistik löschen

1.5.4 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').

1.5.4.1 Rx-verworfen

Anzahl verworfener CHAP-Pakete

1.5.4.2 Rx-Challenge

Anzahl empfangener CHAP-Challenge-Pakete

1.5.4.3 Rx-Response

Anzahl empfangener CHAP-Response-Pakete

1.5.4.4 Rx-Success

Anzahl empfangener CHAP-Success-Pakete

1.5.4.5 Rx-Failure

Anzahl empfangener CHAP-Failure-Pakete

1.5.4.6 Tx-Retry

Anzahl gesendeter Wiederholungen v. CHAP-Challenge-Paketen

1.5.4.7 Tx-Challenge

Anzahl gesendeter CHAP-Challenge-Pakete

1.5.4.8 Tx-Response

Anzahl gesendeter CHAP-Response-Pakete

1.5.4.9 Tx-Success

Anzahl gesendeter CHAP-Success-Pakete

1.5.4.10 Tx-Failure

Anzahl gesendeter CHAP-Failure-Pakete

1.5.4.11 Werte-loeschen

CHAP-Statistik löschen

1.5.5 IPXCP-Statistik

1.5.5.1 Rx-Rejected

Anzahl verworfener IPCP-Pakete

1.5.5.2 Rx-Config-Request

Anzahl empfangener Configure-Request-Pakete für IPXCP

1.5.5.3 Rx-Config-Ack.

Anzahl empfangener Configure-Acknowledge-Pakete für IPXCP

1.5.5.4 Rx-Config-Nak.

Anzahl empfangener Configure-Negative-Acknowledge-Pakete

1.5.5.5 Rx-Config-Reject

Anzahl empfangener Configure-Reject-Pakete für IPXCP

1.5.5.6 Rx-Termination-Request

Anzahl empfangener Terminate-Request-Pakete für IPXCP

1.5.5.7 Rx-Termination-Ack.

Anzahl empfangener Terminate-Acknowledge-Pakete für IPXCP

1.5.5.8 Rx-Code-Reject

Anzahl empfangener Code-Reject-Pakete für IPXCP

1.5.5.9 Tx-Config-Request

Anzahl gesendeter Configure-Request-Pakete für IPXCP

1.5.5.10 Tx-Config-Ack.

Anzahl gesendeter Configure-Acknowledge-Pakete für IPXCP

1.5.5.11 Tx-Config-Nak.

Anzahl gesendeter Configure-Negative-Acknowledge-Pakete

1.5.5.12 Tx-Config-Reject

Anzahl gesendeter Configure-Reject-Pakete für IPXCP

1.5.5.13 Tx-Termination-Request

Anzahl gesendeter Terminate-Request-Pakete für IPXCP

1.5.5.14 Tx-Termination-Ack.

Anzahl gesendeter Terminate-Acknowledge-Pakete für IPXCP

1.5.5.15 Tx-Code-Reject

Anzahl gesendeter Code-Reject-Pakete für IPXCP

1.5.5.16 Werte-loeschen

IPXCP-Statistik löschen

1.5.6 IPCP-Statistik

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

1.5.6.1 Rx-Rejected

Anzahl verworfener IPCP-Pakete

1.5.6.2 Rx-Config-Request

Anzahl empfangener Configure-Request-Pakete für IPCP

1.5.6.3 Rx-Config-Ack.

Anzahl empfangener Configure-Acknowledge-Pakete für IPCP

1.5.6.4 Rx-Config-Nak.

Anzahl empfangener Configure-Negative-Acknowledge-Pakete

1.5.6.5 Rx-Config-Reject

Anzahl empfangener Configure-Reject-Pakete für IPCP

1.5.6.6 Rx-Termination-Request

Anzahl empfangener Terminate-Request-Pakete für IPCP

1.5.6.7 Rx-Termination-Ack.

Anzahl empfangener Terminate-Acknowledge-Pakete für IPCP

1.5.6.8 Rx-Code-Reject

Anzahl empfangener Code-Reject-Pakete für IPCP

1.5.6.9 Tx-Config-Request

Anzahl gesendeter Configure-Request-Pakete für IPCP

1.5.6.10 Tx-Config-Ack.

Anzahl gesendeter Configure-Acknowledge-Pakete für IPCP

1.5.6.11 Tx-Config-Nak.

Anzahl gesendeter Configure-Negative-Acknowledge-Pakete

1.5.6.12 Tx-Config-Reject

Anzahl gesendeter Configure-Reject-Pakete für IPCP

1.5.6.13 Tx-Termination-Request

Anzahl gesendeter Terminate-Request-Pakete für IPCP

1.5.6.14 Tx-Termination-Ack.

Anzahl gesendeter Terminate-Acknowledge-Pakete für IPCP

1.5.6.15 Tx-Code-Reject

Anzahl gesendeter Code-Reject-Pakete für IPCP

1.5.6.16 Werte-loeschen

IPCP-Statistik löschen

1.5.7 CBCP-Statistik

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

1.5.7.1 Rx-verworfen

Anzahl verworfener CBCP-Pakete

1.5.7.2 Rx-Request

Anzahl empfangener CBCP-Request-Pakete

1.5.7.3 Rx-Response

Anzahl empfangener CBCP-Response-Pakete

1.5.7.4 Rx-Acknowledge

Anzahl empfangener CBCP-Acknowledge-Pakete

1.5.7.5 Tx-Request

Anzahl gesendeter CBCP-Request-Pakete

1.5.7.6 Tx-Response

Anzahl gesendeter CBCP-Response-Pakete

1.5.7.7 Tx-Acknowledge

Anzahl gesendeter CBCP-Acknowledge-Pakete

1.5.7.8 Werte-loeschen

CBCP-Statistik löschen

1.5.8 RX-Optionen

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

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

1.5.8.1 LCP

Informationen über Paketgrößen, Steuerzeichen, Sicherungsverfahren und Rückruf. In der Tabelle LCP sind für jeden Kanal gesondert aufgeführt:

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

1.5.8.2 IPXCP

Informationen über Adressen im IPX-Netzwerk

1.5.8.3 IPCP

Informationen über Adressen im IP-Netzwerk. Zu guter Letzt stehen unter IPCP die ausgehandelten IP-Optionen wieder nach Kanal getrennt:

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

1.5.9 TX-Optionen

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

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

1.5.9.1 LCP

Informationen über Paketgrößen, Steuerzeichen, Sicherungsverfahren und Rückruf. In der Tabelle LCP sind für jeden Kanal gesondert aufgeführt:

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

1.5.9.2 IPXCP

Informationen über Adressen im IPX-Netzwerk.

1.5.9.3 IPCP

Informationen über Adressen im IP-Netzwerk. Unter IPCP stehen die ausgehandelten IP-Optionen wieder nach Kanal getrennt:

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

1.5.10 CCP-Statistik

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

1.5.10.1 Rx-verworfen

Anzahl aller verworfenen CCP-Pakete

1.5.10.2 Rx-Config-Request

Anzahl der empfangenen CCP-Anfragen

1.5.10.3 Rx-Config-Ack.

Anzahl der akzeptierten CCP-Anfragen

1.5.10.4 Rx-Config-Nak.

Anzahl der CCP-Anfragen, die aufgrund nicht akzeptierter Parameter der Anfrage zurückgewiesen wurden.

1.5.10.5 Rx-Config-Reject

Anzahl der CCP-Anfragen, die aufgrund anderer Gründe zurückgewiesen wurden.

1.5.10.6 Rx-Termination-Request

Anzahl der CCP-Anfragen nach einem Abbau der Kompression.

1.5.10.7 Rx-Termination-Ack.

Anzahl der bestätigten CCP-Anfragen nach einem Abbau der Kompression.

1.5.10.8 Rx-Code-Reject

Anzahl der zurückgewiesenen CCP-Anfragen, weil die Gegenstelle keine Kompression einsetzen will oder kann.

1.5.10.9 Rx-Reset-Request

Anzahl der CCP-Anfragen nach einer Synchronisation der Kompression (z.B. nach Übertragungsfehlern)

1.5.10.10 Rx-Reset-Ack

Anzahl der bestätigten CCP-Anfragen nach einer Synchronisation der Kompression

1.5.10.11 Tx-Config-Request

Anzahl der gesendeten CCP-Anfragen

1.5.10.12 Tx-Config-Ack.

Anzahl der von der Gegenstelle akzeptierten CCP-Anfragen

1.5.10.13 Tx-Config-Nak.

Anzahl der CCP-Anfragen, die von der Gegenstelle aufgrund nicht akzeptierter Parameter der Anfrage zurückgewiesen wurden.

1.5.10.14 Tx-Config-Reject

Anzahl der CCP-Anfragen, die von der Gegenstelle aufgrund anderer Gründe zurückgewiesen wurden.

1.5.10.15 Tx-Termination-Request

Anzahl der gesendeten CCP-Anfragen nach einem Abbau der Kompression.

1.5.10.16 Tx-Termination-Ack.

Anzahl der gesendeten CCP-Bestätigungen für den Abbau der Kompression.

1.5.10.17 Tx-Code-Reject

Anzahl der zurückgewiesenen CCP-Anfragen, weil der *ELSA LANCOM* keine Kompression einsetzen will (durch Einstellung in der Layer-Liste).

1.5.10.18**1.5.10.19 Tx-Reset-Request**

Anzahl der gesendeten CCP-Anfragen nach einer Synchronisation der Kompression (z.B. nach Übertragungsfehlern)

1.5.10.20 Tx-Reset-Ack

Anzahl der gesendeten CCP-Bestätigungen für eine Synchronisation der Kompression

1.5.10.21 Werte-loeschen

CCP-Statistik löschen

1.5.10.22 Kompressionsfehler**1.5.11 ML-Statistik**

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

1.5.11.1 Buendel-Verb

Anzahl der Verbindungen, die MLPPP verwendet haben

1.5.11.2 Rx-Seq-Verlust

Anzahl der Pakete, bei denen ein Fehler in der Reihenfolge der Sequenznummern aufgetreten ist.

1.5.11.3 Rx-Seq-Wiederholung

Anzahl der Pakete, die der Reihenfolge der Sequenznummern nach verspätet eingetroffen sind.

1.5.11.4 Rx-Mrru-Ueberlauf

Anzahl der Pakete, bei denen nach dem Zusammenbauen eine Verletzung der in der PPP-Verhandlung ausgehandelten MRRU (maximal received reassembled unit) festgestellt wurde.

1.5.11.5 Rx-Header-Fehler

Anzahl der Pakete mit fehlerhaftem Header.

1.5.11.6 Rx-verworfen

Anzahl aller verworfenen MLPPP-Pakete.

1.5.11.7 Rx-Frag-Start

Anzahl der Pakete mit gesetztem Start-Flag (erster Teil eines fragmentierten Pakets).

1.5.11.8 Rx-Frag-Mid

Anzahl der Pakete mit gesetztem Mid-Flag (mittlerer Teil eines fragmentierten Pakets).

1.5.11.9 Rx-Frag-Ende

Anzahl der Pakete mit gesetztem End-Flag (letzter Teil eines fragmentierten Pakets).

1.5.11.10 Rx-unfragmentiert

Anzahl der Pakete mit gesetztem Start- und End-Flag (unfragmentierte Pakete).

1.5.11.11 Werte-loeschen

ML-Statistik löschen

1.5.12 BACP-Statistik

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.1 Rx-Fehler

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.2 Rx-verworfen

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.3 Rx-Call-Request

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.4 Rx-Call-Response

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.5 Rx-Callback-Request

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.6 Rx-Callback-Response

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.7 Rx-Link-Drop-Request

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.8 Rx-Link-Drop-Response

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.9 Rx-Status-Indication

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.10 Rx-Status-Response

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.11 Tx-Call-Request

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.12 Tx-Call-Response

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.13 Tx-Callback-Request

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.14 Tx-Callback-Response

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.15 Tx-Link-Drop-Request

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.16 Tx-Link-Drop-Response

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.17 Tx-Status-Indication

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.18 Tx-Status-Response

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.5.12.19 Werte-loeschen

Löschen der BACP-Statistik

1.6 Bridge-Statistik

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.1 Brg-LAN-Rx

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.2 Brg-LAN-Tx

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.3 Brg-LAN-Filter

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.4 Brg-LAN-Broadcasts

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.5 Brg--LAN-Multicasts

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.6 Brg-WAN-Tx

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.7 Brg-WAN-Rx

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.8 Brg-WAN-Filter

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.9 Brg-WAN-Broadcasts

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.10 Brg-WAN-Multicasts

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.11 Brg-Adressen

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.12 Tabelle-Bridge

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.13 Aufbau-Tabelle

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.6.14 Werte-loeschen

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.7 IPX-Statistik

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

1.7.1 MAC-Statistik

Statistiken aus dem Media Access Control von IPX-Paketen

1.7.1.1 IPX-LAN-Rx

Anzahl vom LAN empfangener IPX-Pakete

1.7.1.2 IPX-LAN-Rx-Broadcasts

Anzahl vom LAN empfangener Broadcast-IPX-Pakete

1.7.1.3 IPX-LAN-Rx-Multicasts

Anzahl vom LAN empfangener Multicast-IPX-Pakete

1.7.1.4 IPX-LAN-Rx-Unicasts

Anzahl vom LAN empfangener direkt adressierter IPX-Pakete

1.7.1.5 IPX-LAN-Tx

Anzahl zum LAN gesendeter IPX-Pakete

1.7.1.6 IPX-WAN-Rx

Anzahl vom WAN empfangener IPX-Pakete

1.7.1.7 IPX-WAN-Rx-Broadcasts

Anzahl vom WAN empfangener Broadcasts

1.7.1.8 IPX-WAN-Rx-Multicasts

Anzahl vom WAN empfangener Multicasts

1.7.1.9 IPX-WAN-Rx-Unicasts

Anzahl vom WAN empfangener direkt adressierter IPX-Pakete

1.7.1.10 IPX-WAN-Tx

Anzahl zum WAN gesendeter IPX-Pakete

1.7.1.11 Werte-loeschen

MAC-Statistik löschen

1.7.2 Watchdog-Statistik

Statistiken für Watchdog-Pakete

1.7.2.1 IPX-Watchdog-LAN-Rx

Anzahl vom LAN empfangener IPX-Watchdog-Pakete

1.7.2.2 IPX-Watchdog-LAN-Tx

Anzahl zum LAN gesendeter IPX-Watchdog-Pakete

1.7.2.3 IPX-Watchdog-WAN-Rx

Anzahl vom WAN empfangener IPX-Watchdog-Pakete

1.7.2.4 IPX-Watchdog-WAN-Tx

Anzahl zum WAN gesendeter IPX-Watchdog-Pakete

1.7.2.5 SPX-Watchdog-LAN-Rx

Anzahl vom LAN empfangener SPX-Watchdog-Pakete

1.7.2.6 SPX-Watchdog-LAN-Tx

Anzahl zum LAN gesendeter SPX-Watchdog-Pakete

1.7.2.7 SPX-Watchdog-WAN-Rx

Anzahl vom WAN empfangener SPX-Watchdog-Pakete

1.7.2.8 SPX-Watchdog-WAN-Tx

Anzahl zum WAN gesendeter SPX-Watchdog-Pakete

1.7.2.9 Werte-loeschen

Watchdog Statistik löschen

1.7.3 Propagate-Statistik

Statistiken für IPX-Propagated-Pakete (IPX-Typ 20)

1.7.3.1 Propagate-LAN-Rx

Anzahl vom LAN empfangener IPX-Propagated-Pakete

1.7.3.2 Propagate-LAN-Filter

Anzahl vom LAN empfangener/gefilterter IPX-Propagated-Pakete

1.7.3.3 Propagate-LAN-Tx

Anzahl zum LAN gesendeter IPX-Propagated-Pakete

1.7.3.4 Propagate-LAN-Socket-Fehler

Anzahl vom LAN über Socket-Filter gefilterter IPX-Propagated-Pakete

1.7.3.5 Propagate-LAN-Hop-Fehler

Anzahl vom LAN über Hop-Count gefilterter IPX-Propagated-Pakete

1.7.3.6 Propagate-LAN-Backroute-Fehler

Anzahl vom LAN zurückzuroutende IPX-Propagated-Pakete

1.7.3.7 Propagate-LAN-Contention

Anzahl vom LAN zu routende Pakete während einer falschen Verbindung

1.7.3.8 Propagate-WAN-Rx

Anzahl vom WAN empfangener IPX-Propagated-Pakete

1.7.3.9 Propagate-WAN-Filter

Anzahl vom WAN empfangener/gefilterter IPX-Propagated-Pakete

1.7.3.10 Propagate-WAN-Tx

Anzahl zum WAN gesendeter IPX-Watchdog-Pakete

1.7.3.11 Propagate-WAN-Socket-Fehler

Anzahl vom WAN über Socket-Filter gefilterter IPX-Propagated-Pakete

1.7.3.12 Werte-loeschen

IPX-Propagated-Paket-Statistik löschen

1.7.4 RIP-Statistik

Statistiken für NetWare-RIP

1.7.4.1 RIP-LAN-Rx

Anzahl vom LAN empfangener RIP-Pakete

1.7.4.2 RIP-LAN-Fehler

Anzahl vom LAN empfangener RIP-Pakete mit fehlerhaftem Inhalt

1.7.4.3 RIP-LAN-Tx

Anzahl zum LAN gesendeter RIP-Pakete

1.7.4.4 RIP-WAN-Rx

Anzahl vom WAN empfangener RIP-Pakete

1.7.4.5 RIP-WAN-Fehler

Anzahl vom WAN empfangener RIP-Pakete mit fehlerhaftem Inhalt

1.7.4.6 RIP-WAN-Tx

Anzahl zum WAN gesendeter RIP-Pakete

1.7.4.7 Tabelle-RIP

Anzeige der RIP-Tabelle

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

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

1.7.4.8 Werte-loeschen

RIP-Statistik löschen

1.7.5 SAP-Statistik

Statistiken für NetWare-SAP

1.7.5.1 SAP-LAN-Rx

Anzahl vom LAN empfangener SAP-Pakete

1.7.5.2 SAP-LAN-Fehler

Anzahl vom LAN empfangener SAP-Pakete mit fehlerhaftem Inhalt

1.7.5.3 SAP-LAN-Tx

Anzahl zum LAN gesendeter SAP-Pakete

1.7.5.4 SAP-WAN-Rx

Anzahl vom WAN empfangener SAP-Pakete

1.7.5.5 SAP-WAN-Fehler

Anzahl vom WAN empfangener SAP-Pakete mit fehlerhaftem Inhalt

1.7.5.6 SAP-WAN-Tx

Anzahl zum WAN gesendeter SAP-Pakete

1.7.5.7 Tabelle-SAP

Anzahl vom LAN empfangener SAP-Pakete

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

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

1.7.5.8 Werte-loeschen

SAP-Statistik löschen

1.7.6 IPX-Router-Statistik

Statistiken des Remote-IPX-Routers

1.7.6.1 IPXr-LAN-Rx

Anzahl vom LAN zu routender IPX-Pakete

1.7.6.2 IPXr-LAN-Tx

Anzahl zum LAN gerouteter IPX-Pakete

1.7.6.3 IPXr-LAN-Hop-Fehler.

Anzahl vom LAN zu routender über Hop-Count gefilterter IPX-Pak.

1.7.6.4 IPXr-LAN-Socket-Fehler

Anzahl vom LAN zu routender über Socket-Filter gefilterter IPX-Pakete

1.7.6.5 IPXr-LAN-Netzwerk-Fehler

Anzahl vom LAN zu routende Pakete zu falschen Netzwerken

1.7.6.6 IPXr-LAN-Backroute-Fehler

Anzahl vom LAN zurückzuroutende IPX-Pakete

1.7.6.7 IPXr-LAN-Contention

Anzahl vom LAN zu routender Pakete während einer falschen Verbindung

1.7.6.8 IPXr-LAN-Down-Fehler

Anzahl vom LAN zu routender IPX-Pakete zu abgemeldeten Netzen

1.7.6.9 IPXr-WAN-Rx

Anzahl vom WAN zu routender IPX-Pakete

1.7.6.10 IPXr-WAN-Tx

Anzahl zum WAN gerouteter IPX-Pakete

1.7.6.11 IPXr-WAN-Hop-Fehler.

Anzahl vom WAN zu routender über Hop-Count gefilterter IPX-Pakete

1.7.6.12 IPXr-WAN-Socket-Fehler

Anzahl vom WAN zu routender über Socket-Filter gefilterter IPX-Pak.

1.7.6.13 IPXr-WAN-Netzwerk-Fehler

Anzahl vom WAN zu routender Pakete zu falschen Netzwerken

1.7.6.14 IPXr-WAN-Backroute-Fehler

Anzahl vom WAN zurückzuroutender IPX-Pakete

1.7.6.15 IPXr-WAN-Down-Fehler

Anzahl vom WAN zu routender IPX-Pakete zu abgemeldeten Netzen

1.7.6.16 IPXr-Int-Rx

Anzahl der Pakete von internen Modulen an den IPX-Router

1.7.6.17 Netzwerke

Tabelle der Netzwerke in der IPX-Routing-Tabelle mit Node-IDs

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

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

Die Einträge haben die folgende Bedeutung:

Gegenstelle	Logischer Name der Gegenstelle, wie in der Routing-Tabelle eingetragen. Zusätzlich ist noch ein Eintrag für die LAN-Anbindung vorhanden. Dieser steht an erster Stelle der Tabelle und hat den Namen „LAN“.
Netzwerk	Adresse des Netzwerks in dem sich die Gegenstelle befindet. Für WAN-Gegenstellen entspricht dieser dem Eintrag in der Routing-Tabelle. Falls in der IPX-Routing-Tabelle (/SETUP/IPX-MODUL/LAN-EINSTELLUNG/NETZWERK) die Autodetect-Funktion eingestellt ist, kann an dieser Stelle abgelesen werden, welches Netzwerk erkannt wurde.
Binding	Ethernet-Binding, auf das die Gegenstelle gebunden ist. Für WAN-Gegenstellen entspricht dieses dem Eintrag in der Routing-Tabelle. Falls in der IPX-Routing-Tabelle (/SETUP/IPX-MODUL/LAN-EINSTELLUNG/NETZWERK) die Autodetect-Funktion eingestellt ist, kann an dieser Stelle abgelesen werden, welches Binding erkannt wurde.
Propagate	Filterflag für IPX Typ 20 (propagated) Frames. Für WAN-Gegenstellen entspricht dieses dem Eintrag in der Routing-Tabelle. Für das LAN ist hier immer Route eingetragen.

Backoff	Aufbau-Zähler für den Exponential-Backoff-Algorithmus. Wenn der Aufbau-Zähler den Wert 16 hat, so wird kein erneuter Versuch mehr durchgeführt, die Route ist damit inaktiv (auch für das LAN möglich).
Zeit	Restzeit bis zum nächsten Aufbauversuch des Exponential-Backoff-Algorithmus in Sekunden. War ein Aufbau erfolgreich, so wird die Restzeit auf Null gesetzt. Damit ist die Route aktiv.
Node-ID	Node-ID des zuständigen Routers im WAN-Netz. Für den LAN-Eintrag ist hier die Node-ID des Routers eingetragen.

1.7.6.18 Aufbau-Tabelle

Tabelle der letzten 20 Pakete, die eine Verbindung erforderten

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

Eine IPX-Aufbau-Tabelle kann wie folgt aussehen:

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

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

1.7.6.19 Werte-loeschen

IPX-Router-Statistik löschen

1.8 TCP-IP-Statistik

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

1.8.1 ARP-Statistik

Statistiken aus dem ARP-Bereich

1.8.1.1 ARP-LAN-Rx

Anzahl vom LAN empfangener ARP-Anfragen und -Antworten

1.8.1.2 ARP-LAN-Tx

Anzahl zum LAN gesendeter ARP-Anfragen und -Antworten

1.8.1.3 ARP-LAN-Fehler

Anzahl vom LAN fehlerhaft empfangener ARP-Anfragen

1.8.1.4 ARP-WAN-Rx

Anzahl vom WAN empfangener ARP-Anfragen und -Antworten

1.8.1.5 ARP-WAN-Tx

Anzahl zum WAN gesendeter ARP-Anfragen und -Antworten

1.8.1.6 ARP-WAN-Fehler

Anzahl vom WAN fehlerhaft empfangener ARP-Anfragen

1.8.1.7 Tabelle-ARP

Anzeige der ARP-Tabelle

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

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

1.8.1.8 Werte-loeschen

ARP-Statistiken löschen

1.8.2 IP-Statistik

Statistiken aus dem IP-Bereich

1.8.2.1 IP-LAN-Rx

Anzahl vom LAN empfangener IP-Pakete

1.8.2.2 IP-LAN-Tx

Anzahl zum LAN gesendeter IP-Pakete

1.8.2.3 IP-LAN-Checksummen-Fehler

Anzahl vom LAN fehlerhaft empfangener IP-Pakete

1.8.2.4 IP-LAN-Service-Fehler

Anzahl vom LAN empfangener IP-Pakete für falschen Dienst

1.8.2.5 IP-WAN-Rx

Anzahl vom WAN empfangener IP-Pakete

1.8.2.6 IP-WAN-Tx

Anzahl zum WAN gesendeter IP-Pakete

1.8.2.7 IP-WAN-Checksummen-Fehler

Anzahl vom WAN fehlerhaft empfangener IP-Pakete

1.8.2.8 IP-WAN-Service-Fehler

Anzahl vom WAN empfangener IP-Pakete für falschen Dienst

1.8.2.9 IP-WAN-Rx-verworfen

Anzahl vom WAN durch Time-Out-Management verworfener Pakete

1.8.2.10 IP-LAN-Fragmentierungs-Fehler

Anzahl vom LAN fehlerhaft empfangener Fragmentierungen

1.8.2.11 IP-WAN-Fragmentierungs-Fehler

Anzahl vom WAN fehlerhaft empfangener Fragmentierungen

1.8.2.12 Werte-loeschen

IP-Statistiken löschen

1.8.2.13 IP-LAN-Fragmentierungen

Anzahl vom LAN empfangener Fragmentierungen

1.8.2.14 IP-LAN-Fragmentierung-erzwungen

Anzahl vom LAN erzwungener Fragmentierungen

1.8.2.15 IP-WAN-Fragmentierungen

Anzahl vom WAN empfangener Fragmentierungen

1.8.2.16 IP-WAN-Fragmentierung-erzwungen

Anzahl vom WAN erzwungener Fragmentierungen

1.8.3 ICMP-Statistik

Statistiken für ICMP-Pakete

1.8.3.1 ICMP-LAN-Rx

Anzahl vom LAN empfangener ICMP-Pakete

1.8.3.2 ICMP-LAN-Tx

Anzahl zum LAN gesendeter ICMP-Pakete

1.8.3.3 ICMP-LAN-Checksummen-Fehler

Anzahl vom LAN fehlerhaft empfangener ICMP-Pakete

1.8.3.4 ICMP-LAN-Service-Fehler

Anzahl vom LAN empfangener, nicht unterstützter ICMP-Pakete

1.8.3.5 ICMP-WAN-Rx

Anzahl vom WAN empfangener ICMP-Pakete

1.8.3.6 ICMP-WAN-Tx

Anzahl zum WAN gesendeter ICMP-Pakete

1.8.3.7 ICMP-WAN-Checksummen-Fehler

Anzahl vom WAN fehlerhaft empfangener ICMP-Pakete

1.8.3.8 ICMP-WAN-Service-Fehler

Anzahl vom WAN empfangener, nicht unterstützter ICMP-Pakete

1.8.3.9 Werte-loeschen

ICMP-Statistiken löschen

1.8.4 TFTP-Statistik

Statistiken für TFTP-Operationen

1.8.4.1 TFTP-LAN-Rx

Anzahl vom LAN empfangener TFTP-Pakete

1.8.4.2 TFTP-LAN-Rx-Read-Request

Anzahl vom LAN empfangener TFTP-Read-Requests

1.8.4.3 TFTP-LAN-Rx-Write-Request

Anzahl vom LAN empfangener TFTP-Write-Requests

1.8.4.4 TFTP-LAN-Rx-Data

Anzahl vom LAN empfangener TFTP-Daten-Pakete

1.8.4.5 TFTP-LAN-Rx-Ack.

Anzahl vom LAN empfangener TFTP-Acknowledges

1.8.4.6 TFTP-LAN-Rx-Option-Ack.

Anzahl vom LAN empfangener TFTP-Option-Acknowledges

1.8.4.7 TFTP-LAN-Rx-Fehler

Anzahl vom LAN empfangener TFTP-Error-Pakete

1.8.4.8 TFTP-LAN-Rx-Unb.

Anzahl vom LAN empfangener, unbekannter TFTP-Pakete

1.8.4.9 TFTP-LAN-Tx

Anzahl auf das LAN gesendeter TFTP-Pakete

1.8.4.10 TFTP-LAN-Tx-Data

Anzahl auf das LAN gesendeter TFTP-Daten-Pakete

1.8.4.11 TFTP-LAN-Tx-Ack.

Anzahl auf das LAN gesendeter TFTP-Acknowledges

1.8.4.12 TFTP-LAN-Tx-Option-Ack.

Anzahl auf das LAN gesendeter TFTP-Option-Ack

1.8.4.13 TFTP-LAN-Tx-Fehler

Anzahl auf das LAN gesendeter TFTP-Error-Pakete

1.8.4.14 TFTP-LAN-Tx-Wiederholungen

Anzahl wiederholt aufs LAN gesendeter TFTP-Pakete

1.8.4.15 TFTP-LAN-Verbindungen

Anzahl zum LAN aufgebauter TFTP-Verbindungen

1.8.4.16 TFTP-WAN-Rx

Anzahl vom WAN empfangener TFTP-Pakete

1.8.4.17 TFTP-WAN-Rx-Read-Request

Anzahl vom WAN empfangener TFTP-Read-Requests

1.8.4.18 TFTP-WAN-Rx-Write-Request

Anzahl vom WAN empfangener TFTP-Write-Requests

1.8.4.19 TFTP-WAN-Rx-Data

Anzahl vom WAN empfangener TFTP-Daten-Pakete

1.8.4.20 TFTP-WAN-Rx-Ack.

Anzahl vom WAN empfangener TFTP-Acknowledges

1.8.4.21 TFTP-WAN-Rx-Option-Ack.

Anzahl vom WAN empfangener TFTP-Option-Acknowledges

1.8.4.22 TFTP-WAN-Rx-Fehler

Anzahl vom WAN empfangener TFTP-Error-Pakete

1.8.4.23 TFTP-WAN-Rx-Unb.

Anzahl vom WAN empfangener, unbekannter TFTP-Pakete

1.8.4.24 TFTP-WAN-Tx

Anzahl auf das WAN gesendeter TFTP-Pakete

1.8.4.25 TFTP-WAN-Tx-Data

Anzahl auf das WAN gesendeter TFTP-Daten-Pakete

1.8.4.26 TFTP-WAN-Tx-Ack.

Anzahl auf das WAN gesendeter TFTP-Acknowledges

1.8.4.27 TFTP-WAN-Tx-Option-Ack.

Anzahl auf das WAN gesendeter TFTP-Option-Ack

1.8.4.28 TFTP-WAN-Tx-Fehler

Anzahl auf das WAN gesendeter TFTP-Error-Pakete

1.8.4.29 TFTP-WAN-Tx-Wiederholungen

Anzahl wiederholt aufs WAN gesendeter TFTP-Pakete

1.8.4.30 TFTP-WAN-Verbindungen

Anzahl zum WAN aufgebauter TFTP-Verbindungen

1.8.4.31 Werte-loeschen

TFTP-Statistik löschen

1.8.5 TCP-Statistik

Statistiken für TCP-Pakete von TCP-Sitzungen zum Router

1.8.5.1 TCP-LAN-Rx

Anzahl vom LAN empfangener TCP-Pakete

1.8.5.2 TCP-LAN-Tx

Anzahl zum LAN gesendeter TCP-Pakete

1.8.5.3 TCP-LAN-Tx-Wdh.

Anzahl zum LAN wiederholt gesendeter TCP-Pakete

1.8.5.4 TCP-LAN-Checksummen-Fehler

Anzahl vom LAN fehlerhaft empfangener TCP-Pakete

1.8.5.5 TCP-LAN-Service-Fehler

Anzahl vom LAN empfangener TCP-Pakete für falschen Port

1.8.5.6 TCP-LAN-Verbindungen

Anzahl der aktuellen TCP-Verbindungen vom LAN

1.8.5.7 TCP-WAN-Rx

Anzahl vom WAN empfangener TCP-Pakete

1.8.5.8 TCP-WAN-Tx

Anzahl zum WAN gesendeter TCP-Pakete

1.8.5.9 TCP-WAN-Tx-Wiederholungen

Anzahl zum WAN wiederholt gesendeter TCP-Pakete

1.8.5.10 TCP-WAN-Checksummen-Fehler

Anzahl vom WAN fehlerhaft empfangener TCP-Pakete

1.8.5.11 TCP-WAN-Service-Fehler

Anzahl vom WAN empfangener TCP-Pakete für falschen Port

1.8.5.12 TCP-WAN-Verbindungen

Anzahl aktueller TCP-Verbindungen vom WAN

1.8.5.13 Werte-loeschen

TCP-Statistiken löschen

1.8.6 DHCP-Statistik

Statistiken aus dem DHCP-Server

1.8.6.1 DHCP-LAN-Rx

Anzahl aus dem LAN empfangener DHCP-Pakete

1.8.6.2 DHCP-LAN-Tx

Anzahl in das LAN gesendeter DHCP-Pakete

1.8.6.3 DHCP-WAN-Rx

Anzahl aus dem WAN empfangener DHCP-Pakete

1.8.6.4 DHCP-Verworfen

Anzahl verworfener DHCP-Pakete

1.8.6.5 DHCP-Rx-Discover

Anzahl empfangener Discover-Messages

1.8.6.6 DHCP-Rx-Request

Anzahl empfangener Request-Messsges

1.8.6.7 DHCP-Rx-Dcline

Anzahl empfangener Decline-Messages

1.8.6.8 DHCP-Rx-Inform

Anzahl empfangener Inform-Messages

1.8.6.9 DHCP-Rx-Release

Anzahl empfangener Release-Messages

1.8.6.10 DHCP-Tx-Offer

Anzahl gesendeter Offer-Messages

1.8.6.11 DHCP-Tx-Ack.

Anzahl bestätigter DHCP-Pakete

1.8.6.12 DHCP-Tx-Nak

Anzahl nicht bestätigter DHCP-Pakete

1.8.6.13 DHCP-Server-Fehler

Anzahl empfangener DHCP-Pakete, die nicht für diesen Server bestimmt waren

1.8.6.14 DHCP-Zugewiesen

Anzahl aktuell zugewiesener Adressen

1.8.6.15 DHCP-MAC-Konflikte

Anzahl abgelehnter Zuweisungen aufgrund belegter IP-Adressen

1.8.6.16 Tabelle-DHCP

Tabelle mit den Zuweisungen von IP-Adressen zu MAC-Adressen

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

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

1.8.6.17 Server-Flags

Ein/Ausschalten der Server-Flags

1.8.6.18 Werte-loeschen

DHCP-Statistik löschen

1.8.7 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.8.8 NetBIOS-Statistik

Statistiken aus dem NetBIOS-Modul

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

1.8.8.1 LAN-Rx

Anzahl der NetBIOS-Pakete, die vom LAN empfangen wurden.

1.8.8.2 LAN-Tx

Anzahl der NetBIOS-Pakete, die auf das LAN gesendet wurden.

1.8.8.3 WAN-Rx

Anzahl der NetBIOS-Pakete, die vom WAN empfangen wurden.

1.8.8.4 WAN-Tx

Anzahl der NetBIOS-Pakete, die auf das WAN gesendet wurden.

1.8.8.5 Registrierungen

Anzahl der erfolgten Namenregistrierungen

1.8.8.6 Konflikte

Anzahl der festgestellten Namenskonflikte. Da das NetBIOS-Modul nur eine Art schwarzes Brett ist, an dem jeder Rechner seinen Namen anheftet, überprüft es auch nicht die Konsistenz der Daten. Daher wird der Zähler nur erhöht, wenn ein Host selbst einen Konflikt festgestellt hat und dieses über einen Broadcast im Netz bekannt macht

1.8.8.7 Freigaben

Anzahl der erfolgten Namensfreigaben

1.8.8.8 Erneuerungen

Anzahl der erfolgten Namenserneuerungen (Refresh)

1.8.8.9 Timeouts

Anzahl der durch Alterung herausgefallenen Namen

1.8.8.10 Hosts

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.8.8.11 Gruppen

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.8.8.12 B-Knoten

Anzahl der gerade aktiven B-Knoten (Broadcast) im Netz

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

1.8.8.13 P-Knoten

Anzahl der gerade aktiven P-Knoten (Peer-to-Peer) im Netz

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

1.8.8.14 M-Knoten

Anzahl der gerade aktiven M-Knoten (Mixed-Mode) im Netz

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

1.8.8.15 W-Knoten

Anzahl der gerade aktiven W-Knoten (Hybrid) im Netz

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

1.8.8.16 Gegenstellen-Tab.

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.8.8.17 Werte-loeschen

Löschen der NetBIOS-Statistik

1.8.9 DNS-Statistik

Statistiken aus dem DNS-Server

In den Unterstatistiken finden Sie dann die weiteren Parameter zu den einzelnen Menüs. Der DNS-Statistik können zusätzliche Informationen über das DNS-Modul entnommen werden.

1.8.9.1 LAN-Rx

Anzahl der DNS-Pakete, die vom LAN empfangen wurden

1.8.9.2 LAN-Tx

Anzahl der DNS-Pakete, die zum LAN gesendet wurden

1.8.9.3 WAN-Rx

Anzahl der DNS-Pakete, die vom WAN empfangen wurden

1.8.9.4 WAN-Tx

Anzahl der DNS-Pakete, die zum WAN gesendet wurden

1.8.9.5 Forwarded

Anzahl der Anfragen, die nicht beantwortet werden konnten und daher über den Forwarding-Mechanismus weitergeleitet wurden

1.8.9.6 Fehler

Anzahl von ungültigen Anfragen

1.8.9.7 DNS-Zugriffe

Gibt an, wie viele Namen aus der DNS-Tabelle aufgelöst wurden

1.8.9.8 DHCP-Zugriffe

Gibt an, wie viele Namen aus der DHCP-Tabelle aufgelöst wurden

1.8.9.9 NetBIOS-Zugriffe

Gibt an, wie viele Namen aus den NetBIOS-Tabellen aufgelöst wurden

1.8.9.10 Filter

Anzahl der über die Filtertabelle gefilterten DNS-Pakete

1.8.9.11 Hit-Liste

In dieser Tabelle tauchen die 16 häufigsten Anfragen auf. Diese können dann unter Umständen über die Filterliste abgeblockt werden.

Die Hitliste hat den folgenden Aufbau:

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

Die einzelnen Felder dieser Liste haben die folgende Bedeutung:

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

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

1.8.9.12 Werte-loeschen

Löschen der DNS-Statistik

1.8.10 HTTP-Statistik

Statistische Angaben zu den HTTP-Verbindungen

1.8.10.1 HTTP-Zugriffe

Gesamtzahl der Seitenabrufe

1.8.10.2 HTTP-nichtgefunden-Fehler

Anzahl der Zugriffe auf nicht im Gerät vorhandene Seiten

1.8.10.3 HTTP-Authentisierungs-Fehler

Anzahl der Zugriffe, die aufgrund eines fehlenden oder falschen Paßwortes abgelehnt wurden.

1.8.10.4 HTTP-Protokoll-Fehler

Anzahl der Zugriffe, die vom Gerät nicht beantwortet werden konnten, weil eine unbekannte HTTP-Anfrage geschickt wurde, oder diese Form der Anfrage nicht zulässig war. Hierzu zählt z.B das Setzen von Werten über eine Read-Only-Verbindung.

1.8.10.5 Werte-loeschen

Zurücksetzen aller Zähler auf Null. Dies erfolgt auch implizit bei einem löschen der Werte im TCP/IP-Menü.

1.9 IP-Router-Statistik

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

1.9.1 IPr-LAN-Rx

Anzahl vom LAN zu routender Datenpakete

1.9.2 IPr-LAN-Tx

Anzahl zum LAN gerouteter Datenpakete

1.9.3 IPr-LAN-lokales-Routing

Anzahl vom LAN empfangener und zum LAN gerouteter Pakete

1.9.4 IPr LAN-Netzwerk-Fehler

Anzahl LAN-Pakete, die nicht geroutet wurden

1.9.5 IPr-LAN-Routing-Fehler

Anzahl LAN-Pakete, die zu einem anderen Router müssen

1.9.6 IPr-LAN-TTL-Fehler

Anzahl LAN-Pakete mit einem abgelaufenen Time-to-Live- Wert

1.9.7 IPr-LAN-Filter

Anzahl der über die Filtertabelle gefilterten LAN-Pakete

1.9.8 IPr-LAN-verworfen

Anzahl der verworfenen LAN-Pakete

1.9.9 IPr-WAN-Rx

Anzahl vom WAN zu routender Datenpakete

1.9.10 IPr-WAN-Tx

Anzahl zum WAN gerouteter Datenpakete

1.9.11 IPr-WAN-Netzwerk-Fehler

Anzahl WAN-Pakete, die nicht geroutet wurden

1.9.12 IPr-WAN-TTL-Fehler

Anzahl WAN-Pakete mit einem abgelaufenem Time-to-Live- Wert

1.9.13 IPr-WAN-Filter

Anzahl der über die Filtertabelle gefilterten WAN-Pakete

1.9.14 IPr-WAN-verworfen

Anzahl der verworfenen WAN-Pakete

1.9.15 IPr-WAN-Typ-Fehler

Anzahl der Pakete vom WAN ohne IP-Router-Kennung

1.9.16 IPr-ARP-Fehler

Anzahl der nicht erfolgreichen Zugriffe auf den ARP-Cache

1.9.17 Aufbau-Tabelle

Tabelle der letzten 20 Pakete, die eine Verbindung erforderten

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

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

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

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

1.9.18 Protokoll-Tabelle

Tabelle über geroutete Pakete, protokollabhängig aufgestellt

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

1.9.19 RIP-Statistik

Statistiken aus dem IP/RIP-Bereich

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

1.9.19.1 RIP-Rx

Anzahl empfangener IP-RIP-Pakete

1.9.19.2 RIP-Request

Anzahl empfangener IP-RIP-Request-Pakete

1.9.19.3 RIP-Response

Anzahl empfangener IP-RIP-Response-Pakete

1.9.19.4 RIP-verworfen

Anzahl verworfener IP-RIP-Pakete

1.9.19.5 RIP-Fehler

Anzahl fehlerhafter IP-RIP-Pakete

1.9.19.6 RIP-Eintrag-Fehler

Anzahl fehlerhafter Einträge in IP-RIP-Paketen

1.9.19.7 RIP-Tx

Anzahl gesendeter IP-RIP-Pakete

1.9.19.8 Tabelle-RIP

Routing-Tabelle der durch RIP-Broadcast gelernten Routen

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

1.9.19.9 Werte-loeschen

IP-RIP-Statistik löschen

1.9.20 Werte-loeschen

IP-Router-Statistik löschen

1.9.21 Service-Tabelle

In der Service-Tabelle werden alle Pakettransporten protokolliert. Die Tabelle hat folgenden Aufbau:

Service	Packet-rx	Packet-tx	Packet-rel	KBytes-rx	KBytes-tx	KBytes-rel
ICMP	0	0	0.00	0	0	0.00
FTP	0	0	0.00	0	0	0.00
HTTP	0	0	0.00	0	0	0.00
SMTP	0	0	0.00	0	0	0.00
DNS	0	0	0.00	0	0	0.00
Telnet	0	0	0.00	0	0	0.00
TFTP	0	0	0.00	0	0	0.00
DHCP	0	0	0.00	0	0	0.00
POP3	0	0	0.00	0	0	0.00
NetBIOS	0	0	0.00	0	0	0.00
IMAP2	0	0	0.00	0	0	0.00
NEWS	0	0	0.00	0	0	0.00
IRC	0	0	0.00	0	0	0.00
SNMP	0	0	0.00	0	0	0.00
other	0	0	0.00	0	0	0.00
total	0	0	0.00	0	0	0.00

1.10 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.

1.10.1 LAN-Akt.-Verbindungen

Anzahl aktueller Konfigurationsverbindungen vom LAN

1.10.2 LAN-Ges.-Verbindungen

Anzahl bisheriger Konfigurationsverbindungen vom LAN

1.10.3 WAN-Akt.-Verbindungen

Anzahl aktueller Konfigurationsverbindungen vom WAN

1.10.4 WAN-Ges.-Verbindungen

Anzahl bisheriger Konfigurationsverbindungen vom WAN

1.10.5 Outband-Akt.-Verbindungen

Anzahl aktueller Outband-Konfigurationsverbindungen

1.10.6 Outband-Ges.-Verbindungen

Anzahl bisheriger Outband-Konfigurationsverbindungen

1.10.7 Outband-Bitrate

Bitrate der letzten Outband Konfigurationssitzung

1.10.8 Login-Fehler

Gesamtzahl der fehlerhaften Logins

1.10.9 Login-Sperren

Anzahl der Login-Sperrungen

1.10.10 Login-Ablehnungen

Anzahl der Login-Versuche, während die Login-Sperre aktiv war

1.10.11 Werte-loeschen

Config-Statistik löschen

1.11 Queue-Statistik

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

1.11.1 LAN-Heap-Pakete

Anzahl verfügbarer Puffer

1.11.2 LAN-Queue-Pakete

Anzahl belegter Puffer

1.11.3 WAN-Heap-Pakete

Anzahl verfügbarer Puffer

1.11.4 WAN-Queue-Pakete

Anzahl belegter Puffer

1.11.5 ARP-Query-Queue-Pakete

Anzahl der ARP-Pakete in der Query-Queue

1.11.6 ARP-Queue-Pakete

Anzahl der ARP-Pakete in der normalen Queue

1.11.7 IP-Queue-Pakete

Anzahl der IP-Pakete in der normalen Queue

1.11.8 IP-Urgent-Queue-Pakete

Anzahl der IP-Pakete in der gesicherten Queue

1.11.9 ICMP-Queue-Pakete

Anzahl der ICMP-Pakete

1.11.10 TCP-Queue-Pakete

Anzahl der TCP-Pakete

1.11.11 TFTP-Queue-Pakete

Anzahl der TFTP-Pakete

1.11.12 SNMP-Queue-Pakete

Anzahl der SNMP-Pakete

1.11.13 Prot-Heap-Pakete

Anzahl der Prot-Heap-Pakete

1.11.14 IPR-Queue-Pakete

Anzahl der Pakete, die noch durch den IP-Router bearbeitet werden sollen.

1.11.15 DHCP-Server-Queue-Pakete

Anzahl der Pakete in der Empfangs-Queue des DHCP-Servers.

1.11.16 IPR-RIP-Queue-Pakete

Anzahl der Pakete in der Empfangs-Queue des IP-RIP-Moduls (für RIP-Anfragen, RIP-Propagierungen ...).

1.11.17 DNS-Sende-Queue

Anzahl der Pakete, die zu DNS- oder NBNS-Servern weitergeleitet werden sollen.

1.11.18 DNS-Empfangs-Queue

Anzahl der Pakete, die von DNS- oder NBNS-Servern kommen und an den Host weitergeleitet werden sollen.

1.11.19 IP-Masq. Sende-Queue

Anzahl der Pakete, die maskiert versendet werden sollen (ins Internet).

1.11.20 IP-Masq. Empfangs-Queue

Anzahl der Pakete, die aus dem Internet empfangen wurden und demaskiert werden müssen.

1.11.21 WLAN-Management-Heap-Pakete

Anzahl der im Puffer verfügbaren Pakete.

1.11.22 PROT-Heap-Pakete

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.23 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.24 IPR-Queue-Pakete

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.25 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.26 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.27 DHCP-Server-Queue-Pakete

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.28 DHCP-client-queue-packets

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.29 IPR-RIP-Queue-Pakete

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.30 DNS-Sende-Queue

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.31 DNS-Empfangs-Queue

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.32 IP-Masq. Sende-Queue

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.11.33 IP-Masq. Empfangs-Queue

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.12 Verbindungs-Statistik

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

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

Die gesamten angefallenen Gebühren werden nicht unmittelbar angezeigt. Es wird jedoch intern eine Summierung der Gebühren durchgeführt, um das Gebührenbudget verwalten zu können.

1.13 Info-Verbindung

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

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

lfc	Status	Mode	Gerätename
Ch01	Bereit		
Ch02	Bereit		

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	bezeichnet den zugehörigen Kanal.
Status	gibt den Zustand der jeweiligen Verbindung an. Mögliche Werte sind: Initialisierung , Setup-WAN , Bereit , Anwahl , Anliegender-Ruf , Protokoll , Verbindung , Rückruf sowie Bündelung und Reserviert . Der Status Bündelung wird im Display (nur <i>ELSA LANCOM Wireless</i>) durch Anfügen von „/2“ in Spalte 15 und 16 der zugehörigen Displayzeile ebenfalls angezeigt. Bündelung erscheint für das zweite Interface, wenn entweder auf dem ersten Interface eine Bündelverbindung aktiviert wurde oder eine Festverbindung mit zwei B-Kanälen eingestellt wurde. Reserviert wird das zweite Interface, wenn auf dem ersten B-Kanal eine Verbindung besteht und die Y-Verbindung deaktiviert wurde.
Mode	gibt die Art des Aufbaus wieder. Möglich sind: Akt. (aktiver Verbindungsaufbau = Anwahl) Pas. (passiver Verbindungsaufbau = Anruf) RR (Aufbau durch Rückruf) Fest (Festverbindung)
Rufnummer	gibt die Rufnummer der Gegenstelle aus der Namenliste an.
Gerätename	gibt den logischen Namen der Gegenstelle an (sofern dieser auflösbar ist). Der Gerätename wird ebenfalls auf dem Display in der entsprechenden Displayzeile mit angezeigt, sobald eine logische Verbindung besteht.
B1-HZ	gibt die Haltezeit (Short-Hold-Zeit) der Verbindung an.
B2-HZ	gibt die Haltezeit (Short-Hold-Zeit) für gebündelte Kanäle dieser Verbindung an.

1.14 Layer-Verbindung

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

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

1.15 Ruf-Info-Tabelle

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

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

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

Systemzeit	Ifc	CLIP-Anrufer	Wahl-Anrufer	Dienst	B-Kanal
0T; 00:01:13	S ₀	4321	1234	HDLC64K	2
0T; 00:01:02	S ₀	4321	1234	HDLC64K	1
0T; 00:00:06	S ₀	5678	1234	HDLC64K	1

Die Einträge haben die folgende Bedeutung:

Systemzeit	Zeitpunkt, zu dem der Ruf ankam. Dabei wird entweder die Betriebszeit des Geräts angezeigt oder die Systemzeit des ISDN-Netzes (falls diese vom ISDN-Anschluß zur Verfügung gestellt wird).
Ifc	Bezeichnet das zugehörige Interface.
CLIP-Anrufer	Die Rufnummer (CLIP) des Anrufers
Wahl-Anrufer	Die vom Anrufer gewählte MSN/EAZ
Dienst	Hier ist der vom Anrufer gewünschte Dienst eingetragen. Mögliche Werte sind HDLC64K, HDLC56K und unbekannt. Ein analoger Ruf wird hier also als unbekannt angezeigt. <i>LANCOM Office</i> -Router können zusätzlich die Werte A-3kHz (analog 3kHz), Sprache (für normale Sprachübertragung) und Fax-G2/3 (für analoge Faxübertragungen nach Gruppe 2 oder 3) angezeigt werden.
B-Kanal	Hier wird der benutzte B-Kanal eingetragen. Ein Wert von 0 bedeutet, daß alle Kanäle bereits belegt sind, es sich also um ein Anklopfen handelt.

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

1.16 Gegenst.-Statistik

In dieser Tabelle werden die letzten hundert Verbindungen mit Informationen über die Gegenstelle angezeigt.

Die Tabelle hat den folgenden Aufbau:

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

Die Einträge haben die folgende Bedeutung:

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

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

1.17 Aktuelle-Zeit

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

1.18 Kanal-Statistik

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

/S ₀ -Bus	Fortlaufende Statusanzeigen
Interface-Info	Statistik über die auf dem ATM-Interface ausgetauschten Zellen
Verbindungs-Info	Information über die Einstellungen für die einzelnen Kanäle
AAL5-Rx-Fehler	Statistik über die Fehler bei der Zellenübertragung
Werte-loeschen	Löscht alle Werte dieser Statistik

● Interface-Info

Im Interface-Info finden Sie genauere Informationen zum ATM-Interface und den darüber ausgetauschten Zellen:

Phy-Signal	Physikalische Verbindung zur Vermittlungsstelle vorhanden
LCR	Physikalische Geschwindigkeit des ATM-Anschlusses
TX-Zellen	Anzahl gesendeter ATM-Nutz-Zellen
TX-OAM-Zellen	Anzahl gesendeter ATM-OAM-Zellen (Zellen mit Überwachungs- und Serviceinformationen, Operation and Maintenance, OAM)

RX-Zellen	Anzahl empfangener ATM-Nutz-Zellen
RX-OAM-Zellen	Anzahl empfangener ATM-OAM-Zellen
UnbRxVpiVci	Anzahl empfangener Zellen mit unbekannten Werten für VPI und/oder VCI
UnbRxPti	Anzahl empfangener Zellen mit nicht unterstützten PTI-Formaten

● Verbindungs-Info

Im Verbindungs-Info finden Sie die für jeden Kanal eingestellten Leistungsparameter:

Kanal	Nummer des logischen Kanals
VPI	Virtual Path Identifier
VCI	Virtual Channel Identifier
AAL-Typ	ATM-Adaption-Layer-Typ
SCR	Sustainable Cell Rate, Grundanteil der Zellenübertragungsrate
SBR	Sustainable Bit Rate, Grundanteil der Übertragungsrate in Bit
PCR	Peak Cell Rate, zulässiger Spitzenwert der Zellenübertragungsrate
PBR	Peak Bit Rate, zulässiger Spitzenwert der Übertragungsrate in Bit
MBS	Maximum Burst Size, Länge der maximal zulässigen SCR-Überschreitung in Zellen

● AAL5-RX-Fehler

Informationen über die Übertragungsverluste:

Kanal	Nummer des logischen Kanals
VPI	Virtual Path Identifier
VCI	Virtual Channel Identifier
CRC-Fehler	Anzahl der Fehler in der Prüfsumme
SAR-Auszeit	Wartezeit, in der ein Paket zusammengesetzt sein muß, bevor es verworfen wird
Ueberggr.-SDU	Anzahl der Pakete, die aufgrund einer Übergröße (mehr als 65k) verworfen wurden
Zell-Verlust	Anzahl der verworfenen Zellen
Wiederanlauf	Anzahl der Zellen, die aufgrund der Suche nach dem Paketanfang verworfen wurden

1.19 Werte loeschen

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.20 Zeit-Statistik

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

Das Menü hat folgenden Aufbau:

1.20.1 Aktuelle Zeit

Aktuelle Zeit des Geräts

1.20.2 Quelle

Quelle der Zeitangabe. Mögliche Werte sind:

- 'ISDN' für die Übernahme der Zeit aus dem ISDN-Netz,
- 'Manuell' für das manuelle Setzen der Zeit mit dem Befehl 'time',
- 'RAM' für die Übernahme der Zeit aus dem Zwischenspeicher des Gerätes nach einem Bootvorgang.

1.20.3 Übernahme

Anzahl der bisher erfolgten Zeit-Übernahmen aus einer der vorher genannten Quellen

1.20.4 ISDN

Weitere Informationen zur Übernahme der Zeit aus dem ISDN-Netz

1.20.4.1 Verbindungen

Anzahl der Versuche, eine Zeitinformation aus dem ISDN-Netz abzulesen

1.20.4.2 Informationen

Anzahl der aus dem ISDN-Netz erhaltenen Zeitinformationen

1.20.4.3 Infofehler

Anzahl der fehlerhaften Zeitinformationen aus dem ISDN-Netz

1.20.4.4 Einheiten

Anzahl der verbrauchten Einheiten

1.20.4.5 Werte-loeschen

Löschen der ISDN-Informationen

1.21 LCR-Statistik

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

Das Menü hat folgenden Aufbau:

1.21.1 Gesamtaufrufe

Gesamtzahl der Aufrufe des LCR

1.21.2 Erfolge

Anzahl der Aufrufe, bei denen der LCR eine passende Regel in seinen Tabellen fand und die Nummer erfolgreich umgeleitet wurde

1.21.3 nicht-gefunden-Fehler

Anzahl der Aufrufe, bei denen der LCR keine passende Regel in seinen Tabellen fand und die Nummer deswegen nicht umgeleitet wurde

1.21.4 fehlende-Zeit-Fehler

Anzahl der Aufrufe, bei denen der LCR mangels fehlender Zeit nicht eingreifen konnte

1.21.5 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.21.6 Provider-Statistik

Eine Tabelle mit allen angerufenen Providern (bzw. deren Vorwahlen), die Anzahl der erfolgreichen bzw. fehlgeschlagenen Anrufe

1.21.7 Werte-loeschen

LCR-Statistik löschen

1.22 S₀-Bus

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

1.22.1 D-Info

Übersicht über den Zustand eines D-Kanals.

Diese Tabelle zeigt allgemeine D-Kanal-Informationen:

Kanal	Kennzeichnung des B-Kanals.
Protokoll	D-Kanal-Protokoll. Entweder das in der Interface-Tabelle fest eingestellte Protokoll oder das bei der Einstellung 'Auto' am ISDN-Anschluß detektierte Protokoll.
Layer-2	Aktivierung der Schicht 2 des D-Kanals ('Ja' oder 'Nein')
TEI	TEI zugewiesen ('Ja' oder 'Nein')
S ₀ -Aktivierung	Zustandsanzeige der Aktivierung ('Ja' oder 'Nein')

1.22.2 D2-Statistik

Aufschlüsselung der Layer-2-Informationen des D-Kanals für die einzelnen B-Kanäle.

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

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

1.23 Gebuehren-Stat.

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

1.23.1 Rest-Minuten

Restbudget in der aktuellen Überwachungsperiode.

1.23.2 Zeit-Tabelle

Genaue Auflistung der durch die einzelnen Module (Router (ISDN) / Router (DSL) / *LANCAPi* (ISDN) / Zeit-Modul (ISDN)) auf dem jeweiligen Interface angefallenen Onlinezeit.

1.23.3 Werte-loeschen

Gebührenstatistik löschen

1.23.4 Rest-Budget

Restbudget in der aktuellen Überwachungsperiode.

1.23.5 Tabelle-Budget

Genaue Auflistung der durch die einzelnen Module (Router/*LANCAPi*/Zeit-Modul) auf dem ISDN angefallenen Gebühreneinheiten.

1.23.6 Resttage/Per.

Anzahl der verbleibenden Tage bis zum Ablauf des Überwachungszeitraums.

1.23.7 Router-Einheiten

Anzahl der von den Routermodulen in der aktuellen Überwachungsperiode verbrauchten Einheiten.

1.23.8 Gesamt-Einheiten

Anzahl der insgesamt in der aktuellen Überwachungsperiode verbrauchten Einheiten.

1.23.9 Router-Minuten-aktiv

Anzahl der von den Routermodulen in der aktuellen Überwachungsperiode verbrauchten Minuten.

1.24 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.25 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.26 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.27 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.28 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.29 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.30 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31 DHCP-Client-Status

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.1 Status

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.2 Lease-Zeit [Sekunden]

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.3 Zugewiesene-IP-Adresse

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.4 Zugewiesene-IP-Netzmaske

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.5 Gateway-IP-Adresse

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.6 Server-IP-Adresse

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.7 Security-Server

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.8 Zeit-Offset

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.9 Zeit-Server

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.10 Tabelle-Zeit-Server

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.11 Tabelle-Router

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.12 Tabelle-Name-Server

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.13 Tabelle-Domain-Name-Server

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.14 Tabelle-Log-Server

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.31.15 Konfigurations-Datei

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.32 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.33 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.34 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.35 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.36 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.37 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.38 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

1.39 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2 Setup

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

2.1 Name

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

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

anzeigen lassen. Standardmäßig ist kein Name eingetragen.

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

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

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

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

2.2 WAN-Modul

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

2.2.1 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.2.2 Namenliste

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

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

● Rückrufoptionen

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

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

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

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

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

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

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

2.2.3 Round-Robin-Liste

Einstellungen verschiedener Gegenstellen-Nummern

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

2.2.4 Layerliste

Einstellungen der verwendeten Layer-Kombinationen

Mit einem Layer definieren Sie eine Sammlung von Protokoll-Einstellungen, die für die Verbindung zu bestimmten Gegenstellen verwendet werden soll.

Layer-Name	Encaps	Lay-3	Lay-2	Lay-1
DEFAULT	LLC/SNAP	TRANS	TRANS	AAL-5
PPP	TRANS	PPP	TRANS	AAL-5

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

Die folgende Tabelle dient als Beispiel und zeigt gleichzeitig die Standardeinstellungen für ein *ELSA LANCOM*:

Layer-Name	Encaps	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	TRANS	PPP	TRANS	bnd+cmpr	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	none	HDLC64K
MLPPP	TRANS	PPP	TRANS	bnd+cmpr	HDLC64K
RAWHDL	TRANS	TRANS	TRANS	none	HDLC64K

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

Layer-Name	Encaps	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	TRANS	PPP	TRANS	bnd+compr.	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	keine	HDLC64K
MLPPP	TRANS	PPP	TRANS	bnd+compr.	HDLC64K
RAWHDL	TRANS	TRANS	TRANS	keine	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 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. Jeder der hier vordefinierten Layer ist vom Benutzer löscht- oder veränderbar.</p>				
Encaps	<p>In der Spalte Encaps können zusätzliche Informationen zu den zu übertragenden Daten festgelegt werden. Folgende Eintragungen sind möglich:</p>				
	ETHER	<p>Die Daten werden mit einem Ethernet-Header versehen. Diese Einstellung ist zur Kommunikation mit älteren <i>ELSA LANCOM</i>-Geräten oder im Bridge-Betrieb notwendig.</p>			

	TRANS	Bei dieser Einstellung wird kein Ethernet-Header ausgegeben. Es werden z.B. reine IP-Datenpakete übertragen. Diese Einstellung sorgt für den größtmöglichen effektiven Datendurchsatz.
Lay-3	In der Spalte Lay-3 können zusätzliche Header für die Datenübertragung im ISDN definiert werden. Folgende Einstellungen sind wählbar:	
	TRANS	Es wird kein zusätzlicher Header eingefügt (größter Datendurchsatz).
	PPP	Es wird eine Verhandlung nach dem Point-to-Point Protocol durchgeführt.
Lay-2	In dieser Spalte wird das Protokoll für ISDN-Layer-2 eingestellt:	
	TRANS	
Lay-1		

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

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

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

2.2.5 PPP-Liste

Einstellung der Parameter für PPP-Verbindungen

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

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

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Gerätename	In dieser Spalte können Sie den Namen eintragen, mit dem sich die Gegenstelle beim Router anmeldet. Die Groß- und Kleinschreibung wird nicht berücksichtigt!	
Authentifizierung	In dieser Spalte können Sie das Sicherungsverfahren, mit dem die Gegenstelle überprüft werden soll, eintragen. Standardwert: PAP	
	Keine	Der Router handelt beim Verbindungsaufbau keine Authentifizierung mit der Gegenstelle aus. Diese kann selbst jedoch eine Authentifizierung vom Router verlangen.

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

2.2.6 Nummernliste

Einstellung der zugangsberechtigten Rufnummern

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

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

Rufnummer	Gerätenamen
875463	AACHEN
040785647	BERLIN

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

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

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

Falls die Einstellung 'Schutz Nummer oder Name' eingestellt ist und ein Anruf einer Gegenstelle erfolgt, wird die dabei übermittelte Rufnummer der Gegenstelle mit den Einträgen in der Nummernliste vergli-

chen. Sind die übermittelte Rufnummer und ein Listeneintrag identisch, ist der Anrufer zum Verbindungsaufbau berechtigt. Aus der Nummernliste kann außerdem der Name der Gegenstelle ermittelt werden und damit der Layer, der für diese Verbindung verwendet werden soll. Mit diesem Layer wird dann die Verbindung aufgebaut und die Namensüberprüfung mit dem gefundenen Layer gestartet (bzw. mit dem Default-Layer, wenn keiner gefunden wurde).

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

2.2.7 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.2.8 Script-Liste

Einstellung der Anwahl-Scripte

Einige Internet-Provider (z.B. CompuServe) führen vor einer PPP-Verhandlung einen scriptgesteuerten Anmeldevorgang durch. Um auch solche Verbindung aufbauen zu können, ist im *ELSA LANCOM* eine einfache Scriptverarbeitung implementiert (siehe 'Script-Verarbeitung').

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

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

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

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

2.2.9 Schutz

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

- Ist der Schutz auf 'keiner' eingestellt, werden grundsätzlich alle anliegenden Rufe angenommen, solange die Gegenseite das Verbindungsprotokoll unterstützt.
- Mit der Einstellung 'Name' werden nur Rufe von Gegenstellen akzeptiert, für die ein Eintrag in der Namenliste vorhanden ist. Durch diese Überprüfung wird ein zusätzlicher Schutz gewährleistet. Diese Überprüfung steht nur bei Verwendung von PPP zur Verfügung.
- Bei der Einstellung 'Nummer' werden nur solche Gegenstellen akzeptiert, die in der Nummernliste als berechnigte Gegenstellen eingetragen sind.

- Auch ein Kombinationsschutz aus Namenliste oder Nummernliste ist mit 'Nr./Name' einstellbar. Damit wird zunächst geprüft, ob ein Eintrag in der Nummernliste vorhanden ist. Wenn das nicht möglich ist, versucht der Router den Namen über die Protokollverhandlung zu ermitteln.

2.2.10 RR-Versuche

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

2.2.11 Router-Interface-Liste

Einstellungen für das Interface der Routermodule

Diese Tabelle enthält die Interface-Einstellungen, die für die Router-Module gelten.

lfc	MSN/EAZ	YV.	CLIP
S0	123456	Aus	Ein

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

2.2.12 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.2.13 Manuelle-Wahl

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

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

2.2.13.1 Aufbau

Parameter: Gegenstellengerätename (nur über Remote-Konfiguration).

Mit dem Befehl

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

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

Bei Aktivierung der Funktion von der Tastatur der Geräte aus erfolgt jeweils unmittelbar die Anzeige der Fehlermeldung 'Keine Gegenst.', weil dabei kein Name eingegeben werden kann. Diese Funktion ist also von der Tastatur der Geräte 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.

2.2.13.2 Abbau

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

2.2.13.3 Status

Zeigt den aktuellen Verbindungsstatus an

2.2.14 Interface-Liste

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

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

lfc	Protokoll	LCR	VPI
ATM-1	PVC	7075	110

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

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

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

`setup/lancapi-modul`

`setup/ab-modul/port-liste`

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

Ifc	Bezeichnet das zugehörige Interface.
Protokoll	
FV-B-Kanal	Einstellung des B-Kanals, auf dem eine Festverbindung ablaufen soll. Mögliche Werte sind: kein : Keine Zuweisung der Festverbindung auf einen bestimmten Kanal. 1 oder 2 : Festverbindung läuft über den angegebenen B-Kanal. Bitte beachten Sie auch die Hinweise zur Einstellung dieser Parameter in der Beschreibung der Festverbindung.
Anwahl-Präe	Globales Anwahlpräfix für alle Module des Geräts. Die hier eingetragenen Ziffern (maximal 8) werden automatisch bei jeder Anwahl vor die gewählte Rufnummer gestellt. Verwenden Sie dieses Präfix z.B. dann, wenn Ihr Router an eine TK-Anlage angeschlossen ist.
Max-pass-Verb	Anzahl der maximal gleichzeitig möglichen passiven Verbindungen
Max-akt-Verb	Anzahl der maximal gleichzeitig möglichen aktiven Verbindungen

2.2.15 Festverbindung

Einstellungen für die virtuellen ATM-Kanäle

2.2.16 Kanal-Liste

Einstellungen für die Verwendung der verfügbaren Kanäle

2.2.17 ISDN-Namenliste

Einstellungen für die Gegenstellen

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

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

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

Geraetenname	Rufnummer	Layername	Kontraktename
AACHEN	F1:	DEFAULT	VBR
BERLIN	F2:	PPP	CBR

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

● Rückrufoptionen

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

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

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

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

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

HINWEIS: 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.

2.2.18 DSL-Namenliste

Einstellungen für die Gegenstellen

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

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

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

Die Bedeutung der Felder ist nachfolgend näher beschrieben:

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

2.2.19 Verkehrskontrakte

Einstellungen für die Leistungsmerkmale der ATM-Verbindungen

2.3 Gebühren-Modul

Über diesen Menüpunkt werden notwendige Einstellungen für den Gebührenschutz vorgenommen.

HINWEIS: *Der Gebührenschutz gilt nicht für die a/b-Ports!*

2.3.1 Budget-Einheiten

Budget an Gebühreneinheiten, das innerhalb des Überwachungszeitraums genutzt werden darf. Steht hier der Wert 0, so ist die Überwachung abgeschaltet.

2.3.2 Tage/Periode

Anzahl Tage in einem Überwachungszeitraum.

2.3.3 Rest-Budget

Restbudget in der aktuellen Überwachungsperiode.

2.3.4 Router-Einheiten

Auflistung der durch Routerbetrieb angefallenen Gebühreneinheiten.

2.3.5 Tabelle-Budget

Genaue Auflistung der durch die einzelnen Module (Router/LANCAPI/Zeit-Modul) auf dem ISDN angefallenen Gebühreneinheiten.

2.3.6 Gesamt-Einheiten

Auflistung der durch die einzelnen Module angefallenen Onlinezeit.

2.3.7 Zeit-Tabelle

Genaue Auflistung der durch die einzelnen Module auf dem jeweiligen Interface angefallenen Onlinezeit.

2.3.8 Minuten-Budget

Onlinezeit, die innerhalb des Überwachungszeitraums genutzt werden darf. Steht hier der Wert 0, so ist die Überwachung abgeschaltet

2.3.9 Rest-Minuten

Restbudget in der aktuellen Überwachungsperiode.

2.3.10 Router-Minuten

Gesamt-Onlinezeit seit Einschalten des Geräts.

2.3.11 Aktivieren-Reserve

Mit dieser Aktion wird das Zusatzbudget freigeschaltet.

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

2.4 LAN-Modul

Unter diesem Menüpunkt werden die für das lokale Netzwerk relevanten Anschlußwerte angezeigt. Über diesen Menüpunkt werden die für das lokale Netzwerk notwendigen Einstellungen vorgenommen. Das Menü hat folgenden Aufbau:

2.4.1 Anschluß

Wahl des Netzwerkanschlusses

2.4.2 Node-ID

MAC-Layer-Adresse des Geräts

Unter diesem Menüpunkt wird die eigene Ethernet-Adresse des Routers angezeigt. Der hier angezeigte Wert wurde vom Hersteller festgelegt und kann nicht verändert werden. Die Anzeige der Ethernet-Adresse erfolgt als zwölfstellige Hexadezimalzahl, wobei die ersten sechs Stellen '00a057' für ein ELSA-Gerät stehen.

2.4.3 Heap-Reserve

Pufferspeicher für die Aufnahme von Datenpaketen aus dem lokalen Netzwerk

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

2.5 Bridge-Modul

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.1 Zustand

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.2 Gegenstelle

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.3 Bridge-Tabelle

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.4 Aging-Minute(n)

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.5 LAN-Einstellung

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.5.1 Broadcast

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.5.2 Multicast

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.5.3 Ziel-Adresse

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.5.3.1 Filter-Typ

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.5.3.2 Filter-Tabelle

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.5.4 Quell-Adresse

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.5.4.1 Filter-Typ

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.5.4.2 Filter-Tabelle

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.6 WAN-Einstellung

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.6.1 Broadcast

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.6.2 Multicast

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.6.3 Ziel-Adresse

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.6.3.1 Filter-Typ

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.6.3.2 Filter-Tabelle

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.6.4 Quell-Adresse

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.6.4.1 Filter-Typ

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.5.6.4.2 Filter-Tabelle

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.6 IPX-Modul

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

2.6.1 Zustand

IPX-Modul ein- oder ausgeschaltet

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

HINWEIS: 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.

2.6.2 IPX-Router

IPX-Router ein- oder ausgeschaltet

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

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

2.6.3 LAN-Einstellung

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

2.6.3.1 Netzwerk

Logische IPX-Netzwerknummer des LAN-Anschlusses

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

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

2.6.3.2 Binding

Einstellung der Ethernet-Frame-Typen für den LAN-Anschluß

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

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

2.6.3.3 SPX-Watchdog

Einstellungen für SPX-Watchdog-Verwaltung

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.

2.6.3.4 IPX-Watchdog

Einstellungen für IPX-Watchdog-Verwaltung

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.

2.6.3.5 NetBIOS-Watch

Einstellungen für NetBIOS-Watchdog-Verwaltung

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

2.6.3.6 Socket-Filter

Filtertabelle für Zielsocketfilterung

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 Verbindungsauf-

bauten führen würden, sind bereits defaultmäßig in der LAN-Filter-Tabelle vorhanden (siehe dazu auch FAQs zum 'IPX-Router').

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

2.6.3.7 Lok.-Routing

Lokales Routing aktiviert oder deaktiviert

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

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

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

2.6.3.8 2.6.3.8 RIP-SAP-Skal.

RIP-SAP-Skalierung aktiviert oder deaktiviert

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

2.6.3.9 LOOP-propagieren

Propagieren von redundanten Routen aktiviert oder deaktiviert

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'.

2.6.4 WAN-Einstellung

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

2.6.4.1 Routing-Tabelle

Router-Tabelle für die Zuordnung von IPX-Netzwerk und Gegenstelle

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

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

Hierbei bedeuten:

- **Gegenstelle:** Name der logischen Gegenstelle (wie in /Setup/WAN-Modul/ Namenliste angegeben).
- **Netzwerk:** Die Adresse des WAN-seitigen Netzwerk. Es muß ein eigenständiges Netzwerk verwendet werden, für die beiden beteiligten Router jedoch das gleiche!
- **Binding:** Zu verwendendes Ethernet-Binding auf der ISDN-Strecke. Diese Angabe wird nur berücksichtigt, wenn Ethernet-Encapsulation im verwendeten Layer eingestellt ist. Wird kein Binding eingegeben, so wird 802.3 angenommen.
- **Propagate:** Dieser Eintrag gibt an, wie mit IPX-Paketen vom Typ 20 (NetBIOS Propagated Frames) verfahren werden soll. Mögliche Einstellungen sind Route oder Filter. Hat dieses Feld den Eintrag **Filter** werden keine Propagated Frames an diese Gegenstelle weitergeleitet. Hat der Eintrag den Wert **Route**, so werden die Pakete an alle gerade erreichbaren Gegenstellen weitergeleitet, d.h., zu der Gegenstelle muß eine Verbindung bestehen, oder es ist mindestens ein Kanal für einen Verbindungsaufbau zur Gegenstelle verfügbar.

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

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

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

Die Default-Einstellung ist 'Ein'.

2.6.4.2 Socket-Filter

Filtertabelle für Ziel-Socketfilterung

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.

2.6.5 RIP-Einstellung

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

2.6.5.1 Tabelle-RIP

Anzeigen der RIP-Tabelle

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

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

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

2.6.5.2 LAN-Filtertab.

Filterbereiche für IPX-Netzwerkadressen (LAN)

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

2.6.5.3 WAN-Filtertab.

Filterbereiche für IPX-Netzwerkadressen (WAN)

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

2.6.5.4 Routen/Frm

Max. # RIP-Einträge pro gesendeten RIP-Frame

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.

2.6.5.5 Aging-Minute(n)

Aging-Zeitraum in Update-Einheiten

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.

2.6.5.6 Spoofing

RIP-Spoofing-Verfahren einstellen

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

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

HINWEIS: 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.

2.6.5.7 WAN-Update-Min.

RIP-Update-Zeitraum, je nach Spoofing wirksam

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

2.6.6 SAP-Einstellung

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

2.6.6.1 Tabelle-SAP

Anzeigen der SAP-Tabelle

Über diesen Menüpunkt werden die Einträge der aktuellen SAP-Tabelle angezeigt. Die Tabelle umfaßt maximal 512 Einträge. Die Tabelle ist nach dem Service-Typ und bei gleichem Typ nach Server-Namen sortiert. Eine beispielhafte SAP-Tabelle könnte wie folgt aussehen:

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

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

2.6.6.2 LAN-Filtertab.

Filterbereiche für IPX-Service-Adressen (LAN)

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

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

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

Anfangsservice	Endservice
030c	030c

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

2.6.6.3 WAN-Filtertab.

Filterbereiche für IPX-Service-Adressen (WAN)

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

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

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

Startservice	Endservice
0004	0004

2.6.6.4 Server/Frm

Max. # SAP-Einträge pro gesendeten SAP-Frame

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.

2.6.6.5 Aging-Minute(n)

Aging-Zeitraum in Update-Einheiten

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.

2.6.6.6 Spoofing

SAP-Spoofing-Verfahren einstellen

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

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

HINWEIS: 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.

2.6.6.7 WAN-Update-Min.

SAP-Update-Zeitraum, je nach Spoofing wirksam

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

2.7 TCP-IP-Modul

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

2.7.1 Zustand

TCP/IP-Modul ein- oder ausgeschaltet

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

2.7.2 IP-Adresse

Hier wird die zur IP-Adresse gehörende Netzmaske angezeigt, wie sie vom Headend bei der Registrierung übermittelt wurde.

● LAN-IP-Adresse

Hier kann eine zweite IP-Adresse für das den Router eingegeben werden. Hier kann die LAN-seitige IP-Adresse für das Gerät eingegeben werden. Mit dieser zweiten IP-Adresse kann das Gerät einerseits für zwei logische IP-Netze als Router dienen, andererseits erhält diese Adresse eine besondere Bedeutung bei Verwendung von IP-Masquerading:

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

In diesem Fall werden alle Rechner, die sich im durch LAN-seitige IP-Adresse und LAN-seitige IP-Netzmaske aufgespannten Netz befinden, hinter der vom Provider zugewiesenen Adresse (bzw. der Cable-IP-Adresse) „versteckt“.

● Intranet-Maske

Hier muß die zur IP-Adresse des lokalen Netzes gehörende Netzmaske eingegeben werden. Die Standardeinstellung ist 255.255.255.0 (Klasse C Netz).

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

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

- LAN-IP-Netzmaske

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

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

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

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

2.7.3 IP-Netz-Maske

Passende IP-Netzmaske des lokalen Netzes

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

2.7.4 Intranet-Adr.

Eigene Intranet-Adresse

2.7.5 Intranet-Maske

Passende Intranet-Netzmaske des lokalen Netzes

2.7.6 Zugangsliste

Einschränkung des Zugriffs auf interne Funktionen über TCP/IP

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

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

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

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

- **SNMP:** die Konfigurations-Schnittstelle auf Basis von SNMP.

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

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

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

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

IP-Adresse	IP-Netz-Maske
192.234.222.0	255.255.255.0

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

2.7.7 DNS-Default

Domain Name Server

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

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

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

2.7.8 DNS-Backup

Backup Domain Name Server

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

2.7.9 NBNS-Default

NetBIOS Name Server

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

2.7.10 NBNS-Backup

Backup NetBIOS Name Server

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

2.7.11 ARP-Aging-Min

Verweildauer für Einträge in der ARP-Tabelle

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.

2.7.12 TCP-Aging-Min

Zeitbeschränkung für Konfigurations-Verbindungen, die inaktiv sind

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

2.7.13 TCP-Max.-Verb.

Max. Anzahl gleichzeitiger Konfigurations-Verbindungen zum *ELSA LANCOM*

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

2.7.14 Cable-IP-Adresse

IP-Adresse des Geräts im Kabelnetz

2.7.15 Cable-IP-Netz-Maske

Passende IP-Netzmaske aus dem Kabelnetz

2.7.16 Tabelle-ARP

ARP-Tabelle für Abb. einer IP-Adresse auf eine MAC-Adresse

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

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

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

2.7.17 LAN-IP-Adresse

IP-Adresse des Geräts im lokalen Netz (LAN)

2.7.18 LAN-IP-Maske

Passende IP-Netzmaske aus dem LAN

2.8 IP-Router-Modul

HINWEIS: In diesem Abschnitt werden die Funktionen des Kabelmodems als IP-Router beschrieben. Wenn also im folgenden von 'Router' geschrieben wird, ist damit das Kabelmodem in der Betriebsart als IP-Router gemeint.

Über dieses Menü können Einstellungen für das IP-Router-Modul vorgenommen werden.

2.8.1 Zustand

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

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

2.8.2 IP-Routing-Tabelle

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

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

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

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

- Die längste Netzmaske steht oben.

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

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

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

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

IP-Adresse	IP-Netz-Maske	Router-Name	Distanz
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.240.0.0	0.0.0.0	0
10.0.0.0	255.0.0.0	0.0.0.0	0
255.255.255.255	0.0.0.0	Kabelnetz	0

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

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

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

IP-Adresse	IP-Netz-Maske	Router-Name	Distanz	Maskierung
192.120.130.10	255.255.255.255	DRESDEN	0	Aus
192.120.130.11	255.255.255.255	DRESDEN	0	Aus
192.120.130.12	255.255.255.255	DRESDEN	0	Aus

IP-Adresse	IP-Netz-Maske	Router-Name	Distanz	Maskierung
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

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

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

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 mit dem Namen 'Cable' steht für das Kabelnetz. Der Router schickt also alles, was er über andere Routen nicht weiterleiten oder verwerfen soll, an das Headend beim Kabelnetzbetreiber.

Um alle Datenpakete an ein bestimmtes Netz z.B. über einen ISDN-Router im lokalen Netz in ein anderes LAN zu routen, tragen Sie die IP-Adresse des anderen Netzes mit der Netzmaske in die Tabelle ein und geben als 'Router' die lokale IP-Adresse des ISDN-Routers ein. Sie verwenden z.B. in Ihrem lokalen Netz die IP-Adressen aus dem Adreß-Kreis 10.1.0.0 (Netzmaske 255.255.255.0). Der ISDN-Router hat die lokale IP-Adresse '10.1.0.99', das andere lokalen Netz (Ihre Filiale) verwendet 10.2.0.0 (Netzmaske 255.255.255.0). Mit den folgenden Einträgen leitet das Kabelmodem alle Datenpakete für das andere Netz an den ISDN-Router weiter und schickt alle anderen Datenpakete in das Kabelnetz (sofern Sie nicht in den verbotenen Bereichen liegen):

IP-Adresse	IP-Netz-Maske	Router-Name	Distanz
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.240.0.0	0.0.0.0	0
10.2.0.0	255.255.255.0	10.1.0.99	0
10.0.0.0	255.0.0.0	0.0.0.0	0
255.255.255.255	0.0.0.0	Cable	0

HINWEIS: Schalten Sie für diese Funktion auch das lokale Routing ein!

2.8.3 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.8.4 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.8.5 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.

2.8.6 Lok.-Routing

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

2.8.7 Routing-Methode

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

Das Menü hat den folgenden Aufbau:

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

2.8.7.1 Routing-Methode

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

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

2.8.7.2 ICMP-Routing-Methode

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

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

2.8.8 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

2.8.8.1 RIP-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.

2.8.8.2 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.
- **Kl+Adr:** Die Netzwerkmaske wird aus der IP-Adressen-Klasse und einem angefügten Teil nach dem Adreßverfahren gebildet. Aus obiger Adresse und der Netzmaske 255.255.0.0 ergibt sich somit die IP-Netzmaske 255.128.0.0.

2.8.8.3 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

2.8.9 Masquerading

In diesem Menü werden die Einstellungen für die Maskierungsfunktion vorgenommen.

2.8.9.1 TCP-Aging-Sekunde(n)

Zeit in Sekunden bis eine TCP-Maskierung ungültig wird

2.8.9.2 UDP-Aging-Sekunde(n)

Zeit in Sekunden bis eine UDP-Maskierung ungültig wird

2.8.9.3 ICMP-Aging-Sekunde(n)

Zeit in Sekunden bis eine ICMP-Maskierung ungültig wird

2.8.9.4 Service-Tabelle

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

Z-Port	Intranet-Adresse
20	10.1.1.10
21	10.1.1.10

Hierbei bedeuten:

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

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

Mit dem Befehl

```
telnet 192.38.50.100:27
```

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

2.8.9.5 Tabelle-Masquerading

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

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

Hierbei bedeuten:

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

2.8.10 Firewall

In diesem Menü werden die Filter für die IP-Pakete eingestellt.

2.8.10.1 Objekt-Tabelle

In der Objektliste können die zu filternden Objekte definiert werden. Objekte können sein:

- Protokolle
- Einzelne Rechner
- Ganze Netze
- Dienste

Bzw. eine beliebige Kombination dieser Elemente. Weiterhin können Objekte rekursiv definiert werden. So könnte zunächst Objekte für die Protokolle TCP und UDP definiert werden. Später kämen dann Objekte z.B. für FTP (= TCP + Ports 20 und 21), HTTP (= TCP + Port 80) und DNS (= TCP, UDP + Port 53) definiert. Diese könnten dann wiederum zu einem Objekt zusammengefaßt werden, daß alle Freigaben enthält.

Die Objektbeschreibung wird in einem String abgelegt. Die einzelnen Elemente der Beschreibung werden durch die folgenden Token separiert.

Token	Bedeutung
%Pxx	Protokoll oder Protokoll-Liste, wenn durch Komma getrennt
%Ax.x.x.x	IP-Adresse oder Adress-Liste, wenn durch Komma getrennt.
%Mx.x.x.x	Netzmaske. Wird zu einer IP-Adresse (%A) keine Maske angegeben, so wird 255.255.255.255 angenommen. Die Netzmaske muß immer nach der Netzadresse angegeben werden

%L	lokales Netz (also die durch IP-Adresse und IP-Netz-Maske sowie durch Intranet-Adresse und Intranet-Maske aufgespannten Netze)
%S	Service (=Port) oder Port-Liste, wenn durch Komma getrennt bzw. Port-Bereich wenn durch 'Minus' getrennt
%H	Host oder Host-Liste, wenn durch Komma getrennt. Hier kann der Name eines Rechners im lokalen Netz oder eines Dial-In-Users angegeben werden. Wenn ein Rechnername angegeben ist, so muß dieser Rechner seine IP-Adresse vom DHCP-Server des LANCOMs beziehen.

Einzelne Beschreibungen werden durch "+" oder ein Leerzeichen voneinander getrennt. Beides ist gleichbedeutend. Bei der späteren Filterbildung wird die Vereinigungsmenge der Objekte ausgewertet, d.h. in dem obigen Beispiel (FTP, HTTP und DNS) würde jeweils ein Filter für die Ports 20-21, 53 und 80 für das Protokoll TCP sowie ein Filter für den Port 53 des Protokolls UDP erzeugt

Die Objekt-Tabelle hat den folgenden Aufbau (Mit DEFAULT-Werten):

Name	Beschreibung
UDP	%P17
TCP	%P6
ICMP	%P1
NETBIOS	%S137-139
LOCALNET	%L
ANY	
ANYHOST	%a0.0.0.0 %m0.0.0.0

Das Objekt "ANY" steht dabei nur für einen Platzhalter, der in der Regelliste z.B. in der Protokoll-Spalte eingesetzt werden kann, falls die jeweils zu filternden Protokolle bereits an Objekte gebunden sind (wie im Beispiel mit FTP, HTTP und DNS)

2.8.10.2 Regel-Tabelle

Über die Regel-Tabelle werden die einzelnen Objekte zu Filterregeln kombiniert. Die Regel-Tabelle enthält das zu filternde Protokoll, die Quell-Objekte, die Ziel-Objekte, sowie die auszuführende Filteraktion.

Das Protokoll, sowie die Quell- bzw. Ziel-Objekte können sowohl aus zusammengestellten Objekten bestehen, als auch direkte Beschreibungen (z.B. %P6 für TCP) beinhalten.

Bei genauer Betrachtung der Aktions-Möglichkeiten stellt man fest, daß sich die bisher implementierten Möglichkeiten auf vier getrennte Einstellungen reduzieren. Daher wurde die Auswahl der Aktionen zunächst durch einen Inputset beschränkt. Er enthält die folgenden Einstellmöglichkeiten:

Immer-Filter	Das Paket wird immer gefiltert
Aufbau-Filter	Das Paket wird gefiltert, wenn ein Aufbau nötig ist
Internet-Filter	Das Paket wird gefiltert, wenn es über die Default-Route gesendet oder von dieser Empfangen wurde
Annehmen	Das Paket wird immer angenommen

Die Regel-Tabelle hat den folgenden Aufbau (Mit DEFAULT-Werten):

Name	Prot.	Quelle	Ziel	Aktion
WINS	UDP, TCP	anyhost netbios	anyhost	Internet-Filt

Im Protokoll-Feld könne neben Objekten und Objektbeschreibungen die Protokollnummern auch direkt angegeben werden, also statt %P6 für TCP reicht Die Angabe der Protokollnummer 6. Weiterhin können hier Objekte zusätzlich zu ,+' und Leerzeichen noch mit einem Komma getrennt werden (wegen Protokoll-Liste). Ein Protokoll-Bereich (Trennung mit ,-') kann jedoch nicht angegeben werden.

Übernahme der alten Filter

Die bisherigen LAN- und WAN-Filter werden als direkte Beschreibung in die Regelliste wie folgt übernommen:

LAN-Filter

Die folgende Tabelle gibt einen Überblick, wie die alten LAN-Filter in der neuen Regel-Tabelle eingetragen werden. Dies wird in der Letzten Spalte anhand des NetBIOS-Filters beispielhaft vorgeführt.

Feld in Regel-Tabelle	Eintrag in LAN-Filter	Ersetzung in Regel-Tabelle	Beispiel NetBIOS
Name	Idx	LAN-Idx	LAN-WIN
Prot.	ICMP	1	6, 17
	TCP	6	
	UDP	17	
	T/U	6, 17	
	Alle	0	
Quelle	Q-von Q-bis	%SQ-von-Qbis	%S137-139
	Quell-Adresse	%AQuell-Adresse	%A0.0.0.0
	Quell-Netz-Mask	%MQuell-Netz-Mask	%M0.0.0.0
Ziel	Z-von Z-bis	%SZ-von-Z-bis	%S0-0
Aktion	Typ	Typ (bleibt erhalten, wird jedoch intern umkodiert)	Immer-Filt.

WAN-Filter

Die folgende Tabelle gibt den entsprechenden Überblick, für die alten WAN-Filter:

Feld in Regel-Tabelle	Eintrag in WAN-Filter	Ersetzung in Regel-Tabelle
Name	Idx	WAN-Idx
Prot.	ICMP	1
	TCP	6
	UDP	17
	T/U	6,17
	Alle	0

Quelle	Q-von Q-bis	%SQ-von-Q-bis
Ziel	Z-von Z-bis	%SZ-von-Zbis
	Ziel-Adresse	%AZiel-Adresse
	Ziel-Netz-Mask	%MZiel-Netz-Mask
Aktion	Keine Eintrag	Immer-Filt.

2.8.10.3 Filter-Liste

Aus Objekt-Tabelle und Regel-Tabelle wird schließlich die Filter-Liste aufgebaut. Dabei wird wie bereits weiter oben erwähnt die Vereinigungsmenge aller durch die Regeln und Objekte definierten Filter gebildet. Mit den Default-Einstellungen in der Objekt- Und Regel-Liste ergibt sich folgende Default-Filterliste

Die IP-Filter sind in einer Tabelle mit dem folgenden Aufbau definiert:

Idx.	Prot	Quell-Adresse	Quell-Netzmaske	Q-von	Q-bis	Ziel-Adresse
WIN	TCP	255.255.255.255	0.0.0.0	137	139	0.0.0.0

Ziel-Netzmaske	Z-von	Z-bis	Aktion
0.0.0.0	53	53	

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.
- **Prot**
Protokoll, das gefiltert werden soll. Möglich sind **TCP**, **UDP**, **ICMP** und **alle**.
Die Einstellung **alle** filtert jedes Paket aus dem spezifizierten Quell-Netz bzw. zum Ziel-Netz.
- **Quell-Adresse, Quell-Netzmaske**
Hiermit kann ein Subnetz des lokalen Netzes angegeben werden, für das der Filter gelten soll. Ist die Quell-Adresse 0.0.0.0 so bedeutet das, daß der Filter auf jeden Rechner angewendet wird. Eine Netzmaske von 0.0.0.0 bedeutet, daß der Filter auf alle Netze angewendet wird (was ebenfalls alle Rechner bedeutet).
- **Q-von, Q-bis**
Quell-Port-Bereich, der gefiltert werden soll. Ein Bereich von 0 bis 0 bedeutet, daß kein Quell-Port von diesem Filter beeinflusst wird.
- **Ziel-Adresse, Ziel-Netzmaske**
Hiermit kann ein Subnetz des lokalen Netzes angegeben werden, für das der Filter gelten soll. Die Ziel-Adresse 0.0.0.0 bedeutet, daß der Filter auf jeden Rechner angewendet wird. Eine Netzmaske von 0.0.0.0 bedeutet, daß der Filter auf alle Netze angewendet wird (was ebenfalls alle Rechner bedeutet).

- **Z-von, Z-bis**
Ziel-Port-Bereich, der gefiltert werden soll. Ein Bereich von 0 bis 0 bedeutet, daß kein Ziel-Port von diesem Filter beeinflusst wird.
- **Aktion**
Der Filter kann ein Paket verwerfen (nicht weiterleiten) oder akzeptieren (weiterleiten).

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

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

2.8.11 Kein Eintrag

2.8.12 Kein Eintrag

2.8.13 Default-Zeittabelle

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

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

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

2.8.14 Nutzung-Default-Listen

Schaltet die Verwendung der Default-Liste ein oder aus.

2.8.15 LAN-Filtertab.

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

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

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

Die Felder der Tabelle haben folgende Bedeutung:

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

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

2.8.16 WAN-Filtertab.

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

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

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

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

- Ziel-Adresse, Ziel-Netzmaske

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

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

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

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

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

2.8.17 Start-Adreß-Pool

Beginn des Adreß-Pools, aus dem die IP-Adressen für einwählende Geräte dynamisch zugewiesen werden. Diese Funktion wird auch als IP-Pooling bezeichnet und z.B. für Remote Access von mehreren Außendienstmitarbeitern verwendet.

Der Adreß-Pool sollte im selben Adreßbereich wie der Router liegen. Legen Sie den Adreßpool nach Möglichkeit so groß aus, daß alle einwählenden Geräte eine IP-Adresse zugewiesen bekommen können (z.B. je eine Adresse für die verfügbaren B-Kanäle).

Wenn das einwählende Gerät bei der Anwahl zunächst eine Verbindung aufbauen kann, diese Verbindung dann jedoch direkt während der Protokollverhandlung wieder getrennt wird, deutet das auf fehlende freie IP-Adressen im IP-Pool hin.

2.8.18 Ende-Adreß-Pool

Ende des Adreß-Pools für IP-Pooling.

2.9 SNMP-Modul

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

/SNMP-Modul	Einstellungen für das SNMP-Modul
Traps-senden	Schalter für die Ausgabe von SNMP-Traps
IP-Trap-Tabelle	Tabelle mit 20 Ziel-Adressen für Trap-Nachrichten
Administrator	Geräte-Administrator
Standort	Geräte-Standort

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

2.9.1 Traps-senden

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

2.9.2 IP-Trap-Tabelle

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

2.9.3 Administrator

Name des Administrators

2.9.4 Standort

Standort des Gerätes

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

2.9.5 Register-Monitor

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

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

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

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

2.9.6 Loesche-Monitor

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

2.9.7 Monitor-Tabelle

Die Monitor-Tabelle hat folgenden Aufbau:

IP-Adresse	Port	MAC-Adresse	Timeout	Geraetenname
10.0.0.53	1057	0080c76da46e	1	LC1

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

2.9.8 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.9.9 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.9.10 Passw.Zwang-fuer-SNMP-leseszugriff

Festlegung, ob für den SNMP-Lesezugriff eine Passwortabfrage erfolgen soll (EIN) oder nicht (AUS).

2.10 DHCP-Modul

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

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

2.10.1 Zustand

Ein: Das Gerät arbeitet als DHCP-Server

Aus: Das Gerät arbeitet nicht als DHCP-Server

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

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

HINWEIS: Falls im TCP/IP-Modul keine Kabel- oder LAN-IP-Adresse eingetragen ist (z.B. Auslieferungszustand), dann verteilt das Kabelmodem im Auto-Modus IP-Adressen aus dem Adreßbereich 10.0.0.2—10.0.0.253 an alle DHCP-Clients.

2.10.2 Start-Adreß-Pool (Ende-Adreß-Pool)

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

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

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

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

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

2.10.3 (Start-Adreß-Pool) Ende-Adreß-Pool

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

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

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

Als IP-Adresse wird dann eine gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit bereits schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an,

und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

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

2.10.4 Netz-Maske

Die Zuweisung der Netzmaske erfolgt analog zur Adreßzuweisung:

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

2.10.5 Broadcast-Adresse

Die Zuweisung der Broadcast-Adresse erfolgt analog zur Adreßzuweisung:

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

2.10.6 Max.-Gültigkeit-Minute(n)

Hier kann die maximale Gültigkeitsdauer eingetragen werden, die der DHCP-Server einem Host zuweist. Der DEFAULT-Wert von 6000 Minuten entspricht ca. 4 Tagen.

2.10.7 Default-Gültigkeit-Minute(n)

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

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

2.10.8 Tabelle-DHCP

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

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

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

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

2.10.9 Host-Tabelle

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.10.10 Alias-Tabelle

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.10.11 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.10.12 Master-Server

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.10.13 Reply-Anpassung

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.10.14 Gateway-Adresse

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.10.15 Relay-Cache

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.11 Config-Modul

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

/Config-Modul	Einstellungen für das Konfigurationsmodul
LAN-Config	Schalter für Konfiguration von der LAN-Seite
WAN-Config	Schalter für Konfiguration von der WAN-Seite
Passwort-Zwang	Paßwortzwang ein/aus, wenn kein Paßwort vorhanden ist
Maximale Verbindungen	Maximale Anzahl gleichzeitiger Verbindungen
Fernconfig-(EAZ-MSN)	Rufnummer für die Fernkonfiguration über PPP

/Config-Modul	Einstellungen für das Konfigurationsmodul
Conf.-Haltezeit	Zeitbeschränkung für Remote-Konfigurationsverbindungen
Login-Fehler	Anzahl für Login-Fehlversuche, bevor die Login-Sperre greift
Sperr-Minuten	Dauer der Sperrung und Zeitraum, bis alte Login-Fehler vergessen sind
Sprache	Sprache für die Konfiguration

2.11.1 LAN-Config

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

2.11.2 WAN-Config

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

2.11.3 Passw.Zwang

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

2.11.4 Maximale-Verb.

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

2.11.5 Conf.-Aging-Min.

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.11.6 Sprache

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

2.11.7 Login-Fehler

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

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

2.11.8 Sperr-Minuten

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

2.11.9 Fernconfig-(EAZ-MSN)

Diese Rufnummer erlaubt die Fernkonfiguration über PPP. Solange keine Nummer eingetragen ist, werden Rufe auf beliebige Nummern für die Fernkonfiguration angenommen.

2.12 ab-Modul

Hier können Sie alle Einstellungen für die a/b-Ports des Gerätes vornehmen.

2.12.1 Port-Liste

Die Port-Liste zeigt Ihnen die aktuelle Konfiguration der ab-Ports.

2.12.2 Amtsholung-Liste

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.12.3 Amtsberechtigung-Liste

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.12.4 Prioritäten-Liste

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.12.5 Klingelfolge

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.12.6 Land

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.13 LANCAP-Modul

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

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

Das *LANCAPi*-Modul hat folgenden Aufbau:

/LANCAPi-Modul	Einstellungen für die <i>LANCAPi</i>
Zugangsliste	Liste der Rechner, die die <i>LANCAPi</i> nutzen dürfen
UDP-Port	UDP-Port für die Kommunikation zwischen <i>LANCAPi</i> -Server und -Clients
Interface-Tabelle	EAZ oder MSN, auf die die <i>LANCAPi</i> reagieren soll
Prioritäten-Tabelle	Priorität für die <i>LANCAPi</i> gegenüber Routerverbindungen

- **Zustand:** 'ein', 'aus' oder 'abgehend'. Bei letztgenannter Einstellung werden keine ankommenden Rufe von der *LANCAPi* angenommen.

2.13.1 Zugangsliste

Grenzen Sie hier den Kreis der Rechner ein, die die *LANCAPi* nutzen dürfen. Diese Tabelle kann maximal 16 Einträge aufnehmen. Ist die Tabelle leer, können alle Rechner auf die *LANCAPi* zugreifen.

2.13.2 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.13.3 UDP-Port

Dieser Port steht in der Standardeinstellung auf '75'. Ändern Sie diesen Port nur dann, wenn andere Geräte in Ihrem Netz schon diesen Port verwenden.

HINWEIS: Beim Umstellen des Ports gehen alle aktiven Verbindungen über die *LANCAPi* verloren!

2.13.4 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.13.5 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.13.6 Interface-Tabelle

Geben Sie die Rufnummern ein, auf die die *LANCAPi* reagieren soll. Wenn Sie mehrere Nummern eingeben wollen, trennen Sie die einzelnen Nummern durch Semikola.

2.13.7 Prioritäten-Tabelle

Mit der Priorität steuern Sie die Möglichkeit, für abgehende Verbindungen über die *LANCAPi* Routerverbindungen zu unterbrechen. Mit der Option '1' werden keine Routerverbindungen unterbrochen, mit der Einstellung '2' werden nur Nebkanäle einer Routerverbindung mit Kanalbündelung unterbrochen, mit der Auswahl '3' werden auch Hauptkanäle einer Routerverbindung unterbrochen.

2.14 Zeit-Modul

Der Least-Cost-Router im Gerät benötigt korrekte Zeitinformationen für die Berechnung der Rufnummernumleitungen über Call-by-Call-Provider. Auch bei einigen Statistiken ist die Anzeige einer präzisen Zeitinformation wünschenswert.

Die Zeit kann entweder manuell gesetzt werden (mit dem Befehl 'time') oder automatisch aus dem ISDN-Netz abgelesen werden.

Für den automatischen Zeitabgleich wird beim Einschalten des Moduls direkt eine vorher bestimmte Gegenstelle angerufen und dabei die Zeitinformation aus dem ISDN-Netz übernommen. Solange das Zeit-Modul eingeschaltet ist, wird bei jeder Verbindung erneut die Zeit aus dem ISDN übernommen.

Das Zeit-Modul hat folgenden Aufbau:

/Zeit-Modul	Einstellungen für das Zeit-Modul
Zustand	Aktivierung des Moduls: Ein, Aus
Aktuelle-Zeit	Anzeige der aktuellen Zeit im Gerät
Zeit-Rufnummer	Rufnummer, zu der eine Verbindung aufgebaut werden soll, um eine Zeitinformation aus dem ISDN-Netz zu erhalten
Anwahl-Versuche	Anzahl der möglichen Versuche, eine Zeitinformation zu erhalten.

2.14.1 Zustand

Aktivierung des Moduls: **Ein, Aus**

2.14.2 Aktuelle-Zeit

Anzeige der aktuellen Zeit im Gerät

2.14.3 Zeit-Rufnummer

Rufnummer, zu der eine Verbindung aufgebaut werden soll, um eine Zeitinformation aus dem ISDN-Netz zu erhalten

2.14.4 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.14.5 Anwahl-Versuche

Anzahl der möglichen Versuche, eine Zeitinformation zu erhalten.

2.15 LCR-Modul

Bei der Einstellung des Least-Cost-Routers geben Sie folgende Informationen an:

- Für welche Module im Gerät sollen die Funktionen des LCR aktiv sein?
- Welche Vorwahlen sollen wann über welchen Call-by-Call-Provider umgeleitet werden?

Das LCR-Modul hat folgenden Aufbau:

/LCR-Modul	Einstellungen für den Least-Cost-Router
Router-Nutzung	LCR für die Routermodule aktivieren, Ein oder Aus
Lancapi-Nutzung	LCR für die <i>LANCAPI</i> aktivieren, Ein oder Aus
ab-Port-Nutzung	LCR für die analogen ab-Ports aktivieren, Ein oder Aus
Zeittabelle	Tabelle der Rufumleitungen
Feiertagstabelle	Liste der Feiertage, die von der Zeittabelle berücksichtigt werden müssen.

2.15.1 Router-Nutzung

LCR für die Routermodule aktivieren, **Ein** oder **Aus**.

2.15.2 Lancapi-Nutzung

LCR für die *LANCAPI* aktivieren, **Ein** oder **Aus**

2.15.3 ab-Port-Nutzung

LCR für die analogen ab-Ports aktivieren, **Ein** oder **Aus**

2.15.4 Zeittabelle

Die Zeittabelle hat 256 Einträge mit folgendem Aufbau:

Index	Praefix	Tage	Start	Stop	Nummernliste	Rueckfall
1	0171	192	0:00	23:59	01013;01070	Ein

Die einzelnen Einträge haben die folgende Bedeutung:

Index	Durchlaufender Index für die Einträge in der Tabelle
Praefix	Vorwahl, die umgeleitet werden soll
Tage	Gültigkeit des Eintrags für Wochen- und Feiertage in Darstellung einer 8-bit-Maske: Bit 0 steht für Montag, Bit 7 für Feiertage. Der Eintrag '31' bezeichnet also alle Werkzeuge, '192' die Sonn- und Feiertage
Start	Anfangszeit für die Gültigkeit des Eintrags an den definierten Tagen
Stop	Endzeit für die Gültigkeit des Eintrags an den definierten Tagen
Nummernliste	Netzkennzahl des Call-by-Call-Providers
Rueckfall	Automatischer Rückfall auf die eigene Telefongesellschaft, falls alle Call-by-Call-Nummern besetzt sind

Beispiel:

`set 1 02 31 1:00 11:59 01030;01090;01070 Ein` leitet alle Fernverbindungen in die Region '02' zwischen ein und zwölf Uhr um auf den Provider mit der Netzkennzahl '01030'. Falls da besetzt ist, werden die Netzkennzahlen '01090' und '01070' versucht. Sind die auch nicht verfügbar, wird die Verbindung über die normale Telefongesellschaft aufgebaut.

2.15.5 Feiertagstabelle

Die Feiertagstabelle hat 256 Einträge mit folgendem Aufbau:

Index	Datum
1	01010000
2	01050000
3	03100000
4	25120000
5	26120000
6	02041999
7	13051999

Die einzelnen Einträge haben die folgende Bedeutung:

Index	Durchlaufender Index für die Einträge in der Tabelle
Datum	Datum der einzelnen Feiertage Geben Sie den Index und das Datum vollständig ohne Trennzeichen ein, also z.B. 'set 8 13041999' für den 13. April 1999 als achten Listeneintrag. Geben Sie als Jahr '0000' für jährlich wiederkehrende Feiertage ein.

2.16 NetBIOS-Modul

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

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

2.16.1 Zustand

Hier schalten Sie das NetBIOS-Modul ein oder aus.

2.16.2 Scope-ID

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

2.16.3 NT-Domaene

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

2.16.4 Gegenstellen-Tab.

In der Gegenstellen-Tabelle werden alle Gegenstellen eingetragen, die NetBIOS Informationen erhalten sollen, bzw. von denen NetBIOS-Information angenommen werden. Wenn das NetBIOS-Modul eingeschaltet ist, werden NetBIOS-Pakete von anderen als den angegebenen Gegenstellen stillschweigend verworfen. Die Gegenstellen-Tabelle hat den folgenden Aufbau:

Name	Typ
AACHEN	Router oder Workstation

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

● Typ

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

2.16.5 Host-Tabelle

Die Host-Tabelle hat den folgenden Aufbau:

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

2.16.6 Gruppentabelle

Die Gruppentabelle sieht entsprechend so aus:

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

Die Felder der Tabellen haben dabei die folgende Bedeutung:

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

● Flags

Die Flags haben folgende Bedeutung:

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

Die Server-Liste hat den folgenden Aufbau:

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

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

Dabei haben die einzelnen Felder die folgende Bedeutung:

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

2.17 DNS-Modul

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

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

2.17.1 Zustand

Zustand des DNS-Moduls (Ein oder Aus)

2.17.2 Domaene

Eigene Domain, optional, maximal 32 Zeichen

2.17.3 DHCP-verwenden

Einstellung für die verwendung des DHCP-Servers (Ja oder Nein)

2.17.4 NetBIOS-verw.

Einstellung für die Verwendung von NetBIOS (Ja oder Nein)

2.17.5 DNS-Tabelle

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

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

Rechnername	Ip-Adresse
HOST10	10.0.0.10

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

2.17.6 Filter-Liste

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

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

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

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

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

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

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

2.17.7 Gültigkeit

Gibt an, welche Gültigkeit einem anfragenden Rechner für einen Namen mitgeteilt wird. Default: 2000

2.18 Accounting-Modul

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

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

Die Accounting-Liste hat folgenden Aufbau:

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

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

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

- Verbindungen

Anzahl der für den User gezählten Verbindungsaufbauten.

2.19 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.19.1 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.19.2 Kein Eintrag

Eine aktuelle Version der Hilfe finden Sie unter www.elsa.de/help.

2.20 HTTP-Modul

Hier können Sie das Verzeichnis ändern, wenn Sie Ihre HTML-Hilfdateien lokal ablegen möchten.

2.20.1 Dokumentenwurzel

Wenn Sie lokal auf die Hilfdateien zugreifen möchten, geben Sie hier das Verzeichnis an, in dem sich die lokale Kopie befindet.

2.21 SYSLOG-Modul

Über den Syslog-Dienst hat man die Möglichkeit Statusmeldungen aus dem Netzwerk zentral zu sammeln. Zudem ist syslog durch die Tatsache, daß die Statusmeldungen im Klartext übertragen werden, deutlich flexibler als z.B. Lösungen, die über SNMP Traps arbeiten, da SNMP nur wenige standardisierte Traps bietet und immer eine MIB mitgeliefert werden muß, die erst die Übersetzung von gerätespezifischen Traps ermöglicht.

Weiterhin bietet Syslog über die Klassifizierung einer Nachricht nach Priorität und Facility die Möglichkeit, gezielt spezielle Nachrichten zu versenden bzw. deren Aussendung zu unterdrücken.

2.21.1 Zustand

Über diesen Menüpunkt wird das SYSLOG-Modul ein- und ausgeschaltet

2.21.2 Tabelle-SYSLOG

In der Syslog-Tabelle (Table-SYSLOG) kann angegeben werden, welcher Rechner welche Syslog-Nachrichten erhält.

Diese Tabelle hat den folgenden (beispielhaften) Aufbau:

Idx.	IP-Address	Source	Level
SALR	10.0.0.170	01	01
ADMA	10.0.0.170	40	ff
CNAL	10.0.0.180	31	0A

Im Feld Idx. wird ein vier Zeichen langer Index für einen Eintrag angegeben, über den die Einträge auseinandergehalten werden. Dies ist nötig, da z.B. zu einer IP-Adresse mehrere Kombinationen von Quelle und Level eingetragen werden könnten.

Das Feld IP-Address enthält nun die IP-Adressen der jeweiligen Empfänger.

Im Feld Source ist die jeweilige Quelle der an die vorgenannte Adresse zu sendenden Nachrichten codiert. Dabei handelt es sich um ein Bitfeld, in dem für jede Quelle genau ein Bit reserviert ist. Für die Zuordnung zwischen Quelle und Bits gilt dabei folgende Tabelle:

Quelle	Bit	Wert
SYSTEM	0	0x01
CONN-LOGIN	1	0x02
CRON	2	0x04
ADMIN-LOGIN	3	0x08
CONNECTION	4	0x10
ACCOUNTING	5	0x20
ADMIN	6	0x40
PACKET	7	0x80

Im Feld Level ist der Alarmlevel der an den jeweiligen Syslogempfänger zu sendenden Nachrichten codiert. Auch hierbei handelt es sich um ein Bitfeld, in dem für jeden Level genau ein Bit reserviert ist. Für die Zuordnung zwischen Leveln und Bits gilt dabei folgende Tabelle:

Level	Bit	Wert
ALERT	0	0x01
ERROR	1	0x02
WARNING	2	0x04
INFO	3	0x08
DEBUG	4	0x10

Eine erzeugte Syslog-Message wird genau dann an den eingetragenen Rechner verschickt, wenn sowohl das passende Quellen- als auch das Level Bit gesetzt sind.

Damit ergibt sich aus der oben beispielhaft beschriebenen Syslog-Tabelle, daß der Rechner 10.0.0.170 folgende Nachrichten erhält:

- SYSTEM_ALERT (Index SALR: Source 01 = SYSTEM, Level 01 = ALERT)
- ADMIN_fff (Index ADMA: Source 40 = ADMIN, Level f f = all levels)

Der Rechner 10.0.0.180 erhält hingegen die folgenden Nachrichten:

- CONN-LOGIN_INFO
- CONN-LOGIN_ERROR
- CONNECTION_INFO

- CONNECTION_ERROR
- ACCOUNTING_INFO
- ACCOUNTING_ERROR

(Index CNAL: Source 31 = CONN-LOGIN + CONNECTION + ACCOUNTING, Level 0A = ERROR + INFO)

2.21.3 Facility-Mapper

Der Facility-Mapper erlaubt eine gezielte Zuordnung zwischen internen Nachrichtenquellen und den im Syslog-Paket gemeldeten Facilities. Die Tabelle hat den folgenden Aufbau (incl.Defaultwerten).

Quelle	Facility
System	KERN
Login	AUTH
Systemzeit	CRON
Konsole-Login	AUTHPRIV
Verbindungen	LOCAL0
Accounting	LOCAL1
Administration	LOCAL2
Router	LOCAL3

Die Quellbits, die in der Syslog-Tabelle eingetragen werden müssen um eine Quelle freizuschalten, entsprechen der Auflistung der Quellen im Facility-Mapper (System => Bit 0, Login => Bit 1 etc.)

2.21.4 Port

Hier wird festgelegt, auf welchem Port die Syslog-Meldungen verschickt werden sollen. Die Default-Einstellung ist Port 514

3 Firmware

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

3.1 Versions-Tabelle

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

3.2 Tabelle-Firmsafe

In dieser Tabelle finden Sie für jede der beiden im Gerät gespeicherten Firmware-Versionen die Angaben über die Position im Speicherbereich (1 oder 2), die Angabe des Zustandes (aktiv oder inaktiv), die Versionsnummer, das Datum, die Größe und den Index (fortlaufende Nummer).

Position	Status	Version	Datum	Groe	Index
1	inaktiv	1.60	23061999	690	6
2	aktiv	1.60	30061999	692	7
3	<Lader>	1.60	07061999	64	0

Um eine inaktive Firmware zu aktivieren, geben Sie den Befehl

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

3.3 Modus-Firmsafe

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

- 'Unmittelbar': Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:
 - Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.
 - Arbeitet die neue Firmware jedoch nicht korrekt, ist das Gerät evtl. nach dem Neustart nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit das Gerät neu.
- 'Login': Um den Problemen einer fehlerhaften Firmware zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.
 - Im Unterschied zur ersten Variante wartet Firmsafe anschließend auf einen erfolgreichen Login. Nur wenn dieser Login während der unter 'Timeout-Firm-

safe' eingestellten Zeit erfolgt, wird die neue Firmware auch dauerhaft aktiviert.

- Wenn das Gerät nicht mehr ansprechbar ist und ein Login somit unmöglich ist, aktiviert Firmsafe automatisch wieder die bisherige Firmware und startet damit das Gerät neu.
- 'Manuell': Auch bei der dritten Möglichkeit können Sie vorher selbst eine Zeit bestimmten (Timeout-Firmsafe), in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, daß die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird.

3.4 Timeout-Firmsafe

Zeit in Minuten für den Test einer neuen Firmware

4 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

4.1 Manuelle Wahl

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

4.1.1 Aufbau

Dieser Menüpunkt baut eine Verbindung auf.

4.1.2 Abbau

Dieser Menüpunkt beendet eine Verbindung

4.1.3 Status

Dieser Menüpunkt zeigt den aktuellen Verbindungsstatus an.

4.2 System-Boot

Über diesen Menüpunkt kann das Gerät neu gestartet werden.

Vor der Ausführung des Befehls werden alle offenen Verbindungen abgebaut bzw. geschlossen.

4.3 System-Reset

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

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

4.4 System-Upload

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

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

