



LANCOM™ Office



© 2000 ELSA AG, Aachen (Germany)

Tutte le indicazioni fornite nel presente manuale sono state date alle stampe dopo un accurato esame. Ciononostante non costituiscono una garanzia assoluta per le caratteristiche del prodotto. ELSA risponde unicamente della merce prevista nelle condizioni di vendita e di consegna.

La distribuzione e la riproduzione della documentazione e del software relativi al presente prodotto nonché l'utilizzo del suo contenuto non sono possibili senza previa autorizzazione scritta di ELSA. Ci si riserva il diritto di apportare quelle modifiche che possano favorire il progresso tecnico.

ELSA ha ottenuto la certificazione DIN EN ISO 9001. Con l'attestato del 15.06.1998, il competente Ufficio di sorveglianza tecnica TÜV CERT certifica la conformità alla normativa, riconosciuta a livello mondiale DIN EN ISO 9001. Il numero di certificazione di ELSA corrisponde a 09 100 5069.

Tutte le dichiarazioni e titoli sull'autorizzazione del prodotto si trovano nell'appendice di questa documentazione, sempre che essi siano stati disponibili al momento della stampa.

Marchi

Windows[®], Windows NT[®] e Microsoft[®] sono marchi registrati della Microsoft, Corp.

Il logo ELSA è un marchio registrato di ELSA AG. Tutti gli altri nomi e denominazioni utilizzati possono essere marchi o marchi registrati dei rispettivi proprietari.

ELSA si riserva il diritto di modificare i dati menzionati senza darne prima comunicazione e non si assume alcuna responsabilità per le eventuali imprecisioni tecniche e/o omissioni.

ELSA AG

Sonnenweg 11

52070 Aquisgrana

Germania

www.elsa.com

Aquisgrana, aprile 2000

Qualche parola di presentazione

Vi ringraziamo per la fiducia accordataci

Con *ELSA LANCOM Office* si è scelto uno router con il quale poter collegare reti locali o singoli computer a Internet tramite una linea ISDN.

Varianti di modelli

La presente documentazione descrive diverse varianti di modelli della serie *ELSA LANCOM Office* che si differenziano per le diverse dotazioni di hardware e software:

- *ELSA LANCOM 800 Office*
- *ELSA LANCOM 1000 Office*
- *ELSA LANCOM 1100 Office*
- *ELSA LANCOM 2000 Office*

*Limitazione del
modello*

Le parti della documentazione che si riferiscono solo ad una parte dei modelli, sono evidenziate opportunamente o nel testo stesso o tramite relative avvertenze accanto ad esso.

Documentazione

La documentazione allegata è costituita da:

- Manuale
Installazione hardware, descrizione delle funzioni e tipi di funzionamento e esempi di configurazione
- Documentazione elettronica (su CD)
Le informazioni di base tecniche (ad esempio sulla tecnica di rete generale, TCP/IP ecc.), la parte di riferimento da consultare con la descrizione completa dei menù

Molti collaboratori/collaboratrici di diverse sezioni dell'azienda hanno contribuito alla preparazione di questa documentazione, al fine di fornire il migliore supporto possibile nell'impiego del prodotto ELSA.



Se si hanno ancora dubbi sui temi trattati in questo manuale o si ha bisogno di un aiuto supplementare, si ha a disposizione il server Internet www.elsa.de ventiquattro ore su ventiquattro. Qui si possono trovare nella sezione 'Support' al punto 'Know-how' molte risposte alle « domande più frequenti ». Inoltre la banca dati tecnici (KnowledgeBase) offre un ampio pool di informazioni. Driver aggiornati, firmware, tool e manuali sono disponibili in ogni momento per essere scaricati.

La KnowledgeBase si trova anche sul CD. A questo scopo avviare il file `Misc\Support\MISC\ELASIDE\index.htm`.

Contenuti

1 Introduzione	11
1.1 Che cosa fa un router?	11
1.2 Che cosa offre un <i>ELSA LANCOM Office</i> ?	13
2 Installazione	21
2.1 Complesso di fornitura	21
2.2 Presupposti di sistema	21
2.3 Impostazione del computer del posto di lavoro	22
2.3.1 Windows 95 e Windows 98	22
2.3.2 Windows NT 4.0	23
2.4 <i>ELSA LANCOM Office</i> si presenta	25
2.4.1 Il lato anteriore dell'apparecchio	25
2.4.2 Il retro dell'apparecchio	28
2.5 Come si può collegare l'apparecchio?	29
2.5.1 Installazione del software	30
2.6 Configurazione	31
2.6.1 Impostazioni di base	31
2.6.2 Impostare l'accesso a Internet	36
3 Possibilità di configurazione	39
3.1 Molte strade portano al <i>ELSA LANCOM</i>	39
3.2 La via diretta: Outband	40
3.2.1 Presupposti per la configurazione outband	40
3.2.2 Configurazione outband con <i>ELSA LANconfig</i>	40
3.2.3 Configurazione outband con emulatore di terminale	41
3.3 La via comoda: Inband	41
3.3.1 Presupposti	41
3.3.2 Alternativa: Gestione indirizzi con il server DHCP	41
3.3.3 La configurazione tramite <i>ELSA LANconfig</i>	42
3.3.4 La configurazione tramite Telnet	43
3.4 L'Accesso remoto: Configurazione tramite Accesso remoto	43
3.4.1 Quello che serve per la configurazione remota	43
3.4.2 Come si prepara la configurazione remota	44
3.4.3 Il primo collegamento remoto con Accesso remoto (<i>ELSA LANconfig</i>)	44
3.4.4 Il primo collegamento remoto con un PPP Client e Telnet	44
3.4.5 Limitazione della configurazione remota	45
3.5 Nuovo firmware con FirmSafe	46



3.5.1 FirmSafe funziona così	47
3.5.2 Un nuovo software si carica così	47
3.6 Che cosa succede sulla linea?	49
3.6.1 <i>ELSA LANmonitor</i>	50
3.7 Documentazioni trace	52
3.7.1 Avviamento di trace	52
3.8 Configurazione con SNMP	54

4 Funzioni e modalità **55**

4.1 Sicurezza per la configurazione	55
4.1.1 Protezione con password	56
4.1.2 Il blocco del login	56
4.1.3 Controllo in arrivo tramite TCP/IP	57
4.2 Sicurezza per la LAN	57
4.2.1 Il controllo	57
4.2.2 La chiamata di risposta	59
4.2.3 Come nascondersi: mascheratura IP (NAT, PAT)	60
4.3 Gestione degli addebiti	60
4.3.1 Limitazione della connessione ISDN in base agli addebiti	61
4.3.2 Limitazione della connessione ISDN in base al tempo	61
4.3.3 Impostazioni nel modulo addebiti	62
4.4 Connessioni ISDN	63
4.4.1 Lista di nomi ISDN	64
4.4.2 Impostazioni di interfaccia	65
4.4.3 Impostazioni di interfaccia router	66
4.4.4 Impostazioni di interfaccia <i>LANCAPI</i>	66
4.4.5 Lista layer	67
4.4.6 Lista round-robin	68
4.4.7 Script	69
4.4.8 Accettazione di chiamate	69
4.4.9 Lista dei numeri	70
4.5 Gestione indirizzi automatica con DHCP	70
4.5.1 Il server DHCP	70
4.5.2 DHCP – 'On', 'off' o 'auto'?	71
4.5.3 Gli indirizzi vengono assegnati in questo modo	72
4.5.4 Configurazione del server DHCP	75
4.6 DNS	78
4.6.1 Che cosa fa un server DNS?	78
4.6.2 Come si imposta il server DNS	80
4.7 NetBIOS proxy	82

4.7.1	In breve: Che cosa è il NetBIOS?	82
4.7.2	Trattamento dei pacchetti NetBIOS	83
4.7.3	Quali sono i presupposti indispensabili?	84
4.7.4	Come si connettono due reti Windows	88
4.7.5	Come si seleziona un computer con accesso remoto	89
4.7.6	Cercato – Trovato: L'ambiente di rete	90
4.8	Il least-cost router	91
4.8.1	Il least-cost-router di <i>ELSA LANCOM</i> opera in questo modo.	92
4.9	<i>ELSA CAPI Faxmodem</i>	97
4.9.1	Installazione	97
4.9.2	Invio di fax tramite <i>ELSA CAPI Faxmodem</i>	98
4.10	Comunicazione di ufficio e <i>ELSA LANCAPI</i>	98
4.10.1	<i>ELSA LANCAPI</i>	98
4.11	L'impianto telefonico incorporato	103
4.11.1	Connessione di terminali analogici	103
4.11.2	Configurazione con <i>ELSA LANconfig</i> e il settaggio assistito	104
4.11.3	Configurazione manuale con <i>ELSA LANconfig</i>	106
4.11.4	Servizio dell'impianto interno tramite telefono	116
4.12	Accounting	124
4.12.1	Configurazione dell'accountings	125
4.12.2	Lettura delle informazioni di accounting	125

5 Appendice 127

5.1	Dati tecnici	127
5.2	Dichiarazioni di conformità	129
5.3	Condizioni generali di garanzia	132

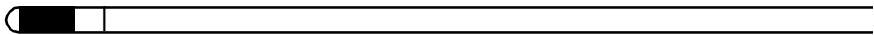
● Index 135

● Technical basics (solo CD) R-1

Network technology	R-1
The network and its components	R-1
Connection modes	R-2
Kinds of networks	R-3
IP addressing	R-3
IP routing and hierarchical IP addressing	R-6
Expansion through local networks	R-8
Point-to-point protocol	R-12
The protocol	R-13
The PPP list	R-14

Everything ok? Checking the line with LCP	R-15
Assigning IP addresses via PPP	R-16
Callback functions	R-17
Fast ELSA callback	R-20
Callback as specified in RFC 1570 (PPP LCP extensions)	R-20
Channel bundling with MLPPP	R-21
IPX routing	R-22
Naming IPX addresses	R-23
Information about the LAN	R-23
IPX routing table	R-23
What happens when data is transmitted on an IPX network?	R-24
RIP and SAP tables	R-25
So many routers around here.....	R-25
Redundant routes	R-25
Exponential backoff.....	R-26
IPX packet filters	R-26
IP routing	R-28
The IP routing table	R-28
TCP/IP packet filters	R-31
Proxy-ARP	R-32
Local routing	R-32
Dynamic routing with IP RIP	R-33
IP masquerading (NAT, PAT)	R-35
DNS forwarding	R-37
Policy Based Routing	R-38
Bridging	R-38
.....	R-40
● Description of the menu options (solo CD)	R-41
Status	R-43
Display and keyboard	R-44
Status/Connection	R-45
Status/Current-time	R-45
Status/Operating-time	R-45
Status/WAN-statistics	R-46
Status/LAN-statistics	R-48
Status/PPP-statistics	R-49
Status/IPX-statistics	R-57
Status/TCP-IP-statistics	R-62
Status/IP-router-statistics	R-68

Status/Config-statistics	R-70
Status/Queue-statistics	R-70
Status/Connection-statistics	R-71
Status/Info-connection	R-72
Status/Layer-connection	R-73
Status/Call-info-table	R-73
Status/Remote-statistics	R-74
Status/SO-bus	R-75
Status/Channel-statistics	R-75
Status/Time-statistics	R-76
Status/LCR-statistics	R-77
Status/Delete-values	R-77
Setup	R-77
Setup/WAN-module	R-78
Setup/LAN-module	R-88
Setup/IPX-module	R-89
Setup/TCP-IP-module	R-97
Setup/IP-router-module	R-101
Setup/SNMP-module	R-109
Setup/DHCP-module	R-110
Setup/NetBIOS-module	R-112
Setup/Config-module	R-114
Setup/LANCAPI-module	R-116
Setup/LCR-module	R-117
Setup/DNS-module	R-118
Setup/Time-module	R-119
Firmware	R-120
Other	R-122



1 Introduzione

Nella messa in opera di infrastrutture per l'intera azienda, l'impiego di soluzioni basate su router ISDN assume un significato di primo piano. La rete ISDN offre, con elevate velocità di trasmissione e con complessi meccanismi di sicurezza, la base economicamente più attraente per superare le distanze nella rete Wide-Area. Con i router si possono collegare a costi bassi le reti locali nate in luoghi diversi (LAN) e singoli PC. Le filiali e le rappresentanze possono essere collegate via ISDN alla rete della centrale in modo trasparente e dispongono della stessa base di dati della centrale stessa.

Il presente capitolo presenta brevemente l'apparecchio e le sue funzioni. Una descrizione dettagliata delle funzioni, del software e del suo utilizzo, come pure una introduzione alle informazioni di base tecniche si trova nei capitoli seguenti.

1.1 Che cosa fa un router?

Con un router le reti locali (LAN) e i PC singoli vengono collegati e in questo modo costituiscono insieme una Wide Area Network (WAN). Ciascun computer di questa WAN può accedere, a seconda della propria abilitazione, ai computer e servizi di tutta la rete. A tal fine il router cerca un percorso attraverso il quale i dati possono essere scambiati tra i computer.

Questo percorso è già pronto sotto forma di connessione ISDN.

Una forma particolarmente diffusa di connessione in rete è rappresentata dalla connessione a Internet. Se si collega la rete locale di un'azienda con la rete di un Provider Internet, tutti i computer della LAN possono accedere ai servizi e alle offerte della World Wide Web.

Tramite i collegamenti ISDN, si possono anche gestire gli accoppiamenti di rete (IP, IPX) o i servizi di accesso remoto per i collaboratori in servizio esterno.

Ma i router possono fare anche di più. Tramite una speciale interfaccia, l'*ELSA LANCAPi*, si possono offrire in tutta la rete locale le moderne funzioni comunicative di un ufficio come fax o EuroFileTransfer. I corrispondenti programmi di comunicazione trasferiscono i dati attraverso la *LANCAPi* al router, e questo poi provvede alla trasmissione dati. In questo modo diventa del tutto superfluo un costoso e impegnativo equipaggiamento delle singole workstation con proprie periferiche di trasmissione dati.

Se necessario, esso stabilisce automaticamente la connessione con la controparte. Naturalmente se si usano linee fisse non è necessario stabilire la comunicazione.

Concretamente, quando si impiega il router?

In pratica in tutte le circostanze in cui si devono collegare tra loro dei computer e un semplice collegamento modem non è più sufficiente. Sono tali per es. le seguenti applicazioni:

- Internet in LAN

In molte aziende aumenta la richiesta di accesso a Internet da tutte le workstation della LAN. Ricerche online, filetransfer e e-mail sono solo alcune delle applicazioni che possono alleggerire il lavoro agli utenti di PC.

Un router collega tutte le workstation della rete locale con la rete globale Internet. Funzioni di sicurezza come mascheratura IP non solo fanno risparmiare sui costi, ma proteggono anche la rete contro gli attacchi dall'esterno.

- Accoppiamento LAN-LAN

Quando gli affari vanno bene può venire il momento di aprire una succursale o una filiale estera. Naturalmente anche la filiale avrà la propria rete e vorrà mantenersi aggiornata.

L'accoppiamento LAN-LAN riunisce le singole LAN in una grande rete, se necessario in continenti diversi. Nelle connessioni tramite linee a selezione, un intelligente line management in cooperazione con raffinati meccanismi di filtro provvede a ridurre i costi di collegamento. Naturalmente è anche possibile operare tramite connessioni fisse, anche in combinazione con linee di selezione.

- Telelavoro con Accesso remoto

Nelle moderne organizzazioni il lavoro di molti collaboratori diventa sempre più indipendente da una località definita – è importante in particolare l'accesso costante alle informazioni comuni, liberamente disponibili.

La parola magica è Accesso remoto. Il telelavoro per i colleghi che hanno il proprio ufficio a casa o il contatto a distanza con la centrale per i collaboratori in servizio esterno diventano possibili attraverso il router della rete locale della centrale. Naturalmente anche in caso di Accesso remoto un *ELSA LANCOM* provvede alla protezione dei dati aziendali: La funzione richiamata tramite nomi registrati e numeri telefonici fornisce

solo a determinate persone la chiave magica per l'accesso. E per facilitare i conti, anche i costi telefonici vengono rilevati in azienda in modo centralizzato.

- **Comunicazione tramite *LANCAPI***

Invio di fax direttamente dalle applicazioni, segreteria telefonica con annunci differenti secondo l'ora e disbrigo di operazioni bancarie possono essere effettuati senza uscire dall'ufficio: Queste funzioni sono consentite dall'impiego della *LANCAPI*.

La *LANCAPI* è una speciale forma di interfaccia CAPI-2.0, con cui si può accedere a programmi applicativi come *ELSA-RVS-COM* o *ELSA-ZOC* sul router.

- **Funzioni telefono**

ELSA LANCOM 2000 Office, oltre alle caratteristiche di router ISDN, dispone di un impianto telefonico con quattro connessioni analogiche (porte a/b). A queste porte si possono connettere terminali analogici come telefoni o apparecchi fax. In questo modo diventa superfluo il costoso acquisto di nuovi terminali ISDN durante la conversione dalla connessione telefonica analogica a una moderna connessione ISDN.

Per i terminali collegati a queste porte un *ELSA LANCOM* offre molte comode funzioni come per es. comunicazioni interne, conversazioni interne, mediazione, richiamata, smistamento chiamate, attesa in linea, impulso di addebito ecc.

1.2 Che cosa offre un *ELSA LANCOM Office*?

Per offrire una breve panoramica sulle capacità dell'apparecchio, vengono presentate nel seguito le principali caratteristiche.

Facile installazione

- Collegare il *ELSA LANCOM* all'alimentazione elettrica
- Realizzare la connessione alla LAN
- Inserire il cavo ISDN
- Avviare
- Il sistema è pronto

Connessione LAN

I router ISDN di *ELSA* operano in Ethernet.

- Attraverso le connessioni 10Base-2 o 10Base-T si collega *ELSA LANCOM 1000 Office* o *ELSA LANCOM 2000 Office* alla 10Mbit LAN.
- Un *ELSA LANCOM 800 Office* trova l'accesso alla rete locale a 10 Mbit tramite il collegamento 10Base-T.
- Un *ELSA LANCOM 1100 Office* viene collegato tramite connessione 10/100Base-T a (Fast-)Ethernet.

Connessione WAN

Un *ELSA LANCOM Office* viene collegato all'interfaccia(e) S_0 di una connessione ISDN in configurazione punto-a-più punti (connessione multipla) o in configurazione punto-a-punto (connessione impianto). Il router riconosce automaticamente il tipo di connessione e il protocollo canale D utilizzato. Si possono utilizzare connessioni a selezione con DSS1 come pure connessioni fisse.

L'opzione di un collegamento dedicato soggetto a costi deve essere abilitata separatamente.

Configurazione

L'impostazione e l'adattamento dell'apparecchio ai propri compiti specifici si realizza in modo rapido e comodo per mezzo del tool di configurazione in dotazione *ELSA LANconfig* per sistemi operativi Windows. Gli utenti di altri sistemi operativi possono usare la configurazione basata su HTML tramite un browser Web, Telnet o un qualsiasi programma terminale.

L'accesso all'apparecchio è possibile da WAN, da LAN o direttamente attraverso la propria interfaccia di configurazione. In caso di configurazione da LAN o da WAN, oltre a TFTP viene anche supportato SNMP.

Gli assistenti d'installazione integrati di *ELSA LANconfig* e la configurazione HTML aiutano a mettere in servizio i dispositivi con poche operazioni.

Software update

Per rimanere sempre nelle condizioni più aggiornate in campo software, le periferiche possiedono una memoria Flash-ROM. In questo modo un nuovo firmware può essere scaricato comodamente, senza dover aprire l'apparecchio.

La versione attuale è sempre disponibile sui nostri servizi online e può essere scaricata via LAN, WAN o attraverso l'interfaccia di configurazione.

FirmSafe

Quando si scarica il nuovo firmware non si corre alcun rischio: La funzione firmsafe consente di gestire due file di firmware nello stesso apparecchio. Se il nuovo firmware dopo l'upload non funziona come desiderato, si può facilmente ritornare alla versione precedente.

Se durante l'upload si verifica un errore (per es. causato da un errore di trasmissione), viene automaticamente ripristinata la precedente versione pronta per il servizio.

Protezione di accesso

Per la protezione contro accessi non autorizzati alla rete aziendale, il router offre oltre alla protezione con password e al riconoscimento del numero telefonico (CLIP) anche una funzione di richiamata, che consente solo il collegamento alla linea verso utenze ISDN prestabilite. I meccanismi di autenticazione in PPP, filtri firewall e mascheratura IP, completano il concetto di sicurezza. Il blocco del login impedisce inoltre gli attacchi Brute-Force e impedisce l'accesso al router dopo un numero definibile di tentativi di login con password sbagliata.

Protezione addebiti

Attivando le « informazioni di addebito durante il collegamento » nella rete ISDN (secondo AOCD), si possono fissare per la linea ISDN gli scatti disponibili per un determinato periodo. In questo modo le spese telefoniche sono sempre sotto controllo.

Se dalla connessione ISDN non vengono trasmesse informazioni di addebito, in alternativa è possibile definire anche il tempo di connessione ISDN attiva per un intervallo di tempo determinato. Quando questo tempo è stato superato, il router non consente più di stabilire autonomamente la connessione.

Least-cost routing

Anche se è possibile un'ampia scelta di offerte per servizi di telecomunicazione, con il least-cost-router si sceglie sempre la linea ISDN più conveniente.

Si definisce prima il provider che offre le tariffe più convenienti per le proprie necessità, e il router seleziona automaticamente per ogni connessione (indifferentemente se via router, *LANCAPI* o porte a/b) il servizio con la tariffa più conveniente.

Controllo ora automatico

Per generare statistiche significative e per scegliere i percorsi di connessione giusti attraverso il least-cost router la periferica ha sempre bisogno dell'ora esatta. Essa può leggere autonomamente quest'ora dalla rete ISDN. In tale modo l'ora interna del router viene confrontata, ogniqualvolta si stabilisce un collegamento o ad ogni accensione della periferica, con l'ora ISDN. Naturalmente è anche possibile impostare l'ora manualmente.

Raggruppamento di canali e compressione

Sulla linea ISDN l'apparecchio supporta il statico e il raggruppamento di canali dinamico tramite MLPPP e BACP. Con la compressione dati Stac (hi/fn) si può realizzare un aumento della velocità di trasmissione dati fino al 400%.

ELSA LANmonitor

Con questo tool nel sistema operativo Windows si hanno le informazioni di stato del router sempre sul monitor. Per ciascuna periferica della rete locale vengono visualizzate le informazioni più importanti, per es.:

- Stato del collegamento per ogni canale di trasmissione
- Nome della controparte collegata
- Quale modulo dell'apparecchio è collegato (router, *LANCAPI*, porta a/b)
- Durata della connessione e velocità di trasmissione
- Estratti dalla statistica dell'apparecchio (ad esempio informazioni dalla trattativa PPP)

Inoltre il software consente di verbalizzare e memorizzare i messaggi sul PC per impieghi successivi.

Display di stato

Spie LED sul pannello anteriore del router ISDN consentono di controllare le connessioni ISDN e Ethernet, le porte a/b e le connessioni di linea attuali e quindi facilitano la diagnosi in caso di possibili anomalie di sistema.

Statistiche

Con le ampie statistiche il *ELSA LANCOM Office* è sotto controllo. Qui si trovano ad esempio tutte le informazioni sui pacchetti di dati trasferiti e si ottimizza in tal modo la configurazione del proprio apparecchio.

DHCP

I router di ELSA dispongono anche delle funzioni di un server DHCP. Con queste si può rendere disponibile un determinato gruppo di indirizzi IP, che poi il server DHCP può assegnare autonomamente alle singole periferiche della rete locale.

In modalità automatica il router può anche stabilire autonomamente tutti gli indirizzi della rete e assegnarli alle periferiche in rete.

Server DNS

Tramite le funzioni di server DNS del router si possono stabilire dei collegamenti tra gli indirizzi IP e i nomi di computer o reti. Nelle richieste a nomi di computer noti, si può in tal modo direttamente correlare la rotta corretta.

Il server DNS può anche accedere ai nomi e alle informazioni IP del server DHCP e del modulo NetBIOS.

Il server DNS può anche essere utilizzato come efficace filtro per gli utenti della propria LAN. Per singoli computer o per intere reti può essere bloccato l'accesso a determinati domini.

ELSA LANCAPI e ELSA CAPI Faxmodem

L'impiego della *LANCAPI* comporta principalmente vantaggi economici. La *LANCAPI* è una speciale forma di interfaccia CAPI-2.0, con cui diversi programmi di comunicazione (per es. *ELSA-RVS-COM* o *ELSA-ZOC*) possono accedere al router attraverso la rete.

Tutte le workstation incorporate nella LAN ottengono attraverso la *LANCAPI* un accesso illimitato alle funzioni di comunicazione per ufficio come fax e EuroFileTransfer. Senza hardware supplementare sulle workstation, tutte le funzioni vengono realizzate attraverso la rete. In questo modo si evita il costoso equipaggiamento delle workstation con interfacce ISDN o modem. Soltanto il software per comunicazione di ufficio viene installato sulle singole workstation.

Quando si inviano fax viene simulato sulla workstation un apparecchio fax ISDN. Con la *LANCAPI* il PC instrada il fax attraverso la rete al router, e questo stabilisce la connessione con il destinatario tramite ISDN.

Con *ELSA CAPI Faxmodem* è disponibile inoltre in ambiente Windows un driver fax (Standard 1) che, come interfaccia tra *ELSA LANCAPI* e

Solo ELSA
LANCOM 2000
Office

l'applicazione, consente l'impiego di programmi fax standard con un *ELSA LANCOM Office*.

Impianto telefonico incorporato

Un *ELSA LANCOM 2000 Office* può fare ancora di più. Quattro porte a/b incorporate consentono la connessione di telefoni, apparecchi fax o modem analogici.

Le porte a/b sono interessanti specialmente durante la conversione dalle linee analogiche alle connessioni digitali (ISDN). E' possibile continuare ad impiegare sulla workstation terminali analogici come telefoni o apparecchi fax con un *ELSA LANCOM 2000 Office*. Questo consente di risparmiare investimenti supplementari in nuovi terminali digitali. Inoltre l'impianto interno del *ELSA LANCOM 2000 Office* garantisce moderne funzioni supplementari ISDN come smistamento di chiamata, richiamata, mediazione, attesa in linea e conferenza a 3, conversazioni interne, chiamata bambino, impulso di addebito e altro ancora.

Collegamento e gestione della linea

Il router controlla tutti i dati di una rete per rilevare se devono essere trasmessi in un'altra rete o a un altro computer. Se risulta necessaria una trasmissione, il router realizza autonomamente la connessione e la chiude dopo la trasmissione. In tale circostanza le unità a pagamento vengono utilizzate fino alla fine, se le informazioni di addebito vengono trasmesse durante la trasmissione.

Per risparmiare sui costi di trasmissione, il router offre diverse possibilità di filtro secondo la modalità di esercizio. Con questi possono essere esclusi dalla trasmissione i dati di intere reti o di parti di reti. Possono anche essere filtrati dalla trasmissione i dati che rientrano in determinati servizi (per es. servizi di stampa).

NetBIOS proxy

Per l'accoppiamento delle peer-to-peer Microsoft, i router di ELSA offrono una particolare funzione: Attraverso il routing integrato di pacchetti IP NetBIOS, l'accoppiamento di due diventa un gioco da ragazzi. Affinché non tutti i pacchetti NetBIOS causino lo stabilimento della connessione, le controparti con cui devono essere scambiate informazioni NetBIOS vengono immesse in una lista.

Come NetBIOS-Proxy, quindi il router risponde in modo locale alle richieste per computer conosciuti ed evita di stabilire la connessione senza necessità.

Compatibilità tramite PPP

Per la comunicazione con prodotti di altri produttori il router supporta tra l'altro PPP, un protocollo molto diffuso per lo scambio di dati tra connessioni punto-a-punto.

Configurazione remota tramite PPP

Una caratteristica eccezionale della configurazione per il router di ELSA, nel cui luogo nessuno può o vuole occuparsi delle impostazioni, è la configurazione remota tramite collegamento ISDN e l'accesso remoto di Windows. In questo caso è sufficiente alimentare elettricamente e collegare alla connessione ISDN la nuova periferica ed è poi possibile eseguire la configurazione del router dalla propria postazione tramite una connessione PPP. In occasione della prima configurazione questo accesso viene protetto con una password e rimane impedito a chiamanti non autorizzati.

Accounting

La maggior parte delle trasmissioni dati tramite il router di ELSA si svolge o con collegamenti tramite chiamata nei quali gli addebiti vengono calcolati secondo il tempo in cui si è in linea, o con collegamenti continui nei quali gli addebiti vengono calcolati sulla base del volume di dati trasmesso. Solo una piccola parte degli utenti utilizza veri collegamenti fissi con addebito forfettario.

Per molti utenti è per questo motivo importante riconoscere quali computer nella propria LAN usino di più le vie di collegamento e quali costi esse causino.

La funzione di accounting *ELSA LANCOM Office* offre la possibilità di correlare i tempi online e il volume di dati trasmesso ai singoli computer interessati al collegamento. In tal modo si possono riconoscere rapidamente configurazioni errate dei computer o del router e i costi possono essere correlati a coloro che li hanno causati.

2 Installazione

Il presente capitolo vi aiuterà a stabilire nel modo più rapido possibile un collegamento con Internet. Si vedrà prima quale sia il complesso di fornitura del prodotto e si conoscerà poi l'apparecchiatura. A questo punto viene mostrato come collegare l'apparecchiatura e come fare a metterla in servizio.

Le seguenti informazioni si rivolgono ad utenti esperti con conoscenze della configurazione hardware e della rete.

2.1 Complesso di fornitura

Prima di iniziare con l'installazione, controllare il contenuto della confezione relativamente alla completezza. Nella scatola dovrebbero trovarsi i seguenti componenti:

- *ELSA LANCOM Office*
- Alimentatore
- cavo di connessione LAN
- cavo di connessione ISDN
- Cavo per l'interfaccia di configurazione (solo con *ELSA LANCOM 1000 Office*, *ELSA LANCOM 2000 Office* e *ELSA LANCOM 1100 Office*)
- Adattatore per il cavo di configurazione (solo con *ELSA LANCOM 1000 Office*, *ELSA LANCOM 2000 Office* e *ELSA LANCOM 1100 Office*)
- Documentazione
- CD con *ELSA LANconfig* e altro software e documentazione elettronica

Se dovesse mancare qualcosa, rivolgersi direttamente al proprio fornitore.

2.2 Presupposti di sistema

I computer che si desidera collegare con l'aiuto dell'apparecchio a Internet, devono soddisfare i seguenti requisiti:

- un sistema operativo qualsiasi sul quale giri il protocollo di rete TCP/IP, ad esempio Windows 95, Windows 98, Windows 2000, Windows NT 4.0, OS/2, Linux o BeOS
- Windows 95, Windows 98, Windows 2000 o Windows NT 4.0 e un lettore di CD per i computer sui quali si desidera installare il software di configurazione *ELSA LANconfig*.

- Scheda di rete Ethernet
- Protocollo di rete TCP/IP installato e collegato alla scheda di rete

2.3 Impostazione del computer del posto di lavoro

Router di ELSA trasforma in un gioco da ragazzi la gestione degli indirizzi in una rete locale. In alcuni computer sono eventualmente necessarie alcune impostazioni per rendere possibile la collaborazione tra il router e tali computer.

2.3.1 Windows 95 e Windows 98

Sull'esempio di Windows 95 e Windows 98 viene mostrato brevemente che cosa si deve impostare sulla workstation per realizzare una corretta comunicazione del computer in rete TCP/IP con il router, se questo non è stato già fatto.

- Installare TCP/IP

Installare il TCP/IP con **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► Aggiungi ► Protocollo**. Selezionare come produttore 'Microsoft' e come protocollo di rete 'TCP/IP'.

- Lasciare assegnare gli indirizzi IP (utilizzare DHCP)

Se il router opera come server DHCP, impostare la workstation per il ricevimento automatico degli indirizzi IP: **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► TCP/IP ► Proprietà ► Indirizzi IP ► Ricevimento automatico degli indirizzi IP**. Inoltre cancellare le eventuali voci presenti per server DNS e Gateway (sulle schede registro 'Gateway' e 'Configurazione DNS'. Dopo il riavvio il computer cerca un server DHCP nella rete e lascia che questo assegni un indirizzo IP.

- Impostare indirizzi IP fissi (non utilizzare DHCP)

Se non si desidera utilizzare un server DHCP in rete, impostare indirizzi IP fissi nella workstation: **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► TCP/IP ► Proprietà ► Indirizzi IP ► Definizione degli indirizzi IP**.

Assegnare indirizzi IP univoci, per es. da un gruppo di indirizzi riservato. Le workstation possono ricevere per es. gli indirizzi da '10.1.1.2' a '10.1.1.253', il router il '10.1.1.1', tutti con la maschera di rete '255.255.255.0'. Controllare nel DOS box se l'indirizzo IP previsto per il

router, per es. il '10.1.1.1', è libero con `ping 10.1.1.1`. Se a questa richiesta non si ottiene risposta, l'indirizzo è probabilmente ancora libero.

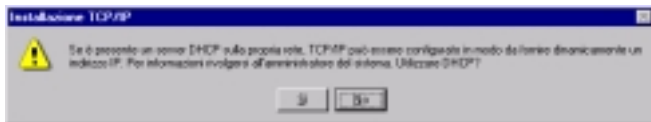
- Introdurre la gateway e il server DNS (non necessario se si utilizza DHCP)
Introdurre l'indirizzo del router della propria rete locale come gateway e come Domain Name Server (server DNS) nelle workstation: **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► TCP/IP ► Proprietà ► Gateway e Configurazione DNS**. Introdurre nella configurazione DNS anche un nome di host. A questo scopo per motivi di coerenza introdurre il nome del PC, che in caso ideale coincide con il nome dell'utente.
- Controllo della configurazione IP
Sotto Windows 95 o Windows 98 si può richiedere la configurazione IP attuale del computer con **Avvio ► Esegui ► winipcfg**. Qui è possibile visualizzare tra l'altro l'indirizzo IP che il server DHCP ha assegnato al computer e gli indirizzi trasmessi per il server DNS e gateway.

2.3.2

Windows NT 4.0

Sull'esempio di Windows NT 4.0 viene mostrato brevemente che cosa si deve impostare sulla workstation per realizzare una corretta comunicazione del computer in rete TCP/IP con il router, se questo non è stato già fatto.

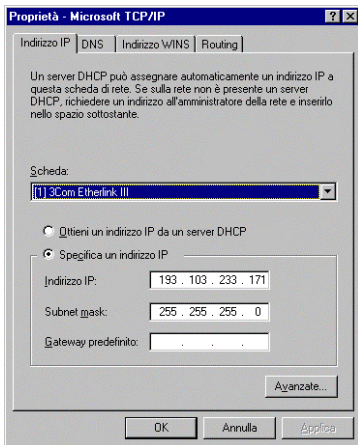
- Installare TCP/IP
Installare TCP/IP con **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► Protocollo ► Aggiungi**. Scegliere quale protocollo di rete 'Protocollo TCP/IP'.
- Lasciare assegnare gli indirizzi IP (utilizzare DHCP)
Se il router opera come server DHCP, impostare la workstation per il ricevimento automatico degli indirizzi IP: Al termine dell'installazione del protocollo di rete, cliccare sul pulsante **Si**.



A questo punto Windows copia i file necessari e richiede un riavvio.

- Impostare indirizzi IP fissi (non utilizzare DHCP)
Se non si desidera utilizzare un server DHCP in rete, impostare indirizzi IP fissi nella workstation: **Avvio ► Impostazioni ► Pannello di**

controllo ► Rete ► Protocollo ► Proprietà. Su questa scheda si può impostare inoltre il gateway standard.



Assegnare indirizzi IP univoci, per es. da un gruppo di indirizzi riservato. Le workstation possono ricevere per es. gli indirizzi da '10.1.1.2' a '10.1.1.253', il router il '10.1.1.1', tutti con la maschera di rete '255.255.255.0'. Controllare nel DOS Box se l'indirizzo IP previsto per il router, per es. il '10.1.1.1', è libero con `ping 10.1.1.1`. Se a questa richiesta non si ottiene risposta, l'indirizzo è probabilmente ancora libero.

- Introdurre il server DNS (non necessario se si utilizza DHCP)

Introdurre nella scheda 'DNS' l'indirizzo del router della propria rete locale e quale Domain Name Server (server DNS) nei computer dei posti di lavoro. Introdurre nella configurazione DNS anche un nome di host. A questo scopo per motivi di coerenza introdurre il nome del PC, che in caso ideale coincide con il nome dell'utente.



- Controllo della configurazione IP

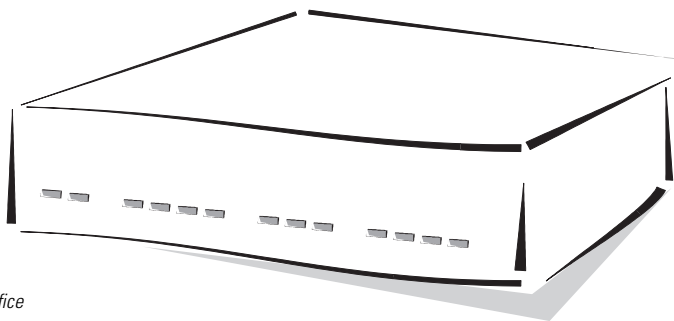
Sotto Windows NT 4.0 si può richiedere la configurazione IP attuale del computer con **Avvio ► Esegui ► ipconfig**. Qui si può vedere quale indirizzo IP il server DHCP ha assegnato al computer e quale indirizzi sono stati comunicati per il gateway (non per il server DNS).

2.4 ***ELSA LANCOM Office* si presenta**

In questo capitolo viene presentato l'hardware dell'apparecchio. Si riceve qualche notizia sul significato degli elementi di visualizzazione e sulle possibilità di connessione.

2.4.1 **Il lato anteriore dell'apparecchio**

Sul lato anteriore si trovano come elementi di visualizzazione alcune spie (LED).



Esempio di modello:
ELSA LANCOM 2000 Office

Power/Msg

Questo LED si accende brevemente una volta quando si inserisce la tensione di alimentazione. Dopo l'autotest, un errore eventualmente riscontrato viene emesso come codice a lampeggio, oppure l'apparecchio entra in servizio e il LED rimane costantemente acceso.

spento		Apparecchio disinserito, ma non senza tensione
rosso	1 x breve	Bootstrap (verifica e caricamento) iniziato
rosso	lampeggiante	Visualizzazione di un errore di bootstrap (codificato con codice a lampeggio)
rosso		Apparecchio pronto per il servizio
rosso	interr.	Messaggio di errore o una protezione addebiti impedisce le chiamate in uscita

Stato S_0

Questo LED indica lo Stato della connessione S_0 :

spento		non connesso o nessuna tensione S_0 (spesso sulle connessioni ISDN la tensione S_0 viene disattivata dopo un periodo di inattività)
verde	lampeggiante	Inizializzazione (entrata in contatto con il punto di connessione)
verde		pronto per il servizio bus (S_0 attivato, TEI presente e protocollo canale D controllato)
verde	Power off	Il LED è acceso quando il LED Power è spento: Apparecchio in Boot-Monitor

a/b 1 fino a a/b 4

Questi LED indicano nel *ELSA LANCOM 2000 Office* lo stato delle connessioni analogiche:

spento		porta a/b in riposo
verde		La connessione è stabilita
verde	lampeggiante	Chiamata in uscita in corso (port offhook) (normalmente lampeggiante)
verde	lampeggiante	- nessun canale B disponibile (sul bus o internamente) - nessun receiver DTMF (più) disponibile - linea ISDN non disponibile
rosso	lampeggiante	Chiamata in arrivo (LED a ritmo di squillo)
rosso	lampeggiante 1 volta	Chiamata in arrivo, MSN ok, porta bloccata per chiamate in arrivo

WAN
Chan1
Chan2

Questi LED indicano lo stato del corrispondente canale ISDN WAN logico (sia in modalità router che in modalità CAPI):

spento		Canale in riposo
rosso	lampeggiante	Chiamata in arrivo
verde	lampeggiante	Chiamata in uscita in corso
rosso		Il canale è fisicamente stabilito/trattativa di protocollo in corso
verde		La rispettiva trattativa di protocollo (X.75, PPP, etc.) è conclusa; il canale è logicamente online
verde/ rosso	brevi lampeggi rossi (durata ca. 1/10 s)	indicano un pacchetto di dati ricevuto

I canali ISDN WAN non hanno un'assegnazione fissa ai canali B!

Fintantoché i LED 'Chan1' o 'Chan2' sono accesi in verde, il collegamento è attivo e soggetto a costi!



WAN
Chan 1+2

Questo LED indica se la connessione ISDN attuale è un raggruppamento di canali statico oppure dinamico.

spento	Nessuna connessione oppure nessun raggruppamento di canali attivo
verde	Raggruppamento di canali statico oppure dinamico attivo

LAN-Tx, -Rx,
LAN-Coll, -Link
LAN-FDpx, -Fast

Questi LED indicano i corrispondenti stati del controller di rete:

LAN-Rx/Tx	giallo	Pacchetto di dati inviato dall'apparecchio alla LAN o dalla LAN all'apparecchio
LAN-Coll	rosso	Collisione di invio
LAN-Link	verde	La connessione alla LAN è stabilita e pronta
LAN-FDpx	verde	Il router invia e riceve dati contemporaneamente
LAN-Fast	verde	ELSA LANCOM si trova in modalità 100 Mbit

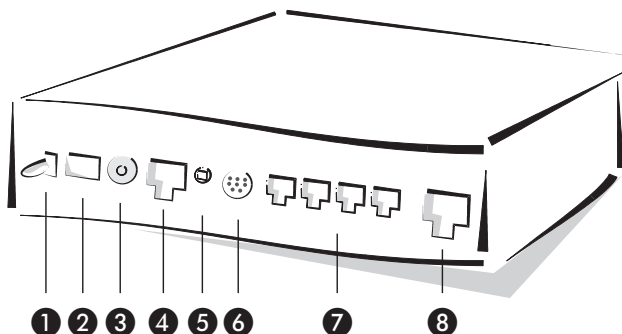


I due LED LAN-FDpx e LAN-Fast valgono solo per le reti da 100 Mbit e sono per questo motivo presenti solo nel ELSA LANCOM 1100 Office.

2.4.2

Il retro dell'apparecchio

Ruotare ora l'apparecchio e osservare il lato posteriore. Di nuovo partendo da sinistra si trova:



Esempio di modello:
ELSA LANCOM 2000
Office

❶ Interruttore on/off

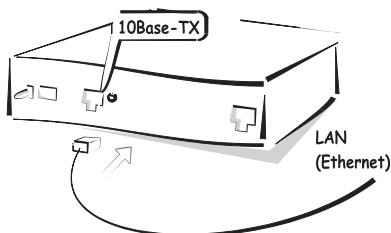
- ② Connessione per l'alimentatore
- ③ 10Base-2 (BNC), solo *ELSA LANCOM 1000 Office* o *ELSA LANCOM 2000 Office*
- ④ 10Base-T (*ELSA LANCOM 800 Office*, *ELSA LANCOM 1000 Office* o *ELSA LANCOM 2000 Office*) per reti 10 Mbit oppure 10/100Base-TX (*ELSA LANCOM 1100 Office*) per reti 10Mbit o 100 Mbit
- ⑤ Commutatore node/hub
- ⑥ Interfaccia di configurazione V.24 (*ELSA LANCOM 1000 Office*, *ELSA LANCOM 2000 Office* o *ELSA LANCOM 1100 Office*)
- ⑦ quattro connessioni analogiche (POTS, porte a/b, solo *ELSA LANCOM 2000 Office*)
- ⑧ Collegamento ISDN S₀

2.5

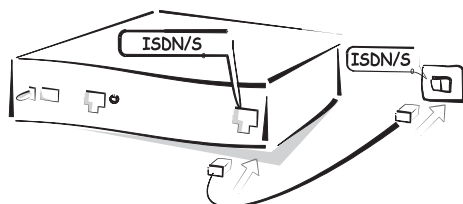
Come si può collegare l'apparecchio?

- ① Collegare il proprio *ELSA LANCOM Office* con la LAN. Innestare a tale scopo il cavo di rete fornito nella presa 10/100Base-TX dell'apparecchio e in una presa di rete libera della propria rete locale (o in una presa libera di un hub della propria LAN).

Esempio di modello:
ELSA LANCOM 800 Office

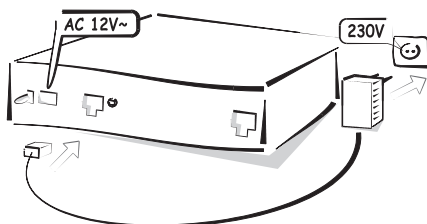


- ② Collegare il proprio *ELSA LANCOM Office* con la rete ISDN. Innestare a tale scopo il cavo di rete fornito nella presa ISDN/S₀ dell'apparecchio e ad una presa per connessione multipla o a impianto ISDN/S₀ (configurazione punto a più punti o punto a punto).



Esempio di modello:
ELSA LANCOM 800 Office

- ③ Alimentare l'apparecchio tramite l'alimentatore con la tensione necessaria e accenderlo. Dopo un breve autotest dell'apparecchiatura, il LED 'Power/Msg' si accende in modo permanente. Il LED 'LAN-Link' indica che è stato stabilito un collegamento corretto con la LAN.



Esempio di modello:
ELSA LANCOM 800 Office



Nel caso in cui tale LED non dovesse accendersi, azionare il commutatore Node/Hub. Se anche in questo caso il LED continua a non accendersi, c'è eventualmente un problema con la scheda di rete o con il cablaggio.

2.5.1 Installazione del software

Il software di configurazione *ELSA LANconfig* per i sistemi operativi Windows permette di impostare il proprio router in modo semplice e comodo per l'impiego desiderato. Con altri sistemi operativi, si può effettuare alternativamente la configurazione con un browser HTML.

Per il servizio di *ELSA LANconfig* si necessita di un PC Windows in LAN.

- ① Installare prima il protocollo di rete TCP/IP sul computer dal quale si desidera impostare il proprio apparecchio.
- ② Installare alla fine *ELSA LANconfig*. Se il programma setup non si avvia automaticamente quando si inserisce il CD *ELSA LANCOM*, da Gestione risorse (Explorer) di Windows fare clic su 'autorun.exe' del CD *ELSA LANCOM* e seguire le ulteriori istruzioni della routine di installazione.

2.6 Configurazione

In questo esempio si mostra il semplice collegamento di una LAN a Internet. La configurazione dell'apparecchiatura è strutturata nei seguenti passi:

- Impostazioni di base
- Impostare l'accesso a Internet

Per le singole parti della configurazione esiste un'apposita tabella informativa. Essa mostra le informazioni di cui si ha bisogno. Prima di iniziare con la configurazione, compilare tale tabella.

2.6.1 Impostazioni di base

Nell'impostazione di base, assegnare all'apparecchio un nome e stabilire gli indirizzi IP per il servizio nella rete locale. Nell'esempio, la distribuzione degli indirizzi IP nella LAN viene effettuata dal server DHCP nel router automaticamente.

Browser HTML

Se non si desidera o se non si può utilizzare *ELSA LANconfig* (ad esempio poiché si è installato un sistema operativo diverso), le impostazioni di base possono essere effettuate anche con un normale browser HTML.

- ① Avviare il proprio browser.
 - Se nella propria LAN finora non si ha né un server DHCP né un server DNS, il router reagisce ad ogni indirizzo che si introduce nel campo relativo. Poiché la maggior parte dei browser normalmente richiamano una determinata pagina, nella maggior parte dei casi il browser visualizzerà automaticamente la schermata di avvio della configurazione del router.
Se il proprio browser normalmente mostra invece una pagina vuota, introdurre un nome qualsiasi nel campo di indirizzo (ad esempio '*ELSA LANCOM Office*'). Anche così viene automaticamente visualizzata la schermata di avvio.
 - Se nella propria LAN si impiega finora già un server DHCP o se si opera sulla base di indirizzi IP fissi, introdurre nel campo dell'indirizzo del browser l'indirizzo 'x.x.x.254', dove 'x.x.x' indica la cerchia d'indirizzi usata finora nella rete.



Se non si sa se nella propria rete sono stati usati finora indirizzi IP, cliccare in Windows 95 o Windows 98 prima su **Avvio ► Esegui**, digitare nella finestra che si aprirà il comando `winipcfg` e confermare con **OK**. Scegliere nella finestra seguente la propria scheda di rete. Se nel campo 'Indirizzo IP' si trova il valore '0.0.0.0', la scheda di rete non ha allora finora nessun indirizzo IP.



In Windows NT si possono controllare gli indirizzi IP con il istruzione `ipconfig`.

- ② Scegliere la voce 'Impostazione di base'.
- ③ Attivare l'opzione 'Stabilisci i parametri IP automaticamente', se **non** si ha confidenza con reti e indirizzi IP e se una delle seguenti supposizioni è vera:
 - L'utente non ha finora usato nella propria rete alcun indirizzo IP, ma adesso desidera farlo. Quali indirizzi IP vengano usati è per l'utente irrilevante. Quale server DHCP, il router in tal caso stabilirà e assegnerà automaticamente gli indirizzi IP a tutti i dispositivi nella LAN.

oppure

 - L'utente non desidera usare indirizzi IP poiché ad esempio si impiega una pura rete Windows.

- ④ Disattiva l'opzione 'Stabilisci i parametri IP automaticamente', se si ha confidenza con reti e indirizzi IP e se una delle seguenti supposizioni è vera:
- L'utente non ha finora usato nella propria rete alcun indirizzo IP, ma adesso desidera farlo. Si desidera però stabilire da sé l'indirizzo IP per il nuovo apparecchio e assegnargli un qualsiasi indirizzo da un'area di indirizzi riservata per scopi privati, ad esempio '10.0.0.1' con la maschera di rete '255.255.255.0'. In tal modo si stabiliscono contemporaneamente anche le aree di indirizzi che il server DHCP alla fine usa per gli altri dispositivi della rete (sempre che il server DHCP non venga disattivato).
 - L'utente ha finora già usato per i computer della LAN indirizzi IP. Assegnare al nuovo apparecchio un indirizzo libero dall'area finora usata e scegliere se l'apparecchio debba operare quale server DHCP o no.



Ulteriori informazioni sulla struttura di reti in generale e sull'indirizzamento IP si trovano nella documentazione elettronica del ELSA LANCOM-CD.

- ⑤ Introdurre una password per l'accesso all'apparecchio e scegliere se esso debba operare quale server DHCP nella LAN.



Disattivare la 'Configurazione automatica delle workstation tramite DHCP' solo se si desidera utilizzare indirizzi IP fissi nella rete oppure se già è attivo un altro server DHCP. Il modo di funzionamento del server DHCP è descritto più avanti in questo manuale.

- ⑥ Introdurre per ogni bus 0 i numeri telefonici ai quali il router deve reagire e, nel caso in cui il router sia collegato ad una centrale telefonica, il numero necessario per avere la linea esterna.

Indicare in questo caso anche se nella propria connessione ISDN vengono inoltrati gli impulsi di conteggio.

Se il campo per i numeri telefonici viene lasciato libero, il router reagisce a tutti i numeri telefonici validi per questa linea.

Con queste impostazioni si è reso noto il nuovo router alla rete locale. Esso stesso è accessibile all'indirizzo IP '10.0.0.1'. Dopo un riavvio, tutti i dispositivi prelevano nella rete locale il proprio indirizzo IP dal server DHCP nel router. In questo caso viene usato automaticamente il pool di indirizzi da '10.0.0.2' a '10.0.0.253'.

Nel caso di una chiamata dalla rete ISDN, l'apparecchio reagisce solo ai numeri telefonici che sono stati riportati per ogni bus S_0 .

ELSA LANconfig

Al primo avvio di *ELSA LANconfig*, viene riconosciuto un nuovo apparecchio nella rete TCP/IP ed esso può essere subito configurato. Per farlo si avvia automaticamente un assistente che è di aiuto per l'impostazione di base dell'apparecchiatura o che può addirittura effettuare da solo tutte le operazioni.

- ① Avviare il nuovo software con **Avvio ► Programmi ► ELSAan ► ELSA LANconfig**.



- ② Scegliere l'opzione 'Tutto impostato automaticamente', se **non** si ha esperienza con reti e indirizzi IP e se è vera una delle seguenti affermazioni:
 - L'utente non ha finora usato nella propria rete alcun indirizzo IP, ma adesso desidera farlo. Quali indirizzi IP vengano usati è per l'utente irrilevante. Il router in tal caso quale server DHCP stabilirà e correlerà gli indirizzi IP per tutte le apparecchiature della rete (LAN e WLAN) automaticamente.
 - oppure
 - L'utente non desidera usare indirizzi IP poiché ad esempio si impiega una pura rete Windows.



*Se non si sa se nella propria rete finora sono stati usati indirizzi IP, cliccare prima su **Avvio ► Esegui**, digitare nella finestra che compare winipcfg*

e cliccare su **OK**. Se nella finestra seguente nel campo 'Indirizzo IP' è riportato il valore '0.0.0.0', il computer non ha finora alcun indirizzo IP.

- ③ Scegliere l'opzione 'Desidero impostare tutto manualmente' se si ha esperienza con le reti e indirizzi IP e se è vera una delle seguenti affermazioni:
- L'utente non ha finora usato nella propria rete alcun indirizzo IP, ma adesso desidera farlo. L'utente stesso desidera però stabilire l'indirizzo IP per il router e attribuirgli un indirizzo qualsiasi compreso nelle aree di indirizzamento riservate per scopi privati, ad esempio '10.0.0.1' con la maschera di rete '255.255.255.0'. In tal modo si stabilisce anche contemporaneamente l'area di indirizzamento che poi il server DHCP userà per le altre apparecchiature della rete (a meno che il server DHCP non venga disattivato).
 - L'utente ha finora già usato per i computer della LAN indirizzi IP. Assegnare al router un indirizzo libero dall'area finora usata e scegliere se l'apparecchio debba operare quale server DHCP o no.



Ulteriori informazioni sulla struttura di reti in generale e sull'indirizzamento IP si trovano nella documentazione elettronica del CD ELSA LANCOM. Il modo di funzionamento del server DHCP è descritto più avanti in questo manuale.

Telnet

Se non si desidera o non si può usare *ELSA LANconfig* o un browser HTML (per es. perché è installato un altro sistema operativo senza browser), le impostazioni di base possono essere effettuate anche tramite un collegamento Telnet.

Avviare il collegamento Telnet all'indirizzo '10.0.0.254', se finora non si sono usati nella propria rete indirizzi IP, o all'indirizzo 'x.x.x.254', dove 'x.x.x' indica l'area di indirizzi finora usata nella rete.

Digitare i seguenti comandi:

- ① Il collegamento Telnet lo si avvia ad esempio con il comando **Avvio ► Esegui** e digitando poi nella finestra che si è aperta `telnet 10.0.0.254`.
- ② Modificare la lingua per la configurazione con il comando:
- ```
set/setup/config-module/language italiano
```

- ③ Indirizzo Intranet e maschera di rete:

```
set /Setup/TCP-IP-module/Indirizzo Intranet.
10.0.0.1

set /Setup/TCP-IP-module/maschera di Intranet
255.255.255.0
```

*Modificando l'indirizzo di Intranet il collegamento Telnet viene interrotto.*

- ④ Disattivare eventualmente la funzione DHCP:

```
set/setup/DHCP-module/operating off
```

*Anche se le voci a questo punto, senza ulteriori spiegazioni, non dicono granché, si raggiunge in tal modo lo stesso traguardo come nel caso dell'impostazione tramite ELSA LANconfig!*

Con queste impostazioni si è reso noto il nuovo router alla rete locale. Esso stesso è accessibile all'indirizzo IP '10.0.0.1'. Dopo un riavvio, tutti i dispositivi prelevano nella rete locale il proprio indirizzo IP dal server DHCP nel router. In questo caso viene usato automaticamente il pool di indirizzi da '10.0.0.2' a '10.0.0.253'.

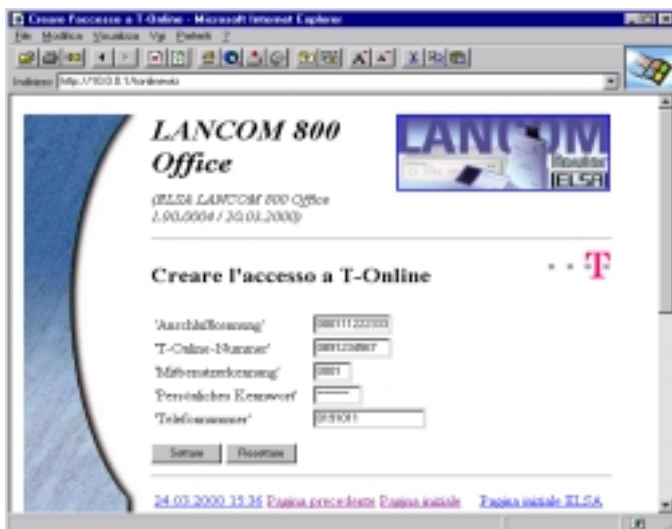
## 2.6.2

### Impostare l'accesso a Internet

Per impostare un accesso a Internet sono disponibili in *ELSA LANconfig* o nella configurazione con un browser HTML, alcuni assistenti che rendono le impostazioni dell'apparecchio veramente molto facili.

#### Browser HTML

- ① Avviare il proprio browser e introdurre nel campo apposito l'indirizzo IP dell'apparecchiatura che si è scelta nell'impostazione di base. Nel caso in cui per l'impostazione di base non sia stato indicato esplicitamente indicato alcun indirizzo IP, l'indirizzo è '10.0.0.1'.
- ② Scegliere il proprio Paese e quindi uno dei provider Internet preimpostati o un accesso generale tramite PPP.
- ③ Introdurre nelle finestre seguenti i dati necessari per il collegamento, come numero telefonico, nome utente e password.



### ELSA LANconfig

- ① Avviare *ELSA LANconfig* con **Avvio ► Programmi ► ELSA ► ELSA LANconfig**.
- ② Marcare il proprio *ELSA LANCOM Office* nella lista delle apparecchiature e richiamare l'assistente.
- ③ Scegliere l'assistente per l'accesso a Internet, il proprio Paese e quindi uno dei provider Internet preimpostati o un accesso generale tramite PPP.
- ④ Introdurre nelle finestre seguenti i dati necessari per il collegamento, come numero telefonico, nome utente e password e chiudere l'assistente con **Fine**.

### Finito!

Con questi pochi clic del mouse si è configurato l'apparecchio per l'accesso a Internet tramite un collegamento ISDN in modo completo. Tutti i computer della propria LAN che prelevano i propri indirizzi IP e gli indirizzi IP per il gateway tramite DHCP dal proprio *ELSA LANCOM Office* possono adesso navigare in Internet a velocità massima...



## 3 Possibilità di configurazione

I router di ELSA vengono sempre forniti con un software aggiornato nel quale sono già presenti alcune impostazioni per l'utente.

Tuttavia rimane necessario un completamento dei dati e un adattamento agli speciali compiti previsti per il router specifico. Queste impostazioni vengono effettuate durante la configurazione.

In questo capitolo vengono presentati i programmi e i percorsi con cui si può accedere all'apparecchio per effettuare tali impostazioni.

Inoltre, se il team di sviluppo ha preparato un nuovo firmware con nuove prestazioni, si trovano le istruzioni per caricare il nuovo software.

### 3.1 Molte strade portano al **ELSA LANCOM**

In linea di principio esistono diverse possibilità per accedere ai router di ELSA:

- Tramite l'interfaccia di configurazione (interfaccia Config) sul pannello posteriore del router (anche denominato outband)  
L'interfaccia di configurazione è disponibile con i modelli *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1000 Office* e *ELSA LANCOM 1100 Office*.
- Tramite la rete collegata, LAN o WAN (inband)
- Tramite una connessione PPP in Accesso remoto o simile (configurazione remota)

Che cosa distingue queste possibilità?

Per un verso l'accessibilità degli apparecchi: La configurazione tramite outband è sempre disponibile. Invece la configurazione inband per es. non è possibile se la rete di trasmissione è disturbata. Anche la configurazione remota dipende dal mezzo di trasmissione, per es. dalla connessione ISDN.

Per un altro verso la necessità di software o hardware supplementare. La configurazione inband richiede uno dei computer, comunque presenti nella LAN o nella WAN, e un software idoneo. La configurazione outband richiede oltre al software anche uno dei computer (con interfaccia seriale) e il corrispondente cavo di configurazione. La configurazione remota richiede un computer con PPP Client, scheda ISDN o interfaccia terminale. La più semplice è la configurazione remota con l'impiego di Accesso remoto e *ELSA LANconfig*.

## 3.2

## La via diretta: Outband

Con la configurazione outband si accede direttamente al router attraverso l'interfaccia di configurazione.

*La configurazione outband è necessaria essenzialmente solo se non si può raggiungere l'apparecchio tramite TCP/IP.*



### 3.2.1

### Presupposti per la configurazione outband

Apparecchiatura necessaria:

- Un router con interfaccia di configurazione, *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1000 Office* o *ELSA LANCOM 1100 Office*
- Un computer con Windows 95, Windows 98 o Windows NT 4.0 e *ELSA LANconfig*  
o

Un computer con qualunque sistema operativo ed un programma di terminale (per es. *Telix* o *Hyperterminal*).

- Il cavo di configurazione in dotazione ed eventualmente l'adattatore 9/25 poli per collegare il computer con il router (porta COM del PC sull'interfaccia di configurazione del router).

### 3.2.2

### Configurazione outband con *ELSA LANconfig*

Avviare *ELSA LANconfig* per es. dalla barra di avvio di Windows con **Avvio ► Programmi ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* cerca automaticamente nella rete locale (ma non sull'interfaccia seriale) le periferiche *ELSA LANCOM*. Una nuova periferica sull'interfaccia seriale si trova con **Unità ► Trova ► Trova tutte le porte seriali**. *ELSA LANconfig* mostra i nuovi router nella lista con la denominazione delle periferiche.

Per un nuovo apparecchio, non ancora configurato sull'interfaccia di configurazione con **Strumenti ► Setup wizard** si possono richiamare diversi help per la configurazione. Selezionare una delle assistenze proposte, e rispondere semplicemente alle domande. Alla fine il *ELSA LANCOM* è impostato per il compito selezionato.

Nella lista delle periferiche trovate, facendo doppio clic sulla denominazione della periferica si può aprire per la modifica la configurazione attuale.



### 3.2.3 Configurazione outband con emulatore di terminale

Se l'emulatore di terminale è avviato, premere solo qualche volta il tasto Return, per riconoscere automaticamente il bit rate (fino a 230 Kbps, 38,4 Kbps come standard).

Dopo l'introduzione della password sono disponibili tutti i comandi della Sezione 'Comandi per la configurazione'.

## 3.3 La via comoda: Inband

Con la configurazione inband, si ha l'accesso al router da qualunque computer della WAN o della LAN. L'accesso può però essere limitato o bloccato del tutto dalla lista di accessi IP. Per la configurazione si utilizza Telnet (in dotazione con la maggior parte dei sistemi operativi) o *ELSA LANconfig* per Windows. *ELSA LANconfig* è incluso nella fornitura del router. Le versioni aggiornate sono sempre disponibili nei nostri servizi online.

### 3.3.1 Presupposti

La configurazione con Telnet o con *ELSA LANconfig* si realizza tramite TCP/IP oppure TFTP. A questo scopo, sul computer utilizzato deve essere installato il TCP/IP e il router ha bisogno di un indirizzo IP con cui possa essere chiamato.

Un apparecchio non ancora configurato ha l'indirizzo IP XXX.XXX.XXX.254. I vari X rappresentano l'indirizzo di rete nella LAN. Se per es. i computer della rete hanno indirizzi come 192.168.130.1, è possibile raggiungere il router con l'indirizzo 192.168.130.254.



*Se nella rete esiste già un computer con l'indirizzo XXX.XXX.XXX.254, assegnare all'apparecchio un nuovo indirizzo tramite la configurazione outband, prima di installarlo nella LAN.*

### 3.3.2 Alternativa: Gestione indirizzi con il server DHCP

Se la configurazione « manuale » degli indirizzi IP corretti non è una necessità assoluta, il server DHCP può eseguire volentieri anche questo compito autonomamente. Utilizzando il server DHCP, si possono lasciar impostare automaticamente gli indirizzi IP per tutti i computer della rete (vedi anche capitolo 'Assegnazione automatica degli indirizzi con DHCP'). In questo caso il router può anche stabilire autonomamente l'indirizzo IP dal lato LAN per sé stesso.

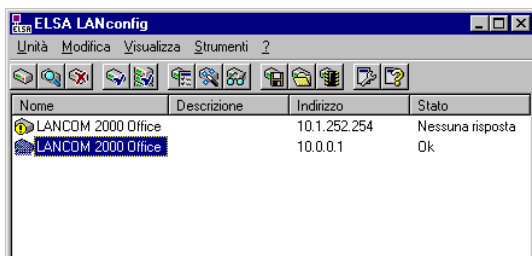
### 3.3.3 La configurazione tramite *ELSA LANconfig*

Richiamare il tool di configurazione *ELSA LANconfig* ad esempio dalla barra di avvio di Windows con **Avvio ► Programmi ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* cerca automaticamente nella rete locale le apparecchiature. Se nella rete locale viene trovata una periferica non ancora configurata, *ELSA LANconfig* avvia autonomamente il settaggio assistito.

Selezionare l'assistenza proposta, e rispondere semplicemente alle domande. Alla fine il router è impostato per il compito selezionato.

Per avviare manualmente la ricerca di una nuova apparecchiatura, cliccare sul pulsante **Trova** o attivare il comando tramite **Unità ► Trova**. *ELSA LANconfig* richiede dove deve eseguire la ricerca. Nel caso della soluzione inband è sufficiente selezionare la rete locale, e si può iniziare.

Appena il *ELSA LANconfig* ha terminato la ricerca, visualizza nella lista tutte le periferiche trovate con i nomi, eventualmente una descrizione, l'indirizzo IP e lo stato.



Per la configurazione delle apparecchiature con *ELSA LANconfig* si può scegliere tra due diverse possibilità di rappresentazione:

- Nella 'rappresentazione semplice' vengono mostrate solo le impostazioni necessarie per i casi applicativi comuni.
- Nella 'rappresentazione completa' vengono visualizzate tutte le impostazioni disponibili. Alcune di esse andrebbero cambiate solo da parte di utenti esperti.

Scegliere il modo di rappresentazione nel menù **Visualizza ► Opzioni**.

Facendo doppio clic sulla periferica evidenziata, cliccando sul pulsante **Configura** o sulla voce di menu **Modifica ► Modifica configurazione File** le impostazioni attuali vengono lette dalla periferica e vengono visualizzate le informazioni generali sulla periferica.

Il restante impiego del programma in linea di principio si spiega da sé oppure mediante la guida in linea. Cliccando sul punto interrogativo in alto a destra in ciascuna finestra oppure cliccando con il tasto destro del mouse su un concetto poco chiaro, in ogni momento si può richiamare l'help contestuale.

### 3.3.4 La configurazione tramite Telnet

Avviare tramite Telnet, ad esempio da un box DOS, la configurazione con il comando:

```
telnet 10.1.80.125
```

Telnet stabilisce una connessione dell'apparecchio con l'indirizzo IP indicato.

Dopo aver introdotto la password (sempre che si sia impostata la protezione della configurazione), si avranno a disposizione tutti i comandi della sezione 'Comandi per la configurazione'.

## 3.4 L'Accesso remoto: Configurazione tramite Accesso remoto

L'impostazione dei router in posizioni remote mediante la configurazione remota è particolarmente semplice utilizzando l'Accesso remoto. Il apparecchio può essere raggiunto dall'amministratore immediatamente e senza alcuna impostazione dopo l'attivazione e il collegamento ISDN. In questo modo, in occasione della connessione di altre reti alla propria LAN, si risparmia tempo e denaro in quanto non è necessario recarsi sul posto né istruire i propri collaboratori locali alla configurazione dei router.

Inoltre si può riservare uno speciale numero telefonico per la configurazione remota. In questo modo un tecnico di assistenza può sempre accedere al router, anche se questo non risponde più a causa di errori di impostazione.

### 3.4.1 Quello che serve per la configurazione remota

- un computer con PPP Client, per es. Windows Accesso remoto
- un programma per la configurazione inband, per es. *ELSA LANconfig* o *Telnet*
- una scheda ISDN, un interfaccia terminale o un *ELSA LANCOM* con *ELSA LANCAPI*

### 3.4.2 Come si prepara la configurazione remota

- ① Collegare il router all'alimentazione.
- ② Collegare l'apparecchio ad un accesso ISDN.

### 3.4.3 Il primo collegamento remoto con Accesso remoto (*ELSA LANconfig*)

- ① Selezionare in *ELSA LANconfig* **Unità ► Nuovo**, attivare 'Connessione Dial-Up' come tipo di connessione e introdurre il numero telefonico del collegamento ISDN a cui è collegato il *ELSA LANCOM*. Eventualmente impostare il tempo dopo cui una connessione senza trasmissione dati deve essere automaticamente chiusa.
- ② *ELSA LANconfig* crea automaticamente una nuova voce nella rete di Accesso remoto. Selezionare per la connessione una periferica con capacità PPP (per es. il driver NDIS WAN in dotazione alla *LANCAPI*), e confermare con **OK**.
- ③ A questo punto *ELSA LANconfig* mostra nella lista delle periferiche una nuova periferica con nome 'Sconosciuto' e con indirizzo uguale al numero telefonico tramite Accesso remoto.

*Con l'introduzione nella lista delle periferiche la connessione in Accesso remoto viene cancellata.*

- ④ Ora si può impostare l'apparecchio tramite Accesso remoto esattamente come tutte le altre periferiche. Per leggere la configurazione l'*ELSA LANconfig* stabilisce una connessione tramite Accesso remoto.

### 3.4.4 Il primo collegamento remoto con un PPP Client e Telnet

- ① Stabilire con il PPP Client una connessione mediante il *ELSA LANCOM*, utilizzando i seguenti dati:
  - Nome utente 'ADMIN'
  - Password come impostata nel *ELSA LANCOM*; all'atto della fornitura non è impostata nessuna password
  - Un indirizzo IP per la connessione, solo se necessario
- ② Avviare una connessione Telnet al *ELSA LANCOM*. A questo scopo utilizzare il seguente indirizzo IP:

- '172.17.17.18', se non è stato stabilito un indirizzo IP per il PPP Client. Il *ELSA LANCOM* utilizza automaticamente questo indirizzo se non ne è stato concordato un altro. Il PC chiamante reagisce al IP '172.17.17.17'.
  - Incrementare l'indirizzo IP del PC di uno, se è stato stabilito un indirizzo. Esempio: Per il PPP Client è stato stabilito il IP '10.0.200.123', allora il *ELSA LANCOM* reagisce al '10.0.200.124'. Eccezione: Se alla fine del IP c'è '254' il router reagisce a 'x.x.x.1'.
- ③ Ora si può impostare il *ELSA LANCOM* tramite Accesso remoto esattamente come tutte le altre periferiche.

### 3.4.5

### Limitazione della configurazione remota

La connessione PPP di una qualunque controparte al router naturalmente si realizza solo se l'apparecchio accetta ogni chiamata con le impostazioni corrispondenti alla modalità PPP. Nello stato di fornitura questo si verifica, poiché il protocollo standard (default layer) è impostato su PPP.

E' possibile che, dopo la prima configurazione, si desideri impostare il default layer per es. per connessioni LAN-LAN su un altro protocollo. In questo caso il apparecchio non accetta più le chiamate tramite Accesso remoto con le impostazioni PPP. Un rimedio possibile si ottiene concordando uno speciale numero telefonico per l'accesso alla configurazione. Se la periferica riceve una chiamata a tale numero, viene sempre utilizzata l'impostazione PPP, indipendentemente dalla restante configurazione del router. Viene accettato solo uno speciale nome utente durante la negoziazione PPP, e questo viene introdotto automaticamente tramite *ELSA LANconfig*.

- ① Passare nell'area di configurazione 'Management' sulla scheda 'Security'.
- ② Selezionare nel campo 'Configurazione degli accessi' se l'impostazione da reti remote deve essere permessa, solo in lettura o negata.

Per una connessione Telnet o di terminale, immettere in alternativa il seguente comando:

```
set /Setup/Config-module/Wan-config
[on][read][off]
```

*Se si desidera bloccare completamente l'accesso al router tramite la WAN, impostare l'accesso da reti remote su 'negato'.*

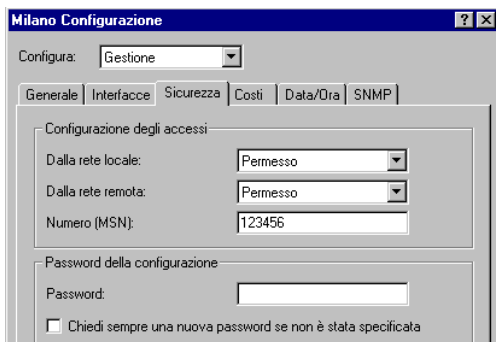


- ③ Introdurre come numero telefonico nel campo 'Configurazione degli accessi' un MSN o EAZ del proprio collegamento ISDN, che non sia utilizzato per il router, la *LANCAPI* o le porte a/b.

Immettere in alternativa il seguente comando:

```
set /Setup/Config-modul/Farconfig-(EAZ-MSN)
123456
```

- ④ Eventualmente proteggere le impostazioni della periferica assegnando una password.



Immettere in alternativa il seguente comando:

```
passwd
```

In questo modo si richiede di immettere una nuova password con conferma.

## 3.5 Nuovo firmware con FirmSafe

Il software delle periferiche ELSA viene continuamente sviluppato. Per fare apprezzare le nuove prestazioni e funzioni, abbiamo attrezzato gli apparecchi in modo che una memoria flash ROM, che trasforma in un gioco da ragazzi il lavoro successivo di modifica del software operativo. Nessuna EPROM da sostituire, nessun involucro da aprire: Si carica semplicemente la nuova versione ed è tutto fatto!

### 3.5.1 FirmSafe funziona così

FirmSafe rende sicuro il caricamento del nuovo software: Il firmware attualmente in uso non viene semplicemente sovrascritto, viene invece memorizzato nell'apparecchio un secondo firmware aggiuntivo.

Una sola delle due versioni di firmware memorizzate nell'apparecchio può essere attiva. Durante il caricamento del nuovo firmware, il firmware non attivo viene sovrascritto. Si può decidere quale firmware deve essere attivato dopo l'upload:

- 'Immediato': La prima possibilità consiste nel caricare ed attivare immediatamente il nuovo firmware. Si possono presentare le seguenti situazioni:
  - Il nuovo firmware viene caricato con successo e poi funziona come voluto. Quindi tutto è a posto.
  - Dopo il caricamento del nuovo firmware l'apparecchio non risponde più. Se già durante il caricamento si verifica un errore, il router riattiva automaticamente il firmware precedente e riavvia l'apparecchio.
- 'Login': Per contrastare i problemi legati a un caricamento difettoso, esiste una seconda possibilità, in cui il firmware viene caricato e immediatamente avviato.
  - A differenza della prima variante, l'apparecchio attende per altri cinque minuti che un login venga eseguito con successo. Solo se tale login ha successo, il nuovo firmware viene attivato in modo permanente.
  - Se l'apparecchio non risponde più, e quindi un login risulta impossibile, il riattiva automaticamente il firmware precedente e riavvia l'apparecchio.
- 'Manuale': Con la terza possibilità si può definire un tempo durante il quale il nuovo firmware viene provato. L'apparecchio si avvia con il nuovo firmware e attende durante il tempo impostato che il firmware caricato venga attivato manualmente e quindi reso operativo in modo permanente.

### 3.5.2 Un nuovo software si carica così

Per l'upload del firmware (così si chiama il caricamento del software), le vie che conducono al traguardo sono diverse:

- *ELSA LANconfig* (consigliato)
- Programmi terminale
- TFTP



Durante il firmware upload tutte le impostazioni rimangono inalterate! Comunque per maggiore sicurezza si dovrebbe salvare prima la configurazione (in **ELSA LANconfig** per es. con **Modifica ► Stampa configurazione File**).

Se la nuova versione caricata contiene parametri che non sono presenti nell'attuale firmware dell'apparecchio, il router completa i valori mancanti con le impostazioni di default.

### **ELSA LANconfig**



Nel *ELSA LANconfig* evidenziare l'apparecchio desiderato nella lista di selezione e cliccare su **Modifica ► Gestione Firmware ► Aggiorna Nuovo Firmware** o direttamente sul pulsante **Aggiornamento Firmware**. Poi selezionare la directory in cui si trova la nuova versione ed evidenziare il file corrispondente.

*ELSA LANconfig* nella descrizione fornisce informazioni sul numero di versione e sulla data e propone di effettuare l'upload. Con **Apri** si sostituisce il firmware presente con la versione selezionata.

Inoltre scegliere se, dopo il caricamento, il firmware deve essere attivato immediatamente in modo permanente, oppure impostare un tempo di prova, in cui il firmware viene abilitato. Per attivare il firmware durante il tempo di prova impostato, cliccare su **Modifica ► Gestione Firmware ► Abilitare firmware in prova**.

### **Emulatore di terminale (per es. Telix o Hyperterminal di Windows)**

Per gli emulatori di terminale, nel menu 'Firmware' con il comando 'set mode-firmsafe' impostare prima la modalità con cui si desidera caricare il nuovo firmware (immediato, login o manuale). Poi eventualmente impostare con 'set Timeout-firmsafe' il tempo di prova per il firmware.

Con il comando 'Firmware-upload' il router viene impostato in modalità di pronto per il caricamento. Infine avviare il processo di upload dall'emulatore di terminale:

- Con *Telix* cliccare sul pulsante **Upload**, impostare 'Xmodem' per il trasferimento e selezionare il file desiderato per l'upload.



- Con Hyperterminal cliccare su **Trasferisci ► Invia file**, selezionare il file, impostare 'XModem' come protocollo e avviare con **Invia**.

### TFTP

Tramite TFTP un nuovo firmware può essere caricato con il comando **writelflash**. Per trasferire un nuovo firmware in un apparecchio con indirizzo IP 194.162.200.17, per es. sotto Windows NT introdurre il seguente comando:

```
tftp -i 194.162.200.17 put lc_1000u.130 writelflash
```

*Con questo comando viene trasmesso il file corrispondente con l'istruzione **writelflash** all'indirizzo IP indicato. Per TFTP deve essere impostato il trasferimento file binario. Peraltro in molti sistemi è predefinito il formato ASCII. In questo esempio per Windows NT questo si realizza per mezzo del parametro '-i'.*

Dopo che l'upload del firmware è stato completato con successo l'apparecchio si riavvia e quindi attiva direttamente il nuovo firmware. Se durante l'upload si hanno errori (errore di scrittura nella Flash-ROM, errore di trasmissione TFTP o simili), FirmSafe attiva il vecchio firmware. La configurazione viene mantenuta.

Con TFTP si possono eseguire anche altri comandi di configurazione. La sintassi si può ricavare facilmente dai seguenti esempi:

- `tftp 10.0.0.1 get readconfig file1` : Legge la configurazione dall'apparecchio con indirizzo 10.0.0.1 e la salva sotto file1 nella directory corrente
- `tftp 10.0.0.1 put file1 writeconfig`: scrive la configurazione dal file1 nell'apparecchio con l'indirizzo 10.0.0.1.
- `tftp 10.0.0.1 get dir/status/verb file2` : Salva le informazioni di connessione attuali nel file2

## 3.6

### Che cosa succede sulla linea?

Dopo la configurazione base degli apparecchi, si ricevono ulteriori importanti indicazioni sui parametri che devono essere ancora modificati specialmente osservando il traffico di dati sulle diverse interfacce dei router.

Oltre alle statistiche dell'apparecchio, che per esempio possono essere lette in una sessione Telnet o di terminale, sono disponibili ulteriori possibilità.

## 3.6.1

**ELSA LANmonitor**

Con il tool di sorveglianza *ELSA LANmonitor*, nei sistemi operativi Windows è sempre possibile farsi visualizzare sullo schermo le più importanti informazioni sullo stato del proprio router. Molti dei messaggi interni dell'apparecchio vengono convertiti in testo, indicano lo stato attuale dell'apparecchio e quindi aiutano nella ricerca difetti.

**Installazione di ELSA LANmonitor**

*ELSA LANmonitor* di regola viene installato automaticamente sul computer da cui si desidera impostare il router con *ELSA LANconfig*.

Se *ELSA LANmonitor* non è ancora installato sul computer, inserire il CD *ELSA LANCOM*. Se il programma setup non si avvia automaticamente quando si inserisce il CD, da Gestione risorse (Explorer) di Windows fare clic su 'autorun.exe' del CD *ELSA LANCOM* e seguire le ulteriori istruzioni della routine di installazione.

Durante l'installazione attivare l'opzione per 'LANmonitor'

*Con ELSA LANmonitor si possono monitorare solo le periferiche raggiungibili inband tramite la rete locale. A questo scopo su questo computer deve essere installato il protocollo di rete TCP/IP. Con questo programma non è possibile operare su router connessi tramite l'interfaccia seriale.*

**La connessione Internet si controlla con ELSA LANmonitor**

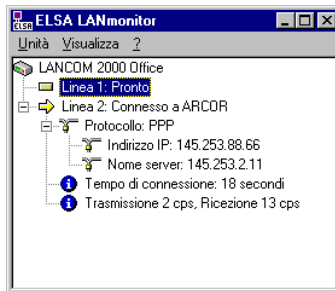
Come esempio delle funzioni di *ELSA LANmonitor* vengono prima illustrate le informazioni che *ELSA LANmonitor* fornisce al provider Internet attraverso la connessione stabilita.

- ① Impostare il router per la connessione al provider, per es. con il 'Setup wizard' di *ELSA LANconfig*.
- ② Avviare *ELSA LANmonitor* con **Avvio ► Programmi ► ELSA ► LANmonitor**. Creare una nuova periferica con **Unità ► Nuovo** e introdurre nella finestra seguente l'indirizzo IP per il router che si desidera monitorare. Se la configurazione della periferica è protetta con una password, introdurre la stessa.

Come alternativa si può selezionare in *ELSA LANconfig* l'apparecchio e avviare il monitoraggio con **Strumenti ► Unità Monitor**.

- ③ *ELSA LANmonitor* crea automaticamente una nuova voce nella lista degli apparecchi e mostra prima lo stato dei canali di trasmissione. Avviare il

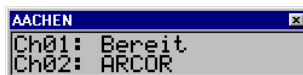
browser Internet e richiamare una qualunque pagina Web. *ELSA LANmonitor* mostra adesso come un collegamento venga stabilito in un canale, e quale controparte venga chiamata nel farlo. Appena la connessione è stata stabilita, il canale B indica con un segno « più » prima della voce che su questo canale sono presenti altre informazioni. Cliccando sul segno « più » si apre una struttura ad albero in cui si possono leggere diverse informazioni.



In questo esempio si possono leggere dalle informazioni di protocollo per il PPP quale indirizzo IP il provider ha assegnato al router per la durata della connessione e quali indirizzi per i server DNS e NBNS sono stati comunicati.

Sotto le informazioni generali si può visualizzare con quali velocità di trasmissione i dati vengono scambiati attualmente con Internet.

- ④ Cliccando con il tasto destro del mouse sul canale attivo si può interrompere manualmente la connessione. A tale scopo si necessita eventualmente della password di configurazione.
- ⑤ Se oltre alle informazioni della lista delle periferiche di *ELSA LANmonitor* si desidera una finestra informativa ridotta in forma di Display LC, cliccare con il tasto destro del mouse sul nome della periferica e selezionare **Display canali**.



Cliccando con il tasto destro del mouse sul campo di visualizzazione del display canali si può impostare questo display virtuale in modo che rimanga sempre in primo piano sullo schermo.

- ⑥ Se si desidera un protocollo delle uscite *ELSA LANmonitor* in forma di file, selezionare nel menu 'Visualizza' le 'Opzioni' e passare alla scheda di registro 'Registrazione'. Attivare il protocollo e impostare se *ELSA LANmonitor* deve creare un file di protocollo giornalmente, mensilmente o continuamente.

## 3.7

## Documentazioni trace

Per controllare i processi interni del router durante la configurazione sono utili le documentazioni trace. Con siffatte documentazioni trace per es. si possono visualizzare i singoli passi della negoziazione PPP. Attraverso l'interpretazione di queste documentazioni, gli operatori esperti possono eventualmente rintracciare gli errori durante lo stabilimento della connessione. Specialmente positivo: Gli errori da rintracciare possono essere trovati sia nella configurazione del proprio router che in quello della controparte.

*Le documentazioni trace sono leggermente ritardate rispetto all'evento reale, ma sempre nella sequenza corretta. Di regola questo non disturba l'interpretazione delle osservazioni, ma dovrebbe essere preso in considerazione per una analisi più precisa.*

### 3.7.1

### Avviamento di trace

Trace viene richiamato secondo la seguente sintassi:

```
trace [code] [parametri]
```

Il comando trace, la chiave, i parametri e i comandi combinati vengono sempre separati tra loro con spazi. Che cosa si trova dietro la chiave e i parametri?

| Questa chiave ... | ... in collegamento con trace genera la seguente reazione: |
|-------------------|------------------------------------------------------------|
| ?                 | Visualizza un testo di aiuto                               |
| +                 | Attiva una documentazione trace                            |
| -                 | Disattiva una documentazione trace                         |
| #                 | Commuta tra diverse documentazioni trace (toggle)          |
| Nessuna chiave    | Visualizza lo stato attuale di trace                       |

| Questo parametro ... | ... in collegamento con trace genera la seguente visualizzazione: |
|----------------------|-------------------------------------------------------------------|
| Status               | Messaggi di stato delle connessioni                               |
| Error                | Messaggi di errore delle connessioni                              |
| ELSA                 | Negoiazione del protocollo ELSA                                   |
| PPP                  | Negoiazione del protocollo PPP                                    |
| IPX-router           | Routing IPX                                                       |
| RIP                  | IPX Routing Information Protocol                                  |
| SAP                  | IPX Service Advertising Protocol                                  |
| IPX-watchdog         | IPX Watchdog spoofing                                             |
| SPX-watchdog         | SPX Watchdog spoofing                                             |
| NetBIOS              | Gestione NetBIOS                                                  |
| Router IP            | Routing IP                                                        |
| IP-RIP               | IP Routing Information Protocol                                   |
| ICMP                 | Internet Control Message Protocol                                 |
| ARP                  | Address Resolution Protocol                                       |
| SCRIPT               | Trattative dello script                                           |
| IP-mascheratura      | Eventi nel modulo mascheratura                                    |
| DHCP                 | Dynamic Host Configuration Protocol                               |
| D-channel dump       | Trace del canale D del bus ISDN collegato                         |

| Questo comando combinato ... | ... in collegamento con trace genera la seguente visualizzazione:                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------------|
| All                          | Tutte le documentazioni trace                                                                                       |
| Display                      | Documentazioni di stato e di errore                                                                                 |
| Protocol                     | Documentazioni ELSA e PPP                                                                                           |
| TCP-IP                       | Documentazioni IP-Rt., IP-RIP, ICMP e ARP                                                                           |
| IPX-SPX                      | Documentazioni IPX-Rt., RIP, SAP, IPX-Wd., SPX-Wd., e NetBIOS                                                       |
| Time                         | Prima della documentazione trace vera e propria visualizza anche il tempo di sistema                                |
| Source                       | Prima della documentazione trace vera e propria visualizza anche il protocollo a cui si riferisce la documentazione |

I parametri allegati vengono elaborati da sinistra verso destra. Pertanto un parametro chiamato prima può anche successivamente essere di nuovo limitato.

### Esempi:

| Questa chiave ...        | ... in collegamento con trace genera la seguente reazione:                                                                                          |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Trace                    | Visualizza tutti i protocolli che possono produrre documentazioni durante la configurazione, e lo stato delle rispettive documentazioni (ON o OFF). |
| Trace + all              | Attiva tutte le documentazioni trace.                                                                                                               |
| Trace + protocol display | Attiva la documentazione di tutti i protocolli di connessione e dei messaggi di stato e di errore.                                                  |
| Trace + all - icmp       | Attiva tutte le documentazioni trace escluso il protocollo ICMP.                                                                                    |
| trace ppp                | Visualizza lo stato attuale del PPP.                                                                                                                |
| Trace # ipx-rt display   | Commuta le documentazioni trace del router IPX e del display.                                                                                       |
| Trace - time             | Disattiva la visualizzazione del tempo di sistema prima della documentazione trace vera e propria.                                                  |

## 3.8

### Configurazione con SNMP

Il Simple Network Management Protocol (SNMP V.1 secondo RFC 1157) consente il monitoraggio e la configurazione delle periferiche di una rete da una posizione centralizzata.

Informazioni dettagliate sulla configurazione di apparecchiature ELSAcon SNMP si trovano nella documentazione elettronica del CD.

## 4 Funzioni e modalità

Questo capitolo presenta le diverse funzioni e modalità dell'apparecchio. In esso si trovano tra l'altro informazioni sui seguenti punti:

- Sicurezza per la configurazione
- Sicurezza per la LAN
- Gestione degli addebiti
- Connessioni ISDN
- Supporto PPP
- Routing IPX (solo *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1100 Office*, *ELSA LANCOM 1000 Office*)
- Routing IP
- Bridging (solo *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1100 Office*, *ELSA LANCOM 1000 Office*)
- Gestione indirizzi automatica con DHCP
- DHCP-Relay-Agent (escluso *ELSA LANCOM 800 Office*)
- Server DNS
- Proxy NetBIOS (solo *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1100 Office*, *ELSA LANCOM 1000 Office*)
- Least-cost router
- *ELSA LANCAPI*
- Controllo ora
- Impianto telefonico (solo *ELSA LANCOM 2000 Office*)
- Accounting

Oltre alla descrizione dei singoli punti, vengono anche fornite indicazioni utili per la configurazione.

Una descrizione dettagliata di tutti i parametri e menu si può trovare nella documentazione elettronica.

### 4.1 Sicurezza per la configurazione

Con la configurazione dell'apparecchio, si definisce una serie di importanti parametri per lo scambio dati: rientrano tra questi per es. la sicurezza della propria rete, i controlli sui costi e l'autorizzazione di singoli partecipanti alla rete.

Naturalmente i parametri impostati non devono essere poi modificati da persone non autorizzate. Pertanto un *ELSA LANCOM Office* offre la possibilità di proteggere la configurazione in vari modi.

## 4.1.1 Protezione con password

La possibilità più semplice per proteggere la configurazione è quella di definire una password. Se non è stata definita una password, chiunque può modificare la configurazione dell'apparecchio.

Il campo per l'immissione della password si trova in *ELSA LANconfig* nel campo di configurazione 'Gestione' sulla scheda di registro 'Sicurezza'. Durante una sessione di terminale o Telnet si attiva la richiesta di password nel menu `/Setup/Config-module/password required`. In questo caso, la password stessa viene impostata con il comando `passwd`.

## 4.1.2 Il blocco del login

La configurazione del *ELSA LANCOM Office* è protetta mediante un blocco del login contro gli « attacchi Brute-Force ». Nel caso di un attacco Brute-Force, un utente non autorizzato tenta di « scassinare » la password per avere così accesso ad una rete, ad un computer o ad un'altra apparecchiatura. Per farlo ad esempio un computer prova automaticamente tutte le possibili combinazioni di lettere e numeri fino a che non ha trovato la password giusta.

Per la protezione contro tali tentativi si può indicare il numero massimo ammesso di tentativi di login. Se questo limite viene raggiunto, l'accesso viene bloccato per un determinato intervallo.

Questi parametri valgono in modo globale per tutte le possibilità di configurazione (outband, Telnet, TFTP/*ELSA LANconfig* e SNMP). Se su un accesso interviene il blocco, anche tutti gli altri accessi vengono automaticamente bloccati.

Per configurare il blocco del login, sono disponibili le seguenti voci in *ELSA LANconfig* nel campo di configurazione 'Gestione' sulla scheda di registro 'Sicurezza' oppure nel menu `/Setup/Config-module`:

- 'Blocca la configurazione dopo ...' (`login-errors`)
- 'Blocca la configurazione per ... minuti' (`lock-minutes`)



### 4.1.3 Controllo in arrivo tramite TCP/IP

Con una speciale lista di filtro, l'accesso alle funzioni interne degli apparecchi può essere limitato tramite TCP/IP. Si definiscono come funzioni interne le sedute di configurazione tramite Telnet o TFTP (*ELSA LANconfig*).

Come standard questa tabella non contiene alcuna voce, in modo da poter avviare anche da computer con indirizzo IP qualunque tramite TCP/IP con Telnet o TFTP l'accesso al router. Con la prima introduzione di un indirizzo IP e della rispettiva maschera di rete il filtro viene attivato, e solo gli indirizzi IP contenuti in questa voce mantengono il diritto di accedere alle funzioni interne. Con ulteriori introduzioni si può ampliare il cerchio degli aventi diritto. Le voci di filtro possono definire sia singoli computer che intere reti.

La lista di accesso si trova in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Generale' oppure nel menu `/Setup/TCP-IP-module/Access List`.

## 4.2 Sicurezza per la LAN

Sicuramente all'utente non piacerà che una persona qualsiasi possa semplicemente dare un'occhiata o modificare i dati dei suoi computer. Un *ELSA LANCOM Office* offre diverse possibilità per limitare l'accesso dall'esterno:

- Protezione di accesso con nome, password e numero d'utenza
- Chiamata di risposta a numeri telefonici stabiliti
- Filtraggio dei pacchetti di dati
- Mascheratura IP (definito anche NAT o PAT)

### 4.2.1 Il controllo

Quale « Identifier » debba essere utilizzato per il riconoscimento del chiamante, viene impostato nell'area di configurazione 'Comunicazione' nella scheda 'Risposta chiamata' o nel menù `/Setup/WAN-module/Protect`. Si hanno le seguenti possibilità di selezione:

- alle: Vengono accettate le chiamate di tutte le controparti.
- per nome: Vengono accettate solo le chiamate delle controparti inserite nella lista dei nomi.
- per numero: Vengono accettate solo le chiamate delle controparti inserite nella lista dei numeri.

- per nome o numero: Vengono accettate solo le chiamate delle controparti inserite nella lista dei numeri ● nella lista dei nomi.

Naturalmente l'identificazione presuppone che venga comunicata dal chiamante la corrispondente informazione.

### Controllo del nome

Se si utilizza il layer ELSA oppure PPP per il canale B, si può trasmettere anche il nome della controparte chiamante. Tuttavia a questo scopo si deve prima stabilire una connessione, poiché il nome non può essere scambiato attraverso il canale D.

La reazione del router è chiara: Se è stata definita una protezione tramite il nome, vengono accettate solo le chiamate con nome conosciuto, le altre vengono respinte.

Se si utilizza il protocollo ELSA viene controllato se il nome comunicato dalla controparte è presente nella lista dei nomi.

Nel protocollo PPP si controlla se il nome della controparte è registrato nella lista PPP come nome utente. Se il nome utente manca, il nome della periferica viene accettato come nome della controparte e controllato. La lista PPP si trova in *ELSA LANconfig* nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Protocolli' oppure nel menu `/Setup/WAN-module/PPP List`.

Non è possibile proteggere con password? Ma certo, questa speciale possibilità esiste nel PPP: Qui si può inoltre richiedere una protezione speciale valevole per questo protocollo secondo PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) o MS-CHAP (variante Microsoft del CHAP). Si tratta della protezione che il proprio apparecchio richiede alla controparte.



*Le procedure di sicurezza PAP, CHAP o MS CHAP naturalmente non si applicano per es. se con il ELSA LANCOM si seleziona direttamente un Internet Service Provider. Probabilmente non è il caso di rispondere all'ISP con la richiesta di una password...*

Da dove arrivano il nome e la password del chiamante?

Se si usa il protocollo ELSA per il canale B, l'identificazione si realizza solo con il nome, senza password. In tale caso il nome è il nome della periferica del router chiamante.

Se si usa il PPP, il nome e la password vengono introdotti quando si stabilisce la connessione con la controparte, per es. nella corrispondente finestra di una connessione in Accesso remoto. Se lo stesso router stabilisce una connessione, viene usato il nome della periferica, la password e il nome utente della lista PPP.

### Controllo del numero

Quando una chiamata arriva attraverso una linea ISDN, nella maggior parte dei casi viene trasmesso tramite il canale D il numero d'utenza del chiamante, già prima che la connessione venga stabilita (CLI – Calling Line Identifier).

Se il numero d'utenza è registrato nella lista dei numeri, l'accesso alla propria rete può essere concesso, oppure il chiamante viene richiamato se è attivata l'opzione di chiamata di risposta. Se nel *ELSA LANCOM* è stata definita una protezione tramite il numero, tutte le chiamate da controparti con numero d'utenza sconosciuto vengono respinte.

La protezione tramite il numero d'utenza può essere utilizzata con tutti i protocolli di canale B (layer).

## 4.2.2

### La chiamata di risposta

Una speciale variante della protezione di accesso si realizza con la funzione di chiamata di risposta: A questo scopo, nella lista dei nomi per il chiamante desiderato si attiva l'opzione 'Richiamo automatico' ed eventualmente si indica il numero d'utenza.

Con le impostazioni nella lista dei nomi e nella lista dei numeri e la selezione del protocollo (ELSA o PPP) si può gestire il comportamento della chiamata di risposta del proprio router :

- Il router può respingere la richiesta di chiamata di risposta.
- Può richiamare un numero d'utenza prestabilito.
- Il numero d'utenza per la chiamata di risposta può essere indicato liberamente dal chiamante.

Inoltre mediante le impostazioni si può definire la ripartizione dei costi per la connessione. Se nella lista dei nomi è definita una chiamata di risposta 'con nome', il router che effettua la chiamata di risposta si accolla tutti gli addebiti tranne uno, quello necessario per la comunicazione del nome. Un'unità viene addebitata al router anche se il chiamante non viene identificato tramite CLI.

Se invece l'identificazione tramite il numero d'utenza del chiamante è consentita e possibile, il chiamante può non subire alcun addebito.

Se il router stesso deve eseguire la chiamata di risposta, per molte controparti si può anche adottare la procedura Fast Call Back (in corso di brevetto). Questa accelera notevolmente la procedura di chiamata di risposta.

## H

### 4.2.3

### Come nascondersi: mascheratura IP (NAT, PAT)

Uno dei compiti più frequenti dei router è attualmente quello di collegare molti posti di lavoro di una LAN alla rete globale, cioè a Internet. Se possibile, chiunque deve poter accedere direttamente a WWW dal posto di lavoro e procurarsi le informazioni più aggiornate per la sua attività.

Ma ci sono obiezioni da parte dei responsabili delle reti, che si preoccupano della sicurezza dei dati della rete aziendale: Ogni workstation in WWW? Ma allora chiunque può entrare dall'esterno! – Ebbene, non è assolutamente così!

Il nascondiglio per tutti i computer in Internet si chiama mascheratura IP. Con questa procedura, solo il modulo router dell'apparecchio viene conosciuto in Internet con il suo indirizzo IP. L'indirizzo IP può essere assegnato in modo fisso o assegnato dinamicamente dal provider. I computer della LAN utilizzano il router come gateway e non possono essere riconosciuti. Il router separa Internet e Intranet come una parete. La mascheratura IP viene anche definita « firewall ».

L'impiego del mascheratura IP viene definito singolarmente per ciascuna rotta della tabella di routing. La tabella di routing si trova in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Routing' oppure nel menu /Setup/IP-router/IP-routing-table.

Ulteriori informazioni si possono trovare nella sezione 'Routing IP: Masquerading IP'.

## 4.3

### Gestione degli addebiti

La caratteristica del router di essere in grado di stabilire collegamenti autonomamente con tutte le controparti desiderate e di terminarli alla fine del trasferimento, rende possibile all'utente un accesso molto comodo per es. a Internet. Nel caso di trasmissione dati tramite linee soggette a costi, a causa di una configurazione errata del router (per es. nella configurazione dei

filtri) o tramite utilizzo eccessivo dell'offerta (per es. un continuo surf in Internet), possono aversi costi elevati.

Per limitare tali costi, il software offre diverse possibilità:

- Gli addebiti di collegamento ISDN possono essere limitati per un determinato periodo.
- I minuti di collegamento ISDN possono essere limitati per un determinato periodo.

### 4.3.1

## Limitazione della connessione ISDN in base agli addebiti

Se in una linea ISDN vengono generati gli impulsi di conteggio, si possono allora limitare gli addebiti di collegamento in modo molto semplice. Nello stato normale è ammesso ad esempio il consumo di massimo 830 unità in sei giorni. Quando questo limite è stato raggiunto, il router non consente un ulteriore stabilimento attivo della connessione.



*Il monitoraggio addebiti del router può essere utilizzato al meglio quando sono attivate le « informazioni di addebito **durante** la connessione » sulla rete ISDN (secondo AOCd). Eventualmente richiedere l'abilitazione di questa caratteristica alla società telefonica. In linea di principio è anche possibile un monitoraggio addebiti con la caratteristica « Informazioni di addebito **dopo** la connessione », tuttavia in questo caso non vengono riconosciute le connessioni prolungate!*



*Se è stato attivato il least-cost routing possono essere stabilite anche connessioni tramite provider che non trasmettono informazioni di addebito!*

### 4.3.2

## Limitazione della connessione ISDN in base al tempo

Se nella linea ISDN non vengono generati gli impulsi di conteggio, il meccanismo della sorveglianza degli addebiti ISDN non funziona. Per es. questo è il caso in cui la trasmissione delle informazioni di addebito non è stata richiesta oppure la società telefonica non trasmette affatto tali informazioni.

Per poter limitare i costi per i collegamenti ISDN anche senza gli impulsi di conteggio, si può gestire la durata massima del collegamento con l'aiuto del tempo. A tale scopo si accorda un budget temporale per un periodo. Nello stato normale è ammesso ad esempio stabilire attivamente collegamenti per un massimo di 210 minuti in sei giorni.



*Se un limite previsto viene raggiunto, tutti i collegamenti aperti del router e stabiliti dal router stesso vengono automaticamente terminati. Solo dopo che è trascorso il periodo attuale i budget vengono di nuovo abilitati e le connessioni attive sono possibili. Naturalmente l'amministratore può anche abilitare in anticipo i budget!*

Con un budget di 0 unità oppure di 0 minuti si può disattivare il monitoraggio degli addebiti oppure del tempo delle funzioni router.

*Solo le funzioni router sono protette in base ad addebiti/tempo! Le connessioni tramite LANCAPI o le porte a/b non vengono rilevate.*



### 4.3.3

## Impostazioni nel modulo addebiti

Le impostazioni di interfaccia si trovano in *ELSA LANconfig* nel campo di configurazione 'Gestione' sulla scheda di registro 'Costi' o nelle sedute Telnet o di terminale nella posizione /Setup/Charges-module.

Nel modulo addebiti si possono impostare, monitorare e utilizzare per la protezione il tempo online e gli addebiti registrati.

- Day(s)/period  
Viene indicata la durata in giorni di un periodo di monitoraggio
- Budget di scatti, budget di minuti ISDN  
Numero di scatti massimo ISDN o di minuti online ISDN in un periodo di sorveglianza
- Budget residuo, minuti ISDN residui  
Scatti o minuti ISDN disponibili nel periodo corrente
- Scatti del router, minuti ISDN del router  
Scatti ISDN o minuti online ISDN per tutti i periodi
- Total-units  
Tutti gli addebiti riferiti all'apparecchio
- Table-budget, Time-table  
Tabelle con gli addebiti oppure i tempi per il rispettivo modulo



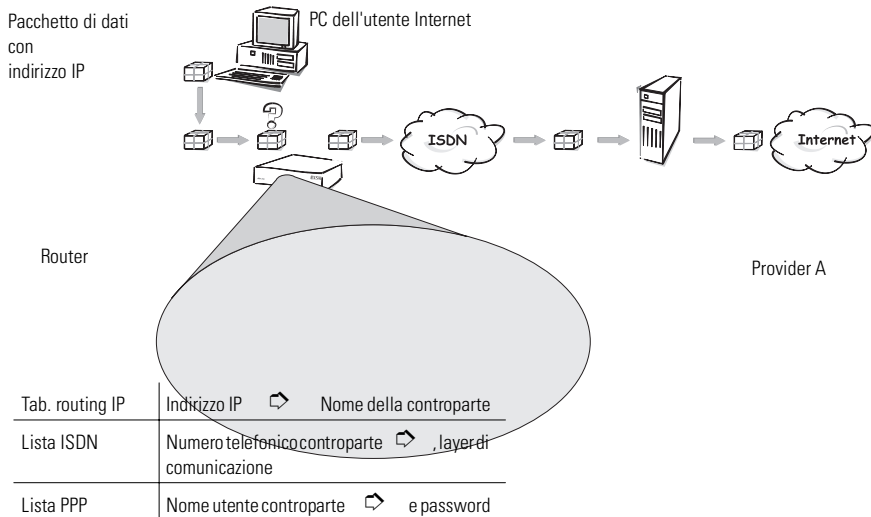
*Le informazioni sugli addebiti e sui tempi di connessione vengono salvate durante un bootstrap (per es. quando si scarica un nuovo firmware) e si perdono solo se l'apparecchio viene disattivato. Tutte le indicazioni di tempo riportate sono in minuti.*

## 4.4 Connessioni ISDN

La comunicazione dati tra due periferiche ISDN si realizza tramite connessioni ISDN. In linea di principio queste connessioni possono essere connessioni a selezione o connessioni fisse.

I moduli router prima determinano solo la controparte a cui un pacchetto di dati deve essere trasmesso. Affinché la corrispondente connessione possa essere selezionata ed event. stabilita, devono essere definiti diversi parametri per tutte le connessioni ISDN necessarie. Questi parametri vengono salvati in diverse liste, che cooperano per stabilire le connessioni corrette.

Si vuole adesso chiarire questo complesso sulla base di un semplice esempio.



Un pacchetto di dati di un computer trova la via verso Internet in prima linea tramite l'indirizzo IP del ricevente. Con questo indirizzo, il computer invia il pacchetto tramite la LAN al router. Il router controlla prima con l'indirizzo IP le tabelle di routing IP e vi trova la controparte appartenente a questo indirizzo, ad esempio 'Provider\_A'. Con questo nome il router controlla quindi

la lista di nomi ISDN e trova il numero telefonico della corrispondente controparte che può essere raggiunta tramite ISDN, incl. il layer di comunicazione da usare. Il router preleva inoltre dalla lista PPP il nome dell'utente e la sua password che sono necessari per effettuare il login al provider A.

Il router può quindi stabilire un collegamento sulla linea ISDN con il router del provider. Non appena il collegamento è stato stabilito, il router può inoltrare il pacchetto di dati in Internet tramite la linea ISDN.

Ulteriori informazioni sulle reti IP ecc., si trovano nelle informazioni di base tecniche della documentazione elettronica sul CD.

Le seguenti sezioni presentano brevemente la lista di nomi ISDN e i parametri in essa contenuti, e mostrano quindi il rapporto con le altre liste e i parametri e come esse vengano configurate nel software.

La lista PPP viene descritta in un capitolo apposito (vedi 'Lista PPP').

Le informazioni sulla tabella di routing IP si trovano nella sezione 'Routing IP'.

#### 4.4.1

### Lista di nomi ISDN

In *ELSA LANconfig*, la lista di nomi si trova nella zona della configurazione 'Comunicazione' nella scheda 'Controparti' o nel caso di sessioni Telnet o di terminale in `/Setup/Modulo WAN/Lista di nomi ISDN`.

Per definire le controparti disponibili, queste vengono immesse nella lista dei nomi con un nome appropriato e parametri aggiuntivi:

- Nome

Con questo nome, la controparte viene identificata nei moduli router.

- Dialup-remote

Questo numero d'utenza deve essere chiamato se il router deve stabilire autonomamente in modo attivo una connessione con la controparte.

Se la controparte può essere raggiunta con diversi numeri d'utenza, immettere gli altri numeri d'utenza nella lista round-robin.

Se tale controparte viene raggiunta tramite una connessione fissa, qui si può indicare il numero d'utenza per una linea di backup tramite connessione a selezione.

- Tempi di attesa

Questi tempi indicano per quanto tempo rimangono attivi i canali B, dopo che



- nei canali stabiliti in modo statico per il tempo di attesa B1 non sono stati più trasmessi dati.
- nei canali stabiliti in modo dinamico per il tempo di attesa B2 la velocità di trasmissione dati è scesa sotto un valore limite prestabilito.
- WAN-layer  
Il layer rappresenta un insieme di protocolli che devono essere utilizzati per questa connessione. Il layer deve essere impostato allo stesso modo sui due lati della connessione.
- Chiamata di risposta  
Se il router riceve una chiamata da questa controparte, qui si può impostare come opzione di non accettare la chiamata. Invece la controparte viene richiamata con le seguenti opzioni:
  - normale chiamata di risposta
  - chiamata di risposta rapida secondo ELSA
  - chiamata di risposta dopo il controllo del nome
  - attesa della chiamata di risposta da parte della controparte secondo la procedura di chiamata di risposta rapida ELSA

#### 4.4.2

### Impostazioni di interfaccia

In *ELSA LANconfig* le impostazioni dell'interfaccia si trovano nella zona della configurazione 'Management' nella scheda 'Interfaces' o nel caso di sessioni Telnet o sessioni di terminale in `/Setup/Modulo WAN/Lista interfacce`.

Nelle impostazioni di interfaccia si definiscono i parametri generali per ogni interfaccia (e quindi per ogni connessione  $S_0$ ). Questi parametri valgono per tutte le modalità degli apparecchi. Questi sono in dettaglio:

- Il protocollo canale D che viene utilizzato per questa connessione  $S_0$ .  
Riconoscimento automatico, DSS1 (Euro-ISDN), DSS1 punto-a-punto, connessione fissa gruppo 0
- Opzione connessione fissa  
Canale B che deve essere utilizzato event. per la connessione fissa.

- Prefisso

Numero che deve essere selezionato prima del numero d'utenza per le chiamate in uscita, per es. il numero identificativo del centralino nel caso di impianti interni.

### 4.4.3

## Impostazioni di interfaccia router

Le impostazioni di interfaccia router si trovano in *ELSA LANconfig* nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Generale' o nelle sedute Telnet o di terminale nella posizione `/Setup/WAN-module/Router-interface-list`.

Nelle impostazioni di interfaccia router si definiscono per ogni interfaccia (e quindi per ogni connessione  $S_0$ ) i parametri che devono essere utilizzati nella modalità router. Questi parametri non valgono per le altre modalità degli apparecchi. Questi sono in dettaglio:

- Numeri d'utenza (MSN/EAZ)

Il router reagisce a questi numeri d'utenza nelle chiamate in arrivo. Più numeri d'utenza vengono separati da « punto e virgola ». Se non si immettono i numeri d'utenza, il router reagisce a tutti i numeri d'utenza.

Il primo numero d'utenza immesso viene trasmesso alla controparte in caso di stabilimento attivo della connessione. Se non si immettono i numeri d'utenza, viene trasmesso il MSN principale della connessione.

- Opzione per la connessione Y

Attivare questa opzione se i due canali B della connessione devono poter stabilire connessioni in parallelo con controparti diverse.

- Soppressione del proprio numero d'utenza

Attivare questa opzione se il proprio numero d'utenza non deve essere indicato alla controparte durante lo stabilimento attivo della connessione del router.

*Questa funzione deve essere supportata dal gestore della rete.*

### 4.4.4

## Impostazioni di interfaccia LANCAPI

Le impostazioni di interfaccia *LANCAPI* si trovano in *ELSA LANconfig* nel campo di configurazione 'LANCAPI' sulla scheda di registro 'Generale' o nelle sedute Telnet o di terminale nella posizione `/Setup/LANCAPI-module/Interface-list`.

Nelle impostazioni di interfaccia router si definiscono per ogni interfaccia (e quindi per ogni connessione  $S_0$ ) i parametri che devono essere utilizzati per la *LANCAPI*. Questi parametri non valgono per le altre modalità degli apparecchi. Questi sono in dettaglio:

- Numeri d'utenza (MSN/EAZ)

La *LANCAPI* reagisce a questi numeri d'utenza nelle chiamate in arrivo. Più numeri d'utenza vengono separati da « punto e virgola ». Se non si immettono i numeri d'utenza, il router reagisce a tutti i numeri d'utenza.

- Accesso alla *LANCAPI*

Qui la funzione della *LANCAPI* per l'interfaccia può essere disattivata completamente, abilitata solo per le chiamate in uscita oppure sia per le chiamate in arrivo che per quelle in uscita.

- Trasmissione del proprio numero d'utenza

Normalmente durante lo stabilimento attivo della connessione tramite la *LANCAPI* viene trasmesso il numero d'utenza impostato nell'applicazione CAPI. Se tale numero d'utenza manca o non è valido, la *LANCAPI* non trasmette alcun numero d'utenza. Con questa opzione si può stabilire che, in caso di mancanza del numero d'utenza dell'applicazione CAPI, al posto di questo venga trasmesso il primo numero presente nel campo 'Numeri d'utenza'.

## 4.4.5

### Lista layer

La lista dei layer di comunicazione si trova in *ELSA LANconfig* nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Generale' o nelle sedute Telnet o di terminale nella posizione `/Setup/WAN-module/Layer-list`.

In un layer si definisce una determinata combinazione di impostazioni di protocollo che deve essere utilizzata per la trasmissione ad altri apparecchi. Questi sono in dettaglio:

- WAN-layer

Con questo nome vengono salvate le impostazioni di protocollo. Selezionare nella lista dei nomi le impostazioni con il nome di layer per la corrispondente connessione.

- Incapsulamento

Impostare qui se un'intestazione Ethernet deve essere aggiunta ai pacchetti di dati. Normalmente è sufficiente l'impostazione

'Trasparente', solo nelle connessioni HDLC verso periferiche esterne questa impostazione può essere necessaria.

- Layer 3

Protocollo layer 3 per la connessione. Viene riconosciuto in parte automaticamente nelle chiamate in arrivo.

Se si utilizza PPP è necessaria una voce aggiuntiva nella lista PPP.

Se si utilizza Script è necessaria una voce aggiuntiva nella lista Script.

- Layer 2

Protocollo layer 2 per la connessione.

- Opzioni

Attiva come opzione la compressione dei dati e il raggruppamento di canali. Queste opzioni saranno efficaci solo se esse vengono supportate dai protocolli sui layer 2 e 3.

- Layer 1

Protocollo layer 1 per la connessione. Viene riconosciuto in parte automaticamente nelle chiamate in arrivo.

## 4.4.6

### Lista round-robin

La lista round-robin si trova in *ELSA LANconfig* nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Controparti' o nelle sedute Telnet o di terminale nella posizione `/Setup/WAN-module/RoundRobin list`.

Se una controparte può essere raggiunta con più numeri d'utenza, immettere nella lista dei nomi prima il primo numero d'utenza e poi tutti gli altri nella lista RoundRobin.

- Sito remoto

Nome della controparte definito per primo nella lista dei nomi.

- Round-robin

Ulteriori numeri d'utenza per tale controparte. Più numeri d'utenza vengono separati da trattini.

- Cominciare con:

Indicare se un nuovo stabilimento della connessione deve essere avviato con l'ultimo numero che ha avuto successo o sempre con il primo numero della lista.

#### 4.4.7

### Script

La lista Script si trova in *ELSA LANconfig* nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Protocolli' o nelle sedute Telnet o di terminale nella posizione */Setup/WAN-module/Script-list*.

Se per la selezione della controparte si rende necessario il trattamento di uno script, qui si può immettere lo script e assegnarlo alla controparte.

Il protocollo layer 3 selezionato nella lista layer per questa connessione deve supportare il trattamento dello script.

- Sito remoto  
Nome della controparte definito per primo nella lista dei nomi.
- Script  
Immettere qui lo script, come descritto nella parte di riferimento della documentazione.

#### 4.4.8

### Accettazione di chiamate

Le impostazioni per l'accettazione di chiamate si trovano in *ELSA LANconfig* nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Accettazione chiamate' o nelle sedute Telnet o di terminale nella posizione */Setup/WAN-module/Protect*.

Con le impostazioni per l'accettazione di chiamate si definiscono le circostanze in cui l'apparecchio accetta le chiamate in arrivo. Queste impostazioni valgono solo per le funzioni router dell'apparecchio.

- Tutte  
Vengono accettate tutte le chiamate.
- Nome  
Tutte le chiamate vengono accettate inizialmente. Nella trattativa di protocollo viene determinato il nome e viene controllato se tale nome è registrato nella lista dei nomi. La connessione viene mantenuta solo in tale caso, altrimenti viene interrotta.
- Per numero  
La chiamata viene accettata solo se la controparte è registrata nella lista dei numeri e il numero d'utenza della controparte viene trasmesso.
- Per nome o numero  
La chiamata viene accettata se uno dei due controlli ha successo.

#### 4.4.9 Lista dei numeri

La lista dei numeri si trova in *ELSA LANconfig* nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Accettazione di chiamate' o nelle sedute Telnet o di terminale nella posizione `/Setup/WAN-module/Number-list`.

La lista dei numeri viene utilizzata per lo stabilimento passivo della connessione per la protezione nell'accettazione di chiamate e per l'avvio di una chiamata di risposta.

- Dialup-remote

Numero d'utenza che viene trasmesso dalla controparte chiamante (event. incl. numero identificativo nazionale e locale).

- Sito remoto

Nome della controparte definito nella lista dei nomi. Se nella lista dei nomi è definita una chiamata di risposta, viene chiamata questa controparte.

### 4.5 Gestione indirizzi automatica con DHCP

Per operare correttamente in una rete TCP/IP tutte le periferiche di una rete locale devono avere indirizzi IP univoci.

Inoltre sono anche necessari gli indirizzi dei server DNS e dei server NBNS ed anche di una -gateway standard, su cui devono essere instradati i pacchetti di dati di indirizzi non raggiungibili localmente.

Per una piccola rete è concepibile introdurre questi indirizzi « a mano » in tutti i computer della rete. In una rete più grande con molte workstation questo può diventare un compito insuperabile.

In tali casi si può utilizzare il DHCP (Dynamic Host Configuration Protocol). Tramite questo protocollo un server DHCP può assegnare dinamicamente in una LAN basata su TCP/IP alle singole stazioni gli indirizzi necessari.

#### 4.5.1 Il server DHCP

*ELSA LANCOM Office* può gestire come server DHCP gli indirizzi IP della propria rete TCP/IP. In tale circostanza esso comunica alle workstation i seguenti parametri:

- Indirizzo IP

- Maschera di rete IP
- Indirizzo broadcast
- Server DNS
- Server NBNS
- Gateway di default
- Periodo di validità dei parametri assegnati

Il server DHCP preleva gli indirizzi IP da un pool di indirizzi liberamente definito oppure determina gli indirizzi autonomamente dai propri indirizzi IP o Intranet.

Un'apparecchiatura completamente non configurata può perfino stabilire nel modo automatico DHCP gli indirizzi IP per sé stessa e per i computer nella rete.

Nel caso più semplice pertanto è solo necessario connettere il nuovo apparecchio nello stato di fornitura in una rete senza altri server DHCP e attivarlo. Il server DHCP allora regola automaticamente in cooperazione con *ELSA LANconfig* e con un'assistenza tutte le successive assegnazioni i indirizzi nella rete locale.

## 4.5.2

### DHCP – 'On', 'off' o 'auto'?

Il 'Server DHCP' può assumere tre diversi stati:

- 'On': Il server DHCP è attivato in modo permanente. Introducendo questo valore viene controllata la configurazione del server (validità del pool di indirizzi).
  - Se la configurazione è corretta l'apparecchio si offre come server DHCP in rete.
  - Se la configurazione non è corretta (per es. confini di pool non validi) il server DHCP si disattiva e si porta nello stato 'Off'.
- 'Off': Il server DHCP è disattivato in modo permanente.
- 'Auto': Il server si trova in modalità automatica. In questo stato l'apparecchiatura cerca dopo l'accensione nella rete locale altri server DHCP. Questa ricerca è riconoscibile per via di una breve accensione del LED Tx dopo l'accensione.
  - Se viene trovato almeno un altro server DHCP, l'apparecchio disattiva il proprio server DHCP. In questo modo si evita tra l'altro che un apparecchio non configurato assegni dopo l'attivazione in rete indirizzi che non si trovano nella rete locale.

- Se non viene trovato nessun altro server DHCP, l'apparecchio attiva il proprio server DHCP.

Dalle statistiche DHCP si può ricavare se il DHCP server è attivo o disattivo.

L'impostazione di default dello stato è 'Auto'.

### 4.5.3

## Gli indirizzi vengono assegnati in questo modo

### Assegnazione degli indirizzi IP

Affinché il server DHCP possa assegnare gli indirizzi IP ai computer della rete, esso deve prima conoscere quali indirizzi può utilizzare per questa assegnazione. Per la scelta dei possibili indirizzi esistono tre diverse opzioni:

- L'indirizzo IP può essere prelevato dal pool di indirizzi impostato (pool indirizzi iniziali fino a pool indirizzi finali). In questo si può introdurre qualunque indirizzo valido nella rete locale.
- Se invece si introduce '0.0.0.0', il server DHCP determina autonomamente i rispettivi indirizzi (iniziali oppure finali) dalle impostazioni per gli indirizzi IP o per gli indirizzi Intranet nel 'modulo TCP/IP'. In questo caso si procede nel modo seguente:
  - Se è introdotto solo l'indirizzo IP o solo l'indirizzo Intranet, per mezzo della rispettiva maschera di rete viene determinato l'inizio o la fine del pool.
  - Se sono indicati entrambi, l'indirizzo Intranet ha la priorità per la determinazione del pool.

Dall'indirizzo utilizzato (indirizzo IP o Intranet) e dalla rispettiva maschera di rete il server DHCP determina il primo e l'ultimo possibile indirizzo IP della rete locale come indirizzo iniziale o finale del pool di indirizzi.

- Se il router non dispone di un proprio indirizzo IP o Intranet, l'apparecchio si trova in uno speciale stato operativo. Esso utilizza autonomamente l'indirizzo IP '10.0.0.254' e il pool di indirizzi '10.x.x.x' per l'assegnazione degli indirizzi IP della rete. In questo stato il server DHCP assegna agli altri computer della rete solo l'indirizzo IP e la rispettiva validità, ma non le altre informazioni.

Se ora si avvia un computer della rete che con le proprie impostazioni di rete richiede un indirizzo IP tramite DHCP, un apparecchio con modulo DHCP attivato gli offre l'assegnazione di un indirizzo. Come indirizzo IP viene prelevato dal pool un indirizzo valido. Se nel passato è già stato assegnato al



computer un indirizzo IP, esso richiede proprio questo indirizzo IP, e il server DHCP tenta di assegnare di nuovo tale indirizzo, se non lo ha già assegnato a un altro computer.

Il server DHCP controlla inoltre se l'indirizzo cercato è ancora libero nella rete locale. Appena è stata riconosciuta l'univocità di un indirizzo, viene assegnato al computer richiedente l'indirizzo trovato.

### **Assegnazione della maschera di rete**

L'assegnazione della maschera di rete avviene in modo analogo all'assegnazione degli indirizzi. Se nel modulo DHCP è indicata una maschera di rete, questa viene utilizzata per l'assegnazione. Altrimenti viene utilizzata la maschera di rete del modulo TCP/IP. L'ordine è in questo caso lo stesso a quello dell'assegnazione degli indirizzi.

### **Assegnazione dell'indirizzo broadcast**

Di regola nella rete locale viene utilizzato per i pacchetti broadcast un indirizzo che si ricava dagli indirizzi IP validi e dalla maschera di rete. Solo in casi speciali (per es. quando si usano sottoreti per una parte delle workstation) può essere necessario utilizzare un altro indirizzo broadcast. In tale caso l'indirizzo broadcast da utilizzare viene introdotto nel modulo DHCP.

*E' opportuno che la modifica del valore predefinito per l'indirizzo broadcast sia eseguita da esperti specialisti di rete. Un errore di configurazione in questo settore può causare indesiderabili e costosi effetti di interruzione delle connessioni!*

### **Assegnazione del server DNS e del server NBNS**

Per questo vengono utilizzate le rispettive voci del 'modulo TCP'.

Se nei corrispondenti campi non è indicato un server, il router fornisce il proprio indirizzo IP come indirizzo DNS. Questo viene determinato come descritto al punto 'Assegnazione di un indirizzo IP'. Il router poi utilizza il DNS forwarding (vedere anche 'DNS forwarding'), per rispondere alle domande DNS o NBNS dell'host.

### **Assegnazione della gateway di default**

L'apparecchiatura assegna al computer richiedente normalmente il proprio indirizzo IP quale indirizzo di gateway.

Se necessario, questa assegnazione può essere soprascritta dalle impostazioni della workstation.



## Periodo di validità di una assegnazione

Gli indirizzi assegnati al computer hanno solo una validità limitata. Dopo che questo periodo di validità è scaduto il computer non può più utilizzarli. Affinché il computer non perda successivamente gli indirizzi (specialmente il proprio indirizzo IP), esso richiede tempestivamente una proroga, che di regola viene sempre concessa. Solo se il periodo di validità scade mentre il computer è spento, questo perde l'indirizzo.

Ad ogni richiesta un host può richiedere un periodo di validità. Tuttavia un server DHCP può assegnare all'host anche un periodo di validità diverso da questo. Il modulo DHCP presenta due impostazioni, con cui si può influire sul periodo di validità:

- Validità massima in minuti

Qui si può introdurre il periodo di validità massimo che il server DHCP può assegnare a un host.

Se un host richiede una validità che supera la durata massima, gli viene assegnata solo questa validità massima!

Il valore di default di 6000 minuti corrisponde a circa 4 giorni.

- Validità di default in minuti

Qui si può introdurre il periodo di validità che viene assegnato se l'host non richiede alcun periodo di validità. Il valore di default di 500 minuti corrisponde a circa 8 ore.

## Richiesta dei valori prefissati per l'assegnazione server DHCP

Di regola quasi tutte le impostazioni dell'ambiente di rete di Windows sono impostate in modo che i parametri necessari vengano richiesti tramite DHCP. Queste impostazioni possono essere controllate facendo clic su **Avvio ► Impostazioni ► Pannello di controllo ► Rete**. Selezionare la voce per 'TCP/IP' sulla propria interfaccia di rete, e aprire le **Proprietà**.

Sulle diverse schede registro ora si può controllare se sono presenti particolari valori per es. per l'indirizzo IP o per la gateway standard. Se si desidera che tutti i valori vengano assegnati dal router, cancellare le corrispondenti voci.

Sulla scheda registro 'Configurazione WINS' deve essere inoltre attivata l'opzione 'Usa DHCP per risoluzione WINS', se si vogliono utilizzare reti Windows via IP con scomposizione del nome tramite server NBNS. Il server DHCP deve inoltre avere un valore NBNS.

## Modifica dei valori prefissati per l'assegnazione computer

Se un computer dovesse usare parametri diversi da quelli ad esso assegnati (ad esempio un gateway standard diverso), è allora necessario impostare tali parametri direttamente nel computer del posto di lavoro. Allora il computer ignora i corrispondenti parametri dell'assegnazione effettuata dal server DHCP.

In ambiente Windows questo si realizza per es. tramite le proprietà dell'ambiente di rete.

Cliccare su **Avvio ► Impostazioni ► Pannello di controllo ► Rete**. Selezionare la voce per 'TCP/IP' sulla propria interfaccia di rete, e aprire le **Proprietà**.

Sulle diverse schede registro si possono introdurre i valori desiderati.

Nel modulo DHCP sotto il punto 'Setup/DHCP/DHCP Tabella' si può controllare (oppure esaminare) l'assegnazione degli indirizzi IP ai rispettivi computer. Questa tabella mostra gli indirizzi IP, l'indirizzo MAC, il periodo di validità assegnati, il nome del computer (se presente) e il tipo di assegnazione degli indirizzi.

Nel campo 'Tipo' è indicato in che modo è stato assegnato l'indirizzo. Il campo può assumere i seguenti valori:

- nuovo  
Il computer ha richiesto per la prima volta. Il server DHCP controlla l'univocità dell'indirizzo che deve essere assegnato al computer.
- sconosc.  
Con il controllo di univocità è stato rilevato che l'indirizzo è stato già assegnato a un altro computer. Il server DHCP non ha alcuna possibilità di ottenere altre informazioni su questo computer.
- stat.  
Un computer ha comunicato al server DHCP di essere in possesso di un indirizzo IP fisso. Questo indirizzo non può più essere utilizzato.
- din.  
Il server DHCP ha assegnato un indirizzo al computer.

## 4.5.4

## Configurazione del server DHCP

Durante la configurazione come server DHCP in linea di principio si presentano due situazioni di partenza:

- Una rete non è stata ancora creata, oppure la rete locale esistente non utilizza un TCP/IP. Con il server DHCP della propria nuova apparecchiatura ELSA, si possono assegnare in una volta a tutti i computer della rete e all'apparecchiatura stessa indirizzi IP.
- Esiste già una rete con TCP/IP, ma senza server DHCP e si vuole passare alla modalità DHCP.

### Configurazione con *ELSA LANconfig* e l'assistenza

In entrambe le situazioni *ELSA LANconfig* fornisce la sua assistenza per effettuare le necessarie impostazioni:

- ① Connettere per mezzo del cavo di rete l'apparecchio non configurato alla rete locale. In questo caso, se si collega l'apparecchio ad un hub, il commutatore node/hub deve trovarsi in posizione 'Node'. Se invece si collega il router direttamente alla scheda di rete di un computer della rete, il commutatore node/hub si deve trovare in posizione 'Hub'.
- ② Accendere l'apparecchio. Il non trova nessun altro server DHCP in rete e attiva le proprie funzioni DHCP.
- ③ Se questo non è stato già fatto, installare il protocollo 'TCP/IP' su tutti i computer della rete locale.
  - Durante l'installazione del protocollo i computer generalmente sono impostati in modo tale da richiedere automaticamente l'indirizzo IP a un server DHCP. Dopo il riavvio, che è collegato con questa installazione, i computer richiedono automaticamente un indirizzo IP al server DHCP.
  - Se il protocollo è stato già installato, attivare la funzione DHCP su tutti i computer della rete locale. A questo scopo per es. sotto Windows 95 con **Avvio ► Impostazioni ► Pannello di controllo ► Rete** aprire la finestra di configurazione delle proprietà di rete. Fare doppio clic sulla voce per il protocollo 'TCP/IP'. Attivare l'opzione 'Ottieni un indirizzo da un server DHCP'. Passare alla scheda registro 'DNS', e cancellare tutti gli indirizzi DNS presenti. Poi cancellare sulla scheda registro 'Gateway' tutte le voci eventualmente presenti e chiudere tutte le finestre con **OK**. Dopo il riavvio, che è collegato con questa impostazione, i computer richiedono automaticamente un indirizzo IP del pool di indirizzi del server DHCP.



- ④ Installare *ELSA LANconfig* su uno dei computer della rete.
- ⑤ Avviare il programma dal gruppo di programmi 'ELSAAn'. Durante l'avvio *ELSA LANconfig* rileva che un router non configurato si trova in rete, e avvia l'assistenza per le impostazioni fondamentali.
  - Se finora nella rete non è stato ancora utilizzato alcun indirizzo IP, scegliere allora in questo assistente l'opzione 'Tutto impostato automaticamente' e cliccare nella finestra successiva il pulsante **Fine**.

L'assistenza assegna al router l'indirizzo IP '10.0.0.1' con maschera di rete '255.255.255.0' e attiva il server DHCP. Dall'indirizzo IP l'apparecchio determina il pool di indirizzi valido per l'assegnazione DHCP.
  - Se prima della conversione alla modalità DHCP nella rete sono stati utilizzati indirizzi IP, selezionare in questa assistenza l'opzione 'Desidero impostare tutto manualmente'. Introdurre nella finestra seguente un indirizzo IP libero del gruppo di indirizzi finora utilizzato, e attivare il server DHCP.

L'assistenza assegna al apparecchio l'indirizzo IP introdotto con la

rispettiva maschera di rete. Dall'indirizzo IP il apparecchio determina il pool di indirizzi valido per l'assegnazione DHCP.

- Dopo alcuni secondi tutti i computer della rete vengono automaticamente controllati ed eventualmente ricevono un nuovo indirizzo IP dal server DHCP. Inoltre vengono comunicati a tutti i computer anche gli altri parametri come indirizzo broadcast, server DNS, gateway di default ecc.

### Configurazione manuale

Se non si vuole eseguire la configurazione con l'assistenza di *ELSA LANconfig*, i parametri per il server DHCP possono anche essere impostati a mano: in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'DHCP' oppure nel menu `/Setup/DHCP-module`.

## 4.6

## DNS

Il Domain Name Service (DNS) nelle reti TCP/IP crea il collegamento tra nomi di computer oppure nomi di rete (domini) e indirizzi IP. In ogni caso questo Service è necessario per la comunicazione in Internet, per es. per poter rispondere a una richiesta secondo 'www.elsa.com' con il corrispondente indirizzo IP. Ma anche nell'ambito di una rete locale o di un accoppiamento LAN ha senso poter assegnare in modo univoco gli indirizzi IP della LAN ai nomi dei computer.

### 4.6.1

### Che cosa fa un server DNS?

I nomi richiesti a un server DNS sono costituiti da più parti: una parte è costituita dal nome vero e proprio del computer o servizio che deve essere chiamato, un'altra parte caratterizza il dominio. Nell'ambito di una rete locale l'indicazione del dominio è opzionale. Esempi di questi nomi possono essere 'www.domain.com' o 'ftp.domain.com'.

In assenza di server DNS nella rete locale ogni nome localmente sconosciuto viene ricercato tramite la rotta di DEFAULT. Utilizzando un server DNS, tutti i nomi che sono noti con i loro indirizzi IP possono essere cercati direttamente presso la corretta controparte. In linea di principio il server DNS può essere un computer separato della rete. Tuttavia i seguenti motivi sono a favore del trasferimento del server DNS direttamente nel *ELSA LANCOM Office*:

- Un *ELSA LANCOM Office* in modalità server DHCP può distribuire autonomamente gli indirizzi IP ai computer della rete locale. Il server

DHCP conosce già tutti i computer della propria rete, che ricevono i loro indirizzi IP tramite DHCP, con nome del computer e indirizzo IP. Un server DNS esterno in caso di assegnazione dinamica dell'indirizzo del server DHCP, potrebbe avere delle difficoltà a tenere aggiornata l'assegnazione tra indirizzo IP e nome.

- Con il routing delle reti Windows tramite NetBIOS un *ELSA LANCOM Office* inoltre conosce i nomi dei computer e gli indirizzi IP delle altre reti NetBIOS collegate. Eventualmente si registrano inoltre nella tabella NetBIOS anche i computer con indirizzo IP impostato in modo fisso ed essi sono in tal modo noti con nomi e indirizzi.
- Il server DNS nel *ELSA LANCOM Office* può essere utilizzato contemporaneamente come comodissimo meccanismo di filtro. Le richieste per determinati domini che non devono essere visitati, possono essere bloccate indicando semplicemente il nome del dominio per intere LAN, solo per reti parziali (sottoreti) o addirittura per singoli computer.

Nelle richieste per determinati nomi, il server DNS include tutte le informazioni a sua disposizione:

- Il server DNS controlla prima se l'accesso a tale nome non è vietato dalla lista di filtro. In questo caso, il computer richiedente viene informato per mezzo di un messaggio di errore del fatto che non ha diritto di accedere a tale nome.
- Poi cerca nella propria tabella DNS statica le voci per il nome corrispondente.
- Se nella tabella DNS non esiste alcuna voce per tale nome, viene effettuata la ricerca nella tabella DHCP dinamica. Se necessario, l'impiego delle informazioni DHCP può essere disattivato.
- Se il server DNS non trova informazioni sui nomi nelle suddette tabelle, viene effettuata la ricerca nelle liste del modulo NetBIOS. Se necessario, anche l'impiego delle informazioni NetBIOS può essere disattivato.

Se il nome ricercato non viene trovato in tutte le informazioni disponibili, il server DNS trasferisce la richiesta tramite il normale meccanismo di forwarding DNS a un altro server DNS (per es. del provider Internet) o invia al computer richiedente un messaggio di errore.

## 4.6.2

## Come si imposta il server DNS

Le impostazioni per il server DNS si trovano in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'DNS'. Procedere all'impostazione del server DNS nel modo seguente:

- ① Attivare il server DNS.

```
set setup/DNS-module/operating on
```

- ② Introdurre il dominio in cui si trova il server DNS. Con l'ausilio di questo dominio il server DNS riconosce su richiesta se il nome ricercato si trova o meno nella propria LAN. L'indicazione del dominio è opzionale.

```
set setup/DNS-module/domain yourdomain.com
```

- ③ Indicare se devono essere utilizzate le informazioni fornite dal server DHCP e dal modulo NetBIOS.

```
set setup/DNS-module/dhcp-usage yes
```

```
set setup/DNS-module/NetBIOS-usage YES
```

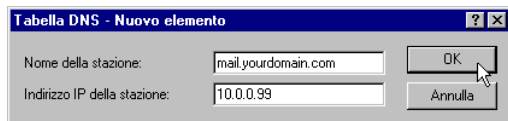


- ④ Il principale compito del server DNS è quello di separare le richieste per nomi in Internet dalle richieste per nomi in altre controparti. Pertanto introdurre nella tabella DNS tutti i computer



- i cui nomi e indirizzi IP si sa che,
- non appartengono alla propria LAN,
- non si trovano in Internet,
- possono essere raggiunti attraverso il router.

Per es. se ci si trova in un ufficio esterno e si vuole raggiungere attraverso il router il mail server della centrale (Nome: mail.yourdomain.com, IP: 10.0.0.99), introdurre:



```
cd setup/DNS-module/DNS-table
```

```
set mail.yourdomain.com 10.0.0.99
```

In questo caso l'indicazione del dominio è opzionale, ma raccomandabile.

Avviando il programma di posta, probabilmente questo ricercherà automaticamente il server 'mail.yourdomain.com'. Il server DNS restituisce l'indirizzo IP '10.0.0.99'. Poi il programma di posta cercherà questo indirizzo IP. Con corrispondenti voci nella tabella di routing IP e nella lista dei nomi ecc. viene automaticamente stabilita la connessione con la rete della centrale, dove finalmente viene trovato il mail server.

- ⑤ Con la lista di filtro si può definire con esattezza chi non ha diritto di accedere a determinati nomi o domini.



```
cd setup/DNS-module/Filter-list
```

```
set 001 www.offlimits-domain.com 0.0.0.0 0.0.0.0
```

Con questa voce (con indice '001') si blocca questo dominio per tutti i computer della rete locale. L'indice '001' è scelto liberamente e serve soltanto per facilitare la lettura. Per l'introduzione del dominio sono anche consentite le wildcard '?' (rappresenta un carattere qualunque) e '\*' (rappresenta un numero qualunque di caratteri). Per es. se solo un

determinato computer (IP 10.0.0.123) non deve accedere ai domini con ,  
introdurre:

```
set 002 *.com 10.0.0.123 255.255.255.255
```

*La hit list delle statistiche DNS riporta i64 nomi più frequentemente richiesti, e rappresenta una buona base per l'impostazione della lista di filtro.*

Con un'opportuna scelta di indirizzi IP e di maschere di rete si possono anche filtrare singoli reparti, se nella propria LAN è impiegato il subnetting. L'indirizzo IP '0.0.0.0' rappresenta sempre tutti i computer di una rete, la maschera di rete '0.0.0.0' tutte le reti.

## 4.7

### NetBIOS proxy

Funzionando come NetBIOS proxy un *ELSA LANCOM Office* può anche instradare pacchetti NetBIOS o rispondere come proxy in modo locale. In questo modo si realizza tra l'altro la possibilità di collegare a costo conveniente reti Windows tramite le funzioni router.

*Questa funzione è disponibile solo con i modelli ELSA LANCOM 2000 Office, ELSA LANCOM 1100 Office e ELSA LANCOM 1000 Office.*

Questa sezione descrive il funzionamento di NetBIOS proxy in generale e la configurazione del router e dei computer partecipanti per la connessione tramite reti Windows.

### 4.7.1

#### In breve: Che cosa è il NetBIOS?

Il NetBIOS serve a connettere in rete più computer in modo semplice e senza complicazioni. Un importante caso di rete NetBIOS è la rete Windows, con cui si possono facilmente connettere in rete diversi computer Windows 3.11, 9x e NT, e in cui le risorse dei diversi computer (unità disco o stampanti) possono essere rese disponibili per tutti gli altri.

In una rete Windows i computer vengono chiamati soltanto tramite i loro nomi. Più computer possono essere riuniti in gruppi e più gruppi in gruppi di nomi (scopes). Affinché un computer possa accedere alle risorse degli altri, i nomi utilizzati devono essere conosciuti in tutta la rete. Affinché non sia necessario mantenere in ciascun computer una tabella dei nomi conosciuti, i computer NetBIOS notificano autonomamente in rete i propri nomi a intervalli regolari.

Naturalmente i nomi così notificati devono anche essere raccolti e tenuti pronti in un punto centrale della rete Windows. Se si devono accoppiare tra loro due reti Windows tramite router, su entrambi i lati della connessione deve essere presente un siffatto punto di raccolta dei nomi, un nameserver NetBIOS (NBNS).

- A questo scopo si può per es. installare nella rete un proprio server WINS (Windows Internet Name Service Server).
- Poiché però molte reti Windows vogliono o devono operare senza un proprio server, si presenta una seconda possibilità: Le informazioni sui nomi utilizzati possono anche essere raccolte su una specie di « tabellone », su cui tutti i computer lasciano solo il loro nomi e i loro indirizzi IP. In questo caso gli stessi computer sono responsabili per la corrispondenza dei loro nomi nella rete.

Un *ELSA LANCOM Office* è dotato di un siffatto tabellone. Attraverso questa semplice realizzazione del NBNS diventa possibile la connessione delle reti Windows anche senza server. I computer delle reti che intendono connettersi notificano i propri nomi anche in un'altra rete e completano il tabellone anche in questa.

## 4.7.2

### Trattamento dei pacchetti NetBIOS

Il comportamento molto loquace dei computer Windows, può causare nei collegamenti telefonici elevati costi poiché ogni pacchetto NetBIOS con informazioni sui nomi conduce automaticamente alla messa in opera del collegamento (ad esempio se gli ISP sono già impostati). Con siffatti pacchetti la linea rimane continuamente occupata e gli addebiti sono corrispondentemente alti, senza che si abbia una trasmissione di dati effettivamente utili.

Per evitare un siffatto stabilimento della connessione non necessario, un *ELSA LANCOM Office* può instradare i pacchetti NetBIOS o rispondere direttamente ad essi come proxy:

- Per effettuare il routing dei pacchetti effettivamente necessari, nel modulo NetBIOS si possono definire le controparti a cui devono essere trasmesse le informazioni sui nomi tramite NetBIOS. Quando si attiva il modulo NetBIOS, dopo un determinato tempo di attesa viene stabilita una connessione con le controparti NetBIOS (se non si tratta di singoli computer con accesso remoto). Se la connessione non ha successo, il tempo di attesa viene prolungato. Con il successivo scambio di informazioni NetBIOS, il tabellone viene completato per la prima volta.

- Funzionando come proxy, l'apparecchio risponde autonomamente alle richieste dirette ai computer che sono già conosciuti nel modulo NetBIOS (sul tabellone nero), come rappresentante del corrispondente computer. Quindi, sia per le richieste per computer della propria LAN che per quelle per computer conosciuti della rete della controparte, dopo il primo scambio di informazioni, non vengono stabilite nuove connessioni.

Affinché le richieste per computer che non si trovano nella propria LAN e neanche nelle controparti NetBIOS stabilite, non causino lo stabilimento della connessione tramite la rotta di DEFAULT di Internet, il filtro IP preimpostato per le porte NetBIOS cattura questi pacchetti ed evita che la connessione venga stabilita.

## 4.7.3

### Quali sono i presupposti indispensabili?

Per una corretta comunicazione tra reti Windows tramite router, sui computer partecipanti devono essere installati alcuni componenti e devono essere effettuate diverse impostazioni nel sistema operativo.

#### Componenti installati

L'installazione dei componenti necessari viene descritta sull'esempio di Windows 95 oppure Windows 98, in ambiente Windows NT 4.0 si esegue in modo analogo. Installare i seguenti componenti su tutti i computer delle reti Windows da connettere:

- Protocollo di rete

NetBIOS è completamente indipendente dal protocollo di trasporto utilizzato. Pertanto una rete NetBIOS può essere trasmessa tramite i protocolli NetBEUI (NetBIOS Extended User Interface), IPX (Internet Packet eXchange, Novell) o IP (Internet Protocol).



*A differenza di IPX e IP, una NetBEUI non consente il routing, e quindi è utilizzabile solo in una rete Windows. Se si devono connettere più reti Windows tramite router, NetBIOS deve essere basato su un protocollo che consenta il routing, per es. nel ELSA LANCOM Office su IP!*

Il routing dei pacchetti NetBIOS nel *ELSA LANCOM Office*, in conseguenza dei migliori meccanismi di filtro, si basa su TCP/IP. Quindi questo protocollo deve essere installato su tutti i computer che devono essere accoppiati.

Per installare il protocollo di rete, cliccare su **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► Aggiungi ► Protocollo.**

Selezionare come produttore 'Microsoft' e come protocollo di rete 'TCP/IP'.

- Client

Il client per reti Windows è necessario affinché i computer possano registrare il nome e la password nella rete Windows.

Per installare il client, cliccare su **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► Aggiungi ► Client**. Selezionare come produttore 'Microsoft' e poi il 'Client per reti Windows'.

- Servizi

L'abilitazione di file e stampanti consente di abilitare unità disco o stampanti per altri utenti della rete Windows.

Per installare l'abilitazione di file e stampanti, cliccare su **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► Aggiungi ► Servizi**. Selezionare come produttore 'Microsoft' e poi la 'Condivisione file e stampanti per reti Microsoft'.

### Impostazioni nella rete Windows

- Definizione di nomi e gruppi

Cliccare su **Avvio ► Impostazioni ► Pannello di controllo ► Rete** e passare alla scheda di registro **Identificazione**.



Il nome del computer deve essere univoco. Questo vale per tutte le reti Windows e per tutti i gruppi presenti in tali reti che devono essere connessi tramite NetBIOS. Anche in gruppi diversi lo stesso nome non deve comparire più volte lo stesso nome.

- **Abilitazione di file e stampanti**

Dopo l'installazione, controllare se è attivata l'abilitazione di file e stampanti. Cliccare a tale scopo **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► Condivisione di file e stampanti**. Selezionare se gli altri utenti della rete Windows possono usare la stampante e/o i file di questo computer.



Tutti gli utenti che vogliono accedere alle risorse abilitate devono registrarsi in Avvio di Windows con nome e password.

Poi in Explorer cliccare con il tasto destro del mouse sulle unità disco, cartelle stampanti che si vogliono abilitare per l'impiego da parte di altri partecipanti alla rete, e selezionare il punto **Condivisione** nel menu di contesto.



Assegnare un nome alla cartella abilitata ed eventualmente introdurre un commento. Con la selezione del Tipo di accesso e la definizione degli Identificativi si stabilisce come deve avvenire l'accesso alle risorse abilitate.



*Si può controllare facilmente se le impostazioni nella rete Windows sono corrette: Il proprio computer deve essere visualizzato nell'ambiente di rete con il rispettivo nome.*

## 4.7.4

## Come si connettono due reti Windows

Quando sono completate tutte le operazioni preliminari, si possono connettere due reti Windows. Le impostazioni per le reti gruppi di lavoro e le reti di dominio (Windows NT) sono analoghe. I seguenti passi devono essere effettuati per entrambi i lati della connessione.

- ① Impostare le due reti per un accoppiamento LAN-LAN tramite TCP/IP, come descritto nel workshop. A questo scopo utilizzare secondo possibilità la comoda assistenza di *ELSA LANconfig*.
- ② Controllare l'impostazione dei filtri IP. Questo filtro deve includere tutti i pacchetti NetBIOS che devono essere inviati tramite la rotta di DEFAULT, in modo che i pacchetti NetBIOS non causino lo stabilimento della connessione tramite la rotta di DEFAULT. Nello stato di fornitura degli apparecchi il filtro è impostato in questo modo:

| Filtro per le reti remote |              |            |             |                 |         |            |          |
|---------------------------|--------------|------------|-------------|-----------------|---------|------------|----------|
| Prima Dest.               | Ultima Dest. | Prima Src. | Ultima Src. | Indirizzo IP    | Netmask | Protocollo | Tipo     |
| 0                         | 0            | 137        | 139         | 255.255.255.255 | 0.0.0.0 | Tutti      | Percorso |

- ③ Poi introdurre la controparte per il routing tramite NetBIOS. Passare in *ELSA LANconfig* nel campo di configurazione 'NetBIOS' e creare una nuova voce nella tabella 'NetBIOS su instradamento IP'.

| NetBIOS sulla tabella di instradamento IP |                  |          |  |
|-------------------------------------------|------------------|----------|--|
| Stazione corrispondente                   | Tipo             |          |  |
| NHAMEL_MOBIL                              | Router           |          |  |
| NHAMEL_RAS                                | Stazione singola |          |  |
|                                           |                  | OK       |  |
|                                           |                  | Annulla  |  |
|                                           |                  | Aggiungi |  |

In caso di configurazione tramite Telnet in alternativa introdurre:

```
cd /Setup/NetBIOS-module/Remote-table
set nhamel.mobil router
```

La voce nel campo 'Tipo' indica se la controparte deve essere selezionata direttamente dopo l'attivazione del modulo NetBIOS, per scambiare le informazioni sui nomi.

*Il parametro 'NT-domain' di regola può essere lasciato vuoto nelle reti Windows 95 o Windows 98. Nell'accesso a computer Windows NT, è necessario registrare il corrispondente dominio o gruppo di lavoro a mano.*





- ④ Se l'accoppiamento NetBIOS utilizza una connessione PPP, si deve controllare nella lista PPP l'attivazione di NetBIOS per la voce corrispondente.
- ⑤ Quando tutte le controparti sono state introdotte, attivare la funzione NetBIOS.

```
cd /Setup/NetBIOS-module
```

```
set operating on
```

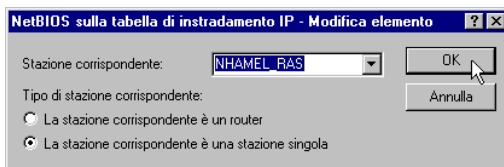
Dopo l'attivazione (dopo un certo tempo di attesa) viene stabilita una connessione con tutte le controparti che non sono contrassegnate come nodi di selezione. Durante questa prima connessione vengono scambiate le necessarie informazioni sui computer delle reti. Soltanto dopo di ciò è possibile accedere ai computer della controparte.

## 4.7.5

### Come si seleziona un computer con accesso remoto

L'accesso a singoli computer remoti tramite accesso remoto su una rete Windows si realizza altrettanto rapidamente.

- ① Il *ELSA LANCOM Office* e il computer con accesso remoto vengono preparati per l'accesso da rete come descritto nel workshop. Anche in questo caso si devono controllare i filtri IP in *ELSA LANCOM Office* (vedere 'Come si connettono due reti Windows').
- ② Se l'assegnazione degli indirizzi IP per la controparte remota viene effettuata dal pool IP, per tale controparte si deve creare una rotta aggiuntiva nella tabella di routing IP.
- ③ Creare anche per le controparti remote una voce nella tabella di routing IP NetBIOS.



```
cd /Setup/NetBIOS-module/Remote-table
```

```
set nhamel.ras workstation
```



*Contrassegnare questa voce come 'Stazione singola', in modo che questa controparte non venga chiamata automaticamente dopo l'attivazione del modulo NetBIOS.*

- ④ Se l'accoppiamento NetBIOS utilizza una connessione PPP, si deve controllare nella lista PPP l'attivazione di NetBIOS per la voce corrispondente.

## 4.7.6

### Cercato – Trovato: L'ambiente di rete

Quando tutti i partecipanti al routing NetBIOS sono preparati, si può partire con il networking Windows.

#### Routing NetBIOS tramite accoppiamento LAN-LAN

Una volta che le reti, dopo che i moduli NetBIOS sono stati attivati, si sono scambiate reciprocamente le informazioni sui computer disponibili, nel *ELSA LANCOM Office* è disponibile una lista con tali nomi di computer. Tramite Telnet con

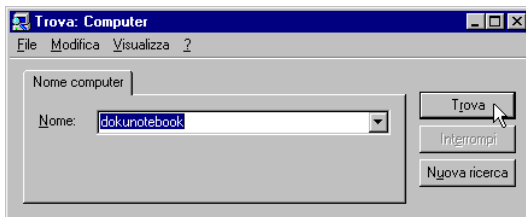
```
dir /Setup/NetBIOS-module/Host-list
```

si può richiamare la lista con i computer raggiungibili attualmente, che per es. si presenta così:

| Nome         | Type | Indirizzo IP        | Sito remoto  | Timeout | Flags |
|--------------|------|---------------------|--------------|---------|-------|
| DOKUNOTEBOOK | 00   | 10.10.0.53          | NHAMEL.MOBIL | 4939    | 0020  |
| DOKUNOTEBOOK | 20   | 10.10.0.53          | NHAMEL.MOBIL | 4939    | 0020  |
| ELSA         | 1d   | 10.10.0.53          | NHAMEL.MOBIL | 4939    | 0020  |
| ELSA.DOKU    | 1d   | 10.1.253.246        | 4935         | 0000    |       |
| ELSA.DOKU    | 1d   | 192.168.100.1<br>62 | 4997         | 0000    |       |
| NHAMEL.MOBIL | 00   | 10.10.0.1           | NHAMEL.MOBIL | 0       | 0020  |

Da questa tabella si può leggere che per es. il computer con nome 'DOKUNOTEBOOK' può essere raggiunto con l'indirizzo IP '10.10.0.53' tramite la controparte 'NHAMEL.MOBIL'. Gli altri parametri vengono spiegati nella descrizione del menu.

Per poter accedere alle risorse abilitate di questo computer, lasciare semplicemente che Explorer cerchi il corrispondente computer con **Avvio ► Trova ► Computer**:



*Per motivi tecnici, in ambiente di rete Windows i gruppi di lavoro e i computer della rete remota non possono essere trovati usando la funzione 'Sfoglia tutta la rete'. Invece i computer remoti possono essere cercati come descritto in precedenza, oppure si stabiliscono nodi e connessioni di unità disco.*

### Routing NetBIOS tramite accesso RAS

In caso di accesso alla rete Windows tramite RAS la procedura risulta leggermente diversa. Le due differenze fondamentali rispetto all'accoppiamento LAN-LAN:

- Dal lato del nodo di chiamata, non è presente una lista di host dalla quale i computer disponibili nella rete di Windows possano essere letti nella controparte. Quindi l'utente RAS deve conoscere i nomi dei computer a cui può e vuole accedere.
- La connessione non viene stabilita automaticamente. Quindi l'utente RAS deve prima stabilire una connessione tramite Accesso remoto con il *ELSA LANCOM Office*.

Quando la connessione è stabilita, si può procedere esattamente come per l'accoppiamento LAN-LAN (tramite **Trova ► Computer**, ma non tramite l'ambiente di rete!) per cercare e accedere ai computer dell'altra rete.

## 4.8

### Il least-cost router

Da quando c'è stata la liberalizzazione del mercato telefonico in Europa gli utenti di servizi di comunicazione possono disporre di una serie di provider (gestori di rete), attualmente caratterizzati da tariffe molto differenziate. Inoltre i provider si distinguono anche se sono collegati in modo fisso e se utilizzano automaticamente sempre la loro rete (preselezione), oppure ad ogni chiamata si decide liberamente quale provider si vuole utilizzare (call-by-call). Per stabilire una connessione tramite un provider call-by-call, dopo aver sollevato la cornetta si compone prima l'opportuno prefisso, per entrare nella

corrispondente rete. Solo dopo questa cifra identificativa di rete si seleziona il normale numero telefonico per raggiungere la propria controparte.

Per le telefonate in determinate ore del giorno e in diverse regioni, purtroppo la tariffa più conveniente non è sempre offerta dallo stesso provider, anzi abbastanza spesso si ottiene da fornitori diversi: al mattino il provider 1, al pomeriggio il provider 2 e per le conversazioni internazionali event. il provider 3. Per telefonare in modo sempre più conveniente, navigare in Internet o trasmettere dati ad altre reti, si dovrebbe effettivamente riflettere prima di ogni connessione su quale tariffa è la più conveniente al momento. Un *ELSA LANCOM Office* evita questa fatica. La funzione che opera in questo caso viene definita *least-cost-routing* LCR. Si definisce prima il provider che offre le tariffe più convenienti per le proprie necessità, e l'apparecchio seleziona automaticamente per ogni connessione (indifferentemente se via router, *LANCAPI* ecc.) il servizio con la tariffa più conveniente.

## 4.8.1 Il least-cost-router di **ELSA LANCOM** opera in questo modo

Il LCR analizza le cifre selezionate per es. dal router o dalla *LANCAPI*. Con *ELSA LANCOM 2000 Office* vengono considerate anche le cifre per la selezione di un apparecchio collegato (per es. telefono o fax).

Dopo ciascuna cifra l'apparecchio controlla se nella 'Tabella del costo minimo...' si trova una coincidenza univoca con il numero già selezionato (prefisso). Se viene trovata una registrazione appropriata, valida per l'ora e la data attuale, viene inserita prima del prefisso la cifra identificativa di rete per lo smistamento della connessione. Solo dopo che il numero d'utenza è stato completato in questo modo, viene trasferito verso l'esterno al centralino.

Quindi il LCR ha bisogno dei seguenti dati:

- Un prefisso, che determina quali numeri devono essere selezionati per uno smistamento.
- Uno o o più numeri identificativi di rete che definiscono il provider che deve essere utilizzato per tale prefisso.
- I giorni feriali e i giorni festivi, per cui la registrazione è valida.
- L'ora del giorno, per cui la registrazione è valida.

### Primi tentativi

Con poche registrazioni si può già risparmiare molto sugli addebiti. La programmazione del LCR verrà spiegata in base a un semplice esempio.

Per es. è ben noto che specialmente nelle conversazioni interurbane o nelle chiamate internazionali si può risparmiare con la procedura call-by-call. Lo stesso vale per le conversazioni con telefoni mobili. Inoltre, attraverso un'indagine presso alcuni fornitori call-by-call (CbC), sono state individuate le tariffe di volta in volta più convenienti. Per es. le prime registrazioni nella tabella LCR si presentano così:

| Prefisso | Inoltra a | Giorni feriali         | Ora del giorno      |
|----------|-----------|------------------------|---------------------|
| 02       | 1055      | Sa + Do                | 0:00h fino a 23:59h |
| 02       | 1088      | Lu + Ma + Me + Gi + Ve | 8:00h fino a 18:00h |
| 0172     | 01099     | tutti i giorni         | 0:00h fino a 23:59h |
| 00       | 1055      | Do                     | 0:00h fino a 23:59h |

Queste 4 registrazioni significano che tutte le connessioni durante il fine settimana con Milano (o altri numeri che cominciano con '02'), devono essere effettuate con il provider con numero identificativo di rete '1055'. Nei giorni feriali si usa per tali chiamate nelle ore tra le 8:00 e le 18:00 il provider con numero identificativo di rete '1088'. Le chiamate a telefono mobile in rete D-2 vengono effettuate sempre con il provider con numero identificativo di rete '01099'. Le conversazioni internazionali di Domenica avvengono tramite il provider con numero identificativo di rete '1055'.

### Per esperti: LCR con sistema

- Nel primo esempio si è visto che già con poche registrazioni è possibile risparmiare sugli addebiti. Se si desidera utilizzare il least-cost router in modo ottimale, è necessario informarsi prima esattamente sulla struttura tariffaria dei fornitori call-by-call che possono essere presi in considerazione. Poi si deve riflettere su come le tariffe e le zone tariffarie possono essere descritte nel modo migliore nella tabella LCR del *ELSA LANCOM Office*. A questo scopo ci sono diverse regole:
- Le possibilità di risparmio univoche possono essere introdotte direttamente:
  - Prefissi di selezione '0177', '0171', '0172' per reti a telefono mobile

- '00' per le chiamate internazionali
- Con un unico '0' vengono smistate prima tutte le connessioni che cominciano con lo zero. Poiché però esistono reti urbane contigue il cui numero comincia con '0' ma che tuttavia vengono addebitate come conversazione urbana, si dovrebbe comporre separatamente questi prefissi annullare lo smistamento. Con questa strategia si considerino anche i numeri speciali come '0800', '0190' ecc.
- Una strategia diversa punta a una regolamentazione per quanto possibile completa degli smistamenti. Si comincia con i prefissi locali e poi si definiscono le zone più grandi. Le zone tariffarie più vicine e quindi più economiche vengono definite con il prefisso più lungo, le rimanenti zone tariffarie più distanti vengono definite con poche cifre.

Naturalmente questa impostazione può essere affinata e sviluppata se necessario. Alcuni suggerimenti che si potrebbero seguire in proposito:

- Alcune reti urbane possono essere raggiunte attraverso un prefisso, ma con la normale tariffa urbana. Se queste zone sono state smistate per mezzo di una registrazione generale, si può smistare il prefisso con tariffa urbana con il prefisso della società telefonica. Una registrazione vuota per il numero identificativo di rete significa anche « nessuno smistamento ».
- E' possibile che la maggior parte delle connessioni ISDN sia diretta verso le stesse reti urbane. Se la maggior parte delle proprie controparti si trova a Milano, tali controparti possono essere raggiunte tramite un determinato fornitore.
- Esaminare le diverse zone tariffarie. I prefissi per le diverse zone possono essere visualizzati per es. in [www.risparmio-telefonico.it](http://www.risparmio-telefonico.it) in Internet.

Una volta trovati i prefissi che da smistare, si può passare all'assegnazione del provider call-by-call. A questo scopo naturalmente ci vogliono le tariffe aggiornate di tutte le possibili società telefoniche. Anche in questo caso Internet può aiutare. Con queste informazioni si può passare ad alimentare il least-cost router ...

### **Il least-cost router si imposta così**

Per impostare il least-cost router si deve rispondere essenzialmente a due domande:

- Quali modalità del *ELSA LANCOM Office* devono utilizzare i servizi del least-cost router?

- Quali chiamate devono essere effettuate attraverso quale provider?

Per rispondere a queste domande, procedere nel modo seguente:

- ① Passare nel *ELSA LANconfig* nel campo di configurazione 'Least-cost router' sulla scheda di registro 'Generale'.
- ② Attivare la funzione del least-cost router. Il least-cost router può essere attivato solo se l'ora dell'apparecchio è stata impostata manualmente o è stata comunicata una volta un'ora valida dalla rete ISDN (vedere anche 'L'ora per la selezione' nel seguito). Attivare il LCR secondo necessità per le seguenti modalità:
  - ☐ Router
  - ☐ Porte a/b (solo *ELSA LANCOM 2000 Office*)
  - ☐ LANCAPI



*Se è stato attivato il least-cost routing anche per i moduli router, possono essere stabilite anche connessioni tramite provider che non trasmettono informazioni di addebito! In questo modo il monitoraggio addebiti fallisce senza segnalazioni. In questo caso utilizzare in alternativa il budget di tempo.*

- ③ Passare alla scheda di registro 'Orari e festività nazionali'. Aprire la **Tabella del costo minimo...**, inserire una nuova voce, e introdurre i dati necessari:
  - ☐ Quale prefisso deve essere smistato?
  - ☐ Su quale provider deve essere smistato questo prefisso? Se si introducono più numeri identificativi di rete separati da punto e virgola, il LCR passa automaticamente al prefisso successivo, se quello precedente è occupato.
  - ☐ In quali giorni e a quali ore deve essere attivo lo smistamento? Tenere presente che non sono possibili ore che superano la giornata (18:00 fino alle 6:00)!
  - ☐ La chiamata deve essere effettuata attraverso la normale società telefonica, se tutte le linee call-by-call sono occupate? Se è disattivata la 'fallback automatico...', eventualmente il LCR dopo l'ultimo numero identificativo di rete ricomincia con il primo ...

**Tabella del costo minimo - Nuovo elemento**

Inoltra questo prefisso:

Verso numero Call-by-Call:

☒ Lunedì ☒ Martedì  
☒ Mercoledì ☒ Giovedì  
☒ Venerdì ☐ Sabato  
☐ Domeniche ☐ Festività nazionali

Ora d'inizio:

Ora di chiusura:

☒ fallback automatico se non può essere stabilito alcun collegamento con i numeri Call-by-Call stabiliti

- ④ Se nella tabella LCR sono state inserite anche registrazioni per i giorni festivi, aprire la lista dei **Festività nazionale**. Introdurre ciascun giorno festivo con la data completa (GG.MM.AAAA).
- ⑤ Controllare l'orologio interno dell'apparecchio (incl. la data), in modo che il LCR possa attivare anche gli smistamenti all'ora giusta (vedere anche nel seguito, 'L'ora per la selezione').



*Costruire la tabella LCR per passi, e controllare ogni volta il risultato. A questo scopo aprire per es. ELSA LANmonitor e avviare attraverso ELSA LANCAPI connessioni verso controparti che dovrebbero essere smistate in base alla tabella. In base al numero d'utenza selezionato si può facilmente vedere se l'impostazione del LCR corrisponde a quella desiderata. Per le connessioni router si può leggere il numero selezionato dal logfile (LANmonitor: **Visualizza ► Opzioni ► Registrazione ► Visualizza**).*

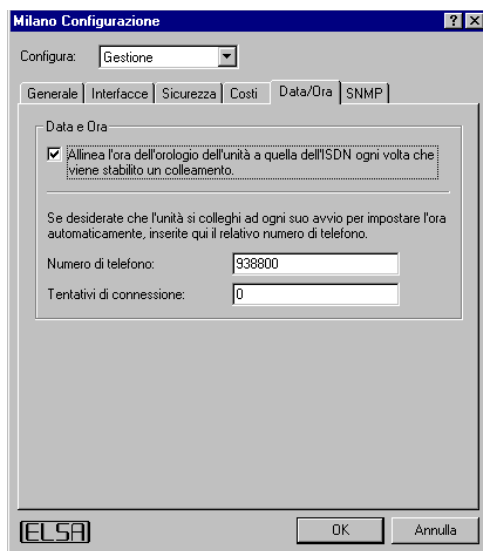
### L'ora per la selezione

Affinché il least-cost router con l'ausilio delle voci della tabella possa effettivamente effettuare le connessione corretta, naturalmente l'orologio interno del *ELSA LANCOM Office* deve essere sempre aggiornato. Anche lo stesso router può essere d'aiuto: Ogni volta che si stabilisce una connessione o si attiva l'apparecchio si può confrontare l'orologio interno con l'ora della rete ISDN.

- ① Passare nel *ELSA LANconfig* nel campo di configurazione 'Gestione' sulla scheda di registro 'Data/Ora'.
- ② Attivare eventualmente l'opzione per la regolazione automatica dell'ora a ogni connessione. Se si preferisce impostare l'ora manualmente, disattivare questa opzione.



- ③ Quando si disattiva l'apparecchio perde l'ora attuale. Introdurre il numero d'utenza di una qualunque controparte se il apparecchio deve stabilire una connessione subito dopo l'avvio e regolare l'ora con la rete ISDN. Selezionare se si tratta di una controparte digitale (per es. mailbox o provider Internet) o di una controparte analogica (annuncio telefonico o servizio viva voce).



*Controllare l'ora dopo la prima trasmissione. Alcuni impianti interni trasmettono al router per es. ore sbagliate che influiscono sul corretto funzionamento del least-cost router!*

## 4.9

### **ELSA CAPI Faxmodem**

Con *ELSA CAPI Faxmodem* è disponibile in ambiente Windows un driver fax (Standard 1), che come interfaccia tra *ELSA LANCAPI* e l'applicazione consente l'impiego di programmi di fax standard con un *ELSA LANCOM Office*.

### 4.9.1

#### **Installazione**

Il *ELSA CAPI Faxmodem* viene presentato per l'installazione tramite il CD-setup. Installare il *ELSA CAPI Faxmodem* sempre insieme con la *ELSA*

*LANCAPI* attuale. Dopo il riavvio, il *ELSA CAPI Faxmodem* è disponibile nel sistema, per es. in ambiente Windows 95 o Windows 98 tramite **Avvio ► Pannello di controllo ► Modem**.

## 4.9.2

### Invio di fax tramite *ELSA CAPI Faxmodem*

Il *ELSA CAPI Faxmodem* viene automaticamente riconosciuto durante l'installazione dai più comuni programmi di fax e identificato come faxmodem 'Class 1'. Con esso è possibile la trasmissione di fax fino a un massimo di 14.400 bps. Se il programma di fax consente una scelta (per es. WinFax oppure Talkworks Pro), selezionare durante la configurazione del modem l'opzione 'CLASS 1 (Software Flow Control)'.



*Il ELSA CAPI Faxmodem è pronto per la trasmissione di messaggi fax solo se la ELSA LANCAPi è attiva. Questo si riconosce per es. dal piccolo simbolo CAPI nell'angolo dello schermo in basso a destra. Fare anche attenzione alle impostazioni della LANCAPi stessa.*

## 4.10

### Comunicazione di ufficio e *ELSA LANCAPi*

La *LANCAPi* di ELSA è una speciale forma della ben nota interfaccia CAPI. CAPI significa Common ISDN Application Programming Interface e realizza la connessione delle interfacce ISDN con i programmi di comunicazione. A loro volta questi programmi consentono ai computer le funzioni di comunicazione di ufficio come per es. un fax o una segreteria telefonica.

Questo capitolo presenta brevemente la *LANCAPi* e i programmi applicativi in dotazione per la comunicazione di ufficio e fornisce istruzioni importanti per l'installazione dei singoli componenti.

### 4.10.1

#### *ELSA LANCAPi*

##### **Quali vantaggi offre la *LANCAPi*?**

L'impiego della *LANCAPi* comporta principalmente vantaggi economici. Tutte le workstation incorporate nella LAN (Local Area Network) ottengono attraverso la *LANCAPi* un accesso illimitato alle funzioni di comunicazione di ufficio come fax, segreteria telefonica, online banking e EuroFileTransfer. Senza hardware supplementare sulle singole workstation, tutte le funzioni vengono realizzate attraverso la rete. In questo modo si evita il costoso equipaggiamento delle workstation con interfacce ISDN o modem. Soltanto

il software per comunicazione di ufficio viene installato sulle singole workstation.

Quando si inviano fax viene simulato sulla workstation un apparecchio fax. Con la *LANCAPi* il PC instrada il fax attraverso la rete al router, e questo stabilisce la connessione con il destinatario.

### Installazione del *LANCAPi* client

La *LANCAPi* è costituita da due componenti, un server (in *ELSA LANCOM Office*) e un client (sui PC). Il *LANCAPi* client viene installato sui computer della rete locale che intendono utilizzare le funzioni della *LANCAPi*.

- ① Inserire il CD *ELSA LANCOM* nell'unità disco CD-ROM. Se il programma Setup non si avvia automaticamente quando si inserisce il CD, in Explorer di Windows fare clic su 'autorun.exe' sul CD *ELSA LANCOM*.
- ② Selezionare la voce 'LANCOM Software installa'.
- ③ Evidenziare l'opzione 'ELSA LANCAPi'. Cliccare su **continua**, e seguire le istruzioni della routine di installazione.

Dopo il riavvio del computer eventualmente necessario la *LANCAPi* è pronta a realizzare tutti i compiti del software di comunicazione di ufficio. Dopo essere stata installata con successo la *ELSA LANCAPi* compare come icona nella barra dei simboli. Facendo doppio clic su questo simbolo si apre una finestra di stato in cui si possono richiamare in ogni momento le informazioni attuali sulla *ELSA LANCAPi*.

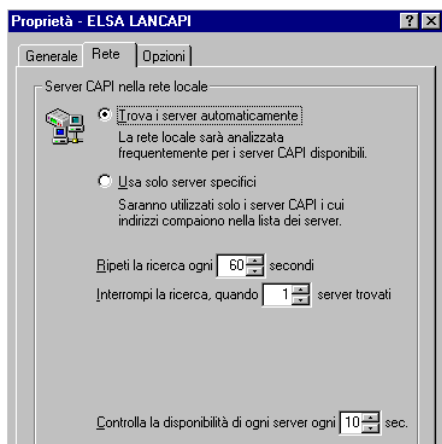
### Impostazione del *LANCAPi* client

Durante l'impostazione del client della *LANCAPi* si definisce quali *LANCAPi* server devono essere utilizzati e come vengono controllati. Se si impiega un solo *ELSA LANCOM Office* della LAN come *LANCAPi* server, in linea di principio si possono lasciare inalterati tutti i parametri predefiniti.

- ① Avviare il *LANCAPi* client dal gruppo di programmi 'ELSAIan'. Sulla scheda registro 'Generale' si trovano le informazioni per il driver per il servizio predisposto.
- ② Passare al registro 'LANCAPi Server'. In questo si può prima scegliere se il PC deve cercare autonomamente il proprio *LANCAPi* server oppure deve essere utilizzato un determinato server.
  - Nel primo caso stabilire in quale intervallo di tempo il client deve cercare un server. La ricerca prosegue fino a quando viene trovato il

numero di server impostato nel campo accanto. Quando è stato trovato il numero di server prescritto, la ricerca termina.

- Se il client non deve cercare automaticamente i server, introdurre nella lista gli indirizzi IP dei server che il client deve utilizzare. Questa impostazione ha senso per es. se più *ELSA LANCOM Office* della LAN operano come *LANCAPI* server e un gruppo di PC deve utilizzare un determinato server.
- Per entrambe le opzioni si può inoltre impostare l'intervallo in cui il client controlla se i server trovati oppure definiti nella lista sono ancora attivi.



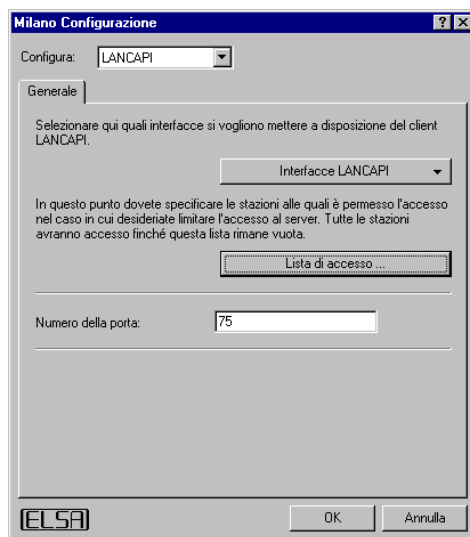
### Impostazione del *LANCAPI* server

Durante l'impostazione del *LANCAPI* server in linea di principio si risponde a due domande:

- A quali numeri d'utenza della rete telefonica deve reagire la *LANCAPI*?
- Quali dei computer della rete locale devono avere accesso tramite la *LANCAPI* alla rete telefonica?

I corrispondenti parametri vengono impostati nel modo seguente:

- ① Avviare *ELSA LANconfig* dal gruppo di programmi 'ELSAIan'. Aprire la configurazione del router facendo doppio clic sul nome della periferica nella lista, e selezionare il campo di 'Configura' '*LANCAPI*'.



- ② Attivare il *LANCAPI* server, o consentire 'solo chiamate in uscita'. In questo caso la *LANCAPI* non reagisce alle chiamate in arrivo e non può essere impiegata per es. per ricevere messaggi fax. Per es. consentire solo le chiamate in uscita se per la *ELSA LANCAPI* non si dispone di un numero d'utenza libero.
- ③ Se si deve attivare il *LANCAPI* server, introdurre nel campo 'Numero (MSN)' i numeri telefonici, a cui la *LANCAPI* deve reagire. Più numeri d'utenza possono essere separati da « punto e virgola ». Se non si introduce alcun numero d'utenza, tutte le chiamate in arrivo vengono comunicate alla *LANCAPI*.
- ④ La *LANCAPI* utilizza la porta predefinita '75' (any private telephony service). Modificare questa impostazione solo se questa porta è già utilizzata nella rete locale per altri servizi.
- ⑤ Se non tutti i computer della rete locale devono avere accesso alle funzioni della *LANCAPI*, i partecipanti autorizzati possono essere definiti esattamente nella lista di accesso (tramite gli indirizzi IP).



*Se si introducono più numeri d'utenza per la LANCAPI, è possibile preparare per le singole workstation per es. un fax personale o una segreteria telefonica personale. A questo scopo durante l'installazione di programmi di*

comunicazione come per es. *ELSA-RVS-COM* sui diverse workstation indicare di volta in volta numeri d'utenza diversi, ai quali il programma deve reagire.

Passare alla scheda registro 'Opzioni'. In questa si definisce come si comporta un *ELSA LANCOM Office* se tramite la *LANCAPI* deve essere stabilita una connessione (chiamata in arrivo o in uscita), ma entrambi i canali B sono occupati (Comando priorità). Sono possibili le opzioni:



- La connessione non può essere stabilita attraverso la *LANCAPI*. Un programma fax che utilizza la *LANCAPI* probabilmente tenterà di nuovo l'invio in un momento successivo.
- La connessione può essere stabilita attraverso la *LANCAPI* se è libero un canale principale. Un canale principale è il canale B sul quale viene creata la prima connessione router. I canali secondari vengono aggiunti solo per il raggruppamento canali. Se sono stabilite contemporaneamente due connessioni router separate per due controparti (due canali principali occupati), la *LANCAPI* deve attendere.
- La connessione può essere stabilita attraverso la *LANCAPI* in ogni caso, una connessione router in corso viene eventualmente interrotta per la durata della conversazione. In questo modo per es. la funzione fax è sempre ottenibile.

### Così si usa la **LANCAPI**

Per usare la *LANCAPI* esistono due possibilità:

- Si impiega un software applicato direttamente a un'interfaccia CAPI (in questo caso la *LANCAPI*), come per es. *ELSA-RVS-COM*. Un siffatto software cerca la CAPI durante l'installazione e successivamente la usa automaticamente.

- Altri programmi come LapLink possono stabilire connessioni su diversi percorsi, per es. tramite la rete di Accesso remoto di Windows. Quando si crea una nuova connessione di accesso remoto si può scegliere quale delle periferiche di comunicazione installate si intende utilizzare. Per la *LANCAP* selezionare la voce 'ISDN WAN Line 1'.

## 4.11

### L'impianto telefonico incorporato

Durante la conversione dalle linee analogiche alle connessioni digitali (ISDN) si pone spesso la domanda sull'utilizzabilità dei terminali analogici già presenti. Quattro porte a/b incorporate in *ELSA LANCOM 2000 Office* consentono la connessione di telefoni, apparecchi fax, segreterie telefoniche o modem analogici.

In questo modo è possibile continuare ad impiegare sulla workstation i terminali analogici. Questo consente di risparmiare investimenti supplementari in nuovi terminali digitali. Inoltre le porte a/b del *ELSA LANCOM 2000 Office* consentono moderne funzioni supplementari ISDN come Smistamento di chiamata, Richiamata, Mediazione, Attesa in linea e Conferenza a 3.

Inoltre con le periferiche collegate alle porte a/b si possono utilizzare le funzioni di un piccolo impianto interno: Per es. si possono effettuare conversazioni interne, smistare una chiamata esterna a un altro apparecchio o mediare tra chiamate interne e esterne.

A questo proposito si notino anche le funzioni del Least Cost Router!

*Le funzioni dell'impianto di telecomunicazione sono disponibili solo con ELSA LANCOM 2000 Office!*



#### 4.11.1

### Connessione di terminali analogici

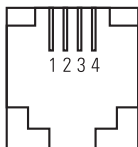
#### Quali periferiche possono essere connesse?

In linea di principio si possono connettere alle porte a/b del *ELSA LANCOM 2000 Office* tutti i terminali analogici:

- Telefoni
- Apparecchi fax gruppo 3
- Segreterie telefoniche
- Modem
- Apparecchi combinati

### Adattatore telefonico (RJ11)

Per poter continuare a utilizzare gli apparecchi analogici (per es. telefono, segreteria telefonica, fax), vengono forniti da ELSA gli adattatori appropriati.



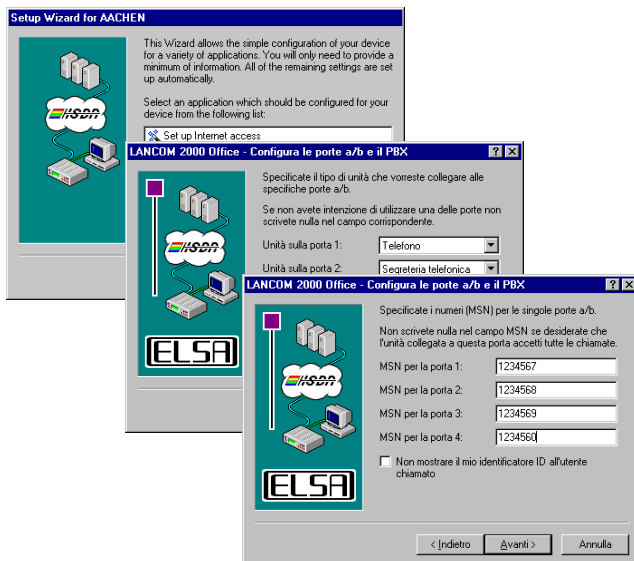
## 4.11.2

### Configurazione con *ELSA LANconfig* e il settaggio assistito

Per la configurazione delle porte a/b e dell'impianto interno del *ELSA LANCOM 2000 Office* è disponibile in *ELSA LANconfig* un'assistenza che si incarica di effettuare tutte le impostazioni necessarie nel software *ELSA LANCOM*. In linea di principio si deve solo indicare quale periferica è stata collegata a ciascuna porta a/b e quale numero d'utenza deve essere assegnato alle singole periferiche.

- ① Avviare *ELSA LANconfig* dal gruppo di programmi 'ELSAIan'.
- ② Evidenziare nella lista delle periferiche il *ELSA LANCOM* per cui si desidera effettuare le impostazioni. Cliccare su **Strumenti ► Setup Wizard**, e selezionare la voce 'Configurare porte a/b e impianto telefonico'.





- ③ Nei successivi passi impostare quale periferica è stata collegata a ciascuna porta, e assegnare il numero d'utenza alle porte a/b.
- ④ Alla fine scegliere se si desidera utilizzare il *ELSA LANCOM* come impianto telefonico oppure se si desidera continuare a utilizzarlo come normale connessione telefonica.
- ⑤ Dopo queste impostazioni è già fatto tutto. Cliccando su **Fine** nella finestra accanto si esce dall'assistenza e si salvano le nuove impostazioni nel *ELSA LANCOM*.

Che cosa si è ottenuto con questa assistenza? Il risultato dipende dal tipo di periferica selezionato per le porte. In particolare, oltre ai numeri d'utenza impostati e ai numero d'utenza interni fissi, valgono le seguenti impostazioni speciali:

- Telefono

Se si connette un telefono a una porta a/b con questa impostazione, durante una conversazione in corso un'altra chiamata per la stessa porta viene segnalata con una battuta d'avviso.

- Segreterie telefoniche

Con la segreteria telefonica le altre chiamate non vengono segnalate con una battuta di avviso, ma è invece possibile accettare la conversazione. Se la segreteria telefonica è stata più veloce ed ha già salutato il chiamante, si può già sollevare semplicemente la cornetta di un altro telefono e così accettare la conversazione.

- Fax e modem

Per gli apparecchi fax e i modem l'assistenza disattiva automaticamente le opzioni descritte, poiché in queste periferiche non è appropriata né la battuta d'avviso né l'accettazione della chiamata.

- Chiamata centralino

- Quando si imposta il *ELSA LANCOM 2000 Office* come impianto interno, quando si solleva la cornetta ci si connette prima con *ELSA LANCOM*. Si può telefonare immediatamente verso l'interno o selezionare lo zero, per ottenere un segnale di libero dal centralino per una conversazione esterna.



*Se il ELSA LANCOM 2000 Office è stato collegato a un impianto interno, selezionando lo zero naturalmente si raggiunge prima l'impianto superiore e si deve eventualmente selezionare ancora lo zero per selezionare il centralino!*

*Si noti inoltre che per es. le voci degli elenchi telefonici o le liste di selezione rapida di telefoni, modem e altre periferiche devono essere completate con lo zero iniziale.*

- Quando si imposta il *ELSA LANCOM 2000 Office* come normale connessione telefonica, quando si solleva la cornetta si sente immediatamente il segnale di libero del centralino (o dell'impianto telefonico a cui è stato collegato il *ELSA LANCOM 2000 Office*). Con questa impostazione è impossibile telefonare all'interno attraverso il *ELSA LANCOM 2000 Office*!

Se il risultato delle impostazioni effettuate usando l'assistenza non corrisponde in qualche punto a quanto desiderato, naturalmente si può modificare la configurazione anche successivamente, come descritto nella sezione seguente.

### 4.11.3

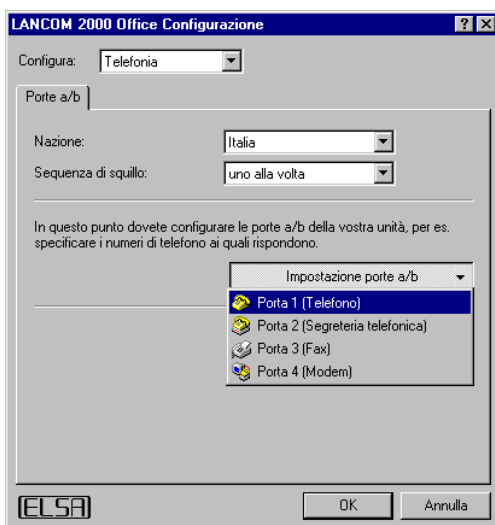
### Configurazione manuale con *ELSA LANconfig*

Per ciascuna delle quattro porte a/b è possibile impostare manualmente come deve comportarsi con le chiamate in arrivo e in uscita.

Selezionare il campo di configurazione 'Telefonia'. Sulla scheda registro 'Porte a/b' impostare prima il Paese in cui viene usato il *ELSA LANCOM 2000 Office*. Inoltre si può selezionare quello che deve succedere in caso di chiamata in arrivo a cui possono reagire più periferiche: Tutte le periferiche squillano singolarmente e in successione, accoppiate o tutte contemporaneamente?



*Fare attenzione al forte consumo di corrente specialmente nei telefoni più vecchi. Se più periferiche di questo tipo squillano contemporaneamente, l'alimentatore del ELSA LANCOM può essere sovraccaricato. In tali circostanze scegliere l'impostazione 'singolarmente' o 'in coppie':*



Nella lista a comparsa per l'impostazione delle porte a/b ora si possono aprire le impostazioni per ciascuna porta per modificarle. Il simbolo accanto alla voce indica il tipo di periferica collegato a tale porta. Selezionare la voce della lista per cui si desidera modificare le impostazioni.

### Impostazioni generali

Nella scheda registro 'Generale' per ciascuna porta a/b utilizzata adattare le seguenti impostazioni:

**Impostazione porte a/b - Porta 1**

Generale | Accesso alla rete pubblica | Classe di servizio | Disponibilità

Numero (MSN): 1234567

Numero da chiamare interno: 11

Descrizione: Telefono

Capacità: Telefonia analogica

☐ Non squillare per le chiamate in ingresso (servizio non-disturbare)  
☐ Attiva l'avviso di chiamata  
☐ Genera un impulso di conteggio (per i telefoni con un display di costo)  
☐ Nasconde il proprio numero di telefono al sito  
☐ Permette l'adozione automatica di un collegamento stabilito da un'altra porta. (per le segreterie telefoniche ad esempio)  
☐ Interconnette automaticamente due chiamate esterne quando si riattacca  
☐ Compongono automaticamente il seguente numero nel momento in cui si solleva il ricevitore del telefono:

Numero: 123666

OK Annulla

- Assegnare alla connessione un 'numero d'utenza': MSN (Multiple Subscriber Number) in caso di connessioni multiple con DSS1 come protocollo canale D, DDI (Direct Dial In) in caso di connessioni di impianto o EAZ (cifra di selezione terminale) in caso di connessioni 1TR6.
  - Se la porta a/b deve reagire a più numeri d'utenza, introdurli separati con « punto e virgola ».
  - Il primo numero d'utenza introdotto in caso di chiamata in uscita viene indicato al centralino e alla controparte.
  - Se non si introduce nessun numero d'utenza, la porta a/b reagisce a tutte le chiamate in arrivo e indica sempre il numero d'utenza principale della connessione al centralino e alla controparte.
- Il numero d'utenza interno è stabilito in modo fisso e non può essere modificato:
  - '11' per la porta a/b 1
  - '12' per la porta a/b 2
  - '13' per la porta a/b 3
  - '14' per la porta a/b 4
- Impostare una descrizione per la porta. Questa descrizione non ha alcun effetto sulle funzioni delle porte o delle periferiche collegate, essa serve

solo per distinguere più facilmente quale periferica è collegata a ciascuna porta. Si può scegliere:

- ☐ Nessuna descrizione
- ☐ Telefoni
- ☐ Apparecchi fax gruppo 3
- ☐ Segreterie telefoniche
- ☐ Modem
- ☐ Apparecchi combinati
- Selezionare il servizio che la porta a/b stessa annuncia alla controparte quando si stabilisce la connessione. Questa impostazione non seleziona l'accettazione delle chiamate in entrata in base alle caratteristiche di servizio! Sono possibili impostazioni:
  - ☐ Analogica 3,1 kHz (impostazione standard)
  - ☐ Lingua
  - ☐ Fax gruppo 2/3
- Attivare o disattivare le seguenti opzioni secondo necessità:
  - ☐ 'Nessun segnale di chiamata ...' attiva o disattiva lo squillo della periferica collegata.
  - ☐ 'Segnalare la chiamata ... con battuta d'avviso' consente la segnalazione di successive chiamate per una porta mentre è già stabilita una connessione.
  - ☐ 'Generare impulso di addebito': Questa funzione genera dalle informazioni di addebito ISDN un impulso di addebito e lo trasferisce alla periferica collegata a tale porta. In caso di telefoni analogici con indicatore di addebito, si possono così controllare i costi per le conversazioni in corso. Disattivare questa opzione per le porte con apparecchi fax o modem, poiché la trasmissione dati può essere disturbata dall'impulso di addebito.



*Gli impulsi di addebito funzionano correttamente solo nelle connessioni con 'AOCD' (Trasmissione di addebito durante la conversazione). In caso di 'AOCE' gli addebiti vengono trasferiti solo dopo che la cornetta è stata appoggiata, e quindi il telefono non è più in grado di conteggiare tutti gli impulsi.*

- ☐ 'Sopprimere l'indicazione del proprio numero ...' impedisce la trasmissione del proprio numero d'utenza alla controparte, se non si desidera che in base al numero d'utenza si possa stabilire il chiamante. Il numero d'utenza viene sempre trasmesso al centralino. La codifica degli addebiti telefonici in base ai numeri d'utenza è

possibile per la società telefonica anche in caso di soppressione della trasmissione del numero d'utenza.



*La possibilità di « eventuale soppressione del numero d'utenza » eventualmente deve essere richiesta specificamente alla società telefonica.*

- 'Accettazione automatica ...' consente di accettare una chiamata a cui un apparecchio su un'altra porta ha già risposto. Di regola questa opzione viene attivata solo per porte con segreteria telefonica.
- 'Conversazioni esterne ...' consente la connessione di chiamate dall'esterno. Se si telefona parallelamente con due controparti esterne, risulta possibile metterle in comunicazione tra loro appoggiando semplicemente la cornetta.



*Anche la possibilità di conversazione esterna deve essere richiesta specificamente alla società telefonica.*

*Si noti che con questo tipo di collegamento vengono addebitati i costi telefonici, anche se non si partecipa più alla conversazione!*

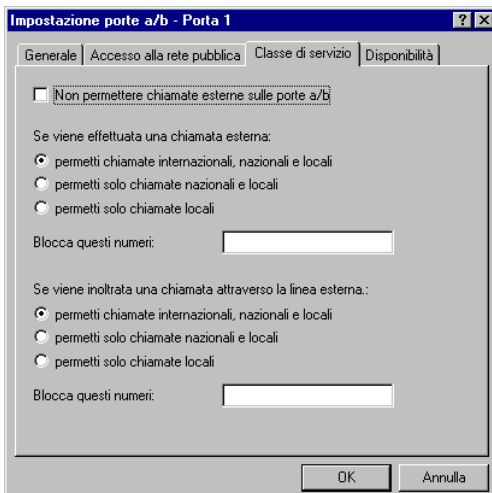
- 'Selezionare automaticamente ... questo numero:' Introdurre un numero d'utenza, che deve essere usato per la funzione Chiamata bambino. In questo caso il numero introdotto viene selezionato cinque secondi dopo che è stata sollevata la cornetta, se non è stato già iniziata un'altra selezione.



*La funzione Chiamata bambino può essere configurata anche usando i tasti del telefono. In questo caso le impostazioni in ELSA LANconfigvengono sovrascritte.*

### **Impostazione della chiamata centralino**

Passare alla scheda registro 'Chiamata centralino'. In questa si può impostare come di deve comportare la porta a/b quando si solleva la cornetta e quando si preme il tasto Flash. Considerare il « Sollevare la cornetta » in senso metaforico, poiché nel caso di un modem o di un apparecchio fax sulla porta considerata naturalmente la procedura di selezione viene avviata in modo diverso ...



Per il comportamento nel sollevare la cornetta si può scegliere tra tre opzioni:

- Nell'opzione 1 quando si solleva la cornetta si stabilisce solo un collegamento al *ELSA LANCOM*. Ora si può telefonare all'interno, e quindi chiamare una periferica su un'altra porta a/b. Per effettuare conversazioni esterne, si hanno le seguenti due possibilità:
  - Se il *ELSA LANCOM* è connesso direttamente con una connessione ISDN, si può selezionare lo '0', per telefonare all'esterno.
  - Se lo stesso *ELSA LANCOM* è collegato a un impianto interno più grande, eventualmente si deve ancora selezionare il numero identificativo del centralino dell'impianto interno, per effettuare telefonate verso l'esterno.
- Nell'opzione 2 quando si solleva la cornetta si stabilisce un collegamento alla connessione a cui è collegato il *ELSA LANCOM*. Questo corrisponde a una connessione interna al *ELSA LANCOM*, in cui poi viene selezionato automaticamente lo '0'. Ora si hanno le seguenti possibilità:
  - Se il *ELSA LANCOM* è connesso direttamente con una connessione ISDN, si può telefonare all'esterno senza altre cifre identificative.
  - Se lo stesso *ELSA LANCOM* è collegato a un impianto interno più grande, eventualmente si deve selezionare il numero identificativo del centralino dell'impianto interno, per effettuare telefonate verso l'esterno.

- Nell'opzione 3 quando si solleva la cornetta si stabilisce un collegamento alla connessione a cui è collegato il *ELSA LANCOM*, dopo la connessione interna al *ELSA LANCOM* viene quindi selezionato automaticamente uno '0'. Inoltre viene anche selezionato il numero introdotto nel campo sull'estremità inferiore della finestra. Con questa impostazione si hanno per es. le seguenti possibilità:
  - Se lo stesso *ELSA LANCOM* è collegato a un impianto interno più grande, si può selezionare automaticamente il numero identificativo del centralino dell'impianto interno, e quindi telefonare verso l'esterno senza dover introdurre altri numeri.
  - Se su un telefono di questa connessione si desidera effettuare soltanto chiamate interurbane attraverso una determinata società telefonica con la procedura Call-by-Call, introdurre accanto al necessario numero identificativo del centralino il prefisso della società telefonica (per es. 0101x). In questo modo ogni volta che si solleva la cornetta si riceve automaticamente un segnale di libero della società telefonica.

### Funzione del tasto Flash (tasto R)

Nella parte inferiore della scheda registro 'Chiamata centralino' si può definire l'effetto che si ottiene premendo il tasto Flash.

*Nella maggior parte dei telefoni il tasto Flash è il tasto di richiamata o tasto R. Spesso la funzione di questo tasto è configurabile. Consultare le informazioni tecniche del telefono per conoscere come è configurato questo tasto alla consegna e come può essere riprogrammato per la funzione Flash. Come Flash regolamentare vengono accettati dal ELSA LANCOM segnali con una lunghezza tra 70 e 300 ms.*

Per la pressione del tasto Flash si può impostare una delle tre opzioni descritte. Le opzioni sono uguali a quelle relative al sollevamento della cornetta:

- Nell'opzione 1 premendo il tasto Flash si stabilisce una connessione all'impianto interno del *ELSA LANCOM*. Quindi si può stabilire una conversazione interna o selezionare lo '0' per stabilire il collegamento con la connessione ISDN (oppure con l'impianto interno generale).
- Nell'opzione 2 premendo il tasto Flash si stabilisce un collegamento diretto con la connessione ISDN (oppure con l'impianto interno generale).
- Nell'opzione 3 premendo il tasto Flash si seleziona automaticamente il numero d'utenza esterno impostato.





Attraverso la cooperazione delle impostazioni per il sollevamento della cornetta e per la pressione del tasto Flash si può adattare in modo mirato l'impianto interno del *ELSA LANCOM* alle proprie necessità. Esempi:

- Il *ELSA LANCOM* è collegato direttamente a una connessione ISDN. Attivare la seconda opzione per il sollevamento della cornetta e la prima opzione per il tasto Flash. Sollevando la cornetta ora si può telefonare all'esterno e premendo il tasto Flash si può commutare a telefonare all'interno.
- Il *ELSA LANCOM* è collegato a un impianto interno più grande. Attivare la prima opzione per il sollevamento della cornetta e la terza opzione per il tasto Flash. Introdurre nel campo 'Numero del centralino' la cifra necessaria per la chiamata centralino dell'impianto interno. Sollevando la cornetta ora si può telefonare all'interno, e premendo il tasto Flash vengono selezionati automaticamente tutti i numeri identificativi del centralino necessari per telefonare all'esterno.

Il tasto Flash assume un'importanza particolare se le connessioni sono appena attive, sono in attesa per la richiamata o se sono state appena selezionate. La seguente tabella fornisce indicazioni su quello che accade nelle diverse situazioni. In linea di massima si può prevedere che premendo il tasto Flash intuitivamente si ottiene quello che si desidera realizzare.

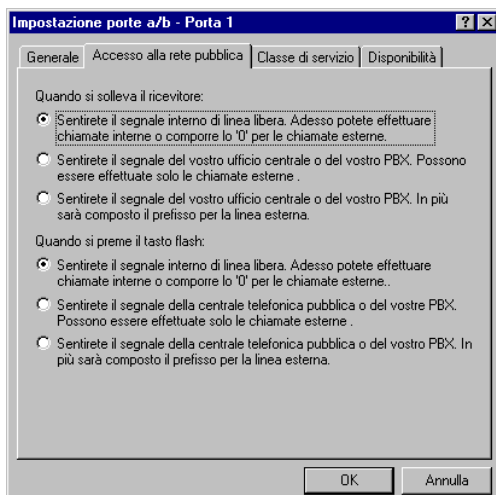
In dettaglio si verifica quanto segue:

| Collegamento               | Stato                                                                                                                                                | Effetto del tasto Flash                                                                               |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| nessuna connessione attiva | - segnale di libero<br>- selezione incompleta<br>- fuori tempo durante una selezione<br>- la controparte squilla<br>- fuori tempo durante lo squillo | La selezione/stabilimento della connessione viene interrotta, e viene eseguita la funzione impostata. |
| una connessione attiva     |                                                                                                                                                      | La connessione viene tenuta in attesa, e viene eseguita la funzione impostata.                        |

| Collegamento                                                                 | Stato                                                         | Effetto del tasto Flash                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| una connessione è in attesa                                                  | - segnale di libero                                           | Viene mediata la connessione in attesa.                                                                                                                                                                                                                                                                                                                   |
|                                                                              | - selezione incompleta<br>- fuori tempo durante una selezione | La selezione viene interrotta, e viene eseguita la funzione impostata.                                                                                                                                                                                                                                                                                    |
|                                                                              | - la controparte squilla<br>- fuori tempo durante lo squillo  | Lo stabilimento della connessione viene interrotta, e viene mediata la connessione in attesa.                                                                                                                                                                                                                                                             |
| una connessione attiva e una connessione in attesa o dà una battuta d'avviso |                                                               | Flash + '0': la connessione in attesa/in battuta d'avviso viene interrotta.<br>Flash + '1': la connessione attiva viene interrotta, e si commuta alla connessione in attesa/in battuta d'avviso.<br>Flash + '2': viene mediato dalla connessione attiva alla connessione in attesa/in battuta d'avviso.<br>Flash + '3': viene attivata la conferenza a 3. |
| conferenza a 3 attiva                                                        |                                                               | Flash + '2': la conferenza a 3 viene interrotta, e viene suddivisa in una connessione attiva e una connessione in attesa.                                                                                                                                                                                                                                 |

### Impostazione della Autorizzazione centralino

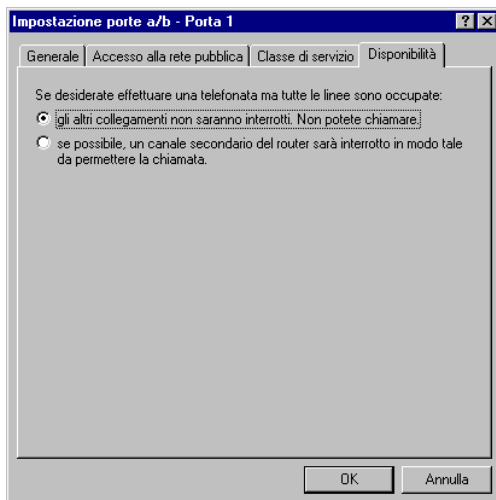
Sulla scheda registro 'Autorizzazione centralino' si può definire per ciascuna porta a/b se sono consentite o meno conversazioni esterne con le periferiche collegate.



Viene sempre mantenuta la funzione di ricevimento delle chiamate. Le conversazioni in uscita possono essere limitate alle conversazioni urbane o alle conversazioni interurbane nazionali. Possono anche essere bloccati determinati numeri d'utenza.

### Impostazione della Disponibilità

Sulla scheda registro 'Disponibilità' si definisce come si comporta il *ELSA LANCOM* se sulle porte a/b deve essere stabilita una connessione (chiamata in arrivo o in uscita), ma entrambi i canali B sono occupati (Comando priorità). Sono possibili le opzioni:



- Non consentire l'interruzione di altre connessioni. La connessione non può essere stabilita sulla porta a/b.
- Interruzione consentita di canali secondari, che per es. sono utilizzati per un raggruppamento canali. La connessione può essere stabilita sulla porta a/b se è libero un canale principale.
- Interruzione consentita di canali principali. La connessione sulla porta a/b può essere stabilita in ogni caso, una connessione router in corso viene eventualmente interrotta per la durata della conversazione. Quindi è sempre possibile essere raggiunti telefonicamente.

*Affinché il ELSA LANCOM 2000 Office possa riconoscere le chiamate in arrivo anche con connessioni in corso, nella connessione deve essere attivata la caratteristica di servizio Battuta d'avviso.*

#### 4.11.4 Servizio dell'impianto interno tramite telefono

Con il *ELSA LANCOM 2000 Office* durante la telefonata si possono utilizzare alcune comode prestazioni (per es. Mediazione). A questo scopo si deve disporre di un telefono adatto per la selezione a tono (selezione multifrequenza) e dotato di tasto R (tasto di richiamata con funzione Hook Flash).

Se non si è sicuri se il telefono opera con selezione a tono o selezione a impulso, questo si può facilmente stabilire facendo attenzione al rumore che

si sente nella cornetta durante la normale selezione: Se si sente un rumore di battito per ciascuna cifra selezionata, si tratta di selezione a impulso; se si sentono dei toni a fischio variabile, si tratta di selezione a tono.

*Determinati servizi (per es. Battuta d'avviso) sono prestazioni che devono essere richieste separatamente alle società telefoniche.*



### Battuta d'avviso

Con questa funzione si può sentire un tono del segnale se è in arrivo un'altra chiamata. Si può decidere se continuare a conversare con la controparte attuale oppure terminare la conversazione e rispondere alla chiamata che segnala il suo arrivo. Per accettare una chiamata che segnala il suo arrivo, procedere nel modo seguente:

- ① Controllare l'attivazione
  - Per controllare se questa caratteristica di servizio è attiva, tenendo sollevata la cornetta introdurre uno dopo l'altro **\*#43#**.
  - Se si sentono due toni acuti, la funzione è attiva. Se si sentono due toni gravi, la funzione non è attiva.
- ② Attivazione della Battuta d'avviso
  - Sollevare la cornetta, e attendere il tono di selezione.
  - Premere in successione sulla tastiera del telefono **\*43#**.
  - Attendere l'annuncio, e appoggiare la cornetta.
- ③ Ricevere la chiamata che segnala il suo arrivo
  - Dopo il tono del segnale premere entro 30 secondi il tasto **R** sulla cornetta.
  - Poi premere la cifra **2**. A questo punto la prima connessione è disattivata, e la seconda conversazione telefonica è attivata.
  - Premere il tasto **R** e la cifra **2**, per commutare tra le due chiamate (mediazione).
- ④ Chiudere la connessione in corso
  - Premere prima il tasto **R**.
  - Poi premere la cifra **1**, per chiudere la connessione attiva.

*Fare attenzione ad appoggiare la cornetta tra le due telefonate per almeno mezzo secondo oppure tenere premuta la forcina.*



- ⑤ Disattivazione della Battuta d'avviso

- Sollevare la cornetta, e attendere il tono di selezione.
- Premere in successione sulla tastiera del telefono **#43#**.
- Attendere l'annuncio, e appoggiare la cornetta.

### Conferenza a 3

Con questa funzione si può telefonare contemporaneamente con due controparti. Si ha la possibilità di chiamare direttamente le due controparti per la conferenza a 3 oppure accogliere nella conversazione una chiamata che segnala il suo arrivo.



*Una conferenza telefonica con tre partecipanti può essere realizzata solo con due chiamanti esterni e una connessione interna. Due partecipanti interni non possono stabilire una conferenza a 3 con un partecipante esterno!*

Per stabilire una conferenza a 3, procedere nel modo seguente:

- ① Conferenza a 3 con chiamata che segnala il suo arrivo
  - Dopo il tono del segnale premere entro 30 secondi il tasto **R** sulla cornetta.
  - Poi premere la cifra **2**. A questo punto la prima connessione è disattivata, e la seconda conversazione telefonica è attivata.
  - Premere di nuovo il tasto **R**.
  - Poi premere la cifra **3**, per attivare la conferenza a 3.
- ② Conferenza a 3 con due connessioni autonome
  - Stabilire prima una connessione con la prima controparte.
  - Poi premere il tasto **R**. Secondo l'impostazione della chiamata centralino si sente un segnale di libero interno o esterno.
  - Introdurre il numero d'utenza della seconda controparte. A questo punto la prima connessione è disattivata, e la seconda conversazione telefonica è attivata.
  - Poi premere la cifra **3**, per attivare la conferenza a 3.
- ③ Chiudere la connessione attiva
  - Premere prima il tasto **R**.
  - Poi premere la cifra **1**, per chiudere la connessione attiva.
- ④ Chiudere entrambe le connessioni



- Appoggiando la cornetta si possono chiudere contemporaneamente entrambe le connessioni della conferenza a 3.

*Fare attenzione all'impostazione dell'opzione 'Trasferire automaticamente le conversazioni esterne riattaccando' per la corrispondente porta a/b. Se questa opzione è attivata, le connessioni non vengono interrotte riattaccando la cornetta, invece i due chiamanti esterni vengono collegati tra loro.*

*Si noti che con questo tipo di collegamento vengono addebitati i costi telefonici, anche se non si partecipa più alla conversazione!*



### **Richiamata/Mediazione**

Con questa funzione si può stabilire in parallelo a una connessione in corso un'altra conversazione, per esempio per chiedere un'informazione. Per attivare la Richiamata, procedere nel modo seguente:

#### **① Stabilire la seconda conversazione**

- Premere prima il tasto **R**.
- Poi introdurre il numero d'utenza desiderato. A questo punto la prima connessione è disattivata, e la seconda conversazione telefonica è attivata (Richiamata).

*La seconda conversazione può essere stabilita sia con una controparte interna che con una esterna.*

#### **② Mediazione**

- Premendo il tasto **R** e la cifra **2**, si può commutare tra le due chiamate (mediazione).

#### **③ Collegamento**

- Appoggiando la cornetta si possono collegare tra loro le due controparti.



*Fare attenzione all'impostazione dell'opzione 'Trasferire automaticamente le conversazioni esterne riattaccando' per la corrispondente porta a/b. Se questa opzione è attivata, si possono collegare tra loro due chiamanti esterni.*

#### **④ Chiudere la connessione in corso**

- Premere prima il tasto **R**.
- Poi premere la cifra **1**, per chiudere la connessione attiva.

*Se si chiude la conversazione attiva riattaccando semplicemente la cornetta, il telefono squilla subito dopo, per richiamare l'attenzione sul chiamante della connessione finora disattiva.*

### Presa di chiamata

Se sono collegati telefoni a diverse porte a/b, con questa funzione si può prendere sul proprio apparecchio una conversazione destinata a un altro telefono.

- ① Sollevare la cornetta, se si sente suonare su un'altra connessione.
- ② Se si sente il segnale di libero interno del *ELSA LANCOM 2000 Office*, selezionare il numero d'utenza interno della porta a/b per cui è in arrivo la chiamata. Se non si sente direttamente il segnale di libero interno del *ELSA LANCOM 2000 Office*, secondo l'impostazione si deve eventualmente premere il tasto **R**, per stabilire la connessione con *ELSA LANCOM 2000 Office*.
- ③ Poi premere la cifra **8**, per prendere la conversazione dall'altra connessione.

*Se è in corso una propria telefonata, secondo l'impostazione del *ELSA LANCOM 2000 Office* premere prima per es. il tasto **R**, per mettere in parcheggio la propria telefonata, e poi prendere con il numero d'utenza interno e la cifra **8** la seconda chiamata sul proprio apparecchio.*

### Smistamento di chiamata

Con questa funzione si può essere reperibili dovunque con il proprio numero d'utenza. Si deve soltanto introdurre il numero di destinazione desiderato, e tutte le chiamate vengono smistate automaticamente a tale numero. Lo smistamento può avvenire immediatamente, dopo 15 secondi o su occupato. Procedere nel modo seguente:

*Prima di utilizzare questa prestazione, si deve assegnare un MSN alle porte a/b. Utilizzare *ELSA LANconfig* per assegnare il MSN.*

- ① Attivazione dello Smistamento di chiamata
  - Sollevare la cornetta, e attendere il tono di selezione.





- Premere in successione sulla tastiera del telefono:
  - \* **21** \* (in caso di Smistamento di chiamata « immediato »)
  - \* **61** \* (in caso di Smistamento di chiamata « dopo 15 secondi »)
  - \* **67** \* (in caso di Smistamento di chiamata « occupato »)
- Introdurre il numero di destinazione desiderato, e premere #.
- Se si sentono due toni acuti, la funzione è attiva, e si può appoggiare la cornetta.

*Se alla corrispondente porta a/b non è stato assegnato un MSN, con la combinazione di tasti \* **x y** \* numero di destinazione \* MSN della porta a/b # si può attivare lo Smistamento di chiamata oppure con # **x y** \* MSN della porta a/b # la si può disattivare (x y rappresenta l'identificativo delle opzioni 'immediato', 'dopo 15 secondi' o 'occupato').*

*Per controllare se questa caratteristica di servizio è attiva, tenendo sollevata la cornetta introdurre (dopo il tono di selezione) in successione # \* **x y** \* MSN della porta a/b #. Se si sentono due toni acuti, la funzione è attiva. Se si sentono due toni gravi, la funzione non è attiva.*

## ② Disattivazione dello Smistamento di chiamata

- Sollevare la cornetta, e attendere il tono di selezione.
- Premere in successione sulla tastiera del telefono:
  - # **21** # (in caso di Smistamento di chiamata « immediato »)
  - # **61** # (in caso di Smistamento di chiamata « dopo 15 secondi »)
  - # **67** # (in caso di Smistamento di chiamata « occupato »)
- Se si sentono due toni acuti, la funzione era attiva ed è stata disattivata, e si può appoggiare la cornetta. Se si sente un tono grave, la funzione non era attiva, oppure eventualmente è stato introdotto un MSN sbagliato!

## Connessione senza selezione

Con questa funzione si ha la possibilità di selezionare automaticamente uno speciale numero di destinazione (per es. chiamata di emergenza). Se entro cinque secondi dopo aver sollevato la cornetta non è stato selezionato alcun numero di chiamata, viene automaticamente selezionato questo speciale numero di destinazione.

Se per esempio si esce di sera, si può introdurre il numero al quale si può essere reperiti. Un bambino deve semplicemente sollevare la cornetta per selezionare automaticamente il numero.

*Questa funzione può anche essere configurata tramite ELSA LANconfig. In questo modo le impostazioni effettuate con i tasti del telefono vengono sovrascritte.*

Procedere nel modo seguente:

- ① Controllare l'attivazione
  - Per controllare se questa caratteristica di servizio è attiva, tenendo sollevata la cornetta introdurre (dopo il tono di selezione) in successione **\*#53#**.
  - Se si sentono due toni acuti, la funzione è attiva. Se si sentono due toni gravi, la funzione non è attiva.  
Fare anche attenzione che secondo l'impostazione della 'Chiamata centralino' per la corrispondente porta a/b si deve eventualmente inserire uno '0' prima del numero d'utenza.
- ② Attivazione della Connessione senza selezione
  - Sollevare la cornetta, e attendere il tono di selezione.
  - Premere in successione sulla tastiera del telefono **\*53\***.
  - Introdurre il numero d'utenza desiderato, e premere **#**.
  - Se si sentono due toni acuti, la funzione è attiva, e si può appoggiare la cornetta.
- ③ Disattivazione della Connessione senza selezione
  - Sollevare la cornetta, e attendere il tono di selezione.
  - Premere in successione sulla tastiera del telefono **#53#**.
  - Se si sentono due toni acuti, la funzione è attiva, e si può appoggiare la cornetta.

*Se è stato introdotto una volta il numero d'utenza per la connessione senza selezione e poi la funzione è stata disattivata, si può riattivare il numero d'utenza memorizzato in qualunque momento con **\*53#** per la connessione senza selezione.*

### **Attivazione della porta a/b per le chiamate**

Con questa funzione si può stabilire se il telefono deve squillare per una chiamata. Questa funzione è particolarmente utile, se si desidera non essere

disturbati. Il chiamante sente soltanto un segnale di occupato. Procedere nel modo seguente:

① Controllare l'attivazione

- Per controllare se questa caratteristica di servizio è attiva, tenendo sollevata la cornetta introdurre (dopo il tono di selezione) in successione **\*#99#**.
- Se si sentono due toni acuti, la funzione è attiva. Se si sentono due toni gravi, la funzione non è attiva.

② Attivazione della porta a/b

- Sollevare la cornetta, e attendere il tono di selezione.
- Premere in successione sulla tastiera del telefono **\*99#**.
- Se si sentono due toni acuti, la funzione è attiva, e si può appoggiare la cornetta.

③ Disattivazione della porta a/b

- Sollevare la cornetta, e attendere il tono di selezione.
- Premere in successione sulla tastiera del telefono **#99#**.
- Se si sentono due toni acuti, la funzione è attiva, e si può appoggiare la cornetta.

### Soppressione del numero d'utenza

Con questa funzione si può sopprimere la trasmissione del proprio numero d'utenza multipla (MSN) alla controparte.

*La possibilità di « eventuale soppressione del numero d'utenza » eventualmente deve essere richiesta specificamente alla società telefonica.*

Procedere nel modo seguente:

① Controllare l'attivazione

- Per controllare se questa caratteristica di servizio è attiva, tenendo sollevata la cornetta introdurre (dopo il tono di selezione) in successione **\*#310#**.
- Se si sentono due toni acuti, la funzione è attiva. Se si sentono due toni gravi, la funzione non è attiva.

② Attivazione della Soppressione del numero d'utenza

- Sollevare la cornetta, e attendere il tono di selezione.



- Premere in successione sulla tastiera del telefono **\*310#**.
- Se si sentono due toni acuti, la funzione è attiva, e si può appoggiare la cornetta.
- ③ Disattivazione della Soppressione del numero d'utenza
  - Sollevare la cornetta, e attendere il tono di selezione.
  - Premere in successione sulla tastiera del telefono **#310#**
  - Se si sentono due toni acuti, la funzione è attiva, e si può appoggiare la cornetta.

## 4.12 Accounting

Nell'accounting, vengono rilevati i tempi in linea e i volumi di dati ed essi vengono correlati a quei computer che li hanno causati. I dati di accounting vengono salvati in una lista dei collegamenti correnti e in una lista dei totali.

In esse vengono registrati i seguenti dati:

- Utente (nome, indirizzo IP, indirizzo MAC)

I tempi in linea e i volumi di dati trasferiti vengono correlati prima agli indirizzi MAC delle interfacce della rete di computer nella LAN. Dai moduli server DHCP o server DNS, il router può eventualmente avere a disposizione informazioni aggiuntive sulla correlazione di indirizzi MAC e nomi di computer. In questo caso, il tempo in linea può anche essere direttamente correlato al nome del computer. Se una correlazione di indirizzo MAC al nome di computer non è possibile, viene registrata un'altra informazione disponibile per contrassegnare l'utente, ad esempio l'indirizzo IP.

Nel caso di partecipanti della rete che hanno accesso alla LAN tramite un collegamento Dial-In, di solito l'indirizzo MAC non è noto. In questo caso il router genera uno pseudo-indirizzo tramite il quale le controparti Dial-In vengono identificate nell'accounting.

- Controparte con la quale il collegamento è stato stabilito
- Tipo del collegamento  
Collegamento telefonico, fisso o DSL
- Volumi di dati in direzione di trasmissione e di ricezione
- Tempo in linea

Nei collegamenti con chiamate che vengono usati da più utenti in comune, l'intera durata di un collegamento può essere più lunga di

quanto l'utente non la usi effettivamente. Per questo motivo, in questi casi la durata del collegamento viene calcolata sulla base della prima e dell'ultima operazione di un utente più il tempo di tenuta valido per il collegamento.

- Numero dei collegamenti

In questo campo viene visualizzato quante volte l'operazione di un utente ha condotto ad una messa in opera del collegamento.

## 4.12.1

### Configurazione dell'accountings

Le impostazioni per l'accounting si trovano in `/Setup/Accounting`. Lì si può attivare o disattivare l'accounting e si può attivare il salvataggio nella flash-ROM. Qui si può inoltre influenzare l'ordine delle tabella dei totali secondo tempo in linea o volume di dati.

## 4.12.2

### Lettura delle informazioni di accounting

Una visualizzazione dei dati registrati è possibile tramite *ELSA LANmonitor*. In questo caso è anche possibile salvare i dati sotto forma di file su un supporto dati.

Nel caso dell'accesso tramite Telnet, i dati registrati possono essere interrogati anche in `/Setup/Accounting`.

Con i dati relativi a nome utente e controparte vengono elencate le seguenti informazioni:

- Nome utente

Nome dell'utente o il suo indirizzo layer-3 (indirizzo IP, indirizzo IPX o nel servizio Bridge di nuovo l'indirizzo MAC)

- Sito remoto

Controparte con la quale l'utente ha scambiato i dati

- Tipo di collegamento

Tipo del collegamento

- Rx-Bytes, Tx-Bytes

Volumi di dati sull'interfaccia

- Tempo totale

Tempo in linea totale per questo utente e questa controparte

- Connessioni

Numero dei collegamenti contati con questa controparte

*Quando un utente stabilisce un collegamento con un'altra controparte, viene introdotta una nuova registrazione nella tabella. Tutti i volumi di trasferimento e i tempi in linea da un utente ad una controparte vengono registrati in una voce.*

*A seconda dell'ordine della lista, nella tabella vengono registrate le 512 voci con i più grandi volumi di trasferimento o con il più lungo tempo in linea.*



| User  | Password | Type       | Connections | Received | Transmitted | Total Online Time     |
|-------|----------|------------|-------------|----------|-------------|-----------------------|
| CLAF3 | ELSA001  | Setup/STCA | 2           | 228 KB   | 41 KB       | 4 minutes, 47 seconds |

# 5 Appendice

## 5.1 Dati tecnici

| Hardware                  |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connessione WAN           | ISDN-So (BRI), configurazione punto-a-punto e punto-a-più punti, I.430 (autosensing)                                                                                                                                                                                                                                                                                                                                                     |
| Connessione LAN           | <p><i>LANCOM 800 Office</i>: Ethernet IEEE 802.3, 10Base-T</p> <p><i>LANCOM 1000 Office</i>: Ethernet IEEE 802.3, 10Base-T, 10Base-2 (BNC), funzionamento full duplex</p> <p><i>LANCOM 1100 Office</i>: Ethernet IEEE 802.3, 10/100Base-T (RJ45, Node/Hub-Switch), Autosensing, 10Base-2 (BNC), funzionamento full duplex</p> <p><i>LANCOM 2000 Office</i>: Ethernet IEEE 802.3, 10Base-T, 10Base-2 (BNC), funzionamento full duplex</p> |
| CPU/memoria               | CPU RISC a 32 bit (Hitachi SH3), 60 MHz, flash ROM da 2 MB, 4 MB RAM                                                                                                                                                                                                                                                                                                                                                                     |
| Alimentazione elettrica   | 12 VA con alimentatore per 230 V, 12 VA; LANCOM 2000: 24 VA                                                                                                                                                                                                                                                                                                                                                                              |
| Esecuzione e dimensioni   | Involucro metallico stabile, connessioni sul lato posteriore; dimensioni 158 x 40 x 125 mm (L x H x P)                                                                                                                                                                                                                                                                                                                                   |
| Condizioni ambiente       | Temperatura: 5– 40°C, umidità dell'aria: 0– 80%, senza condensa                                                                                                                                                                                                                                                                                                                                                                          |
| Autorizzazioni            | Autorizzazioni CE, Svizzera e tutti i Paesi dell'UE:<br>D800109K, ICT D800110K, EN 50082 (Part 1), EN 55022 (Class B), EN 60950, NET3                                                                                                                                                                                                                                                                                                    |
| Software                  |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Modalità di funzionamento | <p>Router IP, server DHCP, client DHCP, server DNS;</p> <p><i>LANCOM 1000/1100 Office</i> oltre a ciò: Router IPX, proxy NetBIOS, Bridge</p> <p><i>LANCOM 2000 Office</i> oltre a ciò: Router IPX, Bridge, proxy NetBIOS, impianto di telecomunicazione</p>                                                                                                                                                                              |
| Protocolli di rete        | <p>Router IP: ARP, PROXY ARP, IP, ICMP, UDP, TCP, RIP-1, RIP-2, DHCP,</p> <p>Router IPX: IPX, SAP, Novell NetBIOS, Novell Burst Mode</p>                                                                                                                                                                                                                                                                                                 |
| Protocolli ISDN           | <p>Connessione ISDN Bus ISDN-So, configurazione punto-a-punto e punto-a-più punti, I.430 (autosensing)</p> <p>Canale D: DSS1 o 1TR6 (Autosensing), supporto di linea dedicata</p> <p>Canale B: PPP (asincrono/sincrono), X.75, HDLC, MLPPP per raddoppio di canale, CAPI 2.0 tramite <i>LANCAPI</i>, compressione Stac</p>                                                                                                               |
| Gestione della linea      | chiamata di risposta automatica con o senza messa in opera del collegamento: Line-on-Demand, modo Short-Hold dinamico, Channel-on-Demand nel caso di raddoppio di canale, selezione Round-Robin, Fast-Call-Back, commutazione prioritaria programmabile, BACP                                                                                                                                                                            |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telefono<br>(porte a/b)      | solo <i>LANCOM 2000 Office</i> : 4 linee analogiche, RJ11 con adattatore RJ11/RJ11, funzioni ISDN: Chiamate interne, trasferimento di chiamata, conversazione intermedia, messa in attesa, richiamata, conferenza a tre, prelievo di chiamata, impulso di conteggio, chiamata linea esterna impostabile, commutazione prioritaria, chiamata bambini                                                                                                                                                     |
| Funzioni security e firewall | PAP e CHAP, MS-CHAP; meccanismi di autenticazione in PPP; possibilità di filtraggio nel servizio IP ( <i>LANCOM 1000/1100/2000 Office</i> anche nel servizio IPX e Bridge), protezione della configurazione tramite liste di accesso e password, mascheratura IP, Meccanismi di protezione ISDN (CLIP, chiamata di risposta ecc.), Password Protection, Accounting                                                                                                                                      |
| Mascheratura IP (NAT/PAT)    | Conversione indirizzo e porta IP tramite un indirizzo IP; assegnazione statica/dinamica dell'indirizzo IP tramite PPP o DHCP; mascheratura di TCP, UDP, ICMP, FTP; DNS-Forwarding; mascheratura inversa per i servizi IP dall'Intranet come ad esempio Web-Server; mascheratura NetBIOS                                                                                                                                                                                                                 |
| Sicurezza di servizio        | Watchdog hardware, autotest regolari, concetto FirmSafe per aggiornamento remoto del software                                                                                                                                                                                                                                                                                                                                                                                                           |
| Protezione addebiti          | Possibilità di stabilire un limite massimo di scatti o di tempo di collegamento in un determinato intervallo                                                                                                                                                                                                                                                                                                                                                                                            |
| Accounting                   | Salvataggio del numero e della durata dei collegamenti                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Management                   | Configurazione TFTP e aggiornamento del firmware, gestione SNMP via SNMP v.1 o v.2, accessi WAN o LAN attivabili separatamente, emissioni di diagnostica per protocolli e interfacce, tool di diagnostica, visualizzazione dello stato <i>ELSA LANmonitor</i> , <i>LANconfig</i> , configurazione remota tramite ISDN, configurazione tramite HTML, <i>ELSA WebConfig</i> ( <i>LANCOM 1000/1100/2000 Office</i> inoltre interfaccia V.24/V.28 outband (mini DIN a 8 poli))                              |
| <b>Materiale fornito</b>     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Accessori                    | Alimentatore, cavo di collegamento ISDN, due cavi LAN Twisted-Pair, documentazione dettagliata e <i>ELSA LANCOM CD</i><br><i>LANCOM 1000/1100 Office</i> oltre a ciò: cavo per interfaccia outband, presa BNC a T<br><i>LANCOM 2000 Office</i> oltre a ciò: Cavo per interfaccia outband, presa BNC a T, 4 connettori RJ11/RJ11<br>Software: <i>ELSA LANCAPI</i> , <i>ELSA LANtools</i> ( <i>ELSA LANconfig</i> , <i>ELSA LANmonitor</i> per la visualizzazione dello stato), <i>ELSA CAPI Faxmodem</i> |
| Assistenza&supporto          | Tramite hotline e Internet                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



## 5.2

## Dichiarazioni di conformità



## KONFORMITÄTSERKLÄRUNG

## DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

Geräteart: ISDN Router  
 Type of Device:  
 Typenbezeichnung: ELSA LANCOM 800 Office  
 Product Name:  
 EG-Baumusterprübscheinungs Nr.: D800109K  
 Registration No.:  
 Benannte Stelle: CETECOM ICT Services GmbH  
 Notified Body: **CE 0682 X**

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:  
 This is to confirm that this product meets all essential protection requirements relating to the

Niederspannungs Richtlinie (73/23/EEG)  
 Low Voltage Directive (73/23/EEG)  
 ISDN Richtlinie (97/346/EEG)  
 ISDN Directive (97/346/EEG)  
 EMV Richtlinie (89/336/EEG)  
 EMC Directive (89/336/EEG)

Zur Beurteilung der Konformität wurden folgende Normen herangezogen:  
 The assessment of this product has been based on the following standards:

EN 50082-1: 1992  
 EN 50081-1: 1992 Teil / part : EN 55022B: 1994  
 EN 60950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997  
 TBR 3

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:  
 On behalf of the manufacturer / importer:

ELSA AG  
 Sonnenweg 11  
 D-52070 Aachen

abgegeben durch: / this declaration is submitted by:

Aachen, 29. Februar 2000  
 Aachen, 29<sup>th</sup> February 2000

I.V. Stefan Kriebel  
 Bereichsleiter Entwicklung  
 VP Engineering



# KONFORMITÄTSERKLÄRUNG

## DECLARATION OF CONFORMITY

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

Geräteart: ISDN Router  
type of device  
Typenbezeichnung: ELSA LANCOM 1100 Office  
product name  
EG-Baumusterprüfbescheinigungs Nr.: D800109K  
Registration no.:  
Benannte Stelle: CETECOM ICT Services GmbH  
Notified Body: **0682 X**

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:  
This is to confirm that this product meets all essential protection requirements relating to the

Niederspannungs Richtlinie (73/23/EWG)  
Low Voltage Directive (73/23/EEC)  
ISDN Vorschrift (97/346/EG)  
ISDN Directive (97/346/EC)  
EMV Richtlinie (89/336/EWG)  
EMC Directive (89/336/EEC)

Zur Beurteilung der Konformität wurden folgende Normen herangezogen:  
The assessment of this product has been based on the following standards

EN 50082: 1992 Teil 1: EN 61000-4-2, 3, 4, 5, 6  
EN 50081: 1992 Teil 1: EN 55022B: 1994  
EN 60950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997  
TBR 3

Diese Erklärung wird verantwortlich für den Hersteller / Importeur  
On behalf of the manufacturer / importer

ELSA AG  
Sonnenweg 11  
D-52070 Aachen

abgegeben durch: / this declaration is submitted by:

Aachen, 8. Februar 1999  
Aachen, February 8<sup>th</sup> 1999

i.V. Peter Wieninger  
Bereichsleiter Entwicklung  
VP Engineering



# KONFORMITÄTSERKLÄRUNG

## DECLARATION OF CONFORMITY

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

Geräteart: ISDN Router  
Type of Device:  
Typenbezeichnung: ELSA LANCOM 1000/2000 Office  
Product Name:  
EG-Baumusterprüfbescheinigungs Nr.: D800109K  
Registration No.:  
Benannte Stelle: CETECOM ICT Services GmbH  
Notified Body: **CE0682 X**

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:  
This is to confirm that this product meets all essential protection requirements relating to the

Niederspannungs Richtlinie (73/23/EWG)  
Low Voltage Directive (73/23/EEC)  
ISDN Richtlinie (97/346/EWG)  
ISDN Directive (97/346/EEC)  
EMV Richtlinie (89/336/EWG)  
EMC Directive (89/336/EEC)

Zur Beurteilung der Konformität wurden folgende Normen herangezogen:  
The assessment of this product has been based on the following standards:

EN 50082-1: 1992  
EN 50081-1: 1992 Teil 1 / part 1: EN 55022B: 1994  
EN 60950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997  
TBR 3

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:  
On behalf of the manufacturer / importer:

ELSA AG  
Sonnenweg 11  
D-52070 Aachen

abgegeben durch: / this declaration is submitted by:

Aachen, 8. April 1998  
Aachen, 8<sup>th</sup> April 1998

i.V. Peter Wieninger  
Bereichsleiter Entwicklung  
VP Engineering

## 5.3

# Condizioni generali di garanzia

La ELSA AG fornisce questa garanzia dal 01.06.1998 agli acquirenti di prodotti ELSA a loro scelta in aggiunta alle rivendicazioni di legge quando sono soddisfatte le seguenti condizioni:

### 1 Estensione della garanzia

- a) La garanzia si estende all'apparecchio fornito e a tutte le parti. Essa viene fornita nella forma per cui le parti che risultano difettose a causa di difetti di fabbricazione o del materiale, nonostante il dimostrato trattamento corretto e il rispetto delle istruzioni d'uso, a nostra scelta vengono sostituite o riparate senza spese. In alternativa ci riserviamo di sostituire l'apparecchio difettoso con un prodotto aggiornato o di rimborsare all'acquirente il prezzo di acquisto originale dietro restituzione dell'apparecchio difettoso. I manuali e l'event. software in dotazione sono esclusi dalla garanzia.
- b) Le spese per materiali e lavoro sono a nostro carico, ma non le spese di spedizione dall'acquirente all'officina di servizio e/o a noi.
- c) Le parti sostituite diventano di nostra proprietà.
- d) Siamo autorizzati, in occasione della riparazione o della sostituzione, ad apportare le modifiche tecniche (per es. aggiornamento del firmware), per adattare l'apparecchio allo stato attuale della tecnica. Nessun costo aggiuntivo viene addebitato all'acquirente per questo. Non sussiste alcun diritto rivendicabile per questo.

### 2 Periodo di garanzia

Per i prodotti ELSA il periodo di garanzia è di sei anni. Fanno eccezione da ciò i monitor ELSA e i sistemi di videoconferenza ELSA; per i quali il periodo di garanzia è di tre anni. Il periodo di garanzia comincia con il giorno della consegna dell'apparecchio da parte del rivenditore ELSA. Le prestazioni di garanzia non comportano un prolungamento del termine di garanzia e non fanno partire un nuovo termine di garanzia. Il termine di garanzia per le parti incorporate scade con il termine di garanzia per l'apparecchio completo.

### 3 Svoltimento

- a) Se entro il periodo di garanzia compaiono difetti nell'apparecchio, le rivendicazioni di garanzia devono essere contestate immediatamente, comunque non oltre sette giorni.
- b) I danni di trasporto riconoscibili dall'esterno (per es. involucro danneggiato) devono essere contestati immediatamente all'addetto al trasporto e a noi. I danni non riconoscibili dall'esterno devono essere contestati immediatamente per iscritto all'addetto al trasporto e a noi dopo che sono stati scoperti, comunque non oltre sette giorni dalla consegna.
- c) Il trasporto in andata o ritorno al punto dove vengono presentate le rivendicazioni di garanzia e/o l'apparecchio riparato viene sostituito, avviene a rischio e a spese dell'acquirente.
- d) Le rivendicazioni di garanzia vengono prese in considerazione solo se insieme all'apparecchio viene presentata la fattura originale.

### 4 Esclusione della garanzia

In particolare, qualunque rivendicazione di garanzia è esclusa

- a) se l'apparecchio è stato danneggiato o distrutto a causa di forza maggiore o per effetto di circostanze ambientali (umidità, fulmini, polvere e altro);
- b) se l'apparecchio è stato conservato o fatto funzionare in condizioni che non rientrano nelle specifiche tecniche;

- c) se il danno sono stati causati da un trattamento non appropriato – in particolare dalla mancata considerazione della descrizione del sistema del manuale d'uso;
- d) se l'apparecchio è stato aperto, riparato o modificato da persone non da noi autorizzate;
- e) se l'apparecchio presenta danni meccanici di qualsiasi genere;
- f) se vengono riscontrati danni al tubo catodico di un monitor ELSA, in particolare a causa di sollecitazioni meccaniche (spostamento della maschera del tubo catodico a causa di urti o danni al vetro), forti campi magnetici in vicinanza (macchie colorate sullo schermo), visualizzazione permanente della stessa immagine (bruciatura del fosforo);
- g) se la luminanza dell'illuminazione posteriore nei pannelli TFT si riduce progressivamente nel corso del tempo;
- h) se la rivendicazione di garanzia non viene presentata secondo il punto 3a) o 3b).

## 5 Errori di comando

Se si riscontra che il funzionamento difettoso dell'apparecchio è stato causato da hardware o software di provenienza esterna, installazione o impiego difettosi, ci riserviamo di addebitare all'acquirente le spese di controllo.

## 6 Regole supplementari

- a) Le suddette disposizioni regolano in modo conclusivo il rapporto legale verso di noi.
- b) Questa garanzia non copre ulteriori rivendicazioni, e in particolare quelle per variazione o diminuzione. Sono escluse le rivendicazioni per rimborso di danni, indipendentemente dal motivo legale. Questo non si applica se per es. in caso di danni alle persone o di danni a cose di uso privato esiste una responsabilità obbligatoria in base alla legge sulla responsabilità per i prodotti o nei casi di dolo o di grave negligenza.
- c) In particolare sono escluse le rivendicazioni per rimborso di mancati guadagni, danni indiretti o conseguenti.
- d) Non ci assumiamo la responsabilità per la perdita di dati e/o il ripristino di dati in caso di lieve o media negligenza.
- e) Nei casi in cui la perdita di dati è stata da noi causata per dolo o per grave negligenza, rispondiamo per il tipico impegno di ripristino, connesso con copie di sicurezza preparate in modo regolare e commisurato al pericolo.
- f) La garanzia si riferisce solo al primo acquirente e non è trasferibile.
- g) Il foro competente è Aachen, se l'acquirente è un commerciante riconosciuto. Se l'acquirente non ha un foro competente generale nella Repubblica Federale Tedesca o dopo la stipula del contratto trasferisce la propria sede o la residenza abituale fuori dal territorio della Repubblica Federale Tedesca, il foro competente è la nostra sede commerciale. Questo vale anche se la sede o la residenza abituale dell'acquirente non è nota al momento della citazione.
- h) Si applica il diritto della Repubblica Federale Tedesca. Nel rapporto tra noi e l'acquirente non si applica il diritto di acquisto UN.



## 6 Index

|                      |      |
|----------------------|------|
| 10/100Base-TX .....  | 29   |
| 100BASE-T .....      | R-88 |
| 10Base-2 (BNC) ..... | 29   |
| 10Base-T .....       | 29   |
| 1TR6 .....           | R-80 |
| 802.2 .....          | R-90 |
| 802.3 .....          | R-90 |

|                                                |                    |
|------------------------------------------------|--------------------|
| <b>A</b>                                       |                    |
| Abilitazione di file e stampanti .....         | 85                 |
| Access-list .....                              | R-99               |
| Accesso remoto .....                           | 12, 39, 43, 59, 83 |
| Accettare la conversazione .....               | 106                |
| Accettazione .....                             | 110                |
| Accoppiamento LAN-LAN .....                    | 12                 |
| Accounting .....                               | 19                 |
| Adattatore .....                               | 40                 |
| Adattatore per il cavo di configurazione ..... | 21                 |
| Adattatore telefonico .....                    | 104                |
| Addebiti .....                                 | 83                 |
| Addebiti di collegamento ISDN .....            | 61                 |
| address pool .....                             | R-110              |
| address ranges .....                           | R-102              |
| Aging-minute(s) .....                          | R-94, R-96         |
| Alimentatore .....                             | 21                 |
| Ambiente di rete .....                         | 90                 |
| AOCD .....                                     | 15, 61             |
| Apple Talk .....                               | R-3                |
| APPP .....                                     | R-84               |
| ARP cache .....                                | R-100              |
| ARP-aging-minute(s) .....                      | R-100              |
| Assegnazione degli indirizzi .....             | 41                 |
| asynchronous PPP .....                         | R-84               |
| Attesa in linea .....                          | 13, 18, 103        |
| Autenticazione .....                           | 15                 |
| Auth. ....                                     | R-85               |

|                                 |            |
|---------------------------------|------------|
| Authentication .....            | R-15, R-19 |
| auto mode .....                 | R-110      |
| Autorizzazione centralino ..... | 114        |

|                              |            |
|------------------------------|------------|
| <b>B</b>                     |            |
| Backoff .....                | R-93       |
| BACP .....                   | 16         |
| Battuta d'avviso .....       | 105, 117   |
| B-channel protocols .....    | R-83       |
| Binding .....                | R-90       |
| Blocco .....                 | 56         |
| Blocco dei domini .....      | 82         |
| Blocco del login .....       | 56         |
| Boot system .....            | R-122      |
| Bridge                       |            |
| configuration .....          | R-39       |
| filtering data packets ..... | R-40       |
| bridge .....                 | R-39       |
| Broadcast address .....      | R-5        |
| Broadcast transfer .....     | R-8        |
| Brute-Force .....            | 15, 56, 57 |
| Budget temporale .....       | 61         |
| Buffers .....                | R-88       |

|                                         |            |
|-----------------------------------------|------------|
| <b>C</b>                                |            |
| Cable .....                             | R-1        |
| Cable network .....                     | R-4        |
| cache .....                             | R-100      |
| Call charge information .....           | R-21       |
| Call charge units .....                 | R-21       |
| call numbers .....                      | R-86       |
| Callback .....                          | R-81       |
| callback .....                          | R-86, R-88 |
| Callback options .....                  | R-82       |
| Call-by-Call .....                      | 91, 93     |
| call-by-call .....                      | R-117      |
| Calling Line Identification Restriction | R-80       |

|                                    |          |                                          |              |
|------------------------------------|----------|------------------------------------------|--------------|
| Canale B .....                     | 51       | Collegamento remoto .....                | 44           |
| stato del collegamento .....       | 16       | Comando priorità .....                   | 102, 115     |
| Canale D .....                     | 59       | Common ISDN Application                  |              |
| Canali principali .....            | 116      | Programming Interface .....              | 98           |
| Canali secondari .....             | 116      | Commutatore Node/Hub .....               | 29           |
| CAPI Faxmodem .....                | 97       | compatibility .....                      | R-83         |
| Caricamento del software .....     | 46       | Complesso di fornitura .....             | 21           |
| Cavo di configurazione .....       | 21       | Compressione .....                       | 16           |
| Cavo di connessione ISDN .....     | 21       | Compressione dati Stac .....             | 16           |
| cavo di connessione LAN .....      | 21       | Computer .....                           | 78           |
| Cavo ISDN .....                    | 13       | Computer raggiungibili .....             | 90           |
| CBCP .....                         | R-18     | Comunicazione di ufficio .....           | 98           |
| CD .....                           | 21       | Comunicazioni .....                      | 13           |
| Cells .....                        | R-1      | Condivisione .....                       | 87           |
| Challenge Handshake Authentication |          | Conferenza a 3 .....                     | 18, 103, 118 |
| Protocol .....                     | 58, R-85 | Config-aging-minute(s) .....             | R-115        |
| Channel bundling .....             | R-21     | Configurare impianto telefonico .....    | 104          |
| dynamic .....                      | R-21     | Configurare porte a/b e impianto         |              |
| static .....                       | R-21     | telefonico .....                         | 104          |
| channel bundling .....             | R-84     | configuration options .....              | R-114        |
| CHAP .....                         | 58, R-85 | Configurazione .....                     | 14           |
| charge .....                       | R-82     | Procedure .....                          | 39           |
| Charges .....                      | R-95     | SNMP .....                               | 54           |
| charges .....                      | R-90     | Configurazione inband .....              | 39           |
| charging information .....         | R-81     | Configurazione outband .....             | 39, 40       |
| charging unit .....                | R-81     | Configurazione punto-a-più punti .....   | 14           |
| Chiamata bambini .....             | 18       | Configurazione punto-a-punto .....       | 14           |
| Chiamata bambino .....             | 110      | Configurazione remota .....              | 19, 39       |
| Chiamata centralino .....          | 106, 110 | Configurazione WINS .....                | 74           |
| Chiamata di risposta .....         | 57, 59   | Connect .....                            | R-87         |
| Fast Call Back .....               | 60       | connection time-outs .....               | R-81         |
| Chiamata esterna .....             | 103      | Connector .....                          | R-88         |
| Chiamate a telefono mobile .....   | 93       | Connessione impianto .....               | 14           |
| Cifra identificativa di rete ..... | 92       | Connessione in rete .....                | 11           |
| CLI .....                          | 59, R-86 | Connessione LAN .....                    | 13           |
| Client per reti Windows .....      | 85       | Connessione multipla .....               | 14           |
| CLIP .....                         | 15       | Connessione PPP .....                    | 39, 45       |
| CLIR .....                         | R-80     | Connessione router di reti Windows ..... | 82           |
| Collegamento alla linea .....      | 18       | Connessione senza selezione .....        | 121          |
| Collegamento ISDN-S0 .....         | 29       | Connessione WAN .....                    | 14           |



|                                    |             |
|------------------------------------|-------------|
| Connessioni .....                  | 28          |
| Connessioni analogiche .....       | 13, 29      |
| Connessioni fisse .....            | 12          |
| Controllo in arrivo .....          | 57          |
| Controllo ora .....                | 16          |
| Controparti NetBIOS .....          | 83          |
| Conversazione urbana .....         | 94          |
| Conversazioni esterne .....        | 110         |
| Conversazioni internazionali ..... | 92          |
| Conversazioni interne .....        | 13, 18, 103 |
| Conversazioni interurbane .....    | 93          |
| Costi di trasmissione .....        | 18          |
| Costi telefonici elevati .....     | 61          |

## D

|                                     |           |
|-------------------------------------|-----------|
| data compression .....              | R-84      |
| Data compression procedure          |           |
| LZS .....                           | R-21      |
| Data packet .....                   | R-1       |
| data transfer .....                 | R-21      |
| Data transmission in an IPX network | R-24      |
| Dati tecnici .....                  | 127, 129  |
| DDI numbers .....                   | R-83      |
| default route .....                 | R-103     |
| Definizione di nomi e gruppi .....  | 85        |
| destination network .....           | R-101     |
| Destination port .....              | R-104     |
| destination ports .....             | R-103     |
| device names .....                  | R-81      |
| Device-name .....                   | R-81      |
| DHCP .....                          | 70, R-110 |
| DHCP per scomposizione WINS .....   | 74        |
| DHCP server .....                   | R-110     |
| dial prefix .....                   | R-82      |
| Dialup-remote .....                 | R-81      |
| Disconnect .....                    | R-87      |
| Display canali .....                | 51        |
| Display di stato .....              | 16        |
| Disponibilità .....                 | 115       |
| Distance of a route .....           | R-29      |

|                                      |                |
|--------------------------------------|----------------|
| DNS .....                            | 78, R-37, R-99 |
| DNS Forwarding .....                 | R-37           |
| DNS forwarding .....                 | R-100          |
| DNS queries .....                    | R-104          |
| DNS-backup-IP-address .....          | R-100          |
| Documentazione .....                 | 21             |
| Documentazione elettronica .....     | 21             |
| Documentazioni trace .....           | 52             |
| Domain Name Service .....            | 78, R-37       |
| Domini .....                         | 78             |
| Driver fax .....                     | 17, 97         |
| DSS1 .....                           | 14, R-80       |
| Dst-address .....                    | R-105          |
| Dst-netmask .....                    | R-105          |
| Durata della connessione .....       | 16             |
| dynamic assignment of the IP address |                |
| .....                                | R-101          |
| dynamic bundling .....               | R-81           |
| Dynamic channel bundling .....       | R-21           |
| Dynamic Host Configuration Protocol  | 70             |
| dynamic IP routing table .....       | R-107          |
| Dynamic routing .....                | R-28           |
| dynamic short-hold .....             | R-81           |

## E

|                              |          |
|------------------------------|----------|
| ELSA CAPI Faxmodem .....     | 17       |
| ELSA-RVS-COM .....           | 13       |
| ELSA-ZOC .....               | 13       |
| E-mail .....                 | 12       |
| Encaps .....                 | R-83     |
| End-address-pool .....       | R-110    |
| Ethernet .....               | 13, R-83 |
| 10/100Base-T .....           | 14       |
| 10Base-2 .....               | 14       |
| 10Base-T .....               | 14       |
| Fast-Ethernet .....          | 14       |
| Ethernet packet format ..... | R-90     |
| EuroFileTransfer .....       | 11, 17   |
| Exclusion routes .....       | R-30     |
| exponential backoff .....    | R-93     |

● **F**

|                                   |                    |
|-----------------------------------|--------------------|
| Fast Call Back .....              | 60                 |
| fast callback procedure .....     | R-82               |
| Fast-Ethernet .....               | 14                 |
| 10/100Base-T .....                | 14                 |
| Fax .....                         | 11, 13, 17, 18, 97 |
| Faxmodem .....                    | 17                 |
| LANCAPi .....                     | 98                 |
| Filetransfer .....                | 12                 |
| Filtri .....                      | 57                 |
| Filtro IP .....                   | 84                 |
| Firewall .....                    | 15                 |
| firewall function .....           | R-104              |
| FirmSafe .....                    | 15                 |
| Firmsafe .....                    | 46                 |
| firmsafe .....                    | R-121              |
| Firmware .....                    | 15, R-120          |
| Firmware upload                   |                    |
| con LANconfig .....               | 48                 |
| con programma di terminale .....  | 48                 |
| con TFTP .....                    | 49                 |
| firmware upload .....             | R-120              |
| Funzione di richiamata .....      | 15                 |
| Funzione Firewall .....           | 60                 |
| Funzioni di sicurezza .....       | 12                 |
| Funzioni supplementari ISDN ..... | 18                 |
| Funzioni telefono .....           | 13                 |

● **G**

|                               |            |
|-------------------------------|------------|
| Gateway .....                 | 60, 70, 73 |
| Gestione degli addebiti ..... | 60         |
| Gestione della linea .....    | 18         |
| Gestione indirizzi .....      | 70         |
| Gestori di rete .....         | 91         |
| Giorni feriali .....          | 92         |
| Giorni festivi .....          | 92         |
| Group table .....             | R-113      |
| Gruppi di nomi .....          | 82         |
| Gruppo .....                  | 82         |

● **H**

|                                 |       |
|---------------------------------|-------|
| HDLC packets .....              | R-84  |
| HDLC56K .....                   | R-84  |
| HDLC64K .....                   | R-84  |
| hierarchical IP addresses ..... | R-6   |
| Host .....                      | R-1   |
| Host table .....                | R-113 |
| Hyperterminal .....             | 40    |

● **I**

|                                          |                     |
|------------------------------------------|---------------------|
| IANA .....                               | R-5                 |
| ICMP .....                               | R-104, R-106, R-108 |
| Identification .....                     | R-78                |
| Identificativi .....                     | 87                  |
| Identificazione .....                    | 85                  |
| Identificazione del chiamante .....      | 58                  |
| Impianto interno .....                   | 103, 112            |
| Impianto telefonico .....                | 13, 103             |
| Impulso di addebito .....                | 13, 18              |
| Inband .....                             | 39, 41              |
| con Telnet .....                         | 43                  |
| Indirizzi IP .....                       | 17                  |
| Indirizzo finale .....                   | 72                  |
| Indirizzo iniziale .....                 | 72                  |
| Indirizzo IP .....                       | 41, 51, 60          |
| Informazioni di addebito .....           | 15, 18, 61          |
| Informazioni sui nomi .....              | 83                  |
| Installazione .....                      | 13                  |
| Interfacce .....                         | 28                  |
| Interfaccia CAPI .....                   | 98                  |
| Interfaccia di configurazione .....      | 39, 40              |
| Interfaccia di configurazione V.24 ..... | 29                  |
| Interfaccia SO .....                     | 14                  |
| Interfaccia seriale .....                | 39                  |
| Interface .....                          | R-1                 |
| Interface list .....                     | R-79                |
| Internet .....                           | 12, 60, R-3         |
| Internet access .....                    | R-17                |
| Internet address .....                   | R-36                |
| Internetwork .....                       | R-3                 |

- Intranet ..... R-98
  - intranet address ..... R-36
  - Intranet-mask ..... R-98
  - inverse masquerading ..... R-107
  - IP ..... R-106
  - IP address ..... R-16, R-98
  - IP addresses ..... R-4
  - IP broadcast ..... R-106
  - IP header ..... R-106
  - IP masquerading ..... R-35, R-101, R-107
    - simple masquerading ..... R-37
    - supported protocols ..... R-37
  - IP multicast ..... R-106
  - IP network ..... R-3
  - IP routing
    - Filter ..... R-31
    - FTP ..... R-31
    - Telnet ..... R-31
  - IP routing table ..... R-28
  - IP-netmask ..... R-98
  - IP-routing-table ..... R-101
  - IPX ..... R-3
  - IPX routing
    - backoff ..... R-24
    - Binding ..... R-23
    - binding ..... R-24
    - exponential backoff ..... R-26
    - Filter ..... R-26
    - Hops ..... R-25
    - network ..... R-23
    - propagate ..... R-24
    - Propagate loop function ..... R-26
    - remote station ..... R-23
    - RIP and SAP tables ..... R-25
    - Tics ..... R-25
  - IPX routing table ..... R-23
  - IPX watchdogs ..... R-28
  - IPX-router ..... R-89
  - IPX-watchdog ..... R-90
  - ISDN layers ..... R-83
  - ISDN network ..... R-4
  - ISDN time ..... R-45
- **K**
- Key ..... R-15, R-85
- **L**
- LAN ..... R-3, R-8
  - LANCAPI ..... 11, 13, 17, 43, 98, R-116
  - LANCAPI Client ..... 99
  - LANCAPI Server ..... 100
  - LAN-Coll ..... 28
  - LANconfig ..... 30, 39, 41, 42, 43, 48, 50
    - assistenza ..... 42
  - LAN-configuration ..... R-115
  - LAN-filter-table ..... R-94, R-96, R-103
  - Langner openISDN config
    - assistenza ..... 42
  - Language ..... R-115
  - LAN-Link ..... 28
  - LANmonitor ..... 16, 50, 96
  - LAN-Rx ..... 28
  - LAN-Tx ..... 28
  - layer name ..... R-81
  - Layer-name ..... R-83
  - LCP echo reply ..... R-16
  - LCP echo request ..... R-16
  - LCR ..... 15, 61, 92, R-117
  - leased-line connection ..... R-83
  - Least Cost Router
    - Caduta automatica ..... 95
    - Monitoraggio addebiti ..... 95
  - Least-Cost-Router ..... 91, 94
  - Least-cost-router
    - Modalità ..... 95
  - Least-Cost-Routing ..... 61
  - Least-cost-routing ..... 15
  - LED ..... 25
  - Limitare i costi ..... 61
  - Limitazione degli addebiti ..... 60

Limitazione della connessione ..... 61  
 Limitazione della connessione in base  
 al tempo ..... 61  
 Line management ..... 12  
 Linee a selezione ..... 12  
 Lista di accessi IP ..... 41  
 Lista PPP ..... 58  
 Local Area Network ..... R-3  
 local network ..... R-3  
 Local-routing ..... R-91, R-105  
 location ..... R-78  
 Lock-minutes ..... R-115  
 Login ..... 47  
 log-in block ..... R-115  
 Login-errors ..... R-115  
 LOOP-propagate ..... R-92  
 Looser ..... R-82  
 LZS data compression ..... R-21

## M

MAC ..... R-8  
 MAC address ..... R-88  
 MAC addresses ..... R-9  
 MAC protocol ..... R-9  
 Mail Server ..... 81  
 manual connection ..... R-87  
 Mascheratura IP ..... 12, 15, 57, 60  
 Masquerading ..... R-101, R-107  
 masquerading ..... R-98  
 Masquerading table ..... R-108  
 Maximum number of simultaneous  
 connections ..... R-115  
 Meccanismi di filtro ..... 12  
 Meccanismo di forwarding DNS ..... 79  
 Media Access Control ..... R-8  
 Mediazione ..... 13, 18, 103, 119  
 Medium ..... R-1  
 Medium Access Control ..... R-8  
 Memoria flash ROM ..... 46  
 Memoria Flash-ROM ..... 14

Messa in opera del collegamento ..... 83  
 MLPPP ..... 16, R-21  
 Modalità ..... 55  
 Modem ..... 18  
 modem operation ..... R-84  
 Modo automatico ..... 71  
 Modo automatico DHCP ..... 71  
 Multilink PPP ..... R-13, R-21  
 Multipoint cabling ..... R-8  
 Multiprotocol capability ..... R-9

## N

Name ..... R-78  
 name server ..... R-99  
 name verification ..... R-86  
 Name-list ..... R-81  
 Nameserver NetBIOS ..... 83  
 Naming IP Addresses ..... R-23  
 NAT ..... 57, 60, R-35  
 NBNS ..... 83, R-100  
 NBNS-backup ..... R-100  
 Negoziazione PPP ..... 45  
 NetBIOS ..... 18, 79, R-91  
     Accesso remoto ..... 89  
     Accoppiamento LAN-LAN- ..... 88  
     Controparte ..... 88  
     Filtri IP ..... 88  
     Protocollo di rete ..... 84  
     TCP/IP ..... 84  
 NetBIOS name server ..... R-100  
 NetBIOS propagated frames ..... R-92  
 NetBIOS-Proxy ..... 82  
 Netmask ..... R-4  
 NetWare server ..... R-90  
 Network ..... R-1, R-90  
 Network adapter ..... R-1  
 Network address ..... R-4, R-92  
 Network cable ..... R-1  
 network connection ..... R-88  
 Network Information Center ..... R-35

Network protocol ..... R-3  
 Networking Windows ..... 90  
 NIC ..... R-35  
 Node-ID ..... R-89  
 Nome utente ..... 45, 59  
 Nomi ..... 82  
 Nomi dei computer ..... 82  
 Nomi di computer ..... 78  
 Nomi di rete ..... 78  
 Novell ..... R-92  
 NT domain ..... R-112  
 number ..... R-81  
 Number list ..... R-86  
 Numeri speciali ..... 94  
 Numero telefonico di configurazione .46

## O

Operating ..... R-89, R-98, R-101  
 Opzioni ..... 102  
 Ora ..... 92, 96  
 Ora del giorno ..... 92  
 Ora della rete ISDN ..... 96  
 Ora ISDN ..... 16  
 orologio interno ..... 96  
 Other ..... R-122  
 Outband ..... 39, 40  
     presupposti ..... 40

## P

Packet ..... R-1  
 PAP ..... 58, R-85  
 Password ..... 46, 50, 57, 58, 59  
 password ..... R-99  
 Password Authentication Protocol .....  
     ..... 58, R-85  
 Password-required ..... R-115  
 PAT ..... 57, 60, R-35  
 Periodo ..... 61  
 Periodo di validità ..... 71, 74  
 physical medium ..... R-1

Point-to-multipoint connection ..... R-2  
 Point-to-point connection ..... R-2  
 point-to-point protocol ..... R-84  
 Pool di indirizzi ..... 72, 77  
 Port number ..... R-37  
 Porta ..... 101  
 Porta a/b ..... 103  
 Porte a/b ..... 13, 18  
     caratteristiche di servizio ..... 109  
     Configurazione ..... 104  
     connessione router ..... 116  
     descrizione ..... 108  
     numero d'utenza ..... 108  
     numero d'utenza interno ..... 108  
     opzioni ..... 109  
 Porte NetBIOS ..... 84  
 Possibilità di risparmio nelle  
 telefonate ..... 93  
 Power ..... 26  
 PPP ..... 19, 51, 59, R-21, R-84, R-86  
     Assigning IP addresses ..... R-16  
     Callback functions ..... R-17  
     checking the line with LCP ..... R-15  
 PPP Client ..... 39, 43  
 PPP LCP Extensions ..... R-20  
 PPP negotiation ..... R-98  
 Precedenza ..... 115  
 Prefisso ..... 91, 92  
 Presa di chiamata ..... 120  
 Preselezione ..... 91  
 Private address spaces ..... R-5  
 Procedura di sicurezza ..... 58  
 Programma di terminale ..... 40  
 Programma terminale ..... 14  
 Programmi di fax standard ..... 97  
 Prohibited address ranges ..... R-102  
 Propagated Frames ..... R-92  
 Propagated frames ..... R-26  
 protect ..... R-86  
 Protezione addebiti ..... 15

|                               |              |
|-------------------------------|--------------|
| Protezione con password ..... | 15, 56       |
| Protezione di accesso .....   | 15, 57       |
| per nome .....                | 57           |
| per nome o numero .....       | 58           |
| per numero .....              | 57           |
| Protocol .....                | R-3          |
| Protocollo di canale B .....  | 58, 59       |
| Protocollo ELSA .....         | 58           |
| Provider .....                | 91           |
| Provider Internet .....       | 11           |
| Proxy .....                   | 18           |
| proxy ARP .....               | R-101, R-102 |
| Proxy-ARP .....               | R-105        |

## R

|                                        |                           |
|----------------------------------------|---------------------------|
| R1-mask .....                          | R-107                     |
| Raggruppamento canali .....            | 116                       |
| Raggruppamento di canali .....         | 16                        |
| dinamico .....                         | 16                        |
| Statico .....                          | 16                        |
| Raggruppamento di canali dinamico ..   | 16                        |
| Raggruppamento di canali statico ..... | 16                        |
| registered IP address .....            | R-5, R-98                 |
| Regolazione automatica dell'ora .....  | 96                        |
| Remote Access .....                    | R-105                     |
| Remote access .....                    | R-16                      |
| remote access .....                    | R-93                      |
| remote station verifications .....     | R-85                      |
| Remote-table .....                     | R-112                     |
| Reset system .....                     | R-122                     |
| Rete 100Mbit .....                     | 29                        |
| Rete 10Mbit .....                      | 29                        |
| Rete urbana .....                      | 94                        |
| Rete Windows .....                     | 74, 82                    |
| Reti NetBIOS .....                     | 79                        |
| Reti Peer-to-Peer .....                | 18                        |
| Reti TCP/IP .....                      | 78                        |
| Reti Windows .....                     | 18                        |
| Ricerca difetti .....                  | 50                        |
| Ricerche online .....                  | 12                        |
| Richiamata .....                       | 12, 13, 18, 103, 112, 119 |
| riconoscimento del numero telefonico   | 15                        |
| RIP .....                              | R-24, R-106               |
| RIP tables .....                       | R-25                      |
| RIP-SAP-scaling .....                  | R-91                      |
| RIP-type .....                         | R-106                     |
| Risorse abilitate .....                | 87                        |
| Round robin list .....                 | R-82                      |
| round robin list .....                 | R-82                      |
| Round-Robin .....                      | R-83                      |
| Router .....                           | R-1                       |
| Router name .....                      | R-29                      |
| Routes/FRM .....                       | R-94                      |
| Routing .....                          | 83, R-6                   |
| Routing Information Protocol .....     | R-24                      |
| Routing table .....                    | R-6                       |
| IP masquerading .....                  | R-30                      |
| special entries .....                  | R-30                      |
| Routing-table .....                    | R-92                      |

## S

|                                      |                |
|--------------------------------------|----------------|
| SAP .....                            | R-24, R-95     |
| SAP services .....                   | R-96           |
| SAP tables .....                     | R-25           |
| scaling .....                        | R-91           |
| Scope ID .....                       | R-112          |
| Scopes .....                         | 82             |
| Script list .....                    | R-86           |
| script processing .....              | R-84, R-86     |
| security procedure .....             | R-85           |
| Segreteria telefonica .....          | 13             |
| Selezione a impulso .....            | 116            |
| Selezione a tono .....               | 116            |
| semipermanent leased-line connection |                |
| .....                                | R-82           |
| Senza impulsi di conteggio .....     | 61             |
| Server DHCP .....                    | 17, 41, 70, 78 |
| Configurazione .....                 | 75             |
| Server DNS .....                     | 17, 70, 73, 78 |
| Informazioni disponibili .....       | 79             |

- Lista di filtro ..... 81
- Meccanismo di filtro ..... 79
- server information ..... R-95
- Server list ..... R-114
- Server NBNS ..... 70, 73, 74
- Server WINS ..... 83
- Server/FRM ..... R-96
- Service Advertising Protocol ..... R-24
- service information ..... R-96
- Service table ..... R-107
- Servizi online ..... 41
- Servizio ..... 78
- Setup
  - DHCP-module ..... R-110
  - IP-router-module ..... R-101
  - IPX-module ..... R-89
  - LAN-module ..... R-88
  - TCP-IP-module ..... R-97
  - WAN-module ..... R-78
- Setup wizard ..... 40
- Shared Medium ..... R-8
- Shared medium ..... R-3
- Short-hold ..... R-81
- Sicurezza ..... 55, 57, 60
- Single User Access ..... 60
- Smistamento ..... 92
- Smistamento chiamate ..... 13
- Smistamento di chiamata ... 18, 103, 120
- SNAP ..... R-90
- SNMP ..... 54, R-109
- Società telefonica ..... 94
- Socket filter ..... R-27
- Socket-Filter ..... R-91
- Socket-filter ..... R-93
- Software update ..... 14
- Sollevarla la cornetta ..... 111
- Soppressione del numero d'utenza  
..... 110, 123
- Sorveglianza ..... 50
- Source port ..... R-104
- Spare-heap-blocks ..... R-89
- special dialing characters ..... R-81, R-82
- speed ..... R-84
- Spie LED ..... 16
- Split horizon ..... R-26
- Spoofing ..... R-95, R-97
- SPX watchdogs ..... R-28
- SPX-watchdog ..... R-91
- Squillo ..... 107
- Stac ..... R-21, R-84
- Standard 1 ..... 17, 97
- Start-address-pool ..... R-110
- static bundling ..... R-81
- Static channel bundling ..... R-21
- static IP address ..... R-101
- Static routing ..... R-28
- Statistiche ..... 16
- Stato SO ..... 26
- Status ..... R-43
  - Call-info-table . R-73, R-74, R-76, R-77
  - Config-statistics ..... R-70
  - Connection-state ..... R-45
  - Connection-statistics ..... R-71
  - Delete values ..... R-77
  - Info-connection ..... R-72
  - IP-router-statistics ..... R-68
  - IPX-statistics ..... R-57
  - LAN-statistics ..... R-48
  - Layer-connection ..... R-73
  - operating time ..... R-45
  - PPP-statistics ..... R-49
  - Queue-statistics ..... R-70
  - SO-bus ..... R-75
  - TCP-IP-statistics ..... R-62
  - WAN-statistics ..... R-46
- Struttura tariffaria ..... 93
- Subnet ..... R-6
- Suppresses the outgoing MSN ..... R-80
- System-administrator ..... R-109
- System-location ..... R-109

● **T**

|                            |                   |
|----------------------------|-------------------|
| Tabella LCR .....          | 92                |
| Table-ARP .....            | R-100             |
| Table-RIP .....            | R-93, R-107       |
| Table-SAP .....            | R-95              |
| Tariffa urbana .....       | 94                |
| Tariffe .....              | 91                |
| Tasto Flash .....          | 112               |
| Tasto R .....              | 112               |
| TCP .....                  | R-104, R-108      |
| TCP max. connections ..... | R-100             |
| TCP/IP .....               | 30, 41, R-3, R-28 |
| TCP/IP stack .....         | R-3               |
| TCP-aging-minute(s) .....  | R-100             |
| Telefono .....             | 13, 18            |
| Telefono mobile .....      | 93                |
| Telelavoro .....           | 12                |
| telephone company .....    | R-117             |
| teleworkers .....          | R-105             |
| Telix .....                | 40                |
| Telnet .....               | 14, 35, 43        |
| Telnet server .....        | R-99              |
| Tempo online .....         | 19                |
| Tentativi di login .....   | 56                |
| Terminali analogici .....  | 18, 103           |
| Terminali digitali .....   | 103               |
| TFTP .....                 | 41                |
| TFTP server .....          | R-99              |
| throughput .....           | R-21              |
| Time .....                 | R-45, R-85        |
| time .....                 | R-119             |
| Time-out .....             | R-21              |
| Timeout .....              | R-111             |
| Tipo di accesso .....      | 87                |
| TOS .....                  | R-106             |
| Trace                      |                   |
| avvio .....                | 52                |
| chiave e parametri .....   | 52                |
| esempi .....               | 54                |
| Trap-IP .....              | R-109             |

|                           |       |
|---------------------------|-------|
| Traps-active .....        | R-109 |
| Trasmissione di fax ..... | 98    |
| trunk seizure .....       | R-82  |
| Type of Service .....     | R-38  |
| Type-of-service .....     | R-106 |

● **U**

|                           |              |
|---------------------------|--------------|
| UDP .....                 | R-104, R-108 |
| Ufficio a casa .....      | 12           |
| Unità .....               | 61           |
| Upload .....              | 15, 47       |
| Upload del firmware ..... | 47           |
| Upload-system .....       | R-122        |
| User name .....           | R-15         |
| Username .....            | R-85         |

● **V**

|                                |        |
|--------------------------------|--------|
| Velocità di trasmissione ..... | 16, 51 |
| verification attempt .....     | R-85   |
| Version-table .....            | R-120  |
| Volume di dati .....           | 19     |

● **W**

|                               |                   |
|-------------------------------|-------------------|
| WAN-Chan1 .....               | 27                |
| WAN-Chan2 .....               | 27                |
| WAN-configuration .....       | R-115             |
| WAN-filter-table .....        | R-94, R-96, R-104 |
| WAN-update-minute(s) .....    | R-95, R-97        |
| watchdog .....                | R-90              |
| Watchdogs .....               | R-28              |
| Wildcard .....                | 81                |
| Windows Internet Name Service |                   |
| Server .....                  | 83                |
| winipcfg .....                | 32, 34            |
| Wireless links .....          | R-1               |
| WWW .....                     | 60                |

● **X**

|                            |      |
|----------------------------|------|
| X.75 data protection ..... | R-84 |
| X.75 secured format .....  | R-84 |



● **Y**

Y connection ..... R-21

Y connections ..... R-80

● **Z**

Zona tariffaria ..... 93





# Technical basics

This chapter is a short introduction into the technology used by your device. Network professionals will find themselves just skimming these pages, but novices will find this section to be very helpful for understanding the technical terms and processes.

## Network technology



*This section will give you a brief introduction to the basics of network technology. These descriptions do **not** cover all possible techniques, processes and terms associated with network technology. They only cover the topic to the degree necessary to provide an understanding of the product information.*

### The network and its components

*Network,  
transmission  
medium,  
interfaces*

Whenever several computers communicate with one another, this connection is called a network. For computers to be able to communicate, they need a physical medium through which the information can be transmitted. This can be a cable or radio link, for example, that is connected to the computers using special interfaces (e.g. network adapters).



*The term network cable (or simply cable) in the following text also refers to any other physical medium that can take on the function of the cable, such as wireless links.*

*Packets  
Cells*

The individual bits of electronic information that are sent from one computer to another through a medium are called packets or cells, depending on the process.



*For most of the following explanations, the difference between packets and cells is irrelevant. Therefore, we will use the term packet or data packet in a general sense and only detail the special characteristics of cells as necessary.*

*Host*

The computer and other terminal devices (e.g. the printer) in a network that generate or process information are called hosts. Ideally, a host is not responsible for the task of forwarding information. A host normally has exactly one interface to the network.

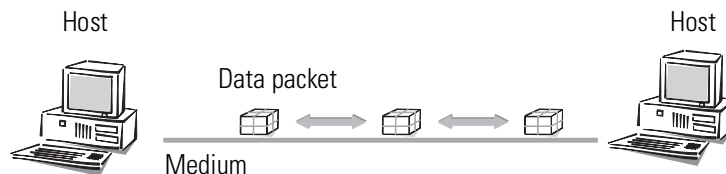
*Router*

The transport of packets between two hosts occurs indirectly through exchanges that pass packets on to the target computer. These exchanges are called routers. A router has at least two interfaces so that it can receive the data from a sender and pass them on to a recipient. Apart from the exchange function, the router also has the properties of a host so that it can also be the recipient of data packets, for configuration purposes for example.

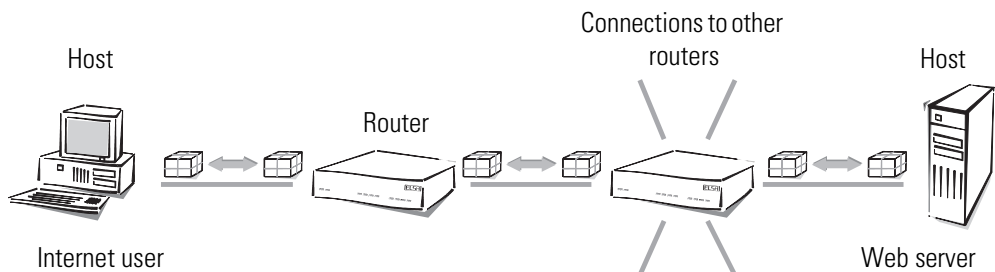
## Connection modes

### *Point-to-point connection*

The connection of exactly two hosts via a medium is called a “point-to-point connection”. In this case a host sends packets that can only be received by **one** specific recipient (unambiguous connection).



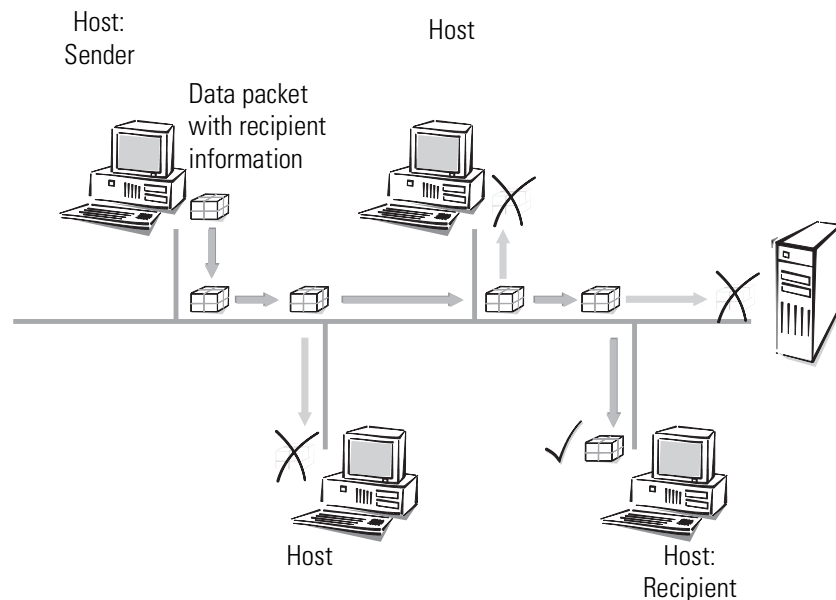
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers will only forward the data packets to one recipient. That's why we also call this connection unambiguous.



*Strictly speaking, the term “point-to-point connection” is not quite correct. For our purposes though, it is sufficient to distinguish this kind of connection from the following “point-to-multipoint connections”.*

### *Point-to-multipoint connection*

Generally speaking, it would be uneconomical to directly connect all computers in a network via point-to-point connection cables, as the computers would then require multiple interfaces. Computers in a network are therefore plugged into a joint medium shared by all hosts. The sender simply sends its packet with instructions concerning the recipient to the medium to which other hosts are connected. The data packet arrives at **every** host in the network. Each host then decides whether it is the recipient of the packet or not. If the packet is addressed to the corresponding host, it will then accept it. If not, the host will ignore (reject) it. This is a “point-to-multipoint connection”, since we are not dealing with an unambiguous connection.



## Kinds of networks

|                                  |                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Protocol</i>                  | An important prerequisite for communications between computers is a common language among the hosts. In the world of network technology this language is called "network protocol" or simply "protocol".                                                                                                                                                                       |
| <i>TCP/IP</i>                    | The most broadly distributed network protocol is the TCP/IP ( <b>T</b> ransmission <b>C</b> ontrol <b>P</b> rotocol/ <b>I</b> nternet <b>P</b> rotocol). It is used mainly in the Internet, but nowadays more and more company networks use it. Examples of other network protocols are IPX or Apple Talk. Because of its wide use, this chapter deals mainly with the TCP/IP. |
| <i>IP network</i>                | All hosts wanting to communicate using the TCP/IP protocol have to be plugged into the same network and have to have the TCP/IP protocol (also known as TCP/IP stack) installed. Such a network is referred to as an IP network.                                                                                                                                               |
| <i>Internetwork<br/>Internet</i> | The connection of multiple networks based on the IP protocol is referred to as an internetwork. The largest union of many small, public IP networks is the Internet.                                                                                                                                                                                                           |
| <i>Local network<br/>(LAN)</i>   | A network covering a limited area with hosts on the same hierarchical level and using the same medium (shared medium) is called a local network ( <b>L</b> ocal <b>A</b> rea <b>N</b> etwork, LAN).                                                                                                                                                                            |

## IP addressing

|                                 |                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Packet-oriented transfer</i> | In IP networks the communication between computers takes place in a packet-oriented fashion. This means that data or messages are packed together in packets of variable length and are as such sent from the source computer to the target computer. Apart from |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

the actual information to be transmitted (useful data), the data packet also contains address and control information.

#### IP address

IP addresses are used in IP networks for communications between various devices. In this case, every host has its own unique address by which it can be identified unambiguously. What does an IP address look like? It consists of four bytes separated by dots, making a total of 32 bits. Each of the four bytes can take on values from 0 to 255, e.g. 192.168.130.124.



*To be precise, the IP address refers to the interface, and not the host itself. A terminal device with more than one interface (such as a router) has to have an IP address at its disposal for every single interface. This is why ISDN routers from ELSA for example, have an IP address for communication with the hosts in their own network, as well as a second IP address for communication with the "outside world" using the ISDN. In the same way, ELSA cable modems have an IP address for their own network and another IP address for the exchange of data with the cable network.*

#### Network address

An IP address contains the address of the network as well as that of the host. The network address is the same for all hosts on one network, whereas the address of the host is exclusive and unique to the network. A router, for example, can have more than one IP address, each one unique to the network.

#### Netmask

How then can you differentiate between the part that determines the network and the part that identifies the host? With the netmask. You know what masks are: they cover up one part of something and only allow a different part to be visible. This is exactly how a netmask operates. It is a number which is identical in structure to the IP address, i.e. 32 zeros or ones. The netmask usually starts with ones at the beginning and ends with zeros. The zeros at the end thus cover the part of the IP address which does not belong to the network address.

Examples:

| This address... | ...in bytes...  | ...looks like this in bits:         |
|-----------------|-----------------|-------------------------------------|
| IP address      | 192.168.120.253 | 11000000.10101000.01111000.11111101 |
| Netmask         | 255.255.255.0   | 11111111.11111111.11111111.00000000 |
| Network address | 192.168.120.0   | 11000000.10101000.01111000.00000000 |

The same IP address, this time with another netmask:

| This address... | ...in bytes...  | ...looks like this in bits:         |
|-----------------|-----------------|-------------------------------------|
| IP address      | 192.168.120.253 | 11000000.10101000.01111000.11111101 |
| Netmask         | 255.255.0.0     | 11111111.11111111.00000000.00000000 |
| Network address | 192.168.0.0     | 11000000.10101000.00000000.00000000 |

You can see from this that an IP address alone is not enough. A host can only be identified unambiguously in combination with a netmask.

And you can also see that there are more bits available to identify the individual hosts in a connected network if there are fewer bits in a netmask that contain a one. While only 254 different addresses could be allocated in the first example with the netmask 255.255.255.0, the second example has as many as  $254 \times 254 = 64516$  different addresses available! The first and the last digit of an address space are reserved for the network address and the broadcast address (addresses for packets to all hosts in an IP network). In the netmask 255.255.255.0 this is the '0' for the network address and the '255' for the broadcast address.

A new notation of the netmask simply attaches the number of bits available for the network address to the IP address: 137.226.4.101/24. The number after the slash tells us that the first 24 bits indicate the network address. This notation reduces the length of the entries in the routing tables.

#### IP address management

The IP addresses must be unique within a specific network in order to avoid confusion. Since the Internet is based on TCP/IP and thus uses IP addresses for its millions of connected computers, all Internet addresses must also be unique. Bodies exist that manage and distribute these publicly-accessible addresses. Since the number of IP addresses theoretically available is limited, these distributing bodies charge high rates for the addresses.

#### Private address spaces

A range of IP addresses are reserved for use free of charge (private address spaces) so that companies do not have to purchase individual IP addresses for every workstation. In a closed network, these addresses can be used as desired, in a private network or company, for example. The same address can be used in other closed networks (e.g. in different companies), but the addresses within one network must be unique.

However, these reserved IP addresses must **not** be made public (on the Internet). Only **those** devices in a network that are connected to a public network (e.g. the router at the interface to the Internet) must have a registered IP address.

The allocation of IP addresses by the IANA (**I**nternet **A**ssigned **N**umbers **A**uthority) permits the following address ranges to be used for private use:

| IP address  | Netmask     | Remark                                                                                                                                                                                                                                     |
|-------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.0.0.0    | 255.0.0.0   | "10" networks: All IP addresses beginning with 10. and whose mask begins with 255. belong to the address range reserved for private use.                                                                                                   |
| 172.16.0.0  | 255.240.0.0 | All IP addresses beginning with 172.16.–172.31. which are associated with a net mask greater than or equal to 255.240.0.0 are within the address range reserved for private networks.                                                      |
| 192.168.0.0 | 255.255.0.0 | All IP addresses beginning with 192.168. and whose mask begins with 255.255. belong to the address range reserved for private use.                                                                                                         |
| 224.0.0.0   | 224.0.0.0   | All IP addresses beginning with a 224 which are associated with a net mask also beginning with 224 are within the reserved address range.<br>This range is reserved for broadcasting purposes and should not be used for private networks. |

There are two considerations when using these IP addresses:

- The IP addresses used in a private network should not leave this network, i.e. an Internet connection is only possible when using IP masquerading, for example.
- The packets for these IP addresses will not be routed in the Internet, i.e. backbone routers will simply reject such IP packets. Depending on the provider, serious consequences may result if such IP packets are released on the Internet.

## **IP routing and hierarchical IP addressing**

### *Routing*

Every IP packet contains the IP addresses of the source and of the recipient. A router receives IP packets at its interface, interprets the destination address and passes the packets on to those interfaces that are nearest to the recipient. Finding the appropriate path is called routing.

### *Routing-table*

Every router manages a table (routing table). This table indicates the quickest interface connection to the host for every host in the network. You can imagine that, as they grow, these tables may exceed the capacity of the router—the Internet, as a worldwide linking up of publicly accessible IP computers contains several millions of hosts.

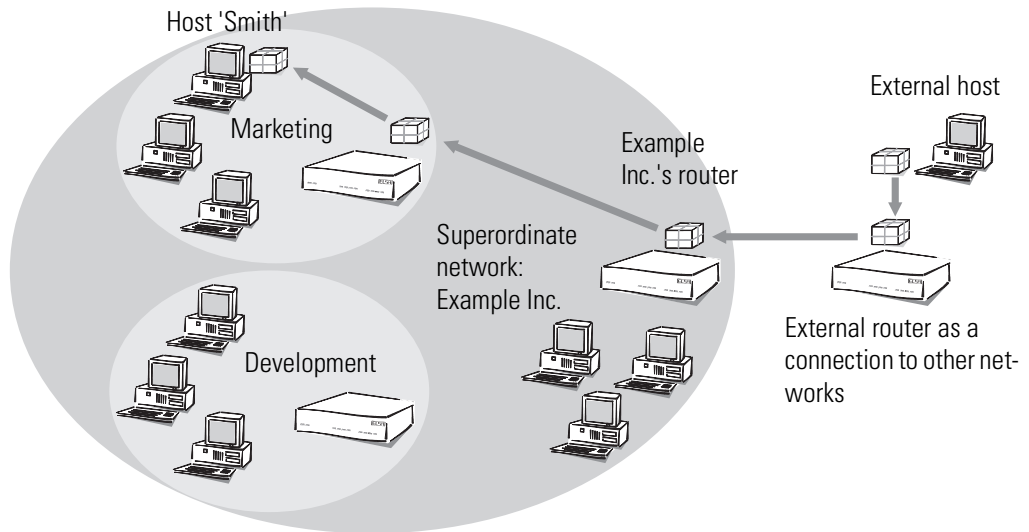
### *Hierarchical IP addresses*

For this reason, hierarchical IP addresses were introduced. This means dividing the IP network into subnets in which IP addresses are appointed from a coherent numerical range. It is possible to establish several hierarchy levels, so that different subnets can be merged. The principle is similar to the hierarchical address used by paper mail, consisting of a country, a city, a street and a number.

The consequences of this hierarchical IP addressing:

- Since all hosts within one network have the same network address, the host address is sufficient for the hosts within this network to communicate with one another.
- A router has to know both the addresses of the hosts that are directly connected to it, and the addresses of all networks and subnets that are reachable via adjacent routers.
- It is **not** necessary for a router to know **all** other possible IP addresses.





As an example, think of a company with one large network, in which the different divisions are incorporated as small subnets. The address of the network for the marketing division is made up hierarchically from the address of the company and that of the department.

Whenever a host external to the company network sends a packet to a host in the Example Inc., this is what happens:

- ① The sender gives the packet the destination address "host 'Smith' – Marketing – Example Inc.".
- ② All an external router that establishes the connections to other networks has to know is how to reach Example Inc. As soon as it receives a packet with the address for Example Inc., it passes the packet on to the router responsible for Example Inc.
- ③ The router at Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division.
- ④ The router in the marketing division receives the packet and extracts from the address the information that it is directed at the marketing division of Example Inc. Since it is itself part of this division, it takes a closer look at the address to find the name of the host. It then passes the packet on to the host of the employee Sam 'Smith'.

Now we shall take a look at the example using proper IP addresses instead of symbolic names. The network of Example Inc. has the numerical space '192.168.100.0' to '192.168.100.255' at its disposal, with the '0' for the network address and the '255' for the sender address.

All the router has to remember is that every address beginning with '192.168.100' is located within the network of Example Inc.

Now imagine a router that is connected to the network of Example Inc. through an interface. If it receives a packet with destination address '192.168.100.4' and netmask '255.255.255.0', it will compare this with every network address it knows. In doing so it carries out a logical AND with the netmask, and compares the results with the network address: '192.168.100.4' AND '255.255.255.0' is '192.168.100.0'. This is the network address of the Example Inc. network. The router recognizes that the recipient is located within Example Inc. and passes the packet on to the appropriate interface for Example Inc. Within Example Inc. the packet is then passed on to the appropriate subnet.

The same procedure is used for the transfer of IP packets within a network:

- ① If a host in the subnet of the development department wants to send a data packet to Mr. 'Smith', the sender attaches the destination address "Host 'Smith' – Marketing – Example Inc.".
- ② The router in the development division receives the packet and extracts from the address the information that it is directed at the marketing division of Example Inc. Since it is itself part of Example Inc., but not of the marketing division, it passes the packet on to the router in the superordinate network.
- ③ The router at the Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division, where the packet is passed on to the recipient.

## Expansion through local networks

*Media access control*

Up to now we have only considered the point-to-point connections. However, many computer networks are based on multipoint cabling such as Ethernet. All computers connected to the same network can then receive the signals of all other computers (so-called broadcast transfer to a shared medium). If several computers are sending simultaneously, the superimposed signals are destroyed. A variety of access methods such as CSMA/CD or Token Ring are implemented in the MAC layer (**M**edia **A**ccess **C**ontrol, MAC) for the avoidance and resolution of such collisions.

*LAN and IP network*

The connection of all computers communicating through a shared medium using a MAC protocol is called a LAN. A LAN forms an independent network and is subordinate to the IP network, i.e. IP networks can use the physical connections of the LAN to establish connections between the hosts and the routers. LAN refers to a limitation of the area covered by the network, not a restriction of the number of workstations connected to it.

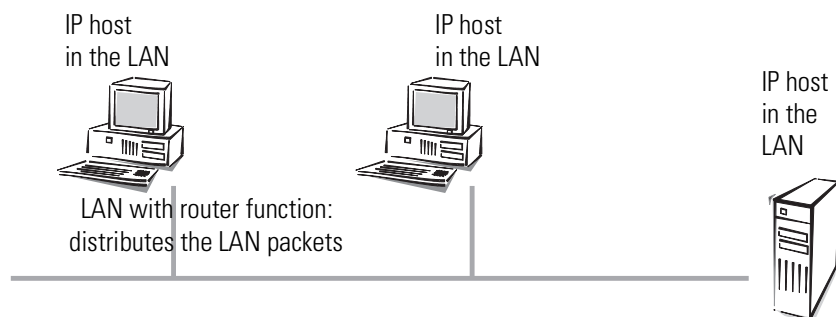
*MAC address* Specific LAN addresses hardwired into the interfaces by their manufacturers are used to manage the transfer in the LAN. Since the LAN addresses are used for communication via the MAC protocol, they are called MAC addresses. They can be thought of as the fingerprint of the interface hardware. MAC addresses can look like this, for example: 00-80-C7-6D-A4-6E.

MAC addresses are independent of IP addresses. An IP host whose interface works through a LAN has an IP and a MAC address. Whereas the structure of IP addresses with its similarity to postal addresses is supposed to simplify routing in enormous IP networks, the fingerprint-like MAC addresses are designed to make the connection to a LAN as easy as possible.

Transfer in LAN is also packet-oriented. Every MAC packet contains the MAC addresses of the source and of the recipient. Although every packet is received by all computers, it is processed only by the target computer. There is an additional MAC broadcast address that is processed by all computers in the LAN.

*IP in the LAN* Every LAN packet contains an entry with the type of the network protocol. An IP packet can be transferred through a LAN by packing it in a LAN packet and adding the 'IP' protocol type to it. Because of the IP entry, the LAN interface at the receiving host recognizes that the LAN packet contains an IP packet, extracts it and processes it as an ordinary IP packet. In this way, IP packets and packets of other network protocols like IPX can be transferred simultaneously through the same LAN without conflicts (this is why a LAN is called multiprotocol-capable).

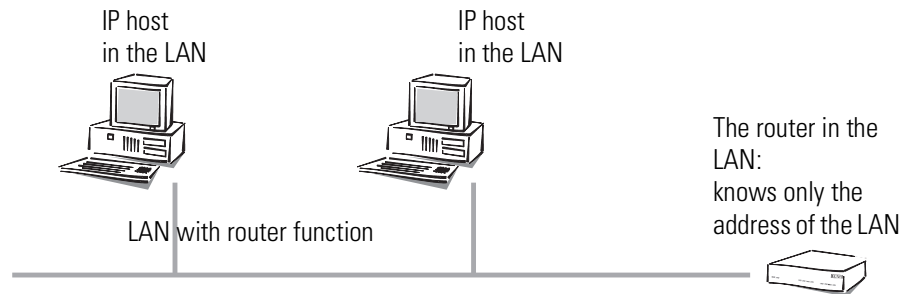
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts gives the packets to the LAN which handles the further distribution of the data packets. This is why only IP addresses from the numerical space of the specific network should be used for the internal communication of the hosts in a LAN through the IP protocol.



To a router in the LAN, a host in its own LAN seems to be located behind another router. So the task for the router is very simple: all it has to know for operating in the IP network are the IP addresses

- of the directly connected hosts and
- of the available networks and subnets,

i.e. all it has to remember is the network address and the netmask of the subnet in the LAN.



In contrast, the host is confronted with a more difficult task than the router. In case of an interface with a point-to-point cable, the host knows that all packets that it sends through the interface automatically arrive at its router, for example. In case of the point-to-multipoint connection to the LAN, it has to distinguish two cases, however.

- A packet with an address outside the LAN is passed on to a router in the LAN that takes care of the further processing of the packet.
- The sending host must send a packet with an address within the LAN directly to the target host, since the router in the network does not know the addresses of all the different hosts.

### **Data transfer within the LAN**

Let's use an example to explain this. Imagine the hosts of the subnet in the marketing division are linked via a LAN. The hosts have IP addresses from the numerical space '137.226.4.1' to '137.226.4.254' (the addresses '137.226.4.0' and '137.226.4.255' are reserved), the network address is '137.226.4.0' and the netmask is '255.255.255.0'. A router connected to the LAN provides access to the wide world of the Internet. Its LAN interface has the IP address '137.226.4.1' and the MAC address '00-80-C7-6D-A4-6E'.

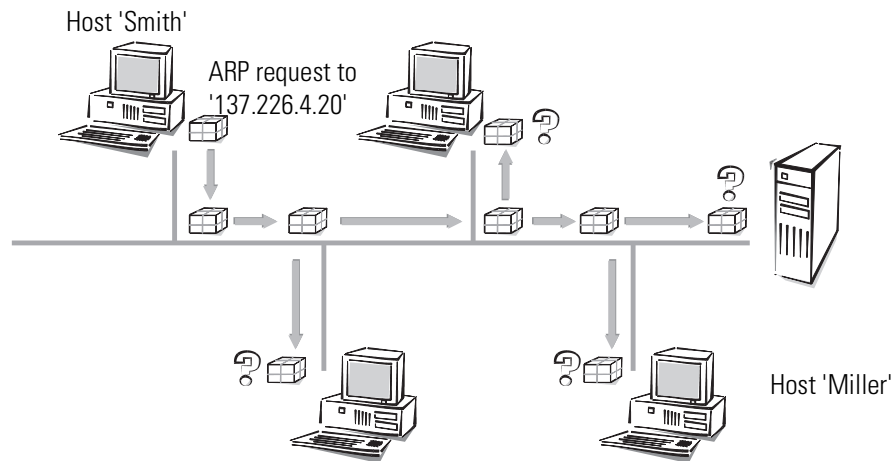
Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). Using the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located in the own network. It therefore has to send the packet through the LAN, directly to host 'Miller'. Unfortunately the LAN interface cannot say: "Send the IP packet to IP address 137.226.4.20", because the LAN interface only understands MAC addresses.

This is why every host has to manage a table that translates IP addresses to MAC addresses. But how do the entries end up in the table? They could be entered manually, but that would not satisfy the objective of making the connection of a new computer to the LAN as easy as possible.

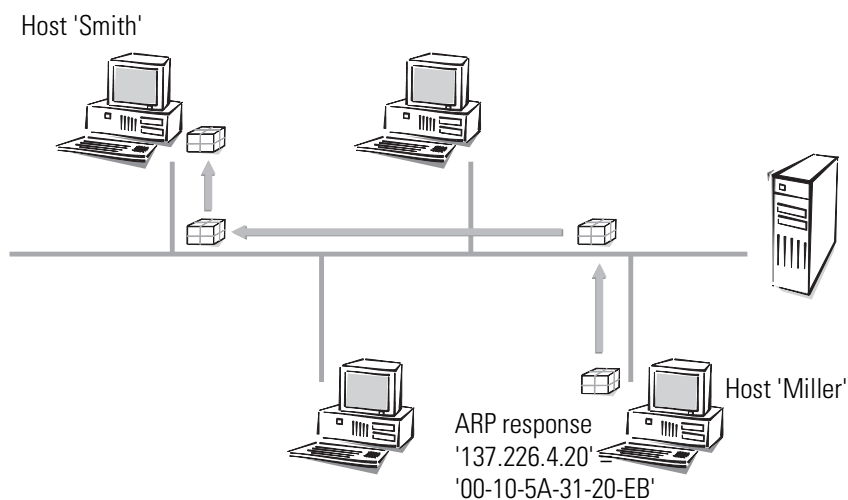
*ARP*

Therefore the LAN has a special mechanism that automates this process: the **A**ddress **R**esolution **P**rotocol, ARP. The table itself is called the ARP table. Whenever a host does

not find an entry in the table for a particular IP address (in our example '137.226.4.20'), it sends an ARP request packet to all hosts in the LAN (with the LAN broadcast address as a target address).



This ARP request packet is simply a question to all hosts listening to the IP address '137.226.4.20'. Host 'Miller' receives the packet, feels addressed and answers with an ARP response packet that it sends directly to host 'Smith' (the MAC address '00-10-5A-31-20-DF' of host 'Smith' is extracted from the sender field in the ARP request packet). Host 'Smith' recognizes this as an answer to its request, extracts the MAC address '00-10-5A-31-20-EB' from the ARP response packet and enters it into its ARP table.



Then it can finally turn to its original task: sending the IP packet to host 'Miller'. It now finds the entry "IP address 137.226.4.20 corresponding to MAC address '00-10-5A-31-20-

EB'' in the ARP table and tells its LAN interface: "Send this IP packet to the computer with the MAC address '00-10-5A-31-20-EB'".

### **Data transfer from the LAN onto the Internet**

Imagine the second task, sending an IP packet from host 'Smith' to the remote host 'External' with IP address 151.189.12.43. Host 'Smith' compares the IP address with its network address and realizes that host 'External' is located outside the LAN. So host 'External' can only be reached through the router. Host 'Smith' finds out the MAC address of the router '00-80-C7-6D-A4-6E' by looking up the router's IP address in the ARP table (if necessary another ARP request is made). So host 'Smith' tells its LAN interface: "Send this IP packet to the computer with the LAN address '00-80-C7-6D-A4-6E'". The router extracts the IP packet from the LAN packet and finds out about the IP address of host 'External'. In the routing table the router then looks for the network address of this host and thus finds the interface through which to pass on the IP packet.

### **LAN coupling on MAC basis**

You know how LANs simplify the connection of computers to a local network. Nearly all house networks are thus LAN based. In some cases a LAN is covers such a large area that the physical characteristics of the cable prohibit the connection of any more computers. This results in the necessity to couple up several LANs in such a way that electrically and in terms of the MAC protocol they act as independent LANs, but for the IP protocol look like one big LAN.

This coupling of LANs is carried out using bridges. A bridge works somewhat like a router, but uses only MAC addresses for routing, not IP addresses. Since MAC addresses do not give any information on the structure of the network the way IP addresses do, every bridge has to know all MAC addresses in the entire LAN.

And so we encounter the same problem that we had with the routers before the introduction of subnets: As the LAN expands, it will at some point exceed the capacity of the address tables of the bridges. So one cannot use bridges to connect an infinite number of LANs. On the other hand, the unstructured MAC addresses allow the bridges to learn automatically about the location of computers in the network, using the received packets. This is called an "intelligent bridge".

## **Point-to-point protocol**

ELSA routers also support the Point-to-Point Protocol (PPP). PPP is a generic term for a whole series of WAN protocols which enable the interaction of routers made by different manufacturers since this protocol is supported by practically all manufacturers.

Due to the increasing importance of this protocol family and the fact that PPP is not associated with any specific operating mode of the routers, we will be introducing the functions of the devices associated with the PPP here in a separate section.

## The protocol

### What is PPP?

The point-to-point protocol was developed specifically for network connections via serial channels and has asserted itself as the standard for connections between routers. It implements the following functions:

- Password protection according to PAP or CHAP
- Callback functions
- Negotiation of the network protocol to be used over the connection established (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP/IPX addresses. This process is carried out using IPCP and IPXCP (IP Control Protocol and IPX Control Protocol).
- Verification of the connection through the LCP (Link Control Protocol)
- Channel bundling (Multilink PPP)

PPP is the standard used by router connections for communication between devices or the WAN connection software of different manufacturers. Connection parameters are negotiated and a common denominator is agreed using standardized control protocols (LCP, IPCP, IPXCP, CCP) which are contained in PPP, in order to ensure successful data transfer where possible.

### What is PPP used for?

It is best to use the point-to-point protocol in the following applications:

- for reasons of compatibility when communicating with external routers, for example
- remote access from remote workstation computers with ISDN adapters
- Internet access (when sending addresses)

PPP as implemented in the *ELSA MicroLink Cable* can be used synchronously or asynchronously and over both a transparent HDLC connection and an X.75 connection.

### The phases of PPP negotiation

Establishment of a connection using PPP always begins with a negotiation of the parameters to be used for the connection. This negotiation is carried out in four phases which should be understood for the sake of configuration and troubleshooting.

- Establish phase

Once a connection has been made at the data communication level, negotiation of the connection parameters begins through the LCP.

This ascertains whether the remote station is also ready to use PPP, and the packet sizes and authentication protocol (PAP, CHAP or none) are determined. The LCP then switches to the opened state.

- Authenticate phase

Passwords will then be exchanged, if necessary. The password will only be sent once if PAP is being used for the authentication process. An encrypted password will be sent periodically at adjustable intervals if CHAP is being used.

There may also be negotiation on a callback using CBCP (Callback Control Protocol) during this phase.

- Network phase

The IPCP and IPXCP protocols have been implemented in the *ELSA MicroLink Cable*.

The IPCP and/or IPXCP network layers can be established following a successful transfer of the password.

IP and/or IPS packets can be transferred from the router modules to the opened line if the negotiation of parameters is successful for at least one of the network layers.

- Terminate phase

In the final phase the line is cleared, when the logical connections for all protocols are cleared.

### **PPP negotiation in the *ELSA MicroLink Cable***

The progress of a PPP negotiation is logged in the devices' PPP statistics and the protocol packets listed in detail there can be used for checking purposes in the event of an error.

The PPP trace outputs offer a further method of analysis. You can use the command

```
trace + ppp
```

to begin output of the PPP protocol frames exchanged during a terminal session. You can perform a detailed analysis once the connection has been broken if this terminal session has been logged in a log file.

### **The PPP list**

You can specify a custom definition of the PPP negotiation for each of the remote stations that contact your net. The PPP list can be found in the *ELSA LANconfig* in the 'Communication' configuration section on the 'Protocols' tab, or in the `/Setup/WAN-module/PPP-list` menu.



The PPP may have up to 64 entries, containing the following values:

| In this column of the PPP list... | ...enter the following values:                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote site                       | Name the remote station uses to identify itself to your router                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Auth.                             | Security method used on the PPP connection ('PAP', 'CHAP' or 'none'). Your own router demands that the remote station observes this procedure. Not the other way round. This means that 'PAP' or 'CHAP' security is not useful when connecting to Internet service providers, who may not wish to provide a password. Select 'none' as the security attribute for connections such as these.                                                                                              |
| Password                          | Password transferred by your router to the remote station (if demanded).<br>A string of asterisks (*) in the list indicates that an entry is present.                                                                                                                                                                                                                                                                                                                                     |
| Time                              | Time between two checks of the connection with LCP. This is specified in multiple of 10 seconds (i.e. 2 for 20 seconds, for instance).<br>Simultaneously the time between two checks of the connection according to CHAP. This time is entered in minutes.<br>The time must be set to '0' for remote stations using Windows 95, Windows 98 or Windows NT.                                                                                                                                 |
| Retries                           | Number of retries for the check attempt. You can eliminate the effect of short-term line interference by selecting multiple retries. The connection will only be dropped if all attempts are unsuccessful. The time interval between two retries is 1/10 of the time interval between two checks.<br>Simultaneously the number of the "Configure requests" that the router maximum sends before it assumes a line error and clears the connection itself.                                 |
| Conf, Fail, Term                  | These parameters are used to affect the way in which PPP is implemented. The parameters are defined in RFC 1661 and are not described in greater detail here. You will find troubleshooting instructions in this RFC in connection with the router's PPP statistics if you are unable to establish any PPP connections. The default settings should generally suffice.<br>These parameters can only be modified via SNMP or TFTP (using the <i>ELSA LANconfig</i> configuration program)! |
| Username                          | The name with which your router logs onto the remote station. The device name of your router is used if nothing is specified here.                                                                                                                                                                                                                                                                                                                                                        |
| Rights                            | Network protocols to be routed over this connection: IP, IPX, NTB (NetBIOS). NetBIOS always requires one of the other two protocols.                                                                                                                                                                                                                                                                                                                                                      |

## Everything ok? Checking the line with LCP

The devices involved in the establishment of a connection through PPP negotiate a common behavior during data transfer. For example, they first decide whether a

connection can be made at all using the security procedure, names and passwords specified.

The reliability of the line can be constantly monitored using the LCP once the connection has been established. This is achieved within the protocol by the LCP echo request and the associated LCP echo reply. The LCP echo request is a query in the form of a data packet which is transferred to the remote station along with the data. The connection is reliable and stable if a valid response to this request for information is returned (LCP echo reply). This request is repeated at defined intervals so that the connection can be continually monitored.

What happens when there is no reply? First a few retries will be initiated to exclude the possibility of any short-term line interference. The line will be dropped and an alternative route sought if all the retries remain unanswered. This may be found in the form of a backup line, for example.



*We recommend that you switch off regular LCP queries in the case of remote access from individual workstation computers using Windows 95, Windows 98 or Windows NT since these operating systems do not respond to LCP echo requests.*

The LCP request behavior is configured in the PPP list for each individual connection. The intervals at which LCP requests should be made are set by the entries in the 'Time' and 'Retries' fields, along with the number of retries that should be initiated without a response before the line can be considered faulty. LCP requests can be switched off entirely by setting the time at '0' and the retries at '0'.

## **Assigning IP addresses via PPP**

In order to connect computers using TCP/IP as the network protocol, all participating computers require a valid and unique IP address. In the event that a remote station does not have an IP address of its own (e.g. an individual computer belonging to a teleworker), the *ELSA MicroLink Cable* can assign an IP address for the duration of the connection to permit communications.

This mode of assigning addresses is run during the PPP negotiation and is used only for connections over the WAN. The assignment of addresses via DHCP, on the other hand, is used only within the LAN.



*Assignment of an IP address will only be possible if the ELSA MicroLink Cable can identify the remote sites by its call number or name when the call arrives, i.e. the authentication process has been successful.*

- For example: Remote access

Address assignment is made possible by a special entry in the IP routing table. 255.255.255.255 is specified as the network mask as the IP address to be assigned to the remote station in the 'Router' field. In this case the router name is the name

the remote station uses to identify itself to the *ELSA MicroLink Cable*.

In this configuration, the addresses of the DNS and NBNS servers (Domain Name Server and NetBIOS Name Server), including those of the backup servers based on the entries in the TCP/IP module are sent to the remote station in addition to the IP address.

For the whole thing to work it follows that the remote station should be configured to take the IP address and the name servers (DNS and NBNS) from the *ELSA MicroLink Cable*. This can be done under Windows Dial-Up Networking, for example, using the 'TCP-settings' under 'IP-address' or 'DNS-configuration'. Enable the 'Server-assigned IP-address' and 'Server-assigned name server addresses' options.

■ For example: Internet access

The assignment of IP addresses can take place the other way round if the *ELSA MicroLink Cable* is used to provide access to the Internet for a local area network. In this case it is possible to configure the *ELSA MicroLink Cable* so that it has no valid Internet IP address of its own but has one assigned to it by the Internet provider for the duration of the connection. The *ELSA MicroLink Cable* also receives information on DNS servers at the provider in addition to the IP address during PPP negotiation.

The *ELSA MicroLink Cable* is only known by its internally valid intranet address on the local area network. This means that all workstation computers on the local area network can access the same Internet account and reach the same DNS server, for example.

Windows users can view the assigned addresses in the *LANmonitor*. In addition to the name of the remote station, the current IP address as well as the addresses of DNS and NBNS servers can be found there. Options such as channel bundling or the duration of the connection are also displayed.



*The ELSA LANmonitor is generally installed automatically during the installation of the ELSA LANconfig. Its description can be found in the 'Configuration modes' chapter in the 'What's happening on the line?' section.*

## Callback functions

In addition to callback via the D channel and via the ELSA protocol, the *ELSA MicroLink Cable* also supports callback via CBCP as specified by Microsoft and via PPP in accordance with RFC 1570 (PPP LCP extensions). There is also the option of a particularly fast callback using a process developed by ELSA.

PCs running Windows 95, Windows 98 or Windows NT can only be called back through the CBCP. The following values have been made available to you in the name list for the

callback entry so that additional call number verification is also possible on the *ELSA MicroLink Cable*:

| This entry is used to...                                   | ...to set the callback so that:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Off                                                        | No callback occurs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Auto (not Windows 95, Windows 98 or Windows NT, see below) | If the remote station is found in the number list, it will be called back. The call is initially rejected and the return call placed as soon as the channel is free (approx. 8 seconds later). If the remote station is not found in the number list, the call is initially accepted as the DEFAULT remote station and the callback is negotiated during the callback protocol negotiation. A charge of one unit is incurred for this.                                                                                                                      |
| Name                                                       | A protocol negotiation is always performed before the return call is placed, even if the remote station is found on the number list (e.g. for computers using Windows that have dialed into the device). A charge of one unit is incurred for this.                                                                                                                                                                                                                                                                                                         |
| ELSA                                                       | If the remote station is found in the number list, a fast callback is performed; i.e. the <i>ELSA MicroLink Cable</i> sends a special signal to the remote station and returns the call immediately once the channel is free. The connection is established in approx. 2 seconds. If the remote station does not cancel the call immediately upon receiving the signal, a fallback to the standard callback procedure is performed after 2 seconds (duration of call establishment approx. 8 seconds). This process is only available for DSS1 connections. |
| Looser                                                     | Use the 'Looser' option if a return call is being expected by the remote station. This setting simultaneously fulfills two tasks. It ensures that the call establishment is canceled locally for incoming calls from a remote station just called, as well as enabling the response to the fast-callback process. In other words, to take advantage of the fast callback, the caller must be in 'Looser' mode, while the station being called must be set to the 'ELSA'.                                                                                    |



*Greatest security is offered by the 'Name' setting if an entry exists in both the number list and the PPP list. The 'ELSA' setting ensures the fastest callback method between two ELSA routers.*

*The 'Name' setting **must** be selected for Windows remote stations.*

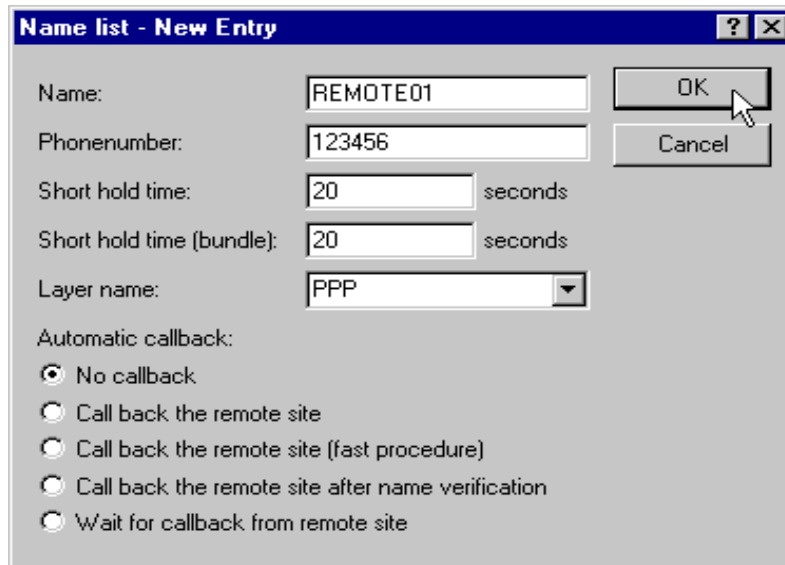
### Microsoft CBCP callback

Microsoft CBCP provides a number of options to determine callback numbers:

- The party called does not call back.
- The party called allows the caller to specify the callback number itself.
- The party called knows the callback numbers and **only** calls these back.

It is possible to use the CBCP from a PC running Windows 95, Windows 98 or Windows NT to establish a connection to the *ELSA MicroLink Cable* have it call you back.

The callback entry and the call numbers entry in the name list are used to select these three possible settings.



The dialog box titled "Name list - New Entry" contains the following fields and options:

- Name:** Text box containing "REMOTE01".
- Phonenumber:** Text box containing "123456".
- Short hold time:** Text box containing "20" followed by "seconds".
- Short hold time (bundle):** Text box containing "20" followed by "seconds".
- Layer name:** Dropdown menu showing "PPP".
- Automatic callback:** A group of five radio buttons:
  - ☒ No callback
  - ☐ Call back the remote site
  - ☐ Call back the remote site (fast procedure)
  - ☐ Call back the remote site after name verification
  - ☐ Wait for callback from remote site

Buttons for "OK" and "Cancel" are located on the right side.

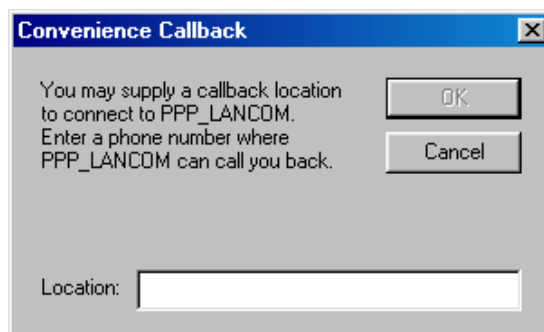
### No callback

For this setting, the callback entry must be set to 'Off' during configuration with a terminal program or via telnet.

### Choose select callback number

The remote station is called back after the name has been verified. The callback entry must have the value 'Name' for this setting and **no** call number may be specified in the name list.

Following the authentication process, the dialog box below will appear in Windows 95 in which the user can specify his call number:



The dialog box titled "Convenience Callback" contains the following text and fields:

You may supply a callback location to connect to PPP\_LANCOM.  
Enter a phone number where PPP\_LANCOM can call you back.

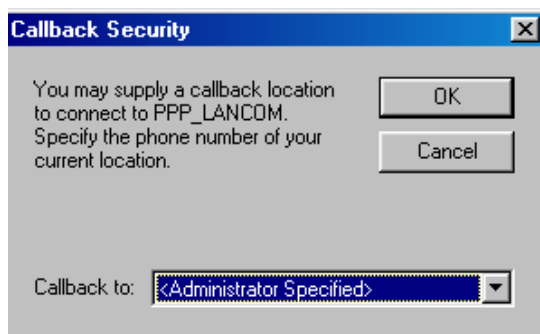
Buttons for "OK" and "Cancel" are located on the right side.

**Location:** Text box for entering a phone number.

### Callback number specified by the *ELSA MicroLink Cable*

The remote station is called back after the name has been verified. The callback entry of the appropriate remote station must have the value 'Name' for this setting and **one** call number must be specified in the name list.

Following the authentication process, the message below will appear in Windows 95 which the user can only confirm:



Callback to a Windows 95, Windows 98 or Windows NT workstation is initiated approximately 15 seconds after the connection is dropped. This delay is specified by Windows and cannot be shortened.

### Fast *ELSA* callback

This fast, *ELSA*-specific process is ideal if two *ELSA MicroLink Cable* are to communicate with one another via callback.

- The caller who would like to be called back sets 'Wait for callback from remote site' in the name list ('Looser' when configuring via a terminal program or Telnet).
- The return caller selects 'Call back the remote site (fast procedure)' in the name list and sets the number ('ELSA').

### Callback as specified in RFC 1570 (PPP LCP extensions)

There are five methods of demanding a callback specified in RFC 1570. All versions are accepted by the *ELSA MicroLink Cable*. All versions will be processed in the same way, however:

The *ELSA MicroLink Cable* drops the connection to the remote station after authentication and then calls it back three seconds later.

## Channel bundling with MLPPP

If you are establishing an ISDN connection to a party supporting PPP you can really speed up your data: You can compress the data and/or use several B channels for the transfer (channel bundling).

Connections using channel bundling differ from "normal" connections inasmuch as they use not only one, but several B channels in parallel for transmitting the data.

MLPPP (Multilink PPP) is used for channel bundling. Of course, this procedure is only available if PPP is being used as the B-channel protocol. MLPPP is ideal, for example, for accessing the Internet via a provider which also supports MLPPP on its dial-up nodes.

### ■ Static channel bundling

If a connection is established with static channel bundling, the router tries to establish the number of B channels specified as 'Minimum' in the channel list. Either the channels specified in the channel list or random free channels are used.

### ■ Dynamic channel bundling

In the case of dynamic channel bundling, the router initially establishes the number of B channels specified as 'Minimum' in the channel list and starts the data transfer. If the router determines that the throughput stays above a certain threshold for a given period of time, it will attempt to add further channels until the number specified as 'Maximum' in the channel list has been reached. Either the channels specified in the channel list or random free channels are also used in this case.

If the dynamic channels are established and the data throughput rate drops below the threshold value, the router waits for the set B2 timeout period and then automatically closes the channels again. Any partly used call charge units are used up fully if call charge information is transmitted during the connection. Therefore, the router only uses the dynamic channels if and as long as it really needs them.

## How to configure channel bundling

Three settings are required to configure a channel-bundled connection:

- ④ Create an entry in the name list for the connection to be established with channel bundling. Select a layer which has set the bundling in the layer-2 options.
  - **compr.** When using the LZS data compression procedure (Stac), the data volume is reduced provided it was not already compressed before. This process is also supported by routers from other manufacturers and by ISDN adapters under Windows operating systems.
  - **bundle** uses several B channels per connection. The channel bundling method is determined by the configuration of the layer 2 options in the layer list, the timeouts in the names list, the setting for the Y connection in the interface table and the setting for the channel table.

- **bnd+compr** uses both compression and channel bundling and therefore provides maximum possible transmission performance.
- ⑤ Enter the holding times for this connection in the name list as well. Please observe the following rules:
- Depending on the application, the B1 holding time should be long enough to ensure that the connection is not prematurely terminated by the brief absence of data packets. Experience has shown that values between 60 and 180 seconds are a good basis which can be adapted as required during operation.
  - The B2 hold time determines the delay time after which the dynamic channels are terminated once the data throughput drops below the threshold value.
- ⑥ Use the channel list to determine the number of channels to be used for the connection. You may also specify the channels to be used, thus keeping certain channels free for dial-up connections via RAS, for example.

The channel list entry determines whether static or dynamic channel bundling will be used (see above). More than one minimum channel results in static bundling, whereas a difference between the minimum and maximum number of channels permits dynamic channel bundling.

- ⑦ Use the entry for the Y connection in the interface list to determine what should happen if an additional connection to a different remote station is requested during an existing connection using channel bundling, but no further B channels are available.
- Y connection **On**: The router interrupts the bundled connection on this interface to establish a connection to the other remote station. When the channel is free again, the originally bundled connection automatically takes the channel back (always in the case of static bundling, only as required when using dynamic bundling).
  - Y connection **Off**: The router holds the existing bundled connection on this interface, the other connection must try a different interface or wait if none of the interfaces with active channel bundling permit a channel to be terminated.

## IPX routing

The IPX router transmits data from networks using IPX/SPX as the network protocols (e.g. Novell networks). A remote network is notified to the computers in the local network by its entry in the IPX routing table. A maximum of 16 different networks can be entered in the routing table.



## Naming IPX addresses

A complete IPX network address comprises three parts: A network number, the MAC address of the network adapter and the socket number.

- The network number can be freely selected. It must, however, be unique on all the addressable IPX networks to ensure correct assignment.
- The MAC address is burnt into each network component. A different address is only used inside the network in special cases.
- An IPX network uses the socket numbers to address a specific service on a computer rather than just the computer itself. Socket numbers identify the various services uniquely.

## Information about the LAN

Several separate LANs required at one location do not necessarily need to have their own cabling. Different logical networks can share one cable. They use different formats for the Ethernet packets to ensure that the data belonging to the various networks does not clash and that one network remains invisible to the others. These formats are determined by the binding belonging to a unique network number on this cable.

You must provide the router with the network number and the binding associated with it to ensure that it too now knows which network it belongs to. If we leave the network address at the default setting '00000000', the router provides the address and the binding itself. It does this by searching on the attached cable for the network from which it receives the most SAP replies.

## IPX routing table

Use the IPX routing table to determine which remote stations (i.e. which other routers or computers) can be reached by the local network and to give it some parameters for connection purposes. The table, which can hold up to 16 entries has the following structure:

| Remote site | Network  | Binding | Propagated | Backoff |
|-------------|----------|---------|------------|---------|
| BRANCH01    | 00000245 | 802.3   | Route      | On      |
| BRANCH02    | 00000320 | SNAP    | Filt.      | On      |
| HEAD OFFICE | 00000420 | 802.2   | Filt.      | Off     |

- Remote site:  
The name of the remote station registered as the device name in the corresponding router on the remote side.
- Network:

The address of the WAN. This is not the address of the destination network, but a third address which represents the network between the two networks to be connected. Thus the following applies:

LAN address 1  $\neq$  WAN address 1 = WAN address 2  $\neq$  LAN address 2  $\neq$  LAN addr.1

■ Binding:

This is where you set which Ethernet binding is to be used on the WAN. This entry is only effective if the layer for this connection supports Ethernet encapsulation. 802.3 is assumed if the entry is missing.

■ Propagated:

A filter for type 20 IPX packets (NetBIOS propagated frames). The Network Basic Input/Output System was originally developed for IBM, and has since also been used by Microsoft in a modified form. This protocol provides services such as name resolution, data protection and correct packet sequencing (secure protocol) in layers 3 and 4 of the OSI model. NetBIOS packets have a special packet type and socket (propagated packets). NetBIOS is primarily used to exchange data between stations on a local network (LAN).

These IPX packets can be excluded from transmission or routed using the 'Filter' property. The 'Route' property transmits the packets if a connection to the remote station concerned is active or a free channel is available for the establishment of an additional connection. The propagated frames are rejected if all the lines to other remote stations are busy.

■ Backoff:

The IPX router uses a special algorithm (exponential backoff) to keep the connection costs arising in the case of erroneous configurations as low as possible.

The backoff function should be switched off if there is no server available on the remote station network (e.g. in the case of remote access from a workstation) (see also exponential backoff).

The default setting is 'On'.

## **What happens when data is transmitted on an IPX network?**

When a device logs on to an IPX network, it first sends a request for the Service Advertising Protocol (SAP) and locates the nearest available server (get nearest server request) in the network numbered '00000000'. A router or server located on this network responds to this request and sends the correct network number.

The servers also regularly transmit information regarding which services they offer and which other networks they can reach. They use the special data packets complying with the Service Advertising Protocol or the Routing Information Protocol (RIP).

Once the IPX router is fully configured and is ready for operation, it proceeds to establish connections to all remote stations which can be reached via the routing tables and then exchanges SAP and RIP information with these networks. The router saves this data to its internal SAP and RIP tables.

## **RIP and SAP tables**

RIP and SAP information is sorted alphabetically in the relevant tables. RIPs are thus only ordered by network and SAPs by service type first, then by server name.

The RIP and SAP tables are updated with each new RIP or SAP packet. The router only incorporates in its table SAP information for which it also has a corresponding RIP entry to ensure that only those services are offered (SAP) which can also be reached (RIP). The entries on the tables indicate, in addition to the information on reachable routes and services, how many routers the path to the destination (hops) passes through or how much time a data packet needs in the destination network (tics = approx. 1/18 of a second), for instance. The router selects the path with the fewest tics and the lowest hop count from the tables and stores only this route if the RIP information offers several different routes to a destination network, for instance.

RIP tables can hold 64 entries and SAP tables 128. If each new packet updates the tables, it stands to reason that the old entries must also disappear at some stage. Entries are artificially aged to do this. The age of all entries on RIP/SAP tables derived from local data transfers is incremented by 1 point every 60 seconds. A new RIP or SAP packet for an entry resets the age to zero. The route or service can be designated unreachable (down) once a selectable age of between 1 and 60 is reached. The entry is deleted when this elapsed time doubles. Additionally, any RIP and SAP information related to this remote station is deleted from the tables and replaced with new information when a connection is established.

## **So many routers around here...**

If the establishment of simultaneous network connections to a greater number of remote stations is required than the number of B channels available, then it's time for a second (third...) router. The same entries are made in the routing tables for all routers to ensure that the brothers function in perfect harmony with each other and that the network really can always find a contact. The same routing information is then sent in the RIP packets to each router, albeit with a higher tic and hop count (`Setup/IPX-module/LAN-config/RIP-SAP-scal . activate`). This marks these routes as a sort of stand-by in the event that all channels are busy on the device addressed.

## **Redundant routes**

A router receiving information in a RIP packet relating to routes with the same tic and hop counts as its own routes (redundant routes) does not, of course, have to reannounce

these routes itself to the sender. Therefore, it only sends these routes to the routers which did not propagate the route. This procedure is known as a "split horizon".

The Propagate loop (`Setup/IPX-module/LAN-Config/LOOP-Prop.`) can be used if it is nevertheless necessary to notify redundant routes to the local network. The routes learned in this way are then flagged in the RIP table with 'LOOP'. Although the propagation of redundant routes is not prohibited by the Novell specification, it should still be avoided as much as possible. Therefore, the default setting is 'Off'.

## Exponential backoff

When switched on, the unit's IPX router attempts to establish suitable connections to receive routing information (RIP and SAP information) required for operation from the remote IPX stations. If this is not possible, due perhaps to a faulty configuration of the IPX router, the exponential backoff algorithm prevents connections constantly being established and thus saves charges.

The router will attempt to reach a remote station again with ever increasing wait times if the first attempt is unsuccessful. The wait time for this is determined as follows:

- The first attempt takes place after  $10 + x$  seconds.  $x$  being a number from 0 to 10.
- The second attempt will be made  $10 + x$  seconds after the first attempt has failed.  $x$  now standing for a number from 0 to 20 seconds.
- The higher value for  $x$  will now be doubled with each repeated attempt. The router finally gives up after the 16th unsuccessful attempt. The continual increase in the wait time means that 16 attempts will take a maximum of one day.

The route will be blocked if all attempts to call the remote station are unsuccessful. You can then only make further attempts at connection by amending the entry in the routing table.



*The time to the next attempt and the number of attempts to establish a connection can be found in the network statistics using (`Status/IPX-module/IPX-router/Networks`).*

## IPX packet filters

The entries in the routing table determine which other networks will be accessible. However, they are then also accessible for data packets which are not actually required in the network of the remote station. These packets can also lead to unwanted connections being established which cost money.

Suitable filters are therefore required. These enable you to exclude from transmission over the WAN or at least restrict data packets which are only used in internal network communications, for example:

- Propagated frames

These special data packets use protocols which cannot in fact be routed. This data is encapsulated in normal IPX packets and sent as broadcast so that they can nevertheless participate in common routing.

These packets are sometimes not desirable in routing. For this reason, you can specify explicitly whether this type of packet is to be routed or filtered.

#### ■ Socket filter

Every packet in an IPX network contains destination and source sockets along with destination and source addresses. Sockets identify the processes for which the data in the packet is intended.

There is a filter table each for sockets from local and remote networks containing the filters which can be used to exclude individual or entire groups of destination sockets. Certain sockets which are known frequently to be the cause of unwanted connections have already been entered in the socket filter table as default settings.

#### ■ RIP and SAP information

A router uses the RIPs to inform the other routers of all the routes (paths to the other networks) known to it using the split horizon principle. This includes the entries from its own routing table and all routes which the router has derived from other routers. It gets its information for this purpose from routers on both local and remote networks. The router enters all available routing information in its internal RIP table.

The servers offer their services in the SAP information. The various services are represented within the SAP information as numbers. Each service (e.g. file server or print server) has a unique number. The router incorporates the information on the services available in its internal SAP table and registers which service is available on which network at which MAC address. At the same time it also establishes whether the service offered is located in a local or remote network and whether it can propagate the service without first establishing a connection.



*You can look at the RIP and SAP tables and their current values in the IPX module (setup/IPX-module/RIP-config or SAP-config) of the router.*

RIP and SAP information are extremely important for devices communicating on a network, which is why there are various different options for setting up the transmission of these packets.

- A LAN and WAN filter table can be used to tell the router not to include information on routes to particular networks or on certain available services in internal or external tables. The affected routes are thus not used, information on them is not provided and the services are not offered in the local network.
- RIP and SAP packets are always transmitted, i.e. no filters are used. These packets, however, must occupy a part of the connection.

- RIP and SAP packets will only be sent if the information they contain has been modified in some way.
- RIPs and SAPs can be transferred at regular, selectable intervals. Information is usually sent out in one minute intervals. The time interval between blocks can be stretched to up to 60 minutes.
- The most economical handling of RIP and SAP packets involves transmitting the information only once, when a connection is established.

■ IPX and SPX watchdogs:

These data packets are used by the server to determine whether workstation computers, for example, are still active or if they can be logged off. To ensure that these "Are you there?" packets for computers on a remote network do not continually result in connections being established, you can set the responses to these requests as follows:

- IPX watchdogs receive no response. The computers are logged off after a time specified on the server.
- IPX and SPX watchdogs can be responded to locally. This procedure is known as spoofing. The router responds in place of the computers addressed, which are then never logged off. It is also recommended that a time is set on the server after which the devices in question are always logged off.
- IPX and SPX watchdogs may of course be routed as normal but this frequently results in a connection being established.



*Further information on IPX, the IPX router and the associated parameters can be found in chapter 'Setup/IPX-module' in the reference manual.*

## **IP routing**

An IP router works between networks which use TCP/IP as the network protocol. This only allows data transmissions to destination addresses entered in the routing table. This chapter explains the structure of the IP routing table of an ELSA router, as well as the additional functions available to support IP routing.

### **The IP routing table**

Use the IP routing table to tell the router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a "route" since it is used to describe the path of the data packet. This procedure is also called "static routing" since you make these entries yourself and they remain unchanged until you either change or delete them yourself. Naturally, there is "dynamic routing", too. The routers use the routes in this way to exchange data between themselves and continually update it automatically. The static

routing table can hold up to 64 entries, the dynamic table can hold 128. The IP router looks at both tables when the IP RIP is activated.

You also use the IP routing table to tell the router the length of this route's path so that it can select the most suitable route in conjunction with IP RIP where there are several routes to the same destination. The default setting for the distance to another router is 2, i.e. the router can be reached directly. All devices which can be reached locally, such as other routers in the same LAN or workstation computers connected via Proxy ARP are entered with the distance 0. The "quality level" of this route will be reduced if the entry addressed has a higher distance (up to 14). "Unfavorable" routes like this will only be used if no other route to the remote station in question can be found.

The routing table can be found in the *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Routing' tab, or in the `/Setup/IP-router-module/IP-routing-table` menu. This, then, is how an IP routing table might look:

| IP address    | Netmask       | Router          | Dis-<br>tance | Mask.  |
|---------------|---------------|-----------------|---------------|--------|
| 192.168.120.0 | 255.255.255.0 | GLASGOW         | 2             | On     |
| 192.168.125.0 | 255.255.255.0 | LONDON          | 3             | Off    |
| 192.168.130.0 | 255.255.255.0 | 191.168.140.123 | 0             | Static |

What do the various entries on the list mean?

#### ■ IP addresses and Network

This is the address of the destination network to which data packets may be sent and its associated network mask. The router uses the network mask and the destination IP address of the incoming data packets to check whether the packet belongs to the destination network in question.

#### ■ Router

The router transmits the appropriate data packets to the IP address and network mask to this remote station. A name is entered at this point if the remote station is a router in another network or an individual workstation computer. This is where the IP address of another router which knows the path to the destination network is entered if the router on the network cannot address the remote station itself.

#### ■ Distance

Number of routers between your own and the destination router. This value is often equated with the cost of the transmission and used to distinguish between inexpensive and expensive call paths for wide-area connections. The distance values entered are propagated as follows:

- All networks which can be reached while a connection is established to a destination network are propagated with a distance of 1.

- All non-connected networks are propagated with the distance entered in the routing table (but with a minimum distance of 2) as long as a free transmitting channel is still available.
- The remaining networks are propagated with a distance of 16 (= unreachable) if there are no longer any channels available.
- Remote stations connected using Proxy ARP are an exception to this. These "Proxy hosts" are not propagated at all.

#### ■ Mask.

Use the 'Masquerade' option in the routing table to inform the router which IP addresses to use when transferring the packets.

- 'Off': No masquerading.
- 'On': This entry requests a random IP address valid in the Internet from your provider which is then used for the connection and masquerading.
- 'stat.': Use this entry to request the assignment of a specific IP address from your provider as entered in the 'TCP/IP' configuration section on the 'General' tab or in the /Setup/TCP-IP-module menu. This address will be used for the connection and masquerading.

For further information see the 'IP Masquerading' section.

#### ■ Following entries have a special meaning:

- IP address 255.255.255.255 with a network mask of 0.0.0.0: This is the default route. Any data packets which cannot be routed by other routing entries are transmitted to the remote station listed here.
- Network mask 255.255.255.255: Entries with completed network masks frequently only identify individual workstation computers (remote access) and not actual networks. A network which is only visible by a single IP address using IP masquerading may sometimes be concealed behind this.
- Router name 0.0.0.0: Exclusion routes. Data packets for this "zero route" are rejected and are not routed any further. This is how routes which are forbidden on the Internet (private address spaces, e.g. 10.0.0.0), for example, are excluded from transmission.

Examples with explanatory notes:

| IP address    | Netmask         | Router        | Dist. | This is what happens:                                                                     |
|---------------|-----------------|---------------|-------|-------------------------------------------------------------------------------------------|
| 192.168.1.9   | 255.255.255.255 | FIELD SERVICE | 2     | The FIELD SERVICE remote station can be reached at IP address 192.168.1.9.                |
| 192.168.120.0 | 255.255.255.0   | Router01      | 2     | All data packets with destination IP addresses 192.168.120.x are transmitted to ROUTER01. |



| IP address      | Netmask       | Router          | Dist. | This is what happens:                                                                                                           |
|-----------------|---------------|-----------------|-------|---------------------------------------------------------------------------------------------------------------------------------|
| 192.168.125.0   | 255.255.255.0 | Router02        | 3     | All data packets with destination IP addresses 192.168.125.x are transmitted to ROUTER02.                                       |
| 192.168.130.0   | 255.255.255.0 | 192.168.140.123 | 0     | All data packets with destination IP addresses 192.168.130.x are transmitted to the router with the IP address 192.168.140.123. |
| 10.0.0.0        | 255.0.0.0     | 0.0.0.0         | 0     | Excludes transmission of all data packets to networks using private address spaces.                                             |
| 255.255.255.255 | 0.0.0.0       | HEAD OFFICE     | 2     | All data packets which cannot be allocated to the entries listed above are transmitted to the HEAD OFFICE remote station.       |



*The sequence of the entries is important here: They are processed from top to bottom. The router sorts entries automatically: Firstly by network masks, in descending order. Then by the IP addresses, in ascending order. This places the 'HEAD OFFICE' entry at the very end of the list. If this entry were at the top of the list, the router would send all (!) data packets not belonging to the local network to the network of the head office.*

## TCP/IP packet filters

You can use your entries in the routing table to determine quite precisely which data should be transferred. Additionally, you can use the '0.0.0.0' entry in the 'Router' field to reject whole groups of IP addresses.

Occasionally, you may wish to restrict a transmission even further. You can do this using a characteristic of TCP/IP, which is to send port numbers for destination and source as well as the source and destination IP addresses with a data packet. The destination port in a data packet stands for the service to be addressed in the TCP/IP network. The destination ports are fixed for the various services on the TCP/IP network (see also 'TCP/IP-ports' in the reference manual). The source ports, on the other hand, may be selected freely within certain ranges.

The router can check the source and destination ports of data packets using the TCP or UDP protocols. It can then deduce the purpose of the data from these ports. For example, FTP accesses or Telnet sessions can be identified. The appropriate filter table can be used to determine that certain data is not to be transferred from the LAN to the remote station. Data for particular ports can also be blocked from entering the LAN from the WAN in the same way. The filter tables can use the filter type along with the definition of the port ranges and associated protocols to determine whether the data in question should never be transmitted or whether it should simply not lead to a call being established (i.e. only be transmitted if a connection already exists).

The IP router has two separate filter tables, for packets coming from the LAN and from the WAN. These filter tables can be found in the *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Filtering' tab, or in the /Setup/IP-router-table/WAN-filter-table or LAN-filter-table menus.

## Proxy-ARP

The proxy ARP is a special feature of the IP router. This proxy is used if the transmission of data to IP addresses takes place in the same logical network as the sender, but the destination address is still reached via a router. This is the case when individual workstation computers (teleworkers) are networked via TCP/IP to the company network. The teleworker then has an IP address which is located in the same local network as all the other computers in the LAN. A data packet from LAN to the teleworker would usually only search for a receiver locally, but would not be able to find one.



*To take advantage of this function, enable the 'Use Proxy ARP' option (in LANconfig in the 'TCP/IP' configuration section on the 'Routing' tab or in the /Setup/IP-router-module menu for other configuration modes).*

The router becomes a proxy for the teleworker with the following entry in the routing table:

| IP address      | Netmask         | Router       | Dis-<br>tance | Mask |
|-----------------|-----------------|--------------|---------------|------|
| 192.168.110.123 | 255.255.255.255 | Teleworker01 | 0             | off  |

Proxy hosts are not propagated in an RIP packet because the router responds to an ARP request for the proxy computer with its own MAC address. The distance is set to '0' on the routing table to indicate this clearly.

The router now responds to the request for the MAC address to the IP address 192.168.110.123 with its own MAC address. This ensures that all packets in the LAN for the teleworker are now automatically sent to the router, and that data is sent on to the computer at the other end of the ISDN connection.

## Local routing

You know the following behavior of a workstation within a local network: The computer searches for a router to assist with transmitting a data packet to an IP address which is not on its own network. This router is usually notified to the operating system by its property of being the default router or gateway. It is often only possible to enter one default router which is supposed to be able to reach all the IP addresses which are unknown to the workstation computer if there are several routers in a network.

Occasionally, however, this default router cannot reach the destination network itself but does know another router which can find this destination.

How can you assist the workstation computer now?

By default, the router sends the computer a response with the address of the router which knows the route to the destination network (this response is known as an ICMP redirect). The workstation computer then accepts this address and sends the data packet straight to the other router.

Certain computers, however, do not know how to handle ICMP redirects. To ensure that the data packets reach their destination anyway, use local routing (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Routing' tab or in the `/Setup/IP-router-module/Local-routing` menu). This is how you tell the router to send the data packet to the other router itself. The router will then no longer send any ICMP redirects.

This may seem to be a good idea in principle, but local routing should still only be used as a last resort, since this function leads to doubling of the number of data packets being sent to the destination network required. The data is first sent to the default router and is then sent on from here to the router which is actually responsible.

## Dynamic routing with IP RIP

In addition to the static routing table ELSA routers also have a dynamic routing table containing up to 128 entries. Unlike the static table, you do not fill this out yourself, but leave it to be dealt with by the router itself. It uses the Routing Information Protocol (RIP) for this purpose. This protocol is used by all routers with RIP in a local network to exchange information regarding the reachable routes.

### What information is propagated by IP RIP?

A router uses the IP RIP information to inform the other routers in the network of the routes it finds in its own static table. The following entries are ignored in this process:

- Rejected routes with the '0.0.0.0' router setting.
- Routes running on other routers in the local network.
- Routes linking individual computers to the LAN by proxy ARP.

Although the entries in the static routing table are set manually, this information changes according to the connection status of the router and so do the RIP packets transmitted.

- If the router has established a connection to a remote station, it propagates all the networks which can be reached via this route in the RIPs with the distance '1'. Other routers in the LAN are thus informed by these means that a connection to the remote station has been established on this router which they can use. The establishment of additional connections by routers with dial-up connections can be prevented, thus reducing connection costs.

- If this router cannot establish a further connection to another remote station, all other routes are propagated with the distance '16' in the RIPs. The '16' stands for "This route is not available at the moment". If a router cannot establish a connection, in addition to the present one, this may be due to one of the following causes:
  - Another connection has already been established on all the other channels (also via the *LANCAP* or a/b ports).
  - The existing connection is using all B channels (channel bundling).



*To take advantage of this function, enable the 'IP RIP' option (in ELSA LANconfig in the 'TCP/IP' configuration section on the 'Router' tab or in the Setup/IP Router-module menu for other configuration modes).*

*Routers with RIP capabilities dispatch the RIP packets approximately every 30 seconds. The router is only set up to send and receive RIPs if it has a unique IP address. The IP RIP module is deselected in the default setting using the IP address XXX.XXX.XXX.254.*

### **Which information does the router take from received IP RIP packets?**

When the router receives such IP RIP packets, it incorporates them in its dynamic routing table, which looks something like this:

| IP address    | Netmask       | Time | Distance | Router        |
|---------------|---------------|------|----------|---------------|
| 192.168.120.0 | 255.255.255.0 | 1    | 2        | 192.168.110.1 |
| 192.168.130.0 | 255.255.255.0 | 5    | 3        | 192.168.110.2 |
| 192.168.140.0 | 255.255.255.0 | 1    | 5        | 192.168.110.3 |

### **What do the entries mean?**

IP addresses and network masks identify the destination network, the distance is taken from the RIP information, the final column indicates the router which announced this route. This leaves the 'Time'. The dynamic table thus shows how old the relevant route is. The value in this column acts as a multiplier for the intervals at which the RIP packets arrive. A '1', therefore, stands for 30 seconds, a '5' for about 2.5 minutes and so on. New information arriving about a route is, of course, designated as directly reachable and is given the time setting '1'. The value in this column is automatically incremented when the corresponding amount of time has elapsed. The distance is set to '16' after 3.5 minutes (route not reachable) and the route is deleted after 5.5 minutes.

Now if the router receives an IP RIP packet, it must decide whether or not to incorporate the route contained into its dynamic table. This is done as follows:

- The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).

- The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.
- The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will always be used.
- The route exists in the table. The new route comes from the same router which notified this route, but has a worse distance than the previous entry. If a router notifies the degradation of its own static routing table in this way (e.g. releasing a connection increases the distance from 1 to 2), the router will believe this and include the poorer entry in its dynamic table.



*RIP packets from the WAN will be ignored and will be rejected immediately. RIP packets from the LAN will be evaluated and will not be propagated in the LAN.*

### **The interaction of static and dynamic tables**

The router uses the static and dynamic tables to calculate the actual IP routing table it uses to determine the path for data packets. In doing so, it includes the routes from the dynamic table which it does not know itself or which indicate a shorter distance than its own (static) route with the routes from its own static table.

### **Routers without IP RIP support**

Routers which do not support the Routing Information Protocol are also occasionally present on the local network. These routers cannot recognize the RIP packets and look on them as normal broadcast or multicast packets. Connections are continually established by the RIPs if this router holds the default route to a remote router. This can be prevented by entering the RIP port in the filter tables.

### **Scaling with IP RIP**

If you use several routers in a local network with IP RIP, you can represent the routers outwardly as one large router. This procedure is known as "scaling". A router like this, with its supposedly inexhaustible supply of routes is created by the continual exchange of information between the routers.

### **IP masquerading (NAT, PAT)**

One continually growing problem for the Internet is the limited number of generally valid IP addresses available. In addition to this, the allocation of fixed IP addresses for the Internet by the Network Information Center (NIC) is an expensive process. What is more obvious than having several computers share one IP address?

This particular solution is called IP masquerading. This is a procedure whereby only one LAN router appears on the Internet with an IP address. This IP address is allocated to the router either permanently by the NIC or temporarily by an Internet provider. All the other computers on the network then "conceal" themselves behind this one IP address. Aside

from the welcome savings, IP masquerading has the added benefit of guarding very effectively against attacks on the local network from the Internet.

### **Two addresses for the router**

Masquerading pits two opposing requirements of the router against one another: While it must have an IP address which is valid on the local network, it must also have an address valid on the Internet. Since these two addresses may not in principle be located on the same logical network, there is only one solution: two IP addresses are required. The router is therefore assigned an **Internet** address and an **intranet** address, each with its own fitting network mask. Use the 'Masquerade' option in the routing table to inform the router which of the two addresses to use when transferring the packets. If a specific address is requested from the provider, two options are available for the actual address assignment:

- The provider assigns the desired address to the router. The network mask now decides how many computers are masked behind the router.
  - IP address with full '255.255.255.255' network mask: This is your own unique IP address, registered by the NIC. None of the other computers on the network have valid Internet addresses and are masked behind the router's fixed address.
  - IP address with an incomplete network mask, e.g. '255.255.255.248': You have several registered IP addresses, one of which you assign to the router. The remaining IP addresses are assigned permanently to devices on the intranet, which can then use unmasked connections to access the Internet. The other devices can still access the Internet using masked connections.
- The provider assigns another address to the router. Then **all** computers in the local network are masked behind the assigned address.

### **How does IP masquerading work?**

Masquerading makes use of a characteristic of TCP/IP data transmission, which is to use port numbers for destination and source as well as the source and destination addresses. When the router receives a data packet for transfer it now notes the IP address and the sender's port in an internal table. It then gives the packet its unique IP address and a new port number, which could be any number. It also enters this new port on the table and forwards the packet with the new information.

The response to this new packet is now sent to the IP address of the router with the new sender port number. The entry in the internal table allows the router to assign this response to the original sender again.

*You can view these tables in detail in the router statistics (see also 'Status').*



## Simple and inverse masquerading

This masking operates in both directions: The local network behind the IP address of the router is masked if a computer from the LAN sends a packet to the Internet (simple masquerading).

If, on the other hand, a computer sends a packet from the Internet to, for example, an FTP server on the intranet, from the point of view of this computer the router appears to be the FTP server. The router knows the intranet address of the server from the entry in the service table (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Masq.' tab or in the `Setup/IP-router-module/Masquerading/Service-table` menu). The packet is forwarded to this computer. All packets that come from the FTP server in the local network (answers from the server) are hidden behind the IP address of the router.

The only small difference is that:

- Access to a service (port) in the intranet from outside must be defined in advance by specifying a port number. The destination port is specified with the intranet address of, for example, the FTP server, on a service table to achieve this.
- When accessing the Internet from the intranet, on the other hand, the router itself makes the entry in the port and IP address information table.

The table concerned can hold up to 2048 entries, that is it allows 2048 **simultaneous** transmissions between the masked and the unmasked network.

After a specified period of time, the router, however, assumes that the entry is no longer required and deletes it automatically from the table.

## Which protocols can be transmitted using IP masquerading?

Naturally, only those which also communicate using ports. Protocols working without port numbers or using ports above IP in the OSI model cannot be masked without special treatment.

The current version of router implements masquerading for the following protocols:

- FTP
- TCP
- UDP
- ICMP

## DNS forwarding

Names rather than IP addresses are generally used to access a server over the Internet. Who knows which address is behind 'www.domain.com'? The DNS server, of course.

DNS stands for Domain Name Service and refers to the assignment of domain names (such as domain.com) to the corresponding IP addresses. This information must be

constantly updated and be accessible all over the world at any time. DNS servers holding long tables containing IP addresses and domain names exist for this purpose.

If a computer calls up a home page from the intranet, it first sends out a DNS request: "Which IP address belongs to `www.domain.com`?" If the router has been specified as the DNS server in the workstations, the request is handled as follows:

- Initially the router checks whether a DNS server has been entered in its own settings (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Addresses' tab or in the `/Setup/TCP-IP-module` menu). If it finds one it connects to this server and retrieves the information required.
- If no DNS server is entered in the router, it will attempt to reach a DNS server over a PPP connection (e.g. from the Internet provider) to get the IP address assigned to the name from there. This can only succeed if the address of a DNS server is sent to the router during PPP negotiation.
- If no connection exists, the default route is established and a search is then carried out there for the DNS server.

This procedure does not require you to have any knowledge of the DNS server address. Entering the intranet address of your router as the DNS server for the workstation computers is sufficient to enable you obtain the name assignment. This procedure also automatically updates the address of the DNS server. The router always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

## Policy Based Routing

Policy-based routing describes a process in which particular data packets are given preferential treatment. This requires evaluation of a special field within the IP data packet, known as the Type of Service (TOS) field. This preferential treatment of a number of data packets can, for example, simplify the configuration of the router via the WAN when large data volumes are to be transferred simultaneously.

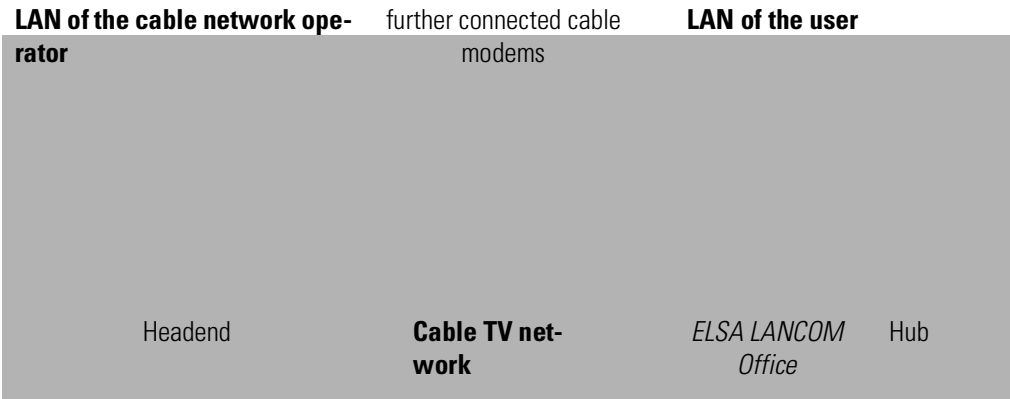


*You can find more information on policy based circuit routing in the 'Description of the menu options'.*

## Bridging

A bridge connects two or more LANs in such a way that they appear to be a single large network. When bridging via cable modems, the LAN of the cable network operator with the headend is on one side and the LAN of the network participants with the cable modem and the local workstations on the other.





In the bridge operating mode, the *ELSA LANCOM Office* transfers all data to computers without locally assigned MAC addresses, between the local network or another local area network (LAN) or a workstation on one side and the cable network on the other side.

The bridge thus learns on its own which MAC addresses are located on its own network and which are located on the other side. After a very high level of data traffic that occurs during the initial negotiations between the two LANs, the network load drops sharply. In this case, the connection will no longer be established so frequently. When receiving data from the cable network, the bridge in the cable modem uses the MAC addresses to determine whether the data is destined for its own LAN. The bridge will only accept data packets that are addressed to MAC addresses in its LAN.

The bridge connects the two participating computers as if they were in fact located in one network. For this reason, however, only those computers which can also theoretically be integrated into a network should be connected. This means that both networks and the network and workstation computer must have the same network addresses.

The bridge is not dependent on the protocol used in layer 3. It operates only with Ethernet addresses (MAC addresses). Please, therefore, ensure that you only use those B-channel protocols in the layer list which have the setting ETHER in the ENCAPS column. Use a protocol other than PPP on layer 3, as this protocol is not supported for the bridge.



*It is not possible to use the bridge via 2 B channels, as MLPPP is used for channel bundling.*

**What do you need to configure the bridge?**

First establish which subscriber numbers the *ELSA MicroLink Cable* should listen to and which it should itself transfer externally (Setup/WAN-Module/Interface).

An entry which includes name and subscriber number must exist in the name list for *ELSA MicroLink Cable* to reach the remote station (Setup/WAN-Module/Name-List).

You should specify the correct remote station to the bridge (Setup/Bridge-Module/Remote-ID) since additional remote stations may be entered in the *ELSA MicroLink Cable* over time. This is because the bridge can only connect precisely two

networks together, while one router can manage several remote stations. You should also set (Setup/Bridge-Module/Operating:On) so that the bridge can function.

The process is now completed. The bridge now sets to work transferring all the data packets for non-local MAC addresses to the remote station set.



*You can find more instructions on how to configure the ELSA MicroLink Cable as a bridge in the appropriate section of 'Workshop' and in the detailed description of the individual menus in the reference section of the manual.*

### What are the filter options?

You may not always wish to transfer all data. Much of the data which is bouncing around in the LAN is of no interest to remote networks or computers. For this reason, you can block transfer of the following data packets or only transfer them if the line has been established already: You can thus block transfer of the following data packets via the bridge:

- Broadcast packets: Data directed at all devices accessible in a network (Setup/Bridge-Module/LAN-config/Broadcast).
- Multicast packets: Data which is transferred to all devices accessible in a group (Setup/Bridge-Module/LAN-config/Multicast).
- Unicast packets: This is data directed only at a specific device (meaning a fixed MAC address).

Special filter lists which exclude certain addresses from a transmission or only allow certain addresses can be set up to handle this data. The bridge filters differentiate here between destination and source addresses. You can first establish for both address types whether the associated table contains the addresses to which data is to be transmitted (Setup/Bridge-Module/LAN-config/Dest.-address/Filter-type/pos) or the addresses to be excluded (.../Filter-type/neg). You then enter the MAC addresses to be filtered into the table itself.



*This method of filtering by entering the exact MAC address naturally demands a certain degree of maintenance effort. Should the addresses change, when a network adapter is changed for example, the new addresses must be entered to ensure that the bridge continues to function.*

# Description of the menu options

The menu tree for *ELSA LANCOM* configuration is divided up into status information, setup parameters, firmware information and 'other'.

In order to help you familiarize yourself with the system, you will first be given an overview of the menu structure.

A complete list of all the menu options will be followed by a detailed description of all displays, menus and actions along with their associated parameters, default settings and input options.









Some of the features described in this Reference Manual apply only to specific models in the *ELSA LANCOM* family. Restrictions with regard to specific models are indicated by the symbol shown here.

You can access the menus when configuring via Telnet or terminal programs and via SNMP (also see 'Configuration Modes').

When configuring with *ELSA LANconfig*, you are provided with an integrated help system that gives you brief descriptions of the individual parameters.
















*All channel-related statistics and menus in this documentation refer to two channels only, even if more than two channels are available to the specific devices. Interface-related information is also provided for a single interface only. The information is equally applicable to the additional channels and interfaces.*

## Symbols







|                                                                                     |            |                                                     |
|-------------------------------------------------------------------------------------|------------|-----------------------------------------------------|
|  | Menu       | Indicates a further submenu.                        |
|  | Info       | Indicates a value that cannot be modified.          |
|  | Value      | Indicates a value that can be modified.             |
|  | Table      | Indicates a table whose entries can be modified.    |
|  | Info table | Indicates a table whose entries cannot be modified. |
|  | Action     | Performs an action.                                 |

## Overview of the menus






















### **Setup**

-  Name
-  WAN-module
-  Charges-module
-  LAN-module
-  IPX-module
-  TCP-IP-module
-  IP-router-module
-  SNMP-module
-  DHCP-module
-  NetBIOS-module
-  Config-module
-  LANCAP-Module
-  LCR-module
-  DNS module
-  Time-module





### **Firmware**

-  Version-table
-  Table-firmsafe
-  Mode-firmsafe
-  Timeout-firmsafe
-  Test-firmware
-  Firmware-upload

### **Status**

-  Connection
-  Current-time
-  Operating-time
-  WAN-statistics
-  LAN-statistics
-  PPP-statistics
-  IPX-statistics
-  TCP-IP-statistics
-  IP-router-statistics
-  Config-statistics
-  Queue-statistics
-  Conn.-statistics
-  Info-connection
-  Layer-connection
-  Call-info-table
-  Remote-statistics
-  S<sub>0</sub>-bus
-  Channel-statistics
-  Time-statistics
-  LCR-statistics
-  Delete-values

### **Other**






















-  Manual-dialing
-  Boot-system
-  Reset-system
-  Upload-system

## Status

The Status menu contains information on the current status and the internal sequences of operations in the LAN and WAN, which can relate to the data transmission route (e.g. dialing or connection) or to statistics (e.g. number of calls received or data blocks transmitted). The statistics displays are an important aid for verifying correct functioning and optimizing parameter settings. In addition, they provide valuable information for error analysis when malfunctions occur.

Most status displays are continually updated and can be deleted with a **value** or set to 0 in the current menu.

The menu has the following layout:

| Status                 |                                                                                     | Running status displays                                                    |
|------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Connection             |    | Status of the WAN route                                                    |
| Current-time           |    | Current time in device                                                     |
| Operating-time         |    | Period of time the device has operated since it was last switched on       |
| WAN-statistics         |    | Displays WAN statistics                                                    |
| LAN-statistics         |   | Displays LAN statistics                                                    |
| PPP-statistics         |  | Point-to-point-protocol statistics                                         |
| IPX-statistics         |  | Statistics from the IPX and IPX router area                                |
| TCP-IP-statistics      |  | Statistics from the TCP/IP area                                            |
| IP-router-statistics   |  | Statistics from the IP router                                              |
| Config-statistics      |  | Remote configuration statistics                                            |
| Queue-statistics       |  | Statistics relating to the packets in the queues of the individual modules |
| Connections-statistics |  | Connection information for each interface                                  |
| Info-connection        |  | Information on the last connection for each interface                      |
| Layer-connection       |  | Information on the B-channel protocol used for each interface              |
| Call-info-table        |  | Information on the last 100 calls received                                 |
| Remote-statistics      |  | Statistics on the last 100 connections                                     |
| S <sub>0</sub> -bus    |  | Status of the S <sub>0</sub> interface                                     |
| Channel-statistics     |  | Information of the status of the individual channels.                      |
| Time-statistics        |  | Time module information                                                    |
| LCR-statistics         |  | Least-cost router information                                              |
| Delete-values          |  | Deletes all values except tables with substatistics.                       |

## Display and keyboard

The display shows status information and error messages issued by the device. The following display modes are available:

- B channel overview (one character per channel)
- B channel status (one line per channel)
- Device status / Device error messages

A total of six keys are available (cursor keys + "Mode" + "Clr"), as well as a two-line display with 40 characters per line, of which 16 characters each are currently displayed. Depending on the devices settings, the text information is displayed in German or English.

### B-channel-overview

In the B channel overview the channels are displayed in the form of a table. The individual fields of the table have the following significance:

|                                            |       |       |       |
|--------------------------------------------|-------|-------|-------|
| P : x (status of port 1, first B channel)  | P : X | P : X | P : X |
| 1 : x (status of port 1, second B channel) | 2 : x | 3 : x | 4 : x |

The following symbols are used for the channel status (shown by x in the table):

|              |                                      |
|--------------|--------------------------------------|
| .            | Channel idle (disabled)              |
| -            | Channel idle (enabled)               |
| E (flashing) | An error has occurred on the channel |
| A (flashing) | Outgoing call                        |
| A            | Connected (outgoing)                 |
| P (flashing) | Incoming call                        |
| P            | Connected (incoming)                 |
| N (flashing) | Negotiation                          |

The cursor keys have no function in this mode.

### B channel status display

The B channel status display shows an excerpt from a table with an entry for each B channel. In the event of changes to the status of a channel, the table will jump to the current entry if no cursor key has been used for at least 5 seconds. The status of the channel is displayed in plain text, e.g.:

CH11: Connection LC\_PPP

CH12: Remote station LC\_PPP not responding

Error messages are retained for 60 seconds. Information with regard to the enabling and disabling of S<sub>0</sub> interfaces is also displayed.

The up and down cursor keys can be used to scroll through the individual lines; use the left and right cursor keys to navigate within the line itself. Although a width of only 16 characters is available, the display has a total width of 40 characters (the visible section can be moved). The display returns to the start 5 seconds after the last horizontal movement.

### Device status and device error messages

Channel-independent device status messages and especially error messages (with simultaneous flashing Power/Msg LED) are displayed in this mode. The unit automatically switches to this mode in the event of an error.


The up and down cursor keys permit scrolling through all available messages. The model number (e.g. "Model 4100") and the firmware version always appear as the final message. This display also appears immediately after switching the unit on, before changing to the last current display mode. The error messages in this mode can also be up to 40 characters long.

The Mode key switches between the display modes described above.

The Clr key clears the errors displayed in the device status and device error message display modes.

### Status/Connection

The **Status/Connection** menu option displays the status messages for the individual channels.

| /Connection-state | Running status displays                                                             |                          |
|-------------------|-------------------------------------------------------------------------------------|--------------------------|
| Connection        |  | CH01: Ready; CH02: Ready |

### Status/Current-time

This displays the current device time, used, e.g., for the least-cost-router calculations or certain statistics. The time can be read from the ISDN (ISDN time, see also Setup/time module) or set manually (with the 'time' command).










### Status/Operating-time

The operating time of the router since it was last started is displayed here in days hours, minutes and seconds.

### Status/WAN-statistics

This option allows you to display the various statistics parameters for the WAN port. A large number of values related to the data volume transferred provide you with useful information on WAN port utilization, errors that have occurred, and the internal resources of the devices that are available in the current operating state.

The WAN statistics are maintained on an interface-specific basis, i.e. separate statistics in which the transferred data and errors are recorded are available for each interface. The **Status/WAN-statistics** menu has the following layout:

| /WAN-statistics             |                                                                                     | Running status displays                                       |
|-----------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Byte-transport-statistics   |    | Statistics on bytes transferred                               |
| Packet-transport-statistics |    | Statistics on data packets transferred                        |
| Error-statistics            |    | Statistics on data errors that have occurred                  |
| WAN-tx-discarded            |    | Number of packets discarded due to an error/lack of resources |
| WAN-heap-packets            |    | Number of buffers in use                                      |
| WAN-queue-packets           |    | Number of buffers available                                   |
| WAN-queue-errors            |   | Number of packets discarded due to a lack of buffers          |
| Throughput-statistics       |  | Statistics for bytes transferred on every channel             |
| Delete-values               |  | Deletes WAN statistics                                        |

Byte-transport-statistics

The menu item **Status/WAN-statistics/Byte-transport-statistics** contains statistics of the bytes transferred over an interface for every available interface. The table maintained here has the following layout:

| Ifc  | CRx-bytes | Rx-bytes | Tx-bytes | CTx-bytes |
|------|-----------|----------|----------|-----------|
| Ch01 | 0         | 0        | 0        | 0         |
| Ch02 | 0         | 0        | 0        | 0         |

Below is a detailed description of the meaning of each field:

|           |                                         |
|-----------|-----------------------------------------|
| Ifc       | Designates the associated channel.      |
| CRx-bytes | Number of bytes received (compressed)   |
| Rx-bytes  | Number of bytes received (uncompressed) |
| Tx-bytes  | Number of bytes sent (uncompressed)     |
| CTx-bytes | Number of bytes sent (compressed)       |



*Packet-transport-statistics*

For each available interface, the **Status/WAN-statistics/Packet-transport-statistics** menu option provides statistics on the data packets transferred via this interface. The table maintained here has the following layout:

| lfc  | Rx | Tx-total | Tx-normal | Tx-reliable | Tx-urgent |
|------|----|----------|-----------|-------------|-----------|
| Ch01 | 0  | 0        | 0         | 0           | 0         |
| Ch02 | 0  | 0        | 0         | 0           | 0         |

Below is a detailed description of the meaning of each field:

|             |                                                                          |
|-------------|--------------------------------------------------------------------------|
| lfc         | Designates the associated channel.                                       |
| Rx          | Number of packets received                                               |
| Tx-total    | Number of packets sent (data and protocol packets)                       |
| Tx-normal   | Number of normal data packets sent                                       |
| Tx-reliable | Number of data packets transferred with secured handling                 |
| Tx-urgent   | Number of data packets transferred with priority handling (urgent queue) |

*Error-statistics*

For each available interface, the **Status/WAN-statistics/Error-statistics** menu option provides statistics on the transmission errors that have occurred on this interface. The table maintained here has the following layout:

| lfc  | Rx-l1-error | Rx-l2-error | Rx-l3-error | Stack-error | Tx-error |
|------|-------------|-------------|-------------|-------------|----------|
| Ch01 | 0           | 0           | 0           | 0           | 0        |
| Ch02 | 0           | 0           | 0           | 0           | 0        |

Below is a detailed description of the meaning of each field:

|             |                                                                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lfc         | Designates the associated channel.                                                                                                                                       |
| Rx-l1-error | Number of layer-3 errors in data received (i.e., the protocol header of layer-3 is incorrect)                                                                            |
| Rx-l2-error | Number of layer-2 errors in data received (i.e., similar to the layer-3 errors, e.g. defective PPP header)                                                               |
| Rx-l3-error | Number of layer-1 errors in data received (similar to layer-3 errors)                                                                                                    |
| Stack-error | Number of transmission errors that occurred while sending                                                                                                                |
| Tx-error    | Number of stack errors for data received. Stack errors are caused when frames are received that cannot be assigned to an internal processing procedure (e.g. IP router). |

### Throughput-statistics

The menu item **Status/WAN-statistics/Throughput-statistics** contains statistics of bytes transferred over this interface for both channels. The table maintained here has the following layout:













| lfc  | Rx/s current | Tx/s current | Rx/s average | Tx/s average |
|------|--------------|--------------|--------------|--------------|
| Ch01 | 0            | 0            | 0            | 0            |
| Ch02 | 0            | 0            | 0            | 0            |











Below is a detailed description of the meaning of each field:

|              |                                                                            |
|--------------|----------------------------------------------------------------------------|
| lfc          | Designates the associated channel.                                         |
| Rx/s current | Throughput on the channel in the last second in the receiving direction    |
| Tx/s current | Throughput on the channel in the last second in the transmission direction |
| Rx/s average | Average throughput on the channel in the receiving direction               |
| Tx/s average | Average throughput on the channel in the transmission direction            |

## Status/LAN-statistics










Similarly to the previous menu option, this option allows you to display the statistics relating to the LAN port. The **Status/LAN-statistics** menu has the following layout:





| /LAN-statistics   | Running status displays                                                             |                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LAN-rx-packets    |  | Number of data packets received                                                                                                                             |
| LAN-tx-packets    |  | Number of data packets sent                                                                                                                                 |
| LAN-rx-errors     |  | Number of data packets incorrectly received                                                                                                                 |
| LAN-tx-errors     |  | Number of data packets incorrectly sent                                                                                                                     |
| LAN-stack-errors  |  | Number of packets without a suitable receive module (bridge/router)                                                                                         |
| LAN-NIC-errors    |  | Number of data packets discarded by the NIC                                                                                                                 |
| LAN-heap-packets  |  | Number of buffers available                                                                                                                                 |
| LAN-queue-packets |  | Number of buffers in use                                                                                                                                    |
| LAN-queue-errors  |  | Number of packets discarded due to a lack of buffers                                                                                                        |
| LAN-collisions    |  | Number of collisions during a send procedure                                                                                                                |
| Link-active       |  | Display of correct Ethernet connection (data transfer possible). Corresponds to the 'Link' LED on the device.                                               |
| Negotiation done  |  | The negotiation of the transfer mode between the router and the remote station is complete. This is only relevant if Setup/LAN/Connection is set to 'Auto'. |

| /LAN-statistics   | Running status displays                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connector         |    | This item shows the connection type currently being used on the Ethernet connection:<br>10B-TX: 10 MBit, half-duplex<br>FD10B-TX: 10 MBit, full-duplex<br>100B-TX: 100 MBit, half-duplex<br>FD100B-TX: 100 MBit, full-duplex<br>If 'Auto' is set under Setup/LAN, then this is the connection type the two units have negotiated. This corresponds to the 'Fast' and 'FDpx' LEDs on the unit. If, on the other hand, a fixed transfer mode has been set, this value will be the same as the one in Setup/LAN/Connection. |
| LAN-rx-bytes      |    | Number of bytes received from the LAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| LAN-tx-bytes      |    | Number of bytes sent to the LAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LAN-rx-broadcasts |    | Number of broadcast packets received from the LAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| LAN-rx-multicasts |    | Number of multicast packets received from the LAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| LAN-rx-unicasts   |    | Number of directly addressed packets received from the LAN                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| LAN-tx-broadcasts |    | Number of broadcasts received from the LAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| LAN-tx-multicasts |    | Number of multicasts received from the LAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| LAN-tx-unicasts   |    | Number of unicasts received from the LAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Delete-values     |  | Deletes LAN statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Status/PPP-statistics

Within the PPP statistics, the states of individual subprotocols of the PPP are managed separately for each interface. However, statistics relating to the frames transmitted for individual subprotocols are maintained only in joint statistics. Consequently, the **Status/PPP-statistics** menu has the following layout:

| /PPP-statistics  | Running status displays                                                             |                                                                                  |
|------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| PPP-phases       |  | Statistics relating to the status of PPP protocol negotiation for each interface |
| LCP-statistics   |  | Displays PPP/LCP statistics                                                      |
| PAP-statistics   |  | Displays PPP/PAP statistics                                                      |
| CHAP-statistics  |  | Displays PPP/CHAP statistics                                                     |
| CBCP-statistics  |  | Displays PPP/CBCP statistics                                                     |
| IPXCP-statistics |  | Displays PPP/IPXCP statistics                                                    |
| IPCP-statistics  |  | Displays PPP/IPCP statistics                                                     |
| CCP-statistics   |  | Displays PPP/CCP statistics                                                      |
| ML-statistics    |  | Displays PPP/ML statistics                                                       |

| /PPP-statistics |                                                                                   | Running status displays                               |
|-----------------|-----------------------------------------------------------------------------------|-------------------------------------------------------|
| BACP-statistics |  | Displays PPP/BACP statistics                          |
| Rx-options      |  | Displays the LCP, IPCP and IPXCP information received |
| Tx-options      |  | Displays the LCP, IPCP and IPXCP information sent     |
| Delete-values   |  | Deletes PPP statistics.                               |

The PPP statistics provide detailed information on the phases of a PPP negotiation, particularly in the event of connection problems with external products. It provides important information for error diagnosis.

#### PPP-phases

For each available interface, the **Status/PPP-statistics/PPP-phases** option provides a list of the current states of PPP protocol negotiation. The table maintained here has the following layout:

| Ifc  | Phase to | LCP     | IPCP    | IPXCP   | CCP     |
|------|----------|---------|---------|---------|---------|
| Ch01 | DEAD     | Initial | Initial | Initial | Initial |
| Ch02 | DEAD     | Initial | Initial | Initial | Initial |

Below is a detailed description of the meaning of each field:

|          |                                                                                                                                                                                                                                                         |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ifc      | Designates the associated channel.                                                                                                                                                                                                                      |
| Phase to | Indicates the current phase of the PPP. The possible values are <b>AUTHENTICAT</b> , <b>NETWORK</b> and <b>TERMINATE</b> .                                                                                                                              |
| LCP      | Status of the 'Link Control Protocol' subprotocol. The possible values are: <b>Initial</b> , <b>Starting</b> , <b>Stopping</b> , <b>Stopped</b> , <b>Closing</b> , <b>Closed</b> , <b>ReqSent</b> , <b>AckRcvd</b> , <b>AckSent</b> and <b>Opened</b> . |
| IPCP     | Similarly to 'LCP', displays the status of the 'IP Control Protocol' subprotocol.                                                                                                                                                                       |
| IPXCP    | Similarly to 'LCP', displays the status of the 'IPX Control Protocol' subprotocol.                                                                                                                                                                      |
| CCP      | Similarly to 'LCP', displays the status of the 'Compression Control Protocol' subprotocol.                                                                                                                                                              |

The current PPP phases are shown under **Status/PPP-statistics/PPP-phases**. As specified above, these phases are the idle (Dead), ready (Establish), access parameter verification (Authenticate) and network phase (Network). In the substatistics, the frames exchanged are encrypted separately by type and quantity.

#### Status/PPP-statistics/LCP-statistics

The **LCP** (Link Control Protocol) negotiates the basic features of the PPP connections. The LCP frames exchanged during PPP negotiation are recorded in statistics and displayed by type and quantity. If the LCP does not change to the OPEN state for a connection, these statistical values provide information on errors that occurred during the initial phase of

PPP negotiation. Below is a detailed description of the meanings of the parameters for these statistics:

|                      |                                                           |
|----------------------|-----------------------------------------------------------|
| Rx-errors            | Number of faulty PPP packets received                     |
| Rx-discarded         | Number of PPP packets discarded                           |
| Rx-config-request    | Number of configure request packets received for LCP      |
| Rx-config-ack.       | Number of configure acknowledge packets received for LCP  |
| Rx-config-nak.       | Number of configure negative acknowledge packets received |
| Rx-config-reject     | Number of configure reject packets received for LCP       |
| Rx-terminate-request | Number of terminate request packets received for LCP      |
| Rx-terminate-ack.    | Number of terminate acknowledge packets received for LCP  |
| Rx-code-reject       | Number of code reject packets received for PPP            |
| Rx-protocol-reject   | Number of protocol reject packets received for PPP        |
| Rx-echo-request      | Number of echo request packets received for LCP           |
| Rx-echo-reply        | Number of echo response packets received for LCP          |
| Rx-discard-request   | Number of discard request packets received for LCP        |
| Tx-config-request    | Number of configure request packets sent for LCP          |
| Tx-config-ack.       | Number configure acknowledge packets sent for LCP         |
| Tx-config-nak.       | Number of configure negative acknowledge packets sent     |
| Tx-config-reject     | Number of configure reject packets sent for LCP           |
| Tx-terminate-request | Number of terminate request packets sent for LCP          |
| Tx-terminate-ack.    | Number of terminate acknowledge packets sent for LCP      |
| Tx-code-reject       | Number of code reject packets sent for PPP                |
| Tx-protocol-reject   | Number of protocol reject packets sent for PPP            |
| Tx-echo-request      | Number of echo request packets sent for LCP               |
| Tx-echo-reply        | Number of echo response packets sent for LCP              |
| Tx-discard-request   | Number of discard request packets sent for LCP            |
| Delete-values        | Deletes LCP statistics                                    |

### Status/PPP-statistics/PAP-statistics

The **PAP** (Password Authentication Protocol) is one of two common procedures for verifying remote stations in the PPP. When a connection is established, it checks the remote station password and enables the connection only after a successful exchange of passwords (refer also to Chapter 'Point-to-Point Protocol'). Below is a detailed description of the meanings of the parameters for these statistics:

|              |                                        |
|--------------|----------------------------------------|
| Rx-discarded | Number of PAP packets discarded        |
| Rx-request   | Number of PAP request packets received |
| Rx-success   | Number of PAP success packets received |

|               |                                            |
|---------------|--------------------------------------------|
| Rx-failure    | Number of PAP failure packets received     |
| Tx-retry      | Number of times PAP request packets resent |
| Tx-request    | Number of PAP request packets sent         |
| Tx-success    | Number of PAP success packets sent         |
| Tx-failure    | Number of PAP failure packets sent         |
| Delete-values | Deletes PAP statistics                     |

### Status/PPP-statistics/CHAP-statistics

The **CHAP** (Challenge Authentication Protocol) is the second option for verifying the remote station under PPP. The password is checked as the connection is established and again at adjustable intervals during the connection (refer also to Chapter 'Point-to-Point Protocol'). Below is a detailed description of the meanings of the parameters for these statistics:

|               |                                                        |
|---------------|--------------------------------------------------------|
| Rx-discarded  | Number of CHAP packets discarded                       |
| Rx-challenge  | Number of CHAP challenge packets received              |
| Rx-response   | Number of CHAP response packets received               |
| Rx-success    | Number of CHAP success packets received                |
| Rx-failure    | Number of CHAP failure packets received                |
| Tx-retry      | Number of times the CHAP challenge packets were resent |
| Tx-challenge  | Number of CHAP challenge packets sent                  |
| Tx-response   | Number of CHAP response packets sent                   |
| Tx-success    | Number of CHAP success packets sent                    |
| Tx-failure    | Number of CHAP failure packets sent                    |
| Delete-values | Deletes CHAP statistics                                |

### Status/PPP-statistics/IPXCP-statistics

When IPX is used, the **IPXCP** (Internet Exchange Protocol Control Protocol) indicates the status of the protocol and the packets exchanged in the negotiation. Below is a detailed description of the meanings of the parameters for these statistics:

|                      |                                                            |
|----------------------|------------------------------------------------------------|
| Rx-discarded         | Number of IPXCP packets discarded                          |
| Rx-config-request    | Number of configure request packets received for IPXCP     |
| Rx-config-ack.       | Number of configure acknowledge packets received for IPXCP |
| Rx-config-nak.       | Number of configure negative acknowledge packets received  |
| Rx-config-reject     | Number of configure reject packets received for IPXCP      |
| Rx-terminate-request | Number of terminate request packets received for IPXCP     |
| Rx-terminate-ack.    | Number of terminate acknowledge packets received for IPXCP |
| Rx-code-reject       | Number of code reject packets received for IPXCP           |
| Tx-config-request    | Number of configure request packets sent for IPXCP         |
| Tx-config-ack.       | Number of configure acknowledge packets sent for IPXCP     |
| Tx-config-nak.       | Number of configure negative acknowledge packets sent      |
| Tx-config-reject     | Number of configure reject packets sent for IPXCP          |
| Tx-terminate-request | Number of terminate request packets sent for IPXCP         |

|                   |                                                        |
|-------------------|--------------------------------------------------------|
| Tx-terminate-ack. | Number of terminate acknowledge packets sent for IPXCP |
| Tx-code-reject    | Number of code reject packets sent for IPXCP           |
| Delete-values     | Deletes IPXCP statistics                               |

### **Status/PPP-statistics/IPCP-statistics**

When IP is used, the **IPCP** (Internet Protocol Control Protocol) indicates the status of the protocol and the packets exchanged in the negotiation.

|                      |                                                           |
|----------------------|-----------------------------------------------------------|
| Rx-discarded         | Number of IPCP packets discarded                          |
| Rx-config-request    | Number of configure request packets received for IPCP     |
| Rx-config-ack.       | Number of configure acknowledge packets received for IPCP |
| Rx-config-nak.       | Number of configure negative acknowledge packets received |
| Rx-config-reject     | Number of configure reject packets received for IPCP      |
| Rx-terminate-request | Number of terminate request packets received for IPCP     |
| Rx-terminate-ack.    | Number of terminate acknowledge packets received for IPCP |
| Rx-code-reject       | Number of code reject packets received for IPCP           |
| Tx-config-request    | Number of configure request packets sent for IPCP         |
| Tx-config-ack.       | Number of configure acknowledge packets sent for IPCP     |
| Tx-config-nak.       | Number of configure negative acknowledge packets sent     |
| Tx-config-reject     | Number of configure reject packets sent for IPCP          |
| Tx-terminate-request | Number of terminate request packets sent for IPCP         |
| Tx-terminate-ack.    | Number of terminate acknowledge packets sent for IPCP     |
| Tx-code-reject       | Number of code reject packets sent for IPCP               |
| Delete-values        | Deletes IPCP statistics                                   |

### **Status/PPP-statistics/CBCP-statistics**

The **CBCP** (Callback Control Protocol) shows the protocol status when the IP is in use and the packets exchanged during negotiation.

|                   |                                             |
|-------------------|---------------------------------------------|
| Rx-request        | Number of CBCP request packets received     |
| Rx-discarded      | Number of CBCP packets discarded            |
| Rx-acknowledge    | Number of CBCP acknowledge packets received |
| Tx-request        | Number of CBCP request packets sent         |
| Tx-response       | Number of CBCP response packets sent        |
| TX-acknowledge    | Number of CBCP acknowledge packets sent     |
| Request-discarded | Number of CBCP request packets discarded    |



|                    |                                              |
|--------------------|----------------------------------------------|
| Response-discarded | Number of CBCP response packets discarded    |
| Ack.-discarded     | Number of CBCP acknowledge packets discarded |
| Delete-values      | Deletes CBCP statistics                      |

### Status/PPP-statistics/CCP-statistics

The statistics of the Compression Control Protocol (CCP) show the packets exchanged for data compression during the PPP negotiation.

|                      |                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------|
| Rx-discarded         | Number of all CCP packets discarded                                                                                      |
| Rx-config-request    | Number of CCP queries received                                                                                           |
| Rx-config-ack.       | Number of CCP queries accepted                                                                                           |
| Rx-config-nak.       | Number of CCP queries rejected because query parameters were not accepted.                                               |
| Rx-config-reject     | Number of CCP rejected for other reasons.                                                                                |
| Rx-terminate-request | Number of CCP queries after releasing the compression.                                                                   |
| Rx-terminate-ack.    | Number of confirmed CCP queries after releasing the compression.                                                         |
| Rx-code-reject       | Number of CCP queries rejected because the remote station will not or cannot apply compression.                          |
| Rx-reset-request     | Number of CCP queries after synchronizing the compression (e.g. after transfer errors)                                   |
| Rx-reset-ack.        | Number of confirmed CCP queries after synchronizing the compression                                                      |
| Tx-config-request    | Number of CCP queries sent                                                                                               |
| Tx-config-ack.       | Number of CCP queries accepted by the remote station                                                                     |
| Tx-config-nak.       | Number of CCP queries rejected by the remote station because of parameters not being accepted.                           |
| Tx-config-reject     | Number of CCP queries rejected by the remote station for other reasons.                                                  |
| Tx-terminate-request | Number of CCP queries sent after releasing the compression.                                                              |
| Tx-terminate-ack.    | Number of CCP confirmations sent for releasing the compression.                                                          |
| Tx-code-reject       | Number of CCP queries rejected because the <i>ELSA LANCOM</i> does not wish to use compression (by layer list settings). |
| Tx-reset-request     | Number of CCP queries sent after synchronizing the compression (e.g. after transfer errors)                              |
| Tx-reset-ack.        | Number of CCP confirmations sent for synchronizing the compression                                                       |
| Delete-values        | Deletes CCP statistics                                                                                                   |

Status/PPP-statistics/ML-statistics

The MLPPP statistics mostly provide information on how the remote station handled the individual packets during a bundled PPP connection.

|                    |                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Bundle-connections | Number of connections that used the MLPPP.                                                                                                         |
| Rx-Seq-loss        | Number of packets in which an error occurred in the sequence of sequence numbers.                                                                  |
| Rx-Seq-repeat      | Number of packets in which the sequence of sequence numbers came late.                                                                             |
| Rx-Mrru-exceeded   | Number of packets in which a violation of the MRRU negotiated in the PPP negotiation was found after assembly (maximum received reassembled unit). |
| Rx-Header-error    | Number of packets with header errors.                                                                                                              |
| Rx-discarded       | Number of all discarded MLPPP packets.                                                                                                             |
| Rx-Frag-start      | Number of packets with a start flag set (first part of a fragmented packet).                                                                       |
| Rx-Frag-mid        | Number of packets with set mid flag (middle part of a fragmented packet).                                                                          |
| Rx-Frag-end        | Number of packets with set end flag (last part of a fragmented packet).                                                                            |
| Rx-not-fragmented  | Number of packets with set start and end flag (unfragmented packets).                                                                              |
| Delete-values      | Delete ML statistics                                                                                                                               |

Status/PPP-statistics/Rx- and Tx-options

The PPP statistics options show what information was exchanged during the negotiation over LCP, IPCP or IPXCP.




Rx-options

This shows information on what the remote station requested (LCP) or what was assigned to the router (IPCP and IPXCP).

Tx-options

This shows information on what the router requested from the remote station (LCP) or what it assigned to it (IPCP and IPXCP).

The two submenus have the same layout:

| /Rx- and Tx-options | Display                                                                             |                                                                                   |
|---------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| LCP                 |  | Information on packet sizes, control characters, security procedures and callback |
| IPXCP               |  | Information on addresses and routing procedures in the IPX network                |
| IPCP                |  | Information on addresses in the IP network                                        |

The LCP table has separate listings for every channel:

|          |                                                                                                                                                                        |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MRU      | <b>M</b> aximum <b>R</b> eceive <b>U</b> nit designates the maximum packet size that the remote station can receive                                                    |
| ACCM     | <b>A</b> synchronous <b>C</b> ontrol <b>C</b> haracter <b>M</b> ap designates the character in the asynchronous data flow that is interpreted as the control character |
| Authent. | Authentication procedure used (PAP/CHAP)                                                                                                                               |
| Callback | Callback negotiation type                                                                                                                                              |

The IPXCP table shows the negotiated IPX option separately for every channel:








|                |                                                                                                                                                                                                                                                  |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network        | Network number of the WAN network                                                                                                                                                                                                                |
| Node-ID        | The Rx options show the node ID assigned to the <i>ELSA LANCOM</i> (generally 000000000000 or the MAC address of the router). The Tx options show the node ID of the remote station (also 000000000000 or the MAC address of the remote station) |
| Routing-method | The routing protocol in use is given here (RIP/SAP or nothing), in the Rx what the remote station has assigned to us and in the Tx the one that the <i>ELSA LANCOM</i> assigns to the remote station.                                            |

Finally, IPCP has the negotiated IP options, again separated according to the channel:

|              |                                                                                                                                                                                                                                                                                    |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP-address   | Again the Rx options have the addresses that were assigned by the remote station and the Tx options have those that the <i>ELSA LANCOM</i> assigned to the remote station (e.g. the IP address of the dial-up node at the Internet provider can easily be read in the Tx options). |
| DNS-default  |                                                                                                                                                                                                                                                                                    |
| NBNS-default |                                                                                                                                                                                                                                                                                    |

## Status/IPX-statistics

The statistics from the IPX area are grouped here and classified by type, socket and router information. The IPX statistics contain the following parameters:

| /IPX-statistics       | Statistics from the IPX and IPX router area                                         |                                                     |
|-----------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------|
| MAC-statistics        |  | Statistics from the IPX packet media access control |
| Watchdog-statistics   |  | Statistics for watchdog packets                     |
| Propagate-statistics  |  | Statistics for IPX propagated packets (IPX type 20) |
| RIP-statistics        |  | Statistics for NetWare RIP                          |
| SAP-statistics        |  | Statistics for NetWare SAP                          |
| IPX-router-statistics |  | Statistics on the remote IPX router                 |
| Delete-values         |  | Deletes IPX statistics                              |

The substatistics then provide you with further parameters for the individual menus.

### **Status/IPX-statistics/MAC-statistics**

These statistics include the following values:

|                       |                                                                |
|-----------------------|----------------------------------------------------------------|
| IPX-LAN-rx            | Number of IPX packets received from the LAN                    |
| IPX-LAN-rx-broadcasts | Number of broadcast IPX packets received from the LAN          |
| IPX-LAN-rx-multicasts | Number of multicast IPX packets received from the LAN          |
| IPX-LAN-rx-unicasts   | Number of directly addressed IPX packets received from the LAN |
| IPX-LAN-tx            | Number of IPX packets sent to the LAN                          |
| IPX-WAN-rx            | Number of IPX packets received from the WAN                    |
| IPX-WAN-rx-broadcasts | Number of broadcasts received from the WAN                     |
| IPX-WAN-rx-multicasts | Number of multicasts received from the WAN                     |
| IPX-WAN-rx-unicasts   | Number of directly addressed IPX packets received from the WAN |
| IPX-WAN-tx            | Number of IPX packets sent to the WAN                          |
| Delete-values         | Deletes MAC statistics                                         |

### **Status/IPX-statistics/Watchdog-statistics**

These statistics include the following values:

|                     |                                                      |
|---------------------|------------------------------------------------------|
| IPX-watchdog-LAN-rx | Number of IPX watchdog packets received from the LAN |
| IPX-watchdog-LAN-tx | Number of IPX watchdog packets sent to the LAN       |
| IPX-watchdog-WAN-rx | Number of IPX watchdog packets received from the WAN |
| IPX-watchdog-WAN-tx | Number of IPX watchdog packets sent to the WAN       |
| SPX-watchdog-LAN-rx | Number of SPX watchdog packets received from the LAN |
| SPX-watchdog-LAN-tx | Number of SPX watchdog packets sent to the LAN       |
| SPX-watchdog-WAN-rx | Number of SPX watchdog packets received from the WAN |
| SPX-watchdog-WAN-tx | Number of SPX watchdog packets sent to the WAN       |
| Delete-values       | Deletes watchdog statistics                          |

### **Status/IPX-statistics/Propagate-statistics**

These statistics include the following values:

|                             |                                                                           |
|-----------------------------|---------------------------------------------------------------------------|
| Propagate-LAN-rx            | Number of IPX propagated packets received from the LAN                    |
| Propagate-LAN-filters       | Number of IPX propagated packets from the LAN that were received/filtered |
| Propagate-LAN-tx            | Number of IPX propagated packets sent to the LAN                          |
| Propagate-LAN-socket-errors | Number of IPX propagated packets from the LAN filtered by socket filter   |

|                                |                                                                           |
|--------------------------------|---------------------------------------------------------------------------|
| Propagate-LAN-hop-errors       | Number of IPX propagated packet filtered from the LAN by hop count        |
| Propagate-LAN-backroute-errors | Number of IPX propagated packets to be backrouted from the LAN            |
| Propagate-LAN-contention       | Number of packets to be routed from the LAN during a defective connection |
| Propagate-WAN-rx               | Number of IPX propagated packets received from the WAN                    |
| Propagate-WAN-filters          | Number of IPX propagated packets from the WAN that were received/filtered |
| Propagate-WAN-tx               | Number of IPX watchdog packets sent to the WAN                            |
| Propagate-WAN-socket-errors    | Number of IPX propagated packets filtered from the WAN by socket filter   |
| Delete-values                  | Deletes IPX propagated packet statistics                                  |

### Status/IPX-statistics/RIP-statistics

These statistics include the following values:

|                |                                                                    |
|----------------|--------------------------------------------------------------------|
| RIP-LAN-rx     | Number of RIP packets received from the LAN                        |
| RIP-LAN-errors | Number of RIP packets with defective content received from the LAN |
| RIP-LAN-tx     | Number of RIP packets sent to the LAN                              |
| RIP-WAN-rx     | Number of RIP packets received from the WAN                        |
| RIP-WAN-errors | Number of RIP packets with defective content received from the WAN |
| RIP-WAN-tx     | Number of RIP packets sent to the WAN                              |
| Delete-values  | Deletes RIP statistics                                             |
| Table-RIP      | Displays RIP table                                                 |

#### Table-RIP

There are 256 entries with RIP information in the **RIP table**. It has the following layout:

| Network         | Hops                                                            | Tics                                 | Node ID                   | Time                                               | Flags                       |
|-----------------|-----------------------------------------------------------------|--------------------------------------|---------------------------|----------------------------------------------------|-----------------------------|
| Network address | Number of routers to be passed on the path to the other network | Time required for this route in tics | MAC address of the server | Number of table updates until the entry is deleted | Local, remote, loop or down |

### Status/IPX-statistics/SAP-statistics

These statistics include the following values:

|                |                                                                    |
|----------------|--------------------------------------------------------------------|
| SAP-LAN-rx     | Number of SAP packets received from the LAN                        |
| SAP-LAN-errors | Number of SAP packets with defective content received from the LAN |
| SAP-LAN-tx     | Number of SAP packets sent to the LAN                              |
| SAP-WAN-rx     | Number of SAP packets received from the WAN                        |
| SAP-WAN-errors | Number of SAP packets with defective content received from the WAN |

|               |                                             |
|---------------|---------------------------------------------|
| SAP-WAN-tx    | Number of SAP packets sent to the WAN       |
| Table-SAP     | Number of SAP packets received from the LAN |
| Delete-values | Deletes SAP statistics                      |

*Table-SAP* There are 512 entries with SAP information in the **SAP table**. It has the following layout:

| Type            | Server-name          | Network         | Node ID                   | Socket                 | Hops                                         | Time                                               | Flags                       |
|-----------------|----------------------|-----------------|---------------------------|------------------------|----------------------------------------------|----------------------------------------------------|-----------------------------|
| Service SAP no. | Server computer name | Network address | MAC address of the server | Socket for the service | Number of routers to the destination network | Number of table updates until the entry is deleted | Local, remote, loop or down |

### Status/IPX-statistics/IPX-router-statistics

These statistics include the following values:

|                           |                                                                           |
|---------------------------|---------------------------------------------------------------------------|
| IPXr-LAN-rx               | Number of IPX packets to be routed from the LAN                           |
| IPXr-LAN-tx               | Number of IPX packets routed to the LAN                                   |
| IPXr-LAN-hop-errors       | Number of IPX packets filtered by hop count to be routed from the LAN     |
| IPXr-LAN-socket-errors    | Number of IPX packets filtered by socket filter to be routed from the LAN |
| IPXr-LAN-net-errors       | Number of packets from the LAN to be routed to incorrect networks         |
| IPXr-LAN-backroute-errors | Number of IPX packets to be backrouted from the LAN                       |
| IPXr-LAN-contention       | Number of packets to be routed from the LAN during a defective connection |
| IPXr-LAN-down-errors      | Number of IPX packets to be routed from the LAN to logged-off networks    |
| IPXr-WAN-rx               | Number of IPX packets to be routed from the WAN                           |
| IPXr-WAN-tx               | Number of IPX packets routed to the WAN                                   |
| IPXr-WAN-hop-errors       | Number of IPX packets filtered by hop count to be routed from the WAN     |
| IPXr-WAN-socket-errors    | Number of IPX packets filtered by socket filter to be routed from the WAN |
| IPXr-WAN-net-errors       | Number of packets from the WAN to be routed to incorrect networks         |
| IPXr-WAN-backroute-errors | Number of IPX packets to be backrouted from the WAN                       |
| IPXr-WAN-down-errors      | Number of IPX packets to be routed from the WAN to logged-off networks    |
| IPXr-intern-rx            | Number of packets from internal modules to the IPX router                 |
| Networks                  | Table of networks in the IPX routing table with node IDs                  |
| Establish-table           | Table of the last 20 packets that required a connection                   |
| Delete-values             | Deletes IPX router statistics                                             |

*Establish-table* The **establish table** is a further submenu option within router statistics. It contains the last 20 entries, which provide information on the system time, the IPX destination address, and the IPX source address of the data packets that have caused a connection to be established.

An IPX establish table might have the following appearance:

| Time         | Destination            | Source                     |
|--------------|------------------------|----------------------------|
| 1T; 16:45:01 | 00000081 ffffffff 0453 | 00000001 00a05702000a 0453 |
| 1T; 10:45:10 | 00000081 ffffffff 0452 | 00000001 00a05702000a 0452 |

The 'Time' is displayed as the device operating time or the ISDN real time (if this is available from the ISDN terminal). The destination address 'fffffff' might refer, for example, to a broadcast packet. The destination and source addresses both consist of the network number, MAC address and the socket number (all hexadecimal values).

*Networks* The **network statistics** are also a submenu option within the IPX router statistics. This table provides more extensive information on a static route (remote station). It has the following layout:

| Remote-ID              | Network         | Binding | Propagate    | Backoff            | Time                                 | Node-ID                   |
|------------------------|-----------------|---------|--------------|--------------------|--------------------------------------|---------------------------|
| Logical remote station | Network address | Binding | Route/Filter | Connection counter | Time remaining until next connection | Node-ID of remote station |










The different entries have the following meaning:

|           |                                                                                                                                                                                                                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote-ID | Logical name of the remote station as it is entered in the routing table. An entry for the LAN link is also present; it is located in the first position in the table and has the name "LAN".                                                                                                                 |
| Network   | Address of the network in which the remote station is located. For remote WAN stations, this corresponds to the entry in the routing table. If the autodetect function is configured in the IPX routing table (/SETUP/IPX-MODULE/LAN-CONFIGURATION/NETWORK), the network that was detected is displayed here. |
| Binding   | Ethernet binding to which the remote station is linked. For remote WAN stations, this corresponds to the entry in the routing table. If the autodetect function is configured in the IPX routing table (/SETUP/IPX-MODULE/LAN-CONFIGURATION/NETWORK), the binding that was detected is displayed here.        |
| Propagate | Filter flag for IPX type 20 (propagated) frames. For remote WAN stations, this corresponds to the entry in the routing table. For the LAN, a route is always entered here.                                                                                                                                    |

|         |                                                                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backoff | Connection counter for the exponential backoff algorithm. When the connection counter reaches a value of 16, no more attempts are made, meaning that the route is deactivated (also possible for the LAN).                               |
| Time    | Time remaining (specified in seconds) until the next connection attempt is made by the exponential backoff algorithm. When a connection has been successfully established, the remaining time is set to zero, thus activating the route. |
| Node ID | Node ID of the responsible router in the WAN network. The node ID of the router is entered here for the LAN entry.                                                                                                                       |

## Status/TCP-IP-statistics

The TCP/IP-related statistics are shown here, broken down according to the various TCP/IP sub-protocols. The TCP/IP statistics contain the following parameters:

| /TCP-IP-statistics |                                                                                     | Statistics from the TCP/IP area                            |
|--------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------|
| ARP-statistics     |    | Statistics from the ARP area                               |
| IP-statistics      |    | Statistics from the IP area                                |
| ICMP-statistics    |    | Statistics for ICMP packets                                |
| TFTP-statistics    |    | Statistics for TFTP operations                             |
| TCP-statistics     |  | Statistics for TCP packets from TCP sessions to the router |
| DCHP-statistics    |  | Statistics from the DCHP server                            |
| Delete-values      |  | Deletes TCP/IP statistics                                  |
| NetBIOS-statistics |  | NetBIOS module statistics                                  |
| DNS-statistics     |  | Statistics from the DNS server                             |

The substatistics then provide you with further parameters for the individual menus.

### Status/TCP-IP-statistics/ARP-statistics

These statistics include the following values:

|                |                                                            |
|----------------|------------------------------------------------------------|
| ARP-LAN-rx     | Number of ARP requests and responses received from the LAN |
| ARP-LAN-tx     | Number of ARP requests and responses sent to the LAN       |
| ARP-LAN-errors | Number of ARP requests incorrectly received from the LAN   |
| ARP-WAN-rx     | Number of ARP requests and responses received from the WAN |
| ARP-WAN-tx     | Number of ARP requests and responses sent to the WAN       |
| ARP-WAN-errors | Number of ARP requests incorrectly received from the WAN   |
| Table-ARP      | Displays ARP table                                         |
| Delete-values  | Deletes ARP statistics                                     |



*Table-ARP*

There are 128 entries with ARP information in the **ARP table**. It has the following layout:

| IP-address                                               | Node-ID                | Last-access                        | Connect         |
|----------------------------------------------------------|------------------------|------------------------------------|-----------------|
| IP address that has previously been found by ARP request | Associated MAC address | Time since the last access in tics | Local or remote |

### Status/TCP-IP-statistics/IP-statistics

These statistics include the following values:

|                        |                                                                     |
|------------------------|---------------------------------------------------------------------|
| IP-LAN-rx              | Number of IP packets received from the LAN                          |
| IP-LAN-tx              | Number of IP packets sent to the LAN                                |
| IP-LAN-checksum-errors | Number of IP packets incorrectly received from the LAN              |
| IP-LAN-service-errors  | Number of IP packets received from the LAN for an incorrect service |
| IP-WAN-rx              | Number of IP packets received from the WAN                          |
| IP-WAN-tx              | Number of IP packets sent to the WAN                                |
| IP-WAN-checksum-errors | Number of IP packets incorrectly received from the WAN              |
| IP-WAN-service-errors  | Number of IP packets received from the WAN for an incorrect service |
| IP-WAN-rx-disconnect   | Number of packets from the WAN discarded by timeout                 |
| Delete-values          | Deletes IP statistics                                               |

### Status/TCP-IP-statistics/ICMP-statistics

These statistics include the following values:

|                          |                                                            |
|--------------------------|------------------------------------------------------------|
| ICMP-LAN-rx              | Number of ICMP packets received from the LAN               |
| ICMP-LAN-tx              | Number of ICMP packets sent to the LAN                     |
| ICMP-LAN-checksum-errors | Number of ICMP packets incorrectly received from the LAN   |
| ICMP-LAN-service-errors  | Number of non-supported ICMP packets received from the LAN |
| ICMP-WAN-rx              | Number of ICMP packets received from the WAN               |
| ICMP-WAN-tx              | Number of ICMP packets sent to the WAN                     |
| ICMP-WAN-checksum-errors | Number of ICMP packets incorrectly received from the WAN   |
| ICMP-WAN-service-errors  | Number of non-supported ICMP packets received from the WAN |
| Delete-values            | Deletes ICMP statistics                                    |

**Status/TCP-IP-statistics/TCP-statistics**

These statistics include the following values:

|                         |                                                                   |
|-------------------------|-------------------------------------------------------------------|
| TCP-LAN-rx              | Number of TCP packets received from the LAN                       |
| TCP-LAN-tx              | Number of TCP packets sent to the LAN                             |
| TCP-LAN-tx-repeats      | Number of TCP packets repeatedly sent to the LAN                  |
| TCP-LAN-checksum-errors | Number of TCP packets incorrectly received from the LAN           |
| TCP-LAN-service-errors  | Number of TCP packets received from the LAN for an incorrect port |
| TCP-LAN-connections     | Current number of TCP connections from the LAN                    |
| TCP-WAN-rx              | Number of TCP packets received from the WAN                       |
| TCP-WAN-tx              | Number of TCP packets sent to the WAN                             |
| TCP-WAN-tx-repeats      | Number of TCP packets repeatedly sent to the WAN                  |
| TCP-WAN-checksum-errors | Number of TCP packets incorrectly received from the WAN           |
| TCP-WAN-service-errors  | Number of TCP packets received from the WAN for an incorrect port |
| TCP-WAN-connections     | Current number of TCP connections from the WAN                    |
| Delete-values           | Deletes TCP statistics                                            |

**Status/TCP-IP-statistics/TFTP-statistics**

These statistics include the following values:

|                           |                                                          |
|---------------------------|----------------------------------------------------------|
| TFTP-LAN-rx               | Number of TFTP packets received from the LAN             |
| TFTP-LAN-rx-read-request  | Number of TFTP read requests received from the LAN       |
| TFTP-LAN-rx-write-request | Number of TFTP write requests received from the LAN      |
| TFTP-LAN-rx-data          | Number of TFTP data packets received from the LAN        |
| TFTP-LAN-rx-ack.          | Number of TFTP acknowledges received from the LAN        |
| TFTP-LAN-rx-option-ack.   | Number of TFTP option acknowledges received from the LAN |
| TFTP-LAN-rx-errors        | Number of TFTP error packets received from the LAN       |
| TFTP-LAN-rx-bad-packets   | Number of unknown TFTP packets received from the LAN     |
| TFTP-LAN-tx               | Number of TFTP packets sent to the LAN                   |
| TFTP-LAN-tx-data          | Number of TFTP data packets sent to the LAN              |
| TFTP-LAN-tx-ack.          | Number of TFTP acknowledges sent to the LAN              |
| TFTP-LAN-tx-option-ack.   | Number of TFTP option acknowledges sent to the LAN       |
| TFTP-LAN-tx-errors        | Number of TFTP error packets sent to the LAN             |
| TFTP-LAN-tx-repeats       | Number of TFTP packets repeatedly sent to the LAN        |
| TFTP-LAN-connections      | Number of TFTP connections established to the LAN        |
| TFTP-WAN-rx               | Number of TFTP packets received from the WAN             |
| TFTP-WAN-rx-read-request  | Number of TFTP read requests received from the WAN       |

|                           |                                                          |
|---------------------------|----------------------------------------------------------|
| TFTP-WAN-rx-write-request | Number of TFTP write requests received from the WAN      |
| TFTP-WAN-rx-data          | Number of TFTP data packets received from the WAN        |
| TFTP-WAN-rx-ack.          | Number of TFTP acknowledges received from the WAN        |
| TFTP-WAN-rx-option-ack.   | Number of TFTP option acknowledges received from the WAN |
| TFTP-WAN-rx-errors        | Number of TFTP error packets received from the WAN       |
| TFTP-WAN-rx-bad-packets   | Number of unknown TFTP packets received from the WAN     |
| TFTP-WAN-tx               | Number of TFTP packets sent to the WAN                   |
| TFTP-WAN-tx-data          | Number of TFTP data packets sent to the WAN              |
| TFTP-WAN-tx-ack.          | Number of TFTP acknowledges sent to the WAN              |
| TFTP-WAN-tx-option-ack.   | Number of TFTP option acknowledges sent to the WAN       |
| TFTP-WAN-tx-errors        | Number of TFTP error packets sent to the WAN             |
| TFTP-WAN-tx-repeats       | Number of TFTP packets repeatedly sent to the WAN        |
| TFTP-WAN-connections      | Number of TFTP connections established to the WAN        |
| Delete-values             | Deletes TFTP statistics                                  |

### Status/TCP-IP-statistics/DHCP-statistics

These statistics include the following values:












|                    |                                                                        |
|--------------------|------------------------------------------------------------------------|
| DHCP-LAN-rx        | Number of DHCP packets received from the LAN                           |
| DHCP-LAN-tx        | Number of DHCP packets sent to the LAN                                 |
| DHCP-WAN-rx        | Number of DHCP packets received from the LAN                           |
| DHCP-discard       | Number of DHCP packets discarded                                       |
| DHCP-rx-discover   | Number of discover messages received                                   |
| DHCP-rx-request    | Number of request messages received                                    |
| DHCP-rx-decline    | Number of decline messages received                                    |
| DHCP-rx-inform     | Number of inform messages received                                     |
| DHCP-rx-release    | Number of release messages received                                    |
| DHCP-tx-offer      | Number of offer messages sent                                          |
| DHCP-tx-ack.       | Number of DHCP packets acknowledged                                    |
| DHCP-tx-nak.       | Number of DHCP packets not acknowledged                                |
| DCHP-server-err.   | Number of DHCP packets received that were not intended for this server |
| DHCP-assigned      | Number of addresses currently assigned                                 |
| DHCP-MAC-conflicts | Number of assignments rejected because IP addresses were in use        |
| Table-DHCP         | Table containing assignments of IP addresses to MAC addresses          |
| Delete-values      | Deletes DHCP statistics                                                |

*Table-DHCP*      There are entries with DHCP information in the **DHCP table**. It contains 16 entries (or multiples of 16). The table adapts dynamically to the given requirements and grows or shrinks accordingly. It has the following layout:

| IP-address                   | Node-ID                | Timeout                                    | Hostname      | Type            |
|------------------------------|------------------------|--------------------------------------------|---------------|-----------------|
| IP address assigned via DHCP | Associated MAC address | Duration of assignment validity in minutes | Computer name | Assignment type |

**Status/TCP-IP-statistics/NetBIOS**

Additional information about the NetBIOS module can be found in the /Status/TCP-IP-statistics/NetBIOS-statistics menu. This menu has the following structure:

|                |                                                                                     |                                                                                                                                                                                                                                                                                                          |
|----------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LAN-Rx, WAN-Rx |    | Number of NetBIOS packets received by the LAN or WAN                                                                                                                                                                                                                                                     |
| LAN-Tx, WAN-Tx |    | Number of NetBIOS packets sent to the LAN or WAN                                                                                                                                                                                                                                                         |
| Registers      |    | Number of name registrations performed                                                                                                                                                                                                                                                                   |
| Conflicts      |    | Number of detected name conflicts. As the NetBIOS module is only a billboard to which each computer attaches its name, it also does not verify the consistency of the data. The counter is thus only incremented if a host determines a conflict and broadcasts a message to the network to this effect. |
| Releases       |  | Number of name shares performed                                                                                                                                                                                                                                                                          |
| Refreshs       |  | Number of name renewals performed                                                                                                                                                                                                                                                                        |
| Timeouts       |  | Number of names dropped due to aging                                                                                                                                                                                                                                                                     |
| B-Nodes        |  | Number of currently active B nodes (broadcast) in the network                                                                                                                                                                                                                                            |
| P-Nodes        |  | Number of currently active P nodes (peer-to-peer) in the network                                                                                                                                                                                                                                         |
| M-Nodes        |  | Number of currently active M nodes (mixed-mode) in the network                                                                                                                                                                                                                                           |
| W-Nodes        |  | Number of currently active W nodes (hybrid) in the network                                                                                                                                                                                                                                               |

*B-Nodes*      Broadcast nodes. A B node performs name negotiations exclusively via broadcasts. Such a computer is not visible over a router connection, since broadcasts may not be routed.












*P-Nodes*      Point-to-point nodes. For name negotiations, a P node requires a NetBIOS nameserver (NBNS) as well as a NetBIOS datagram distribution server (NBDD) to transfer datagrams over a router.

*M-Nodes*      Mixed nodes. This type is a mixture of B and P nodes. It acts as a B node in the local network; if the required partner can't be found in the local network, it attempts to locate it using an NBNS query (P node behavior).

*W-Nodes*      This type of node is not permissible according to RFC, but was introduced nevertheless by Microsoft as a hybrid node.

### Status/TCP-IP-statistics/DNS-statistics

The DNS statistics provide supplementary information about the DNS module. This menu has the following structure:

|                |                                                                                     |                                                                                                                |
|----------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| LAN-Rx         |    | Number of DNS packets received by the LAN                                                                      |
| LAN-Tx         |    | Number of DNS packets sent on the LAN                                                                          |
| WAN-Rx         |    | Number of DNS packets received by the WAN                                                                      |
| WAN-Tx         |    | Number of DNS packets sent on the WAN                                                                          |
| Forwarded      |    | Number of requests that could not be fulfilled and were thus forwarded                                         |
| Errors         |    | Number of invalid requests                                                                                     |
| DNS-access     |    | Indicates the number of names that were looked up from the DNS table                                           |
| DHCP-access    |    | Indicates the number of names that were looked up from the DHCP table                                          |
| NetBIOS-access |    | Indicates the number of names that were looked up from the Net-BIOS tables                                     |
| Hit-list       |    | This table contains the 16 most popular requests. These may then be prohibited via the filter list if desired. |
| Delete values  |  | Deletes DNS statistics                                                                                         |

The hit list has the following structure:

| Domain       | Requests | Time                | IP-address |
|--------------|----------|---------------------|------------|
| www.elsa.com | 1        | 00.00.0000 00:00:29 | 10.0.0.123 |






















The individual fields of this list have the following significance:

|            |                                                                          |
|------------|--------------------------------------------------------------------------|
| Domain     | Name of the requested computer                                           |
| Requests   | Total number of requests for this name since its appearance in the table |
| Time       | Time of the last request                                                 |
| IP-address | Address of the computer that last requested this name                    |

This list is sorted according to the frequency of requests. When the table is full, the names that have not been requested for the longest period will be deleted to make room for new entries.

Status/IP-router-statistics

This menu groups together the statistics from the IP router module.

| /IP-router-statistics  | Statistics from the IP router area                                                  |                                                               |
|------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------|
| IPr-LAN-rx             |    | Number of data packets to be routed from the LAN              |
| IPr-LAN-tx             |    | Number of data packets routed to the LAN                      |
| IPr-LAN-local-routings |    | Number of packets received from the LAN and routed to the LAN |
| IPr-LAN-network-errors |    | Number of LAN packets that were not routed                    |
| IPr-LAN-routing-errors |    | Number of LAN packets that must be sent to another router     |
| IPr-LAN-ttl-errors     |    | Number of LAN packets with an expired time-to-live value      |
| IPr-LAN-filters        |    | Number of LAN packets filtered by the filter table            |
| IPr-LAN-discards       |    | Number of LAN packets discarded                               |
| IPr-WAN-rx             |    | Number of data packets to be routed from the WAN              |
| IPr-WAN-tx             |    | Number of data packets routed to the WAN                      |
| IPr-WAN-network-errors |    | Number of WAN packets that were not routed                    |
| IPr-WAN-ttl-errors     |   | Number of WAN packets with an expired time-to-live value      |
| IPr-WAN-filters        |  | Number of WAN packets filtered by the filter table            |
| IPr-WAN-discards       |  | Number of WAN packets discarded                               |
| IPr-WAN-type-errors    |  | Number of packets from the WAN without an IP router ID        |
| IPr-ARP-errors         |  | Number of unsuccessful accesses to the ARP cache              |
| Delete-values          |  | Deletes IP router statistics                                  |
| Establish-table        |  | Table of the last 20 packets that required a connection       |
| Protocol-table         |  | Table of routed packets arranged by protocol                  |
| RIP-statistics         |  | Statistics from the IP/RIP area                               |
| Delete values          |  | Deletes IP-router statistics                                  |

*Establish-table* The **establish table** contains the last 20 entries, which provide information on the system time, destination and source addresses, IP protocol, destination port and source port of the data packets that should have caused a connection to be established.

An IP router establish table might have the following appearance:

| Time         | Dest.-address  | Src.-address   | Prot. | D-port | S-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   |

The 'Time' is displayed as either the device operating time or the system time of the ISDN (if provided by the ISDN terminal). The destination and source addresses are IP addresses. The protocol might refer, for example, to tcp, udp, or the like; the destination and source ports provide a more detailed description of the relevant services (e.g. Telnet via TCP and D-port 23, name server via UDP and D-port 53).

#### Protocol-table

The protocol table also supplies valuable information on the volume of packets transferred to the LAN or WAN. These values are encrypted as per the various IP protocols, such as ICMP, TCP, UDP.

A protocol table might have the following appearance:

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

#### Status/IP-router-statistics/RIP-statistics

This option allows you to display the IP-RIP packets received by the device. These substatistics provide you with the following entries:

|                  |                                                       |
|------------------|-------------------------------------------------------|
| RIP-rx           | Number of IP-RIP packets received                     |
| RIP-request      | Number of IP-RIP request packets received             |
| RIP-response     | Number of IP-RIP response packets received            |
| RIP-discards     | Number of IP-RIP packets discarded                    |
| RIP-errors       | Number of defective IP-RIP packets                    |
| RIP-entry-errors | Number of defective entries in IP-RIP packets         |
| RIP-tx           | Number of IP-RIP packets sent                         |
| Table-IP-RIP     | Routing table of routes learned through RIP broadcast |
| Delete values    | Deletes RIP-statistics                                |

#### Table-RIP












The associated RIP table contains all of the routes learned from the network. The router itself maintains this table; you cannot modify it manually.

An IP-RIP table might have the following appearance:

| IP-address    | IP-netmask    | Time | Distance | Router       |
|---------------|---------------|------|----------|--------------|
| 223.245.254.0 | 255.255.255.0 | 1    | 1        | 192.38.9.100 |
| 223.245.257.0 | 255.255.255.0 | 1    | 1        | 192.38.9.200 |










## Status/Config-statistics

This menu allows you to display the statistics from the remote configuration area. It allows you to retrieve information on the number of past and present configuration sessions at any time. Encryption is performed by LAN, WAN and outband port.




















| /Config-statistics         | Remote configuration statistics                                                     |                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| LAN-active-connections     |    | Current number of active configuration connections from the LAN                 |
| LAN-total-connections      |    | Total number of configuration connections from the LAN up until the present     |
| WAN-active-connections     |    | Current number of active configuration connections from the WAN                 |
| WAN-total-connections      |    | Total number of configuration connections from the WAN up until the present     |
| Outband-active-connections |    | Current number of active outband configuration connections                      |
| Outband-total-connections  |    | Total number of previous outband configuration connections up until the present |
| Outband-bitrate            |    | Bit rate of the last outband configuration session                              |
| Login-errors               |   | Total number of defective logins                                                |
| Login-locks                |  | Number of login locks                                                           |
| Login-rejects              |  | Number of login attempts while the login lock was active                        |
| Delete-values              |  | Deletes the config statistics                                                   |

## Status/Queue-statistics

These statistics allow you to observe the flow of the individual packets through the various modules of the *ELSA LANCOM*.

| /Queue-statistics             | Statistics on the queue                                                             |                                           |
|-------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------|
| LAN-heap-packets              |  | Number of buffers available               |
| LAN-queue-packets             |  | Number of buffers in use                  |
| WAN-heap-packets              |  | Number of buffers available               |
| WAN-queue-packets             |  | Number of buffers in use                  |
| Bridge-internal-queue-packets |  | Number of bridge packets from the LAN     |
| Bridge-external-queue-packets |  | Number of bridge packets from the WAN     |
| ARP-query-queue-packets       |  | Number of ARP packets in the query queue  |
| ARP-queue-packets             |  | Number of ARP packets in the normal queue |
| IP-queue-packets              |  | Number of IP packets in the normal queue  |



| /Queue-statistics          |                                                                                     | Statistics on the queue                                                                             |
|----------------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| IP-urgent-queue-packets    |    | Number of IP packets in the secured queue                                                           |
| ICMP-queue-packets         |    | Number of ICMP packets                                                                              |
| TCP-queue-packets          |    | Number of TCP packets                                                                               |
| TFTP-queue-packets         |    | Number of TFTP packets                                                                              |
| SNMP-queue-packets         |    | Number of SNMP packets                                                                              |
| IPX-queue-packets          |    | Number of IPX packets                                                                               |
| RIP-queue-packets          |    | Number of RIP packets                                                                               |
| SAP-queue-packets          |    | Number of SAP packets                                                                               |
| IPX-watchdog-queue-packets |    | Number of watchdog-packets                                                                          |
| SPX-watchdog-queue-packets |    | Number of SPX watchdog packets                                                                      |
| IPX-router-queue-packets   |    | Number of IPX router packets                                                                        |
| Prot-heap-packets          |    | Number of prot heap packets                                                                         |
| IPr-queue-packets          |    | Number of packets remaining to be processed by the IP router.                                       |
| DHCP-server-queue-packets  |   | Number of packets in the receive queue of the DHCP server.                                          |
| IPR-RIP-queue-packets      |  | Number of packets in the receive queue of the IP-RIP module (for RIP queries, RIP propagations...). |
| DNS-Tx-queue-packets       |  | Number of packets to be forwarded to DNS or NBNS servers.                                           |
| DNS-Rx-queue-packets       |  | Number of packets that come from DNS or NBNS servers and are to be forwarded to the host.           |
| IP-Masq.-Tx-queue-packets  |  | Number of packets to be sent masked (to the Internet).                                              |
| IP-Masq.-Rx-queue-packets  |  | Number of packets received from the Internet and have to be demasked.                               |

## Status/Connection-statistics

This menu allows you to display connection times, all charges incurred and other useful information related to ISDN port utilization.

For each available interface, the **Status/Conn.-statistics** menu option provides statistics on the connections established via this interface. The table maintained here has the following layout:

| Ifc  | Connection | Active | Passive | Errors | Con.-Time     | Charge |
|------|------------|--------|---------|--------|---------------|--------|
| Ch01 | 0          | 0      | 0       | 0      | No connection | 0      |
| Ch02 | 0          | 0      | 0       | 0      | No connection | 0      |

Below is a detailed description of the meaning of each field:

|            |                                                                                                                               |
|------------|-------------------------------------------------------------------------------------------------------------------------------|
| Ifc        | Designates the associated channel.                                                                                            |
| Connection | Indicates the number of connections to the particular channel.                                                                |
| Active     | Indicates the number of connections actively established for the channel.                                                     |
| Passive    | Indicates the number of connections established for the channel by incoming calls.                                            |
| Errors     | Indicates the number of connection errors.                                                                                    |
| Con.-Time  | Indicates the period of time the current connection has existed. If no connection exists, "No-connection" is output.          |
| Charge     | Indicates the amount of charges for the current connection. This value is reset to zero when a new connection is established. |

The total charges incurred are not displayed directly. However, the charges are totaled internally in order to permit the management of the charges budget (also see **Setup/Charges-module**).

## Status/Info-connection

The menu item **Status/Info-connection** has additional information on the current connection status (logical remote station etc.) for every available interface. The table maintained here has the following layout:

| Ifc  | Status | Mode | Dialup-remote | Device-name | B1-DT | B2-DT |
|------|--------|------|---------------|-------------|-------|-------|
| Ch01 | Ready  |      |               |             | 0     | 0     |
| Ch02 | Ready  |      |               |             | 0     | 0     |

Below is a detailed description of the meaning of each field:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ifc    | Designates the associated channel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Status | Indicates the status of the particular connection.<br>The possible values are: <b>Init</b> , <b>Setup WAN</b> , <b>Ready</b> , <b>Dial</b> , <b>Incoming call</b> , <b>Protocol</b> , <b>Connection</b> , <b>Callback</b> , <b>Bundle</b> and <b>Reserved</b> . The <b>Bundle</b> status is indicated in the display <i>ELSA LANCOM Business 4100</i> by the addition of a <b>"/2"</b> in columns 15 and 16 of the associated display line. <b>Bundle</b> is displayed for the second interface either when a bundle connection has been activated via the first interface or when a leased-line connection with two B channels has been set. <b>Reserved</b> is displayed for the second interface when a connection exists to the first B channel and the Y connection has been deactivated. |
| Mode   | Reflects the type of establishment. The following are possible:<br><b>Active</b> (active call establishment = dialing)<br><b>Passive</b> (passive call establishment = call acceptance)<br><b>CB</b> (call establishment via callback)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|               |                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dialup-remote | Indicates the call number of the remote station from the name list.                                                                                                                         |
| Device-name   | Indicates the logical name of the remote station (if it can be detected). The device name is also displayed on the appropriate display line as soon as a logical connection is established. |
| B1-DT         | Indicates the short timeout for the connection.                                                                                                                                             |
| B2-DT         | Indicates the short timeout for bundled channels for this connection.                                                                                                                       |

## Status/Layer-connection

The menu item **Status/Layer-connection** has information on the B-channel protocol used on the interface for every available interface. The entries in this table correspond to those in the layer list **Setup/WAN-module/Layer-list** in the WAN module. An additional entry exists for the interface itself. The menu has the following layout:

| Ifc  | WAN-layer | Encaps. | Lay-3 | Lay-2    | L2-Opt. | Lay-1   |
|------|-----------|---------|-------|----------|---------|---------|
| Ch01 | DEFAULT   | ETHER   | ELSA  | X.75ELSA | compr.  | HDLC64K |
| Ch02 | PPPHDL    | TRANS   | TRANS | PPP      | none    | HDLC64K |

## Status/Call-info-table

This table displays the last ten incoming calls, regardless of whether the router answered these calls.

This allows you, for example, to determine the internal MSN used when the system is operated in connection with a PBX. The table has the following layout:

| System-Time  | Ifc            | CLIP-Caller | Dial-Caller | Capab.  | B-chan. |
|--------------|----------------|-------------|-------------|---------|---------|
| OT; 00:20:57 | S <sub>0</sub> | 5678        | 1234        | HDLC64K | 2       |
| OT; 00:20:46 | S <sub>0</sub> | 4321        | 1234        | HDLC64K | 1       |
| OT; 00:19:47 | S <sub>0</sub> | 4321        | 1234        | HDLC64K | 1       |
| OT; 00:11:33 | S <sub>0</sub> | 5678        | 1234        | HDLC64K | 1       |
| OT; 00:01:13 | S <sub>0</sub> | 4321        | 1234        | HDLC64K | 2       |
| OT; 00:01:02 | S <sub>0</sub> | 4321        | 1234        | HDLC64K | 1       |
| OT; 00:00:06 | S <sub>0</sub> | 5678        | 1234        | HDLC64K | 1       |

The different entries have the following meaning:

|             |                                                                                                                                                   |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| System-time | Time when the call came. Either the device operating time or the system time of the ISDN is displayed (if made available from the ISDN terminal). |
| Ifc         | Designates the associated interface.                                                                                                              |
| CLIP-Caller | Call number (CLIP) of the caller                                                                                                                  |

|             |                                                                                                                                        |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Dial-Caller | The MSN/EAZ dialed by the caller                                                                                                       |
| Capab.      | The service requested by the caller.<br>Possible values are HDLC64K, HDLC56K and unknown. An analog call is displayed as unknown here. |
| B-chan.     | The B channel used. A value of 0 means that all channels have already been seized, i.e. call waiting is activated.                     |

*A tip for those using a router in a PBX: Following a call to any ISDN device under the number of the ISDN bus, the MSN/EAZ displayed under 'Dial-Caller' is exactly the entry that must be entered in the router at /SETUP/WAN-MODULE/ROUTER-INTERFACE-LIST/MSN-EAZ in order for a call to be correctly answered from an external station.*

## Status/Remote-statistics

This table shows the last hundred connections of the *ELSA LANCOMs* with information on the remote station.

The table has the following layout:

| Conn.-start  | Remote-ID  | Mode    | Ifc  | Conn.-time | Charge |
|--------------|------------|---------|------|------------|--------|
| OT; 00:20:57 | LONDON     | Active  | Ch01 | 50         | 5      |
| OT; 00:20:46 | MANCHESTER | Passive | Ch02 | 230        | 10     |



The different entries have the following meaning:

|             |                                                                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Conn.-start | Time at which the connection was established. Either the device operating time or the system time of the ISDN is displayed (if made available from the ISDN terminal).                     |
| Remote-ID   | Logical remote station name                                                                                                                                                                |
| Mode        | Type of connection establishment:<br>Active – the connection was actively established by the device<br>Pas. – The device received a call<br>CB – The device called the remote station back |
| Ifc         | Interface, over which the connection is made (Ch01, Ch02).                                                                                                                                 |
| Conn.-time  | Duration of the connection in seconds                                                                                                                                                      |
| Charge      | Charges for this connection in units                                                                                                                                                       |

A connection remains in the table for at least as long as it is established. Every new connection fills the table from top to bottom. If an existing connection is the lowest entry in the table, an already released connection will be deleted from the table instead if necessary.

## Status/S<sub>0</sub>-bus

This option allows you to display the current status of the S<sub>0</sub> interface. The statistics have the following layout:

| /S <sub>0</sub> -bus |                                                                                   | Running status displays                                                   |
|----------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| D-info               |  | Overview of the D channel status                                          |
| D2-statistics        |  | Breakdown of the Layer-2 information of the D channel for the B channels. |

### D-info

This table shows general information related to the D channel:

|                            |                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Channel                    | B-channel identification.                                                                                                                  |
| Protocol                   | D-channel protocol. Either the protocol fixed in the interface table or the protocol detected in the 'Auto' settings at the ISDN terminal. |
| Layer-2                    | Activation of layer 2 of the D channel ('Yes' or 'No')                                                                                     |
| TEI                        | TEI assigned ('Yes' or 'No')                                                                                                               |
| S <sub>0</sub> -activation | Displays activation status ('Yes' or 'No')                                                                                                 |

### D2-statistics

This table shows layer 2 information for the individual B channels:

|               |                                                                                         |
|---------------|-----------------------------------------------------------------------------------------|
| Channel       | B-channel identification.                                                               |
| TEI           | <b>T</b> erminal <b>E</b> quipment <b>I</b> dentifier assigned by the switching center. |
| L2-activation | Activation of layer 2 of the D channel ('Yes' or 'No').                                 |
| Connections   | Number of connections made over the displayed TEI.                                      |

## Status/Channel-statistics

This table shows information on the current status of the two B channels. The information from this table is primarily used for output via *ELSA LANmonitor*. Therefore, some values are shown simply as bits with no further explanation.

The table has the following layout:

| Channel               | State    | App      | Mode    | Cause | Dialup-remote | Sub-address | Charge | Conn.-time | Extra | ISDN-display |
|-----------------------|----------|----------|---------|-------|---------------|-------------|--------|------------|-------|--------------|
| S <sub>0</sub> -1-ERR | 00000000 | Router   | active  | 0000  | 0241123456    | 00000000    | 3      | 0          |       |              |
| S <sub>0</sub> -1-B1  | 00000000 | a/b      | active  | 0000  | 0241123457    | 00000000    | 2      | 20         |       |              |
| S <sub>0</sub> -1-B2  | 00000000 | LAN-CAPI | passive | 0000  | 0241123458    | 00000000    | 4      | 180        |       |              |





Below is a detailed description of the meaning of each field:

|               |                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Channel       | Channel for the entry is valid. Only the latest status of a channel is ever displayed. A dedicated "channel" is maintained for error messages on channels.           |
| State         | The status of a channel is shown here as, e.g., 'ready'.                                                                                                             |
| App           | Application that occupies the channel: Router, <i>LANCAPI</i>                                                                                                        |
| Mode          | Types of last connection establishment: active or passive                                                                                                            |
| Cause         | Last error                                                                                                                                                           |
| Dialup-remote | Remote station call number: with active establishment the number dialed, with incoming calls the number sent.                                                        |
| Subaddress    | Addition to application that, e.g., indicates the logical channel for the router for the <i>LANCAPI</i> , e.g., the IP address of the client that is using the CAPI. |
| Charge        | Number of charging units incurred for this connection.                                                                                                               |
| Conn.-time    | Duration of the last connection on this channel                                                                                                                      |
| Extra         | Additional information on the connection, e.g. the name of the remote station for router connections.                                                                |
| ISDN-display  | Information from the switching center, e.g. error messages, if connected to the PBX possibly also the caller's name, etc.                                            |

## Status/Time-statistics

This menu has information on the current time in the device and on the path over which the *ELSA LANCOM Office* has obtained the time.

The menu has the following layout:

| /Time statistics |                                                                                     | Time module statistics                                                                                                                                                                                                     |
|------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Current-time     |  | Current device time.                                                                                                                                                                                                       |
| Source           |  | Time output source. The possible values are:<br>'ISDN' for time taken from the ISDN,<br>'Manual' for the manual setting of the time with the 'time' command,<br>'RAM' for time imported from the device RAM after booting. |
| Setup            |  | Number of time imports from one of the above sources.                                                                                                                                                                      |
| ISDN             |  | Additional information on time import from the ISDN                                                                                                                                                                        |

## Status/Time-statistics/ISDN







These statistics include the following values:

|               |                                                           |
|---------------|-----------------------------------------------------------|
| Connection    | Number of attempts to read time information from the ISDN |
| Information   | Number of time updates received from the ISDN             |
| Info-error    | Number of erroneous time updates received from the ISDN   |
| Units         |                                                           |
| Delete values | Deletes ISDN statistics                                   |

## Status/LCR-statistics

This menu has information on the current time in the device and on the path over which the *ELSA LANCOM Office* has obtained the time.

The menu has the following layout:

| /LCR-statistics     |                                                                                   | Least-cost router statistics                                                                                              |
|---------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Total calls         |  | Total number of LCR calls                                                                                                 |
| Found-events        |  | Number of calls in which the router found a suitable rule in its tables and successfully rerouted the connection.         |
| Not-found-errors    |  | Number of calls in which the router did not find a suitable rule in its tables and thus could not reroute the connection. |
| Missing time-errors |  | Number of calls in which the LCR could not become active due to lack of time                                              |
| Provider-statistics |  | A table with all providers used (or their prefixes), the number of successful and unsuccessful calls                      |
| Delete values       |  | Deletes LCR statistics                                                                                                    |









## Status/Delete-values








With the exception of the tables, this option allows you to delete all the values in the substatistics. To do so, enter the following command:

```
do delete-values
```

## Setup

This menu allows you to query and modify all the system parameters that are necessary to the functioning of the devices.

| /Setup           |                                                                                     | System configuration                |
|------------------|-------------------------------------------------------------------------------------|-------------------------------------|
| Name             |  | Entering the device name            |
| WAN-module       |  | WAN settings                        |
| Charges-module   |  | Charge management settings          |
| LAN-module       |  | LAN settings                        |
| IPX-module       |  | IPX module (IPX router) settings    |
| TCP-IP-module    |  | TCP/IP module settings              |
| IP-router-module |  | IP router module settings           |
| SNMP-module      |  | Settings for configuration via SNMP |

| /Setup         |                                                                                   | System configuration           |
|----------------|-----------------------------------------------------------------------------------|--------------------------------|
| DHCP-module    |  | DHCP server settings           |
| NetBIOS-module |  | Settings for the NetBIOS proxy |
| Config-module  |  | Configuration module settings  |
| LANCAPI-module |  | <i>ELSA LANCAP</i> i settings  |
| LCR-module     |  | Least-cost router settings     |
| DNS module     |  | DNS server settings            |
| Time-module    |  | Time module settings           |

### Name

Here you can enter the device name (maximum 16 characters). The set of characters available includes uppercase and lowercase letters as well as some special characters. You can display the full range of available characters during a configuration session by entering the following command:

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

In the default configuration, no name is entered.







The device name is required for identification purposes; it is a prerequisite for any connection via the IPX or IP router module, since the routers can exchange data only with known remote stations, and is also required for the unambiguous identification of a remote bridge station.

In the case of PPP connections, either the user name with the password from the PPP list or the device name is transferred to the remote station as a device ID during a verification by PAP or CHAP.







In addition, the device names you assign must be unique. For example, you might match the device names to the location (e.g. Glasgow, London, Provider, etc.).

## Setup/WAN-module

This menu groups together all the settings necessary for starting up the WAN interface and controlling connections to logical remote stations.

| /WAN-module           |                                                                                     | WAN settings                                   |
|-----------------------|-------------------------------------------------------------------------------------|------------------------------------------------|
| Interface-list        |  | S <sub>0</sub> interface settings              |
| Router-interface-list |  | Router module settings                         |
| Channel-list          |  | Settings for the use of the available channels |
| Name-list             |  | Remote station settings                        |
| RoundRobin-list       |  | Settings for different remote station numbers  |
| Layer-list            |  | Settings for the layer combinations used       |



| /WAN-module          |                                                                                   | WAN settings                                                |
|----------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------|
| PPP-list             |  | Parameter settings for PPP connections                      |
| Number-list          |  | Settings for call numbers with access authorization         |
| Script-list          |  | Dial script settings                                        |
| Manual-dialing       |  | Settings for manual connection control                      |
| Protect              |  | Protection for answering incoming calls                     |
| CB-attempts          |  | Number of callback attempts when the remote station is busy |
| Backup-delay-seconds |                                                                                   |                                                             |

*Interface-list*

This table contains the interface settings, which apply to all operating modes (modules) of the devices.

| Ifc | Protocol | LL-B-chan. | Dial-prefix |
|-----|----------|------------|-------------|
| S0  | Auto     | 1          | 0           |

Additional, special interface settings are also available for the various modules, e.g. the call numbers to which a module should react, see also

`Setup/WAN-module/Router-interface-list`

`setup/lancapi-module`

Below is a detailed description of the meaning of each field:

|             |                                                                                                                                                                                                                                                                                                                                                  |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ifc         | Designates the associated interface.                                                                                                                                                                                                                                                                                                             |
| Protocol    | D-channel protocol setting. The possible values are:<br><b>Auto</b> : automatic detection of the D-channel protocol<br><b>DSS1</b> : Euro-ISDN<br><b>1TR6</b> : National ISDN<br><b>GRP0</b> : Leased-line connection group 0<br><b>P2P-DSS1</b> : Point-to-point connection                                                                     |
| LL-B-chan.  | B-channel settings for a leased-line connection. The possible values are:<br><b>none</b> : Leased-line connection not assigned to a specific channel.<br><b>1</b> or <b>2</b> : Leased-line connection operates over the assigned B channel.<br>Please refer to the information on setting these parameters in the fixed connection description. |
| Dial-prefix | Global dialing prefix for all modules of the devices. The digits entered here (maximum 8) are automatically prefixed to the selected call number in every call. Use this prefix when, for example, the router is connected to a PBX.                                                                                                             |

*Router-  
interface-list*

This table contains the interface settings that apply to the router modules of the *ELSA LANCOM*.

| Ifc | MSN/EAZ | YC. | CLIP |
|-----|---------|-----|------|
| S0  | 123456  | Off | On   |

Below is a detailed description of the meaning of each field:

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ifc     | Designates the associated interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MSN-EAZ | <p>If your device is connected to an ISDN port with 1TR6, enter the EAZ to which the interface is to respond.</p> <p>If your device is connected to an ISDN port with DSS1, enter the MSN to which the interface is to respond. If you wish the interface to respond to several different MSNs, enter them here separated by semicolons. A '#' in the list enables any number of incoming MSNs.</p> <p>For outgoing calls, the first MSN in this list will be reported to the remote station. If no MSN is entered, the switching center sends the main MSN of the terminal.</p>                                                                                                                                       |
| YC.     | <p>This entry can be used to control the interface's ability to establish Y connections. Possible settings are:</p> <p><b>On:</b> Y connection is supported; a number of connections can be established simultaneously (default). A channel bundling connection is broken off when a second connection to another remote station has to be established.</p> <p>Refer also to the settings for the availability of the <i>LANCAP</i>.</p> <p><b>Off:</b> Y connection not supported; only one connection can be established. The second connection is blocked. If a connection to an additional remote station is to be established, this establishment is rejected. A channel bundling connection is not affected.</p> |
| CLIP    | <p>Calling Line Identification Protocol: Suppresses the outgoing MSNs.</p> <p>Possible values:</p> <p><b>Yes:</b> Activate CLIR, do not send MSN.</p> <p><b>No:</b> Deactivate CLIR, send MSN to remote station.</p> <p>Please note: The "selective suppression of call number transmission" may be a service feature that will have to be obtained from the telephone company.</p>                                                                                                                                                                                                                                                                                                                                    |

*Channel list*

The channel list specifies the number and sequence of the channels to be established.

| Device-name | Min | Mx | Order           | Backup |
|-------------|-----|----|-----------------|--------|
| LONDON      | 2   | 2  | 1-1;1-2         | 1      |
| INTERNET    | 2   | 2  | 1-1;1-2;2-1;2-2 | 0      |
| DEFAULT     | 1   | 2  | 0               |        |

Below is a detailed description of the meaning of each field:

|             |                                                                                                           |
|-------------|-----------------------------------------------------------------------------------------------------------|
| Device-name | Name of the remote station that is also used in the name and PPP lists.                                   |
| Min         | Number of static channels. These channels are used during every call establishment to the remote station. |

|        |                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mx     | The maximum number of channels to be used for this remote station. The Max-Min difference is the number of dynamic channels.                                                                                                                                                                                                                                                            |
| Order  | This defines which channels are to be established on which S <sub>0</sub> bus.<br>Syntax: [<BusNo>-<ChannelNo>];<BusNo>-<ChannelNo>]...<br>Possible values: 1 to 4 for the busses, 1 or 2 for the channel.<br>If no entry has been made, a random channel on a random bus will be used.<br>If one or more leased lines are to be used, an entry must be available for each leased line. |
| Backup | Number of possible backup connections. These connections will be established in the event that all valid leased-line channels are down.<br>Backup connections always use a random channel on a random bus.                                                                                                                                                                              |

*Name-list*

The names entered in the name list are needed by the router to determine the correct remote station and corresponding layer name. The name list is also used for the callback function.

The name list can contain 64 different device names and might, for example, have the following appearance:

| Device-name | Dialup-remote | B1-DT | B2-DT | WAN-layer | Callback |
|-------------|---------------|-------|-------|-----------|----------|
| GLASGOW     | 875463        | 180   | 0     | PPPHDL    | On       |
| LONDON      | 040785647     | 20    | 20    | DEFAULT   | Off      |

Below is a detailed description of the meaning of each field:

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device-name   | In the <b>Device Name</b> column, you can enter an original remote station name, which you must then assign to the relevant remote station via the <b>Name</b> option in the <b>Setup</b> menu.                                                                                                                                                                                                                                                                                                                                |
| Dialup-remote | In this column, you can store the number to be called and, if applicable, supplement it with special dialing characters (see above, default: None).                                                                                                                                                                                                                                                                                                                                                                            |
| B1-DT         | In this column, you can define appropriate connection time-outs (in seconds) for the first B channel.<br>If no data is being transmitted when this time expires, the connection on this channel is released (default: 20).<br>If charging information is transmitted over the ISDN network during the connection, the <i>ELSA LANCOM</i> will make full use of every charging unit and will only terminate the connection just before the beginning of the next unit. This function is also referred to as dynamic short-hold. |
| B2-DT         | In this column, you can define appropriate connection time-outs for the second B channel (same as B1-DT, default: 20).<br>The B2 hold time controls the bundling behavior during a channel bundling. Values of 0 or 9999 identify static bundling, values between them dynamic bundling.                                                                                                                                                                                                                                       |
| WAN-layer     | In this column, a name is stored that must also be entered in the layer list. This establishes the transfer protocol required for this connection.                                                                                                                                                                                                                                                                                                                                                                             |
| Callback      | In this column, you can define whether a callback is to be made for the relevant remote station (Off/Name/Auto/Looser/ELSA; default: Off).                                                                                                                                                                                                                                                                                                                                                                                     |

■ Callback options

|                                                            |                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Off                                                        | No callback is made.                                                                                                                                                                                                                                                                                                                                   |
| Looser                                                     | The router stops attempting to establish a connection when there is a call from this remote station (reciprocal call establishment). This setting must be used when a callback from the remote station is expected.                                                                                                                                    |
| Auto<br>(not applicable to<br>Windows 9x or<br>Windows NT) | The connection will be rejected and a direct callback will be initiated if the remote station is specified in the number list. This means that the caller is not charged. If the remote station is not specified in the number list, a callback will be negotiated in a protocol negotiation (ELSA or PPP). A charge of one unit is incurred for this. |
| Name                                                       | This setting forces a protocol negotiation. This enables call number protection to be set in the number list and also a callback to be started using the protocol negotiation. A charge of one unit is incurred for this.                                                                                                                              |
| ELSA                                                       | This setting enables a particularly fast callback procedure. The called-back remote station must use the 'looser' setting.                                                                                                                                                                                                                             |

- The special dialing characters in the table below can be entered along with the call number in the name list, round robin list, or logical dial prefix. They control the line access, the use of a semipermanent leased-line connection or determine the interface to be used for the connection:

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| # | Trunk seizure (only with some PBXs).                                                                                                                                                                                                                                                                                                                                                                                                               |
| F | The remote station can be reached via the leased-line connection only.<br>Syntax: F[channel:][subscriber number]<br>The channel and subscriber number are both optional.<br>In the case of several leased lines, the channel specifies the B channel to be used.<br>Depending on the setting in the channel list, the subscriber number indicates whether a dynamic channel bundling or backup line is to be realized over the dial-up connection. |

When **S** or **S2** is appended to the call number, the semipermanent connection (SPV) is activated for the D-channel protocol 1TR6.

*You must subscribe to an SPV through your telephone company for a fixed payment.*

*If you forget to append an **S** or **S2**, the SPV will behave like a standard dial-up line and your charges will be unnecessarily high. The telecommunications provider then charges you the fixed charges and the dial-up line charges incurred during the time the line was used.*

*RoundRobin-list* The round-robin list enables a remote station to be reached with several call numbers. It has the following layout:

| Device-name | RoundRobin     | Head |
|-------------|----------------|------|
| GLASGOW     | 4321-5555-6666 | Last |

Below is a detailed description of the meaning of each field:

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device-name | In the device name column, you can enter a remote device name from the name list. If one line in the Round Robin list is insufficient for all desired call numbers, the line can be extended as shown below: The # character and a unique index are added to the device name (e.g. GLAS-GOW#1) and it is entered on the next line.                                                                                                                                                                                             |
| Round-Robin | The DDI numbers of all possible remote stations are entered here under their corresponding device names. The individual DDI numbers must be separated by hyphens.                                                                                                                                                                                                                                                                                                                                                              |
| Head        | In the <b>Head</b> column, the following entries are possible:<br><b>Last:</b> The next connection to be established will begin with the DDI that was successfully used for establishing the last connection (default).<br><b>First:</b> The next connection to be established will always begin with the first DDI.<br>For a logical remote station, this field can be modified only by means of its <b>first</b> entry in the table. The field is automatically updated when other entries are made for this remote station. |

#### Layer-list

In the layer list, you can freely define the different B-channel protocols by combining various ISDN layers. This enables compatibility to devices from other manufacturers that use different B-channel protocols to be set.

The following table below is provided as an example and also shows the default settings for an *ELSA LANCOM Office*:

| WAN-layer | 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 |

Below is a detailed description of the meaning of each field:

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                              |  |  |  |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
| WAN-layer | In this column, you can enter an original name designating the layer combination that you use. These names can then be used in the name list 'layer name' column depending on their spelling to set the protocol.<br>If an entry with the name <b>DEFAULT</b> is defined in this column, the settings stored there are always used when no layer name can be assigned (e.g. a caller does not transmit his or her call number). This entry is also used when a group 0 leased-line connection is established. If the <b>DEFAULT</b> entry is not present, a B channel protocol developed by ELSA is used as the default. The user may delete or change any of the layers predefined here. |                                                                                                                                                                              |  |  |  |
| Encaps.   | Additional information regarding the data to be transmitted may be specified in the <b>Encaps</b> column. The following entries are possible:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                              |  |  |  |
|           | ETHER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | The data is provided with an Ethernet header. This setting is required for communication with older <i>ELSA LANCOM</i> devices.                                              |  |  |  |
|           | TRANS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | No Ethernet header is sent in this setting. Only "pure" IP data packets are transferred, for example. This setting provides the greatest possible effective data throughput. |  |  |  |

|         |                                                                                                                                         |                                                                                                                                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lay-3   | In the lay-3 column, you can define additional headers for data transmission in ISDN. You can select from among the following settings: |                                                                                                                                                                                                                     |
|         | TRANS                                                                                                                                   | No additional header is inserted (higher data throughput). Always select this setting if the remote station sends the data transparently via ISDN layer 3 (e.g. transparent HDLC, transparent X.75LAPB).            |
|         | PPP                                                                                                                                     | A negotiation is performed according to the point-to-point protocol.                                                                                                                                                |
|         | APPP                                                                                                                                    | A negotiation is performed as per the asynchronous PPP. APPP is then used when synchronous PPP is not possible because the connection does not permit a synchronous transmission (e.g. for analog modem operation). |
|         | SCPPP                                                                                                                                   | Following completion of script processing, a synchronous PPP negotiation is initiated.                                                                                                                              |
|         | SCAPPP                                                                                                                                  | Following completion of script processing, an asynchronous APPP negotiation is initiated.                                                                                                                           |
|         | SCTTRANS                                                                                                                                | Following completion of script processing, a connection exists to the remote station. No further protocol negotiation is performed.                                                                                 |
| Lay-2   | In this column, you can select the protocol for ISDN layer 2:                                                                           |                                                                                                                                                                                                                     |
|         | TRANS                                                                                                                                   | The data is packed directly in HDLC packets. Always select this setting if communication is to take place via transparent HDLC.                                                                                     |
|         | X.75LAPB                                                                                                                                | The data is exchanged in X.75 secured format. Always select this setting if the remote station is to work with X.75 data protection.                                                                                |
| L2-Opt. | The L2-opt. enables the setting of an option for the data transfer setting under Lay-2 with an additional <i>ELSA LANCOM</i> .          |                                                                                                                                                                                                                     |
|         | none                                                                                                                                    | No data compression or channel bundling is performed.                                                                                                                                                               |
|         | compr.                                                                                                                                  | Stac data compression will be used. Compression as per Stac (Hi/fn) must be used in connection with PPP or multilink PPP. Stac compression may also be used in connection with Windows remote stations.             |
|         | bundle                                                                                                                                  | Channel bundling is performed via several B channels. Channel bundling is only possible for the Lay-2 settings of 'PPP'.                                                                                            |
|         | bnd+cmpr                                                                                                                                | Channel bundling and data compression takes place over two B channels.                                                                                                                                              |
| Lay-1   | The lay-1 column allows you to define the speed at which the data is sent in ISDN.                                                      |                                                                                                                                                                                                                     |
|         | HDLC64K                                                                                                                                 | The data is transmitted at 64,000 bps.                                                                                                                                                                              |
|         | HDLC56K                                                                                                                                 | The data is transmitted at 56,000 bps. This setting is especially important for connections in the USA.                                                                                                             |
|         | V110_9K6                                                                                                                                | Data is transferred at 9,600 bps in a V.110 connection, when connecting to GSM mobile phones, for example.                                                                                                          |
|         | V110_19K2                                                                                                                               | Data is transferred at 19,200 bps in a V.110 connection.                                                                                                                                                            |
|         | V110_38K4                                                                                                                               | Data is transferred at 38,400 bps in a V.110 connection.                                                                                                                                                            |

To link to devices from other manufacturers, please check with that manufacturer for the data format used (PPP is almost universally supported).

For Internet and remote access, PPP is generally specified.

*PPP-list*

The router needs the device names contained in the PPP list in order to determine the security procedure settings suitable for the connection and to determine the PPP parameters. It contains a maximum of 64 entries and is structured as follows:

| Device-name | Auth. | Key   | Time | Try | Conf | Fail | Term | Username | Rights |
|-------------|-------|-------|------|-----|------|------|------|----------|--------|
| GLASGOW     | CHAP  | ***** | 0    | 5   | 10   | 5    | 2    | ELSA     | IP     |

Not all parameters can be reached via the telnet configuration. Use *ELSA LANconfig* so far as possible.

Below is a detailed description of the meaning of each field:

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                           |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device-name         | In the Device-name column, you can enter the name with which the remote station logs onto the router.<br>In the case of connections via the data transmission network, this is the name entered as "Username". For remote access via the data transmission network, the 'Username' field (see below) is not evaluated!<br>Entries are not case-sensitive!                                                        |                                                                                                                                                                                                                                                           |
| Auth.               | In this column, you can enter the security procedure to be used for verification of the remote station. Default: PAP                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                           |
|                     | None                                                                                                                                                                                                                                                                                                                                                                                                             | The router does not negotiate authentication with the remote station when establishing a connection. However, the remote station can itself require authentication from the router. This is the case when dialing up a connection to an ISP, for example. |
|                     | PAP                                                                                                                                                                                                                                                                                                                                                                                                              | The remote station is checked as per the Password Authentication Protocol.                                                                                                                                                                                |
|                     | CHAP                                                                                                                                                                                                                                                                                                                                                                                                             | The remote station is checked as per the Challenge Handshake Authentication Protocol.                                                                                                                                                                     |
| Key                 | A password may be entered in this column. Its presence is indicated by the symbol * and it is used to check the remote station. It may consist of 95 characters (7-bit ASCII, including spaces). Default: None.<br>The <code>set ?</code> command shows a list of the allowable characters.                                                                                                                      |                                                                                                                                                                                                                                                           |
| Time                | In this column, you can enter the period of time between two remote station verifications specified in minutes. The CHAP protocol must be set here. Default: 0                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                           |
| Try                 | In this column, you can specify the number of times the verification attempt is to be repeated. If verification fails, the connection is immediately terminated. Default: 5                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                           |
| Conf, Fail and Term | These parameters may be used to influence the operation of the PPP. They are defined and described in RFC 1661. The default values are sufficient for most remote stations. If nothing is entered here, the values 0,0,0 appear in the display but the default values 10, 5, 2 are still used.<br>These parameters can only be changed via SNMP or TFTP (using the <i>ELSA LANconfig</i> configuration program)! |                                                                                                                                                                                                                                                           |
| Username            | The user name (max. 64 characters) transmitted to the remote station during PPP negotiation. The router identifies itself to the remote station with it.<br>If no user name is entered, the device name serves as the user name.<br>Entries are case-sensitive here.                                                                                                                                             |                                                                                                                                                                                                                                                           |
| Rights              | Network protocols to be routed over this connection: IP, IPX, NTB (NetBIOS). NetBIOS always requires one of the other two protocols.<br>The routing of IP or NetBIOS via PPP always requires a suitable route (in the IP routing table for IP or in the remote-station table for NetBIOS).                                                                                                                       |                                                                                                                                                                                                                                                           |

*Number-list*

Under this option, a number list is managed in which you can enter 64 different call numbers with their associated device names. This list can be used to assign the call numbers (CLI) transferred by remote stations to the remote station names.

The entries in the number list for the two calling devices GLASGOW and LONDON might appear as in the table below, thus permitting the name to be derived from the call number supplied and, if applicable, permitting a callback to be initiated via the name list:

| Dialup-remote | Device-name |
|---------------|-------------|
| 875463        | GLASGOW     |
| 040785647     | LONDON      |

This number list is required for passive connection establishment. The remote station call numbers must be entered without leading zeros.

The D-channel protocol that is currently activated is then used for a call number test.

If the 'Protect number' setting is selected and a call is received from a remote station, the remote station call number sent is compared to the entries in the number list. If the station number sent is identical to an entry in the list, the caller is authorized and the connection is established.

If the 'Protect no./name' setting is selected and a call is received from a remote station, the remote station call number sent is compared to the entries in the number list. If the call number sent is identical to an entry in the list, the caller is authorized to establish the connection. In addition, it is possible to derive the name of the remote station from the number list and, therefore, the layer that is to be used for this connection. The connection is then established using this layer and name verification is initiated using the layer detected (or using the default layer if no layer is detected).

If the name of the remote station (and thus the layer to be used) cannot be determined using the number list, the call will be accepted using the default layer and the name list will be checked for a suitable entry after the protocol (PPP) negotiation.

*Script-list*

Some Internet providers (e.g. CompuServe) conduct a script-controlled log-on procedure before a PPP negotiation. In order to be able to establish this type of connection as well, a simple script processing procedure is also implemented in the *ELSA LANCOM* (see 'Script processing').

In this table, the scripts are defined and assigned to the remote stations. The table has the following layout:

| Device-name | Script                                      |
|-------------|---------------------------------------------|
| CSEVERE     | <>[Host]<CIS>[User]\$U[Password]\$P[PPP]\$C |




The entries in the script list have the following meaning:



- Device name: Name of the logical remote station
- Script: All commands to be executed—a maximum of 58 characters per line is available. If the required command sequence is longer, an additional entry for the logical remote station may be added as in the round-robin list. The syntax for this is: Device name followed by '#' and a number. The entries are processed from top to bottom.

### Setup/WAN-module/Manual-dialing

This option can be used for manual connection control for testing purposes.

| /Manual-dialing |                                                                                   | Settings for manual connection control  |
|-----------------|-----------------------------------------------------------------------------------|-----------------------------------------|
| Connect         |  | Establishes a connection.               |
| Disconnect      |  | Termination of connections              |
| State           |  | Displays the current connection status. |

#### Connect

Parameter: Remote station's device name (via remote configuration only).

You can use the command

Do /Setup/WAN-module/Manual-dialing/Connect to remote station

to initiate the manual establishment of a connection via remote configuration. The remote station's device name specified as a parameter must also be entered in the name list with a call number.

When the function is activated by the keyboard of the *ELSA LANCOM*, the error message 'No remote station' is displayed, because a name cannot be entered here. Therefore, this function must not be used from the keyboard of the *ELSA LANCOM*. If you attempt to establish a connection to a logical remote station for which no call number is specified in the name list, the 'No number' error message is displayed.

#### Disconnect

This command allows you to release an existing connection. If a connection is released manually, the name of a remote station may also be entered in the remote configuration. In this case, only the connection to the remote station specified is released. If a connection to the remote station specified does not exist, there is no further response. However, if a remote station name is not entered, all existing connections will be released.

### Setup/WAN-module/protection

This option allows you to select the conditions under which incoming calls are to be answered at the transmission module.

- If 'Protect' is set to 'none', all pending calls are answered provided that the remote end supports the connection protocol.

- If this option is set to 'name', calls are accepted only from remote stations for which an entry is found in the name list. This verification provides additional protection. This verification is only available when using PPP.
- If this option is set to 'number', calls are accepted only from remote stations that are entered in the number list as authorized remote stations.
- The 'no./name' setting allows you to select combined protection using a name list and number list. First a verification that there is an entry in the number list is made. If this is not possible, the router will attempt to determine the name using the protocol negotiation.

### Setup/WAN-module/CB-attempts




This option allows you to set the number of times (from 1 to 9) a callback is to be attempted when the remote station is busy. For international connections, you should enter a value from 3 to 5 in order to optimize the callback functionality. The default setting is 3.

### Setup/WAN-module/Backup-delay-seconds

The backup start time indicates the number of seconds to elapse before the first backup attempt is started after determining that the leased line is down. If the value 0 is entered, no backup connection will be established actively.

## Setup/LAN-module

This menu allows you to select the settings needed for the local network. The menu has the following layout:

| /LAN-module | LAN settings                                                                        |                                                          |
|-------------|-------------------------------------------------------------------------------------|----------------------------------------------------------|
| Connector   |  | Selection of the network connection                      |
| Node-ID     |  | MAC layer address of the device                          |
| Spare-heap  |  | Buffers that receive data packets from the local network |

*Connector*

This option allows you to select from among the following network connections:

| Connect  | Meaning                                                                                                                                                                         |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto     | Default setting; enables the Autosense function of the network chip. This automatically sets the router to the port in use without requiring manual configuration of this item. |
| 10BTX    | 10BASE-T in half-duplex mode                                                                                                                                                    |
| FD10BTX  | 10BASE-T in full-duplex mode                                                                                                                                                    |
| 100BTX   | 100BASE-T in half-duplex mode                                                                                                                                                   |
| FD100BTX | 100BASE-T in full-duplex mode                                                                                                                                                   |

*When making settings for the fast-Ethernet operation, please note that the selected transfer mode must also support the additional terminals.*

*When the system is switched off and on again, the last port to be selected remains activated.*

#### Node-ID







This option allows you to display the router's own Ethernet address. The value displayed here was set at the factory and cannot be changed. The Ethernet address is displayed as a 12-digit hexadecimal value, with the first six digits '00a057' standing for an ELSA device.

#### Spare-heap

The spare heap blocks for the local network affect the number of buffers that are always available for receiving frames from the local network. The default value is 10, which ensures that, e.g., four Telnet sessions can be activated via the local network at any time.

## Setup/IPX-module

This menu allows you to enter settings for the IPX module, particularly for the IPX router. The menu has the following layout:

| /IPX-module | IPX module (IPX router) settings                                                    |                                          |
|-------------|-------------------------------------------------------------------------------------|------------------------------------------|
| Operating   |   | Activates or deactivates the IPX module. |
| IPX-router  |  | Activates or deactivates the IPX router. |
| LAN-config  |  | Settings for the LAN side                |
| WAN-config  |  | Settings for the WAN side                |
| RIP-config  |  | RIP settings                             |
| SAP-config  |  | SAP settings                             |

#### Operating

This option allows you to activate or deactivate the IPX module. In the default configuration, the IPX module is activated.

*Remote configuration via DOS/IPX and the IPX router can be used only if the IPX module is activated. For local configuration via a LAN, the router does not have to be activated.*










#### IPX-router

This option allows you to activate or deactivate the IPX router. In the default configuration, the IPX router is deactivated.

*When the IPX router is activated, the IPX module is also activated. The IPX router can be activated only if different, permissible network addresses are entered under LAN-configuration and WAN-configuration.*

## Setup/IPX-module/LAN-configuration

Settings for the LAN data packets may be made here. The menu has the following layout:

| /LAN-configuration |                                                                                   | Settings for the LAN side                                 |
|--------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------|
| Network            |  | Logical IPX network number of the LAN port                |
| Binding            |  | Ethernet frame type setting for the LAN port              |
| IPX-watch          |  | Settings for IPX watchdog management                      |
| SPX-watch          |  | Settings for SPX watchdog management                      |
| NetBIOS-watch      |  | Settings for NetBIOS watchdog management                  |
| Socket-filter      |  | Filter table for destination socket filtering             |
| Loc.-routing       |  | Activates or deactivates local routing.                   |
| RIP-SAP-scal.      |  | Activates or deactivates RIP-SAP scaling.                 |
| LOOP-prop.         |  | Activates or deactivates propagation of redundant routes. |

### *Network*

The NetWare network number of the network (8-digits, hexadecimal) that is connected to the LAN port under the binding (see below) may be entered here. If there is a NetWare server in the local network, the router can automatically detect the network number and the binding.

The default value is '00000000' and means that the router should automatically detect the network number.

### *Binding*

This option allows you to select the Ethernet packet format (Auto, II, 802.3, 802.2, SNAP) for the LAN port. This format must match the Ethernet format used in the local network under the above-mentioned network number.

The default is 'auto' and means that the router should automatically detect the binding (only if there is a NetWare server in the local network).

### *IPX-watch*

This option allows you to define the type of management used for IPX watchdog packets.

- **Filt.** means that the IPX watchdog packets are neither answered nor transferred locally. Users are always logged off after the period of time set in the NetWare server.
- **Route** causes the watchdog packets to be transferred and, consequently, also causes a regular establishment of connections by means of the server's watchdog packets.
- **Spoof** (default) ensures that IPX watchdog packets are answered locally by the router and therefore that users are no longer automatically logged off. This setting is especially economical but steps must be taken in the server to ensure that users are logged off at specific times in order to prevent the usage of too many user licenses.

- SPX-watch* This option allows you to define the type of management used for SPX watchdog packets.
- **Route** causes the SPX watchdog packets to be transferred and, consequently, also causes a regular establishment of connections by means of the server's SPX watchdog packets.
  - **Spoof** (default) causes SPX watchdog packets to be answered locally. This setting is especially economical.

*NetBIOS-watch* This item specifies how NetBIOS watchdog packets should be treated. NetBIOS watchdog packets occur, e.g., if Windows networks are connected by IPX. The same options are available as with IPX or SPX watchdog packets (filter, route, spoof).

*Socket-filter* The socket filter table permits the selective filtering of LAN packets to specific ranges of destination sockets. Filtering is performed for both single IPX packets and propagated IPX packets. The following sockets (which are periodically sent in the network and, therefore, would result in connections being established too frequently) are already entered in the LAN filter table as default values (for details, also see FAQs on the 'IPX router').

| Start-socket | End-socket |
|--------------|------------|
| 0455         | 0457       |
| 0550         | 0555       |
| 1401         | 1402       |
| 1480         | 1481       |
| 83ba         | 83ba       |
| 900F         | 9010       |

*Loc.-routing* This setting supports the scaling of multiple routers in a local network. When all the channels for one router are already seized and packets for other remote stations are still being received at this router, other routers in the LAN may still have free channels.

If the 'Loc.-routing' option is activated, the router forwards the packets in the local network to a router that has propagated a route to the remote station desired. The router has saved this route, although it is less efficient than its own, and marked it with the 'reserve' flag in the RIP table.

The default setting for this option is 'Off' since an IPX client sends a RIP request for the relevant route after a timeout, thus automatically finding a different router through which it can access the destination network.

*RIP-SAP-scal.* Another option for supporting scaling is to propagate every route to which there is an active connection with a somewhat better tic count than the actual one. This will ensure that all clients will send their packets for these routes to the router that has the connection. In addition, in the event that all channels are busy, the routes that are no longer available will be propagated as 'DOWN'. Because one or more broadcasts are

sent on the LAN by this procedure every time a connection is established and released (which may require other routers for additional broadcasts and may result in a high network load), this feature can be activated and deactivated. The default setting is 'Off'.



*LOOP-prop.*

Redundant routes, i.e. routes with the same tic and hop count, are only sent to the remote station by which they were not received (split horizon). When the 'LOOP-prop.' function is activated, these routes can still be propagated. Redundant routes are identified in the RIP table by means of the LOOP flag.

Although the propagation of redundant routes is not prohibited by the Novell specification, it should still be avoided as much as possible. Therefore, the default setting is 'Off'.

### Setup/IPX-module/WAN-configuration

This option allows you to maintain the data packet settings for the WAN port. The menu has the following layout:

| /WAN-configuration |                                                                                   | Settings for the WAN side                                   |
|--------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------|
| Routing-table      |  | Routing table for IPX network and remote station assignment |
| Socket-filter      |  | Filter table for destination socket filtering               |

*Routing-table*

The routing table can hold up to 16 remote stations and destination networks. It contains the following entries:

| Remote-ID                      | Network         | Binding                | Propagate      | Backoff  |
|--------------------------------|-----------------|------------------------|----------------|----------|
| Name of the IPX remote station | Network address | 802.3, II, 802.2, SNAP | Route / Filter | On / Off |

The columns have the following meanings:

- **Remote-ID:** Name of the logical remote station (as specified in /Setup/WAN-module/Name-list).
- **Network:** Address of the network on the WAN side. A standalone network must be used, but it must be same for both of the participating routers!
- **Binding:** The Ethernet binding to be used on the ISDN route. This setting is taken into account only if Ethernet encapsulation is set in the layer used. If no binding is specified, a value of 802.3 is assumed.
- **Propagate:** This entry indicates how IPX type-20 packets (NetBIOS propagated frames) are to be handled. The possible settings are Route and Filter. With **Filter**, no propagated frames are routed to the remote station. If the entry has the value **Route**, the packets are forwarded to all currently available remote stations, i.e., there must be a connection to the remote station, or there must be at least one channel available for establishing a connection the remote station.

If no connection or channel is available, the packet is discarded. As a result, the maximum number of remote stations that can receive propagated frames corresponds to the number of possible simultaneous connections. The default setting is 'Filter'.

- **Backoff:** The IPX router uses a special algorithm (exponential backoff) to keep the connection charges as low as possible in the event of erroneous configurations (see below).

If there is no server in the remote network (e.g. with remote access from a workstation), the router cannot detect this and the corresponding remote station will be deactivated after a day at the latest. In order to prevent this from happening, the exponential backoff algorithm can be deactivated for these remote stations.

The default setting is 'On'.

Socket-filter

The socket filter table permits the selective filtering of WAN packets to specific ranges of destination sockets. Filtering is performed for both single IPX packets and propagated IPX packets.

**Setup/IPX-module/RIP-configuration**

This option allows you to store settings for RIP data packets (router information). The menu has the following layout:








| /RIP-configuration |                                                                                     | RIP settings                                         |
|--------------------|-------------------------------------------------------------------------------------|------------------------------------------------------|
| Table-RIP          |  | Displays the RIP table.                              |
| LAN-filter-table   |  | Filter ranges for IPX network addresses (LAN)        |
| WAN-filter-table   |  | Filter ranges for IPX network addresses (WAN)        |
| Routes/Frm         |  | Max. no. of RIP entries per RIP frame sent           |
| Aging-minute(s)    |  | Aging period in update units                         |
| Spoofing           |  | Sets RIP spoofing procedure                          |
| WAN-update-min.    |  | RIP update period; effectiveness depends on spoofing |

Table-RIP

This option allows you to display the entries in the current RIP table. The table contains a maximum of 256 entries.

The entries in the RIP table might, for example, look like the entries shown below with the networks 00000001, 00000002, 00000010, 00000081, where these networks can be accessed via different routers. The flags can be used to determine where these networks are located with relation to the particular router (**local** or **remote**). The entry **direct** indicates whether this network is directly the local or remote network. **DOWN** indicates

a network that is known but is not currently available. The table is sorted by the network numbers.

| Network  | Hops | Tics | Node-ID      | Time | Flags          |
|----------|------|------|--------------|------|----------------|
| 00000001 | 0    | 1    | 00a05702000a | 0    | local, direct  |
| 00000002 | 1    | 2    | 00608c70ab56 | 1    | local          |
| 00000010 | 2    | 7    | 00A057020014 | 1    | local, DOWN    |
| 00000081 | 1    | 6    | 00a05702000b | 0    | remote, direct |

*LAN-filter-table* The LAN filter table permits the selective filtering of routes that are 'learned' via the local network. Filtered routes do not appear in the IPX-RIP table.

A LAN filter table for filtering routes in the range from 00001000 to 00001fff might, for example, have the following appearance:

| Start-net | End-net  |
|-----------|----------|
| 00001000  | 00001fff |

*WAN-filter-table* The WAN filter table permits the selective filtering of routes that are 'learned' via the wide-area network. Filtered routes do not appear in the IPX-RIP table.

A WAN filter table for filtering routes in the range from 00002000 to 00002fff might, for example, have the following appearance:

| Start-net | End-net  |
|-----------|----------|
| 00002000  | 00002fff |

*Routes/FRM* This parameter sets the maximum number of routes that can be included in a RIP frame. The specified value originally defined by Novell is 50. Today, however, it is common practice to pack a higher number of routes in each frame in order to reduce network utilization. If all participating devices in the network support a higher number, this value can be raised as high as 182.

*Aging-minute(s)* This option allows you to set the number of times the RIP table will be updated until an entry in the RIP table ages, i.e. until the route recorded there is marked as 'not reachable (down)'. You can enter a value from 1 to 60; the default value is 3.



*Spoofing*

This option allows you to determine how the router will handle RIP packets.

- If you select **Off**, RIP packets are handled in the WAN in precisely the same manner as in local networks. RIP data are sent to the remote side in the event of new information and at intervals of one minute, i.e. a connection is established.
- With the **Trig** setting, the RIP data is sent to the remote end any time changes are detected.
- With the **Time** setting, the RIP data is sent to the remote end at selectable intervals (see below).
- **pBack** (default) is the most economical setting. In this case, the RIP data is sent to the remote end only when a connection is activated.








*When spoofing is set to **pBack**, entries in the RIP table age only when a new connection is established and an entry has been explicitly marked as 'not reachable'.*

*WAN-update-min.*

The periodic transfer interval for a spoofing time control in which RIP data can be transferred to the remote side is given here. You can enter a value from 1 to 60 minutes; the default value is 5.

**Setup/IPX-module/SAP-configuration**

This option allows you to store settings for SAP data packets (server information).

| /SAP-configuration |                                                                                     | SAP settings                                          |
|--------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------|
| Table-SAP          |  | Displays the SAP table.                               |
| LAN-filter-table   |  | Filter ranges for IPX service addresses (LAN)         |
| WAN-filter-table   |  | Filter ranges for IPX service addresses (WAN)         |
| Server/Frm         |  | Max. no. of SAP entries per SAP frame sent            |
| Aging-minute(s)    |  | Aging period in update units                          |
| Spoofing           |  | Sets SAP spoofing method.                             |
| WAN-update-min.    |  | SAP update period; effectiveness depends on spoofing. |

*Table-SAP*

This option allows you to display the entries in the current SAP table. The table contains a maximum of 512 entries. It is sorted first by service type and then by server name. A SAP table might, for example, have the following appearance:

| Type | Server-name | Network  | Node-ID      | Socket | Hops | Time | Flags |
|------|-------------|----------|--------------|--------|------|------|-------|
| 0004 | Y           | 000000c1 | 000000000001 | 0451   | 1    | 1    | local |
| 0047 | X           | 00000001 | 0000c0123456 | 8060   | 1    | 0    | local |
| 0107 | Z           | 000000c1 | 000000000001 | 8104   | 2    | 1    | local |

Different SAP types are stored in the table. The server name, the applicable network, the server MAC address (000000000001 for internal server networks), the socket number and information on the location of the server must be read.

*LAN-filter-table* Entries in the LAN filter table make it possible to exclude specific service information ranges of a Novell network from being included in the SAP table and therefore to make better use of the resources of the IPX router. This also prevents unwanted connections from being established by these SAPs (services).

None of the service information located within a range of filters entered in the LAN filter table is transferred by the local network to the IPX router's SAP table. They are also not transferred to the remote station of the IPX router and therefore are also not available there.

For example, the service information for the printer server is often unnecessary for the remote station of the IPX router. If this information is to be excluded from the SAP table by means of the LAN filter table, the following entry is required:

| Start-service | End-service |
|---------------|-------------|
| 030c          | 030c        |

For a list and description of SAP services, please refer to the section entitled 'Novell SAP Numbers'.

*WAN-filter-table* As with the LAN filter table, you can use the WAN filter table to prevent ranges of service information from being transferred from the WAN to the SAP table.

Therefore, the blocked services have resulted in the establishment of a connection to the remote station before the destination router could filter them on the WAN side.

The layout and function of the WAN filter table are exactly the same as that of the LAN filter table. A WAN filter table for filtering file services might, for example, have the following appearance:

| Start-service | End-service |
|---------------|-------------|
| 0004          | 0004        |

*Server/FRM* This parameter sets the maximum number of services that can be included in a SAP frame. The specified value originally defined by Novell is 7. Today, however, it is common practice to pack a higher number of services in each frame in order to reduce network utilization. If all participating devices in the network support a higher number, this value can be raised as high as 22.

*Aging-minute(s)* This option allows you to set the number of times the SAP table will be updated until an entry in the SAP table ages, i.e. until the service recorded there is marked as "not reachable (down)". You can enter a value from 1 to 60; the default value is 3.

*Spoofing*

This option allows you to determine how the router will handle SAP packets.

- If you select **Off**, SAP packets are handled in the WAN in precisely the same manner as in local networks. SAP data are sent to the remote side in the event of new information and at intervals of one minute, i.e. a connection is established.
- With the **Trig** setting, the SAP data is sent to the remote end any time changes are detected.
- With the **Time** setting, the SAP data is sent to the remote end at selectable intervals (see below).
- **pBack** (default) is the most economical setting. In this case, the SAP data is sent to the remote end only when a connection is activated.















*When spoofing is set to **pBack**, entries in the RIP table age only when a new connection is established and an entry has been explicitly marked as 'not reachable'.*

*WAN-update-min.*

The periodic transfer interval for a spoofing time control in which SAP data can be transferred to the remote side is given here. You can enter a value from 1 to 60 minutes; the default value is 5.

## Setup/TCP-IP-module

This menu allows you to enter settings for the TCP/IP module. The menu has the following layout:

| /TCP-IP-module | TCP/IP module settings                                                              |                                                                                 |
|----------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Operating      |  | Activates or deactivates the TCP/IP module.                                     |
| IP-address     |  | Local IP address                                                                |
| IP-netmask     |  | Local network's matching IP network mask                                        |
| Intranet addr. |  | Local Intranet address                                                          |
| Intranetmask   |  | Local network's matching Intranet network mask                                  |
| Access-list    |  | Restricts access to internal functions via TCP/IP.                              |
| DNS-default    |  | Domain name server                                                              |
| DNS-backup     |  | Backup domain name server                                                       |
| NBNS-default   |  | NetBIOS name server                                                             |
| NBNS-backup    |  | Backup NetBIOS name server                                                      |
| Table-ARP      |  | ARP table for mapping an IP address onto a MAC address                          |
| ARP-aging-min. |  | Dwell time for entries in the ARP table                                         |
| TCP-aging-min. |  | Time limit for configuration connections that are inactive                      |
| TCP-max.-conn. |  | Max. number of simultaneous configuration connections to the <i>ELSA LANCOM</i> |

*Operating* The TCP/IP module of the router may be activated or deactivated here. In the default configuration, the TCP/IP module is activated.

*Configuration via TCP/IP using Telnet and the IP router is possible only if the TCP/IP module is activated.*

*IP address* The IP address for the router may be entered here. The default address on delivery is '0.0.0.0'.

If IP masquerading is used, this address takes on a special meaning in connection with the Intranet address:

If the IP address is assigned to the router by the Internet provider by PPP, all computers in the network linked by IP address and IP network mask are normally routed. These computers can then also be accessed directly from the Internet.

*IP-netmask* The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network). A network mask of 255.255.255.255 means that there is only one computer in this network (the router itself). This setting (an IP address registered in the Internet with a fully assigned network mask) can be used for masquerading via a raw IP access, such as that offered by the provider of the individual network. With such an access an IP address is not assigned to the router by a PPP negotiation, but it must have a fixed IP address registered in the Internet.

*Intranet-address* A second IP address for the router may be entered here. This enables the router to be used as a router for two logical IP networks and also this address has a specific meaning with the use of IP masquerading:

In this case, all computers that are in the network linked by Intranet address and Intranet mask are hidden behind the address assigned by the provider (or the Internet address (IP address)).

The default address on delivery is '0.0.0.0'.

*Intranet-mask* The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network).



*If neither an IP nor an Intranet address has been specified, the device responds to a default IP address, the first three digits of which are identical to the first three digits of the sending device XXX.XXX.XXX.YYY. The device can then be reached by dialing the IP address XXX.XXX.XXX.254.*

*In the event that such an address already exists in the network, a different address must be entered via outband configuration (terminal program).*



*If both an IP address and an Intranet address have been entered, the network defined by an IP address and IP network mask must contain only workstations (i.e. no routers).*

*Access-list*

The access to “internal functions” of the router may be controlled by an access list in TCP/IP applications.



*The configuration data of the device are protected by a password, however this is always transferred in plain text, making it possible in principle to detect it and for any computer to read the configuration or to delete it. In order to prevent this from happening, the access list can be used to determine which computers or which networks can access the configuration.*

For reasons of consistency, the access control is based on all “internal functions” of the router. The term “internal functions” refers to the following:

- Telnet server: the configuration interface based on the Telnet protocol
- TFTP server: the configuration interface based on the TFTP protocol
- SNMP: the configuration interface based on the SNMP

Each of the maximum of 16 entries in the access list has the following structure:

| IP-address                                         | IP-netmask                         |
|----------------------------------------------------|------------------------------------|
| IP address of the authorized user (or user circle) | IP network mask of the user circle |

Once an IP workstation with its IP address and the network mask 255.255.255.255 is entered into the list, the internal functions of the router can only be accessed from this computer. Any requests from devices with different IP addresses are ignored.

If a complete network has access enabled to an *ELSA LANCOM*, this can be done as follows for a class C network:

| IP-address    | IP-netmask    |
|---------------|---------------|
| 192.234.222.0 | 255.255.255.0 |

With this entry all IP addresses in the class C network 192.234.222.0 are authorized to use internal functions of the router.

*DNS-default*

The entry **DNS** (Domain Name Server) is required to announce the name server responsible for their own network for computers that have direct access via PPP to the router.

If the router is configured for access to the Internet via an Internet Service Provider, the DNS server is usually given by the provider. There are then two possible settings in the router:

- '0.0.0.0' is entered as the address of the DNS server. All computers in the local network can then use the provider's DNS server.
- The router's own IP address is entered as the DNS server. Then he uses the DNS information from the provider not only for its own local network but also forwards this information (DNS forwarding). Remote stations such as computers that dial in via remote access can then also access the provider's DNS server. This procedure is also referred to as DNS forwarding.

*DNS-backup* With the entry **DNS-Backup** a second name server can be named, which is used if the DNS fails.

*NBNS-default* The entry **NBNS-default** (NetBIOS Name Server) is required to announce the NBNS responsible for their own network for computers that have direct access via PPP to the router.

*NBNS* With the entry **NBNS-Backup** a second name server can be named, which is used if the NBNS fails.

*Table-ARP* This option allows you to display the ARP table (ARP cache), which is managed automatically for the purpose of mapping IP addresses onto physical terminal addresses. Individual entries can be removed from this table but no new entries can be entered manually.

The entries in the ARP table might, for example, have the following appearance if different devices with different IP addresses (192.168.139.20, 192.168.130.30) communicated with the router:

| IP-address     | Node-ID      | Last-access  | Connect |
|----------------|--------------|--------------|---------|
| 192.168.130.20 | 0000c0717860 | 6780443 tics | local   |
| 192.168.130.30 | 0800091eebf4 | 6214514 tics | local   |












*ARP-aging-min.* This option allows you to enter a time (from 1 to 99 minutes) at the end of which the ARP table is automatically updated, i.e. all IP addresses that have not been accessed since the last automatic update are removed. The default setting is 15 minutes.

*TCP-aging-min.* If data transfer stops during a TCP connection to the router, e.g. if the user does not enter any more data during the remote configuration, it will automatically release the TCP connection on expiry of the time entered here. Possible settings are from 1 to 99 minutes; The default setting is 15 minutes.

*TCP-max.-conn.* The maximum number of allowable connections possible at the same time can be set here. DEFAULT setting is '0', meaning the same as "any number".

## Setup/IP-router-module

This menu allows you to enter settings for the IP router module. The menu has the following layout:

| /IP-router-module |                                                                                    | IP router module settings                                                      |
|-------------------|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Operating         |   | Activates or deactivates the IP router module.                                 |
| IP-routing-table  |   | Router table for IP network and remote station assignment                      |
| LAN-filter-table  |   | Negative/connect filter table for the TCP/UDP destination ports of LAN packets |
| WAN-filter-table  |   | Negative filter table for the TCP/UDP destination ports of WAN packets         |
| Proxy-ARP         |   | Activates/deactivates the proxy ARP function                                   |
| Loc.-routing      |   | Activates/deactivates local routing                                            |
| Start-WAN-Pool    |   | Start of the address pool for dynamic address assignment for remote access     |
| End-WAN-Pool      |   | End of the address pool.                                                       |
| Routing-method    |   | Routing method for IP packets                                                  |
| RIP-config        |   | Settings for IP-RIP operation                                                  |
| Masquerading      |  | Settings for IP masquerading                                                   |

### Operating

This option allows you to activate or deactivate the IP router module. In the default configuration, the IP router module is activated.

*Activating the IP router module also activates the TCP/IP module.*

### IP-routing-table

The routing table can contain a maximum of 128 entries of destination network addresses or direct IP addresses with netmasks, and the names or IP addresses of other local routers. Alternatively, you can enter a setting by means of which packets to specific destination IP addresses are discarded and are not answered by proxy ARP. This is done by entering 0.0.0.0 for the name of the responsible router.

The 'Masquerade' field indicates whether the route should be masked or not. The following options are offered here:

- **On:** IP masquerading is switched on and functions with dynamic assignment of the IP address by the remote station. In this procedure the router queries the IP address '0.0.0.0' at the remote station and is assigned a random IP address by the remote station, which is then used for further processing.
- **Off:** Masquerading is switched off.
- **Static:** IP masquerading is switched on and functions with assignment of a static IP address previously assigned by the remote station. In this procedure the router queries the IP address entered under 'Setup/TCP-IP-module' at the remote station

and is assigned this address by the remote station. Use this setting when the remote station (e.g. your Internet provider) has assigned you a fixed IP address in the access data. Of course, this procedure will only function when this address has also been entered in the router as the IP address.

The IP routing table is generally sorted as shown below:

- The longest network mask is placed on top.
- For network masks of equal length, the one with the smallest IP address is placed on top.

In order to identify the correct remote station, the router searches the routing table from top to bottom using the destination IP address received. If a matching entry is found, the router name found is used for establishing the connection.

Address ranges that are prohibited in the Internet are excluded from transmission by preset entries in the IP routing table (the router name 0.0.0.0 means that packets to these addresses are not transmitted). The IP routing table below is provided by way of example and also shows the default settings:

| IP-address  | IP-netmask  | Router-name | Distance | Masquerade |
|-------------|-------------|-------------|----------|------------|
| 192.168.0.0 | 255.255.0.0 | 0.0.0.0     | 0        | Off        |
| 172.16.0.0  | 255.240.0.0 | 0.0.0.0     | 0        | Off        |
| 10.0.0.0    | 255.0.0.0   | 0.0.0.0     | 0        | Off        |
| 224.0.0.0   | 224.0.0.0   | 0.0.0.0     | 0        | Off        |

However, if these addresses are required for Intranet use, for example, it is possible to delete the predefined entries at any time. If the routing table contains no entries with the router name 0.0.0.0, the router processes all IP addresses with valid routes.

- Example
  - The local network address is 192.120.130.0.
  - Three terminal units must be available via proxy ARP with the IP addresses 192.120.130.10, 192.120.130.11 and 192.120.130.12 via an *ELSA LANCOM* 'Leeds'.
  - Two destination networks 192.120.131.0 and 192.120.132.0 can be accessed by the remote stations 'GLASGOW' and 'LONDON'.
  - Data packets for the destination network 193.140.300.0 are to be sent to another local router with the IP address 192.120.130.200.
  - Absolutely nothing is to be transmitted to the destination network 193.140.200.0.
  - All other non-local data packets must be sent to the router 'PROVIDER' at the Internet service provider.



In this example, the router table would contain the following entries:

| IP-address      | IP-netmask      | Router-name     | Distance | Masquerade |
|-----------------|-----------------|-----------------|----------|------------|
| 192.120.130.10  | 255.255.255.255 | LEEDS           | 0        | Off        |
| 192.120.130.11  | 255.255.255.255 | LEEDS           | 0        | Off        |
| 192.120.130.12  | 255.255.255.255 | LEEDS           | 0        | Off        |
| 192.120.131.0   | 255.255.255.0   | GLASGOW         | 0        | Off        |
| 192.120.132.0   | 255.255.255.0   | LONDON          | 0        | Off        |
| 193.140.200.0   | 255.255.255.0   | 0.0.0.0         | 0        | Off        |
| 193.140.300.0   | 255.255.255.0   | 192.120.130.200 | 0        | Off        |
| 255.255.255.255 | 0.0.0.0         | PROVIDER        | 0        | On         |

*If the connection to the selected remote station is to be realized via a PPP connection, the IP rights must be enabled for the corresponding entry in the PPP table.*

The last line is an entry for the "default route". The IP address 255.255.255.255 means the same as 0.0.0.0 (for technical reasons, 0.0.0.0 cannot be entered in the first column). Because it contains the IP network mask 0.0.0.0, this line is always appropriate after the rest of the table has been searched. Therefore, the router sends everything that it cannot transfer over other routes and should not discard or that comes from a WAN terminal and is not local to the router at the provider.

**LAN-filter-table** This table allows you to filter specific ranges of destination ports. In addition, you can determine how the packets are to be filtered. If packets with the entered ports are received from the LAN side, they will not be forwarded (always filter) unless a connection is currently in place (connect filter) or unless they can be routed over other than the DEFAULT route (I-Net filter).

The LAN port filters are defined in a table with the following layout:

| Idx. | D-st. | D-end | S-st. | S-end | Src.-addres     | Src-netmask | Prot              | Type              |
|------|-------|-------|-------|-------|-----------------|-------------|-------------------|-------------------|
| WIN  | 0     | 0     | 137   | 139   | 255.255.255.255 | 0.0.0.0     | TCP<br>and<br>UDP | Always<br>s-filt. |

The table fields have the following meaning:

■ **Idx.**

Unique index. This entry is required to enable the filters to be distinguished. The index may be four characters long and selected as desired.

- **D-st., D-end**  
Destination port range that is to be filtered. A range of 0 to 0 means that no destination port is affected by this filter.
- **S-st., S-end**  
Source port range that is to be filtered. A range of 0 to 0 means that no source port is affected by this filter.
- **Src-address, Src-netmask**  
A subnetwork of the local network for which the filter is valid can be entered here. A source address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).
- **Prot**  
Protocol that is to be filtered. Possible entries are **TCP**, **UDP**, **ICMP** and **all**.  
The setting **all** filters out every packet from the specified source network or to the destination network.
- **Type**  
Filter type. The possible values are Always-filt., Connect-filt. and Internet-filt.
  - **Always** filter: The packet is discarded.
  - **Connect** filter: The packet is discarded if there is no connection to the remote station.
  - **Internet** filter: The packet is discarded if its destination can be accessed only via the default route.

The default filter is entered in the above table. It suppresses the unwanted and cost-intensive connections in Windows networks on IP. These networks regularly send items such as DNS queries to the local network, which are routed to the Internet without this filter.

*WAN-filter-table*

This table allows you to enter specific ranges of destination ports. If packets with the entered ports are received from the WAN side, they will not be forwarded (firewall function).

The WAN port filters are defined in a table similar to the LAN filter table:

| Idx. | D-st. | D-end | S-st. | S-end | Dst.-address | Dst-netmask | Prot        |
|------|-------|-------|-------|-------|--------------|-------------|-------------|
| WIN  | 53    | 53    | 137   | 139   | 0.0.0.0      | 0.0.0.0     | TCP and UDP |

The fields in the table have the same meaning as in the LAN filter table, with the following exception:

■ Dst-address, Dst-netmask

A subnetwork of the local network for which the filter is valid can be entered here. A destination address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).

The table entries are sorted in a similar fashion to the IP router table:

■ Longest network mask is placed on top.

■ For two network masks of equal length, the one with the smaller IP address is placed on top.

Network masks and IP addresses of 0.0.0.0 can be used as "wildcards". Specified computers and networks may be simultaneously subjected to targeted filtering while others pass the router unfiltered.

The tables are processed from top to bottom. As soon as a matching filter is found, the packet is handled accordingly.

*Proxy-ARP*

This option allows you to activate or deactivate the proxy ARP mechanism (default: 'Off'). This function permits data to be transmitted to IP addresses within the same logical network as the sender, e.g. when linking individual workstation computers (teleworkers) to the corporate network via TCP-IP.

*Loc.-routing*

Local routing enables the router to forward data packets via the local network. The local routing is necessary if the router, as the default gateway for the workstations receives packets for destination networks to which it cannot establish a connection itself. If the router cannot return the address of the appropriate router to the workstation via IMCP, it will forward the data to the corresponding router itself (see also 'Local Routing'). Since this setting increases network utilization in the LAN, the default setting is 'Off'.

*Start-address-pool*

Start of the address pool used for the dynamic assignment of IP addresses for devices dialing in. This function is also known as IP pooling and can be used for remote access by several field staff members, for example.

The address pool should be in the same address range as the router. If possible, ensure that the address pool is large enough that an IP address can be assigned to every device dialing in (e.g. one address for each of the available B channels).

If the device dialing in can initially establish a connection, only to have it terminated again during the protocol negotiation, this is a sign of insufficient free IP addresses in the IP pool.



*End-address-pool*

End of the address pool for IP pooling.

### Setup/IP-router-module/Routing-method

The router offers two methods for IP routing, which can be separately set for IP and ICMP packets. Both methods are based on the evaluation of the field 'Type-of-service' in the IP header.

The menu has the following layout:

| /Routing-method     |                                                                                   | Routing method settings         |
|---------------------|-----------------------------------------------------------------------------------|---------------------------------|
| Routing-method      |  | Routing method for IP packets   |
| ICMP-routing-method |  | Routing method for ICMP packets |

*Routing-method* This option allows you to define the routing method used for IP packets:

- If you select 'Normal', all IP packets are handled in the same way as per the routing specifications of the Internet protocol.
- If you select 'Type-of-service', IP packets are placed in the urgent queue or reliable queue, depending on the contents of the 'Type-of-service' field. All other packets are placed in the normal send queue. In this way, transmission is guaranteed, provided that it is possible.




*ICMP-routing-method*

This option allows you to define the routing method used for ICMP packets:

- If you select 'Normal', the ICMP packets are handled like any other IP packets as per the routing specifications of the Internet protocol.
- If you select 'Reliable', all ICMP packets received are placed in the reliable queue.

### Setup/IP-router-module/RIP-configuration

This option allows you to enter settings for the management of IP-RIP packets. The menu has the following layout:

| /RIP-configuration |                                                                                     | Settings for IP-RIP operation |
|--------------------|-------------------------------------------------------------------------------------|-------------------------------|
| RIP-Type           |  | RIP compatibility switch      |
| R1-mask            |  | Management of network masks   |
| Table-IP-RIP       |  | Dynamic IP routing table      |

*RIP-type*

This option allows you to select the method to be used for handling the IP-RIP packets. The different settings have the following meaning:

- **Off:** IP-RIP is not supported (default).
- **RIP-1:** RIP-1 and RIP-2 packets are received but only RIP-1 packets are sent.
- **R1-comp:** RIP-1 and RIP-2 packets are received. RIP-2 packets are sent as an IP broadcast.
- **RIP-2:** Same as **R1-comp** except that all RIP packets are sent to the IP multicast address 224.0.0.9.

*R1-mask*

If **RIP-1** is set, this option allows you to influence the management of network masks. Therefore, these settings are required only for subnetting under **RIP-1**. The different settings have the following meaning:

- **Class** (default): The network mask used in the RIP packet is derived directly from the IP address class, i.e. the following network masks are used for the network classes:
  - Class A: 255.0.0.0
  - Class B: 255.255.0.0
  - Class C: 255.255.255.0
- **Address**: The network mask is derived from the first bit that is set in the IP address entered. This and all high-order bits within the network mask are set. Thus, for example, the address 127.128.128.64 yields the IP network mask 255.255.255.192.
- **Cl+Addr**: The network mask is formed from the IP address class and a part attached after the address procedure. Thus, the above-mentioned address and the network mask 255.255.0.0 yield the IP network mask 255.128.0.0.

*Table-IP-RIP*






This option allows you to display the entries in the current dynamic IP routing table.

An IP-RIP routing table might, for example, have the following appearance:

| IP-address    | IP-netmask    | Time | Distance | Router       |
|---------------|---------------|------|----------|--------------|
| 223.245.254.0 | 255.255.255.0 | 1    | 1        | 192.38.9.100 |
| 223.245.257.0 | 255.255.255.0 | 1    | 1        | 192.38.9.200 |

**Setup/IP-router-module/Masquerading**

This menu allows you to enter settings for the masking function. The menu has the following layout:

| /Masquerading        | Settings for IP masquerading                                                        |                                                             |
|----------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------|
| TCP-aging-second(s)  |  | Time in seconds after which a TCP masking becomes invalid   |
| UDP-aging-second(s)  |  | Time in seconds after which a UDP masking becomes invalid   |
| ICMP-aging-second(s) |  | Time in seconds after which an ICMP masking becomes invalid |
| Service-table        |  | Static masquerading table                                   |
| Table-masquerading   |  | Dynamic masquerading table                                  |

*Service-table*

The use of inverse masquerading makes 'services' (e.g. a file server) selectively visible in the Internet by entering specified ports in the service table in the IP network, while all other services and computers remain invisible from the local network (see also 'IP Masquerading (NAT, PAT)').

The service table (also called the static masquerading table) can contain up to 16 entries and has the following layout:

| D-port | Intranet addr. |
|--------|----------------|
| 20     | 10.1.1.10      |
| 21     | 10.1.1.10      |

The different columns have the following meaning:

- D-port: Destination port for the particular entry
- Intranet-addr.: Destination IP address for the computer in the local network

Through this assignment, it is possible, for example, to address the relevant service directly via telnet. Enter the IP address of the router and attach the port number, separated by a double point, to the address.

You can use the command

```
telnet 192.38.50.100:27
```

to connect directly to a news server that can be reached via a router with the IP address 192.38.50.100.

*Table-  
masquerading*

With IP masquerading, the IP addresses of computers in the local network are rendered invisible to external devices by means of a conversion of addresses and ports in the router. The dynamic masquerading table displays the IP addresses from the local network that the router is currently masking. The dynamic masquerading table can contain up to 2048 entries and has the following layout:








| Intranet addr. | S-port | Protocol | Timeout |
|----------------|--------|----------|---------|
| 10.1.1.10      | 1234   | TCP      | 10      |

The different columns have the following meaning:

- Intranet-addr.: IP address of the computer in the local network
- S-port: Source port for this entry
- Protocol: Protocol used (TCP/UDP/ICMP)
- Timeout: Time in seconds until the entry is removed from the table

## Setup/SNMP-module

This menu allows you to enter settings for configuration of the router via SNMP. The menu has the following layout:

| /SNMP-module     | SNMP module settings                                                              |                                                                                             |
|------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Send-Traps       |  | Switch for issuing SNMP traps                                                               |
| IP-Trap-Table    |  | Table with 20 destination addresses for trap messages                                       |
| Administrator    |  | Device administrator                                                                        |
| Location         |  | Device location                                                                             |
| Register-monitor |  | Command to set a destination address to which the traps are to be sent                      |
| Delete-monitor   |  | Command to delete an address that was set with 'Register-monitor'                           |
| Monitor-table    |  | Table with all currently active destination addresses that were set with 'Register-monitor' |

*Send-Traps* This entry controls trap output (No/Yes).

*IP -Trap-Table* Enters the IP addresses to which the trap messages will be sent.

*Administrator* Administrator's name

*Location* Device location

You can also query the last two parameters via SNMP (MIB-2).

*Register-monitor* This command logs on applications with the router to retain targeted trap information. The *ELSA LANmonitor*, for example, queries the channel statistics in this way and converts them to a graphic display (under Windows).

In principle, any SNMP manager can use this command to obtain information from the router. The syntax

```
register-monitor IP-address:port mac address timeout
```

is used to direct the router to enter the given address in the monitor table and to send traps to it. If the traps are not received within the set hold time, the address will be automatically deleted from the table. A hold time of '0' permanently retains the entry in the table.

*Delete-monitor* This command removes the entries from the monitor table.









*Monitor-table* The monitor table has the following structure:

| IP-address | Port | MAC-Address  | Timeout |
|------------|------|--------------|---------|
| 10.0.0.53  | 1057 | 0080c76da46e | 1       |

This entry indicates, for example, that an *ELSA LANmonitor* has logged on to the router.

Setup/DHCP-module

This menu allows you to enter settings for the DHCP server. The menu has the following layout:


| /DHCP-server-module          | DHCP server settings                                                              |                                                                |
|------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------|
| Operating                    |  | Switch for activating the DHCP module                          |
| Start-address-pool           |  | Start address for the address pool                             |
| End-address-pool             |  | End address for the address pool                               |
| Netmask                      |  | Network mask for the address pool                              |
| Broadcast-address            |  | Broadcast address for the LAN                                  |
| Max.-lease-time-minute(s)    |  | Maximum period of validity for the address assignment via DHCP |
| Default-lease-time-minute(s) |  | Default period of validity for the address assignment via DHCP |
| Table-DHCP                   |  | Table of current assignments via DHCP                          |

Operating

On: The device operates as a DHCP server

Off: The device does not operate as a DHCP server

Auto: The device regularly checks whether there is another DHCP server in the LAN. If not, it operates as a DHCP server and issues IP addresses to local clients.



If there is no IP or Intranet address entered in the TCP/IP module (e.g. delivery status), the router will issue IP addresses from the address range 10.0.0.2 - 10.0.0.253 to all DHCP clients in auto mode.

Start-address-pool  
End-address-pool

The IP address assigned is taken from the address pool selected ('Start-address-pool' to 'End-address-pool'). Any valid addresses in the local network can be entered here.

If 0.0.0.0 is entered instead, the device will determine the appropriate addresses (start or end) from the settings under 'Setup/TCP module'. The procedure is as follows:

- If only the IP address or only the Intranet address is entered, the start or end of the pool is determined by means of the associated network mask.
- If both addresses have been specified, the Intranet address has priority for determining the pool.
- The start address of the pool is either the address given in the DHCP module or the first valid address in the local network.
- The end address of the pool is either the address given in the DHCP module or the last valid address in the local network.



A valid address is then taken from the pool for the IP address. If the computer was already assigned an IP address at some point in the past, it requests this same address and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

The DHCP server also checks whether the address that is to be assigned to the computer is unique in the local network. It does this by issuing an ARP request to the address. If the ARP request is answered, the DHCP server begins the procedure again with a new address. As soon as the uniqueness of an address has been established, the requesting computer is assigned the address found.

*Netmask* The network mask is assigned in the same way as the address:

The system either assigns the network mask entered in the DHCP module or uses the network mask that belongs to the local network (determined during address assignment).

*Broadcast* The broadcast mask is assigned in the same way as the address:

The system either assigns the broadcast address entered in the DHCP module or uses the broadcast address that belongs to the local network (determined during address assignment).

*Max.-lease-time-minute(s)* Here you can enter the maximum period of validity that the DHCP server assigns a host. The DEFAULT value of 6000 minutes equals approximately 4 days.

*Default-lease-time-minute(s)* Here you can enter the period of validity that is assigned if the host makes no request. The DEFAULT value of 500 minutes equals approximately 8 hours.

*Table-DHCP* In the DHCP module, the 'Table-DHCP' option allows you to verify (or look up) the assignment of IP addresses to the relevant computers. This table has the following layout:

| IP-address | Node-ID      | Timeout | Hostname | Type |
|------------|--------------|---------|----------|------|
| 10.1.1.10  | 00a0570308e1 | 500     | ELSA     | new  |

- IP-address: IP address assigned
- Node-ID: Computer's Ethernet address
- Timeout: Time remaining until the assignment becomes invalid
- Hostname: Computer's name in plain text if it was transmitted in the request
- Type: This field contains additional information on the assignment.








The 'Type' field specifies how the address was assigned. This field can assume the following values:

- **new**: The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.

- **unkn.:** While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.
- **stat.:** A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.
- **dyn.:** The DHCP server assigned an address to the computer.

## Setup/NetBIOS-module

The Setup/NetBIOS-module menu contains the settings for the NetBIOS module. The menu has the following structure:

|                 |                                                                                     |                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Operating       |    | On or off                                                                                                       |
| Scope-ID        |    | NetBIOS scope in which the router is located.                                                                   |
| NT-Domain       |    | Workgroup/domain in which the router is located.                                                                |
| Remote-table    |    | All remote stations with which NetBIOS information is to exchanged must be entered in the remote-station table. |
| Group-list      |    | All workgroups known to NetBIOS are recorded in the group list.                                                 |
| Host-list       |   | All computer names known to NetBIOS are recorded in the host list.                                              |
| Server-list     |  | All servers that have logged onto the network are recorded in the server list.                                  |
| Watchdogs       |                                                                                     |                                                                                                                 |
| Update          |                                                                                     |                                                                                                                 |
| WAN-Update-Min. |                                                                                     |                                                                                                                 |

Scope-ID

The Scope-ID menu item can be used to specify the NetBIOS scope in which the device is located. It then sees only those NetBIOS packets originating in the same NetBIOS scope; all other packets are automatically rejected. The scope ID is only used in conjunction with Windows name servers (WINS). This entry can generally be left blank.

NT-Domain

A workgroup/domain can be specified in the NT domain item to trigger the search procedure when starting the NetBIOS module. This is required if the network does not contain any computers running Windows 95 or Windows 98.

Remote-table

All remote stations that are to provide or receive NetBIOS information must be entered in the remote-table. When the NetBIOS module is switched on, NetBIOS packets from remote stations other than those specified will be rejected automatically. The remote-table has the following structure:

| Name    | Type                  |
|---------|-----------------------|
| GLASGOW | Router or workstation |

If the connection to the selected remote station is to be realized via a PPP connection, the NetBIOS rights must be enabled for the corresponding entry in the PPP table.

#### Type

The 'Type' field specifies whether the remote station is a router or a workstation. In the case of a workstation, all of the known names and servers in the local network and all other connected routers are logged off and deleted from their respective tables as soon as the connection to the remote station is closed.

#### Host table

The host table has the following structure:

| Name        | Type | IP-address | Remote station | Timeout | Flags |
|-------------|------|------------|----------------|---------|-------|
| REMOTE      | 00   | 10.0.1.100 | GLASGOW        | 5000    | xx20  |
| WORKSTATION | 00   | 10.0.0.10  |                | 5000    | xx00  |

#### Group table

The group table thus looks like this:

| Group/Domain | Type | IP-address | Remote station | Timeout | Flags |
|--------------|------|------------|----------------|---------|-------|
| WORKGROUP    | 1e   | 10.0.0.10  |                | 5000    | xx00  |
| WORKGROUP    | 1e   | 10.0.1.100 | GLASGOW        | 5000    | xx20  |

The fields of the table have the following significance:

|                |                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Name           | Name of the host in the host table.                                                                                                                 |
| Group/Domain   | Name of the group or domain in the group list. Groups and NT domains are handled in the same manner from the NetBIOS point of view.                 |
| Type           | WINS type of the host. The type is not relevant for NetBIOS, but Microsoft Networks assign certain properties to the name on the basis of the type. |
| IP-address     | IP address of the owner of the name. The same name can be assigned to multiple IP addresses in the group list.                                      |
| Remote station | Name of the remote station for which the name became known.                                                                                         |
| Timeout        | Time until the name is no longer valid. The time-out is also associated with an aging counter in the flags.                                         |
| Flags          | The flags contain additional information pertaining to the name.                                                                                    |

#### Flags

The flags have the following significance:

|        |                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x0003 | This counter increments up each time the validity expires. The entry will be deleted if the name is not refreshed after the second expiration at the latest. |
| 0x0004 | This identifies an entry that still needs to be transferred.                                                                                                 |
| 0x0008 | This identifies an entry that is queued for deletion, i.e. the name has not yet been refreshed after the establishment of a connection.                      |
| 0x0010 | Reserved                                                                                                                                                     |

|        |                                   |
|--------|-----------------------------------|
| 0x0020 | This identifies a remote station. |
| 0x0040 | Reserved                          |
| 0x0080 | Reserved                          |

The server list has the following structure:

| Host        | Group/<br>Domain | UPD | IP-address | OS-<br>Ver | SMB-<br>Ver | Server-<br>type | Remote<br>station | Time-<br>out | Flags |
|-------------|------------------|-----|------------|------------|-------------|-----------------|-------------------|--------------|-------|
| REMOTE      | WORKGROUP        | 00  | 10.0.1.100 | 0400       | 010f        | 0004140b        | GLASGOW           | 13           | 0020  |
| WORKSTATION | WORKGROUP        | 07  | 10.0.0.10  | 0400       | 0415        | 00452003        |                   | 31           | 0000  |






Unlike the host and group lists, this table fills gradually, as the NetBIOS module depends on messages from the servers themselves.





The individual fields have the following significance:

|                |                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------|
| Host           | Name of the server                                                                                                     |
| Group/Domain   | Workgroup or domain in which the server is located.                                                                    |
| UPD            | Update counter: indicates the number of times that the server has already propagated itself                            |
| IP-address     | Address of the server                                                                                                  |
| OS-Ver         | Operating system version number                                                                                        |
| SMB-Ver        | Version number of the SMB protocol used                                                                                |
| Server-type    | Bit mask in which the services of the server are coded                                                                 |
| Remote station | Name of the remote station from which the server was announced                                                         |
| Timeout        | Time until the entry loses its validity (for entries from the LAN) or time until the router propagates a remote entry. |
| Flags          | Corresponds to the flags in the host or group tables.                                                                  |

## Setup/Config-module

This menu allows you to enter settings for router configuration options. The menu has the following layout:

| /Config-module      |                                                                                     | Configuration module settings                      |
|---------------------|-------------------------------------------------------------------------------------|----------------------------------------------------|
| LAN-config          |  | Switch for configuring from the LAN side           |
| WAN-config          |  | Switch for configuring from the WAN side           |
| Password-required   |  | Password required on/off if there is no password   |
| Farconfig-(EAS-MSN) |  | Subscriber number for remote configuration via PPP |
| Maximum-connections |  | Maximum number of simultaneous connections         |

| /Config-module         |                                                                                   | Configuration module settings                                          |
|------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Config-aging-minute(s) |  | Time limit for remote configuration connections                        |
| Login-errors           |  | Number for failed log-in attempts before the log-in block is activated |
| Lock-minutes           |  | Duration of block and period until old log-in errors are forgotten     |
| Display contrast       |                                                                                   |                                                                        |
| Language               |  | Configuration language                                                 |

*LAN-config* This option allows you to define whether remote configuration from the LAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **On**.

*WAN-config* This option allows you to define whether remote configuration from the WAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **Off**.

*Password-required* This specifies whether a new password should be requested every time a remote configuration is begun (**On**), or the password request should be suppressed (**Off**). The default setting for this option is **On**.

*Farconfig-(EAZ-MSN)* This subscriber number permits remote configuration via PPP. If no number is specified here, remote-configuration calls will be accepted on all numbers.

*Maximum connections* This option allows you to display the maximum number of remote configuration sessions that can occur simultaneously for the device.

*Config-aging-minute(s)* If data transmission halts during a remote configuration session, e.g. because the user is no longer entering data, the device automatically releases the connection at the end of the time period specified here. Possible settings are from 1 to 99 minutes; the default setting is 5 minutes.

*Login-errors* This entry specifies the number of failed attempts allowed before the log-in block is activated. An empty password (simply pressing <ENTER> at the password prompt) is not considered an attempt and therefore does not activate the block.



*The default value is 5. A lower value may cause the log-in block to be activated with only one access on an older ELSA LANconfig! In this case obtain an updated ELSA LANconfig version over our online media.*

*Lock-minutes* This entry has two meanings. It indicates how long the access is blocked if the log-in block has been activated. It also sets the period after which the device forgets all prior login errors.





*Language* This option allows you to select whether you will use the German or English version of the software for performing the configuration.

Setup/**LANCAP**-module

Configuring *LANCAP* basically involves answering two questions:

- What call numbers from the telephone network should *LANCAP* respond to?
- Which of the computers in the local network should be able to access the telephone network via *LANCAP*?
- Via which UDP port do the *LANCAP* server and *LANCAP* clients communicate?

The *LANCAP* module has the following layout:

| /LANCAP-module | LANCAP settings                                                                   |                                                                                                                                                           |
|----------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access-list    |  | List of computers allowed to use the <i>LANCAP</i>                                                                                                        |
| Interface-list |  | Activation of the <i>LANCAP</i> for the various interfaces and specification of the various subscriber numbers to which the <i>LANCAP</i> should respond. |
| Priority-list  |  | Priority for the <i>LANCAP</i> versus router connections                                                                                                  |
| UDP-port       |  | UDP port for communication between the <i>LANCAP</i> server and clients                                                                                   |

Access-list

This option allows you to limit the circle of computers permitted to use the *LANCAP*. This table can have a maximum of 16 entries. If the table is empty, all computers can access the *LANCAP*.

Interface-table

The interface table appears as follows:

| lfc  | Operating | EAZ-MSN(s) | Force-Out-MSN |
|------|-----------|------------|---------------|
| S0-1 | Outgoing  | 123456     | no            |

The fields of the table have the following significance:

|               |                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lfc           | Designates the associated interface                                                                                                                                                                       |
| Operating     | This item determines whether <i>LANCAP</i> operation is permitted on this interface for outgoing calls, incoming and outgoing calls (On) or whether <i>LANCAP</i> operation is disabled completely (Off). |
| EAZ-MSN(s)    | Enter the EAZs or MSNs on which the <i>LANCAP</i> should respond to incoming calls here; these EAZs/MSNs will also be displayed to the exchange during outgoing calls.                                    |
| Force-Out-MSN | If no outgoing MSN has been configured for the CAPI application, this item can be used to determine whether the <i>LANCAP</i> transfers the first EAZ/MSN on the list.                                    |

Priority-table

The priority for a port controls the option for breaking outgoing connections via the *LANCAP* router connections. Option '1' does not break router connections, the setting '2' breaks only auxiliary connections of a router connection with channel bundling, the selection '3' also breaks main channels of a router connection.

## Setup/LCR-module

Enter the following information when setting the least-cost router:

- For which modules in the device should the LCR functions be active?
- Which area codes should be diverted when via which call-by-call provider?

The LCR module has the following layout:

| /LCR module           |                          | Least-cost router settings                                    |
|-----------------------|--------------------------|---------------------------------------------------------------|
| Router-usage          | <input type="checkbox"/> | Activate LCR for the router modules, <b>On</b> or <b>Off</b>  |
| Lancapi-usage         | <input type="checkbox"/> | Activate LCR for the <i>LANCAPI</i> , <b>On</b> or <b>Off</b> |
| Timetable             | <input type="checkbox"/> | Call forwarding table                                         |
| Celebration-day-table | <input type="checkbox"/> | List of holidays affecting the timetable.                     |

### Timetable

The table has 256 entries and the following structure:

| Index | Prefix | Days | Start | Stop  | Number-list | Fallback |
|-------|--------|------|-------|-------|-------------|----------|
| 1     | 0171   | 192  | 0:00  | 23:59 | 01013;01070 | On       |

The individual entries have the following meaning:

|             |                                                                                                                                                                                                      |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index       | Continuing index of entries in the table.                                                                                                                                                            |
| Prefix      | Area code to be diverted.                                                                                                                                                                            |
| Days        | Validity of the entry for week days and holidays shown in an 8-bit mask: Bit 0 represents Monday, bit 7 holidays. The entry '31' therefore designates all business days, '192' Sundays and holidays. |
| Start       | Beginning time for the validity of the entry on the defined days.                                                                                                                                    |
| Stop        | Termination time for the validity of the entry on the defined days.                                                                                                                                  |
| Number-list | Network identification number of the call-by-call providers.                                                                                                                                         |
| Fallback    | Automatic fallback to your own telephone company if all call-by-call numbers are busy.                                                                                                               |

Example:

`set 1 02 31 1:00 11:59 01030;01090;01070 On` diverts all long-distance calls to region '02' between one and twelve o'clock to the provider with the network identification number '01030'. If this number is busy, the network identification numbers '01090' and '01070' will be attempted. If they are also not available, the connection will be made via the normal telephone company.

*Celebration-day-table*

The celebration-day-table has 256 entries and the following structure:








| Index | Date     |
|-------|----------|
| 1     | 01010000 |
| 2     | 01050000 |
| 3     | 03100000 |
| 4     | 25120000 |
| 5     | 26120000 |
| 6     | 02041999 |
| 7     | 13051999 |

The individual entries have the following meaning:

|       |                                                                                                                                                                                                                       |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index | Continuing index of entries in the table                                                                                                                                                                              |
| Date  | Dates of holidays.<br>Enter the index and the date in full without separators, e.g. 'set 8 13041999' for April 13, 1999 as the eighth entry in the list.<br>Enter '0000' as the year for annually occurring holidays. |

## Setup/DNS-module

The settings for the DNS server can be modified here as required. The menu contains the following items (incl. their default settings):

|               |                                                                                     |                                                                                             |
|---------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Operating     |  | On (default) or off                                                                         |
| Domain        |  | Own domain, optional, 32 characters max.                                                    |
| DHCP-usage    |  | Yes (default) or no                                                                         |
| NetBIOS-usage |  | Yes (default) or no                                                                         |
| DNS-table     |  | Static DNS table for the manual association of IP addresses to names, 64 entries            |
| Filter-list   |  | Filter list for the exclusion of prohibited domains, 64 entries                             |
| Leasetime     |  | Specifies the name validity information to be given to a requesting computer. Default: 2000 |

*DNS-table*

The DNS table contains a simple association of local names to IP addresses. The table is sorted alphabetically by names.



The table is restricted to 64 entries, as large networks are configured more effectively using the DHCP server, which can also be used to handle name requests. The table has the following layout:

| Hostname | IP-address |
|----------|------------|
| Host10   | 10.0.0.10  |

The name is restricted to a maximum of 32 characters. Longer names are not necessarily practical in a local network.

#### Filter-list

The filter list contains the entries for prohibited domains. In addition, it is possible to specify for whom a given domain will be prohibited. This is set using an IP address/netmask pair. An IP address of 0.0.0.0 prohibits this domain for all computers. A subnet mask of 0.0.0.0 prohibits the domain for all networks. The table has the following layout:

| Idx. | Domain | IP-Address | Netmask |
|------|--------|------------|---------|
| F001 | *xxx*  | 0.0.0.0    | 0.0.0.0 |

Clear IDs can be freely selected and assigned to the filters in the 'Idx.' field.

Enter the name of the domain to be prohibited in the 'Domain' field. Wildcards such as '?' and '\*' may be used. The wildcard '?' replaces exactly one character, while '\*' can stand for a random number of characters. Multiple instances of the wildcard '\*' can be used. For example, \*xxx\* filters all names containing the letters xxx in any position within the name.

The IP address and subnet mask fields can be used to specify the subnet for which the domain will be prohibited.

The filter table is sorted according to the subnet masks in descending order (the longest at the top); entries with identical subnet masks are sorted according to the IP addresses in ascending order. In the event of identical IP addresses, the entries are sorted in ascending order according to the domain to be prohibited.

The table is searched from top to bottom and an error message is returned to the requesting computer in the event of a match.





## Setup/Time-module

The least-cost router in the device requires correct time information to calculate the call number diversions via call-by-call provider. Precise time information is also desirable for some statistics.

The time may be set manually (with the 'time' command) or automatically read from the ISDN network.







For automatic time comparison when the module is switched on, a previously specified remote station is called directly and the time information is taken from the ISDN network. So long as the time module is switched on, the time will be taken from the ISDN every time the router establishes a connection.

The time module has the following layout:

| /Time-module     | Time module settings                                                              |                                                                                                  |
|------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Operating        |  | Activating the module: <b>On, Off</b>                                                            |
| Current-time     |  | Displays the current time in the device.                                                         |
| Time-call-number |  | Call number to which a connection must be established to receive time information from the ISDN. |
| Call-attempts    |  | Number of possible attempts to receive time information                                          |

## Firmware

The various firmware parameters can be called up and a firmware upload started from this menu:

| /Firmware        | Display and keyboard settings                                                       |                                                                                      |
|------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Version-table    |  | Displays hardware releases and serial numbers for the router                         |
| Table-firmsafe   |  | Information on the two firmware versions stored in the device and on the bootloader. |
| Mode-firmsafe    |  | Firmware activation mode                                                             |
| Timeout-firmsafe |  | Time in minutes required to test new firmware                                        |
| Test-firmware    |  | Tests the inactive firmware                                                          |
| Firmware-upload  |  | Initiates a firmware upload                                                          |

### Version table

The version table displays the firmware version and serial number of the device.

| lfc | Module               | Version                | Serial-number |
|-----|----------------------|------------------------|---------------|
| lfc | LANCOM Business 4100 | 1.60.0012 / 30.06.1999 | 8427.000.020  |

*Table firmsafe* This table provides the following details for the two firmware versions stored in the device: the position in memory (1 or 2), status information (active or inactive), the version number, the date, the size and the index (sequential number).

| Position | Status   | Version | Date     | Size | Index |
|----------|----------|---------|----------|------|-------|
| 1        | Inactive | 1.60    | 23061999 | 690  | 6     |
| 2        | Active   | 1.60    | 30061999 | 692  | 7     |
| 3        | <loader> | 1.60    | 07061999 | 64   | 0     |

Enter the following command to activate an inactive firmware version:





```
set <position number> active.
```

*Mode-firmsafe* Only one of the firmware versions stored in the device can be active at any one time. When new firmware is loaded the inactive firmware is overwritten. You can decide which firmware will be activated after the upload:

- 'immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
  - The new firmware is successfully loaded and then operates as desired. Everything is then in order.
  - However, if the new firmware does not operate correctly, it may not be possible to communicate with the device after the restart. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- 'login': To prevent problems caused by defective firmware, the second option will load the firmware and start it immediately.
  - In contrast to the first option, the firmsafe will wait until it has successfully logged on over outband or inband (by telnet). In contrast to the first option, the firmsafe will wait until it has successfully logged on (by telnet). The new firmware will only be permanently activated when the login occurs successfully within the time set under 'Timeout firmsafe'.
  - If the device no longer responds and it is therefore impossible to log in, the firmware automatically loads the previous firmware version and reboots the device with it.
- 'manual': The third option allows you to set a period (Timeout firmsafe) beforehand for testing the new firmware. The device will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective.

# Other

The **Other** menu allows you to manage the following functions:

| /Other         | Various functions                                                                 |                             |
|----------------|-----------------------------------------------------------------------------------|-----------------------------|
| Manual-dialing |  | Connection testing          |
| Boot-system    |  | Boots the device.           |
| Reset-system   |  | Resets to factory settings. |
| Upload-system  |  | Loads new firmware.         |

## Other/Manual Dialing

Select this option when you wish to establish a connection manually for testing purposes.

Boot-system

This option allows you to reboot the device.  
*Before executing the command all open connections (ISDN or TCP) will be released or closed.*

Reset-system

This option resets all the settings that have been entered. The device is reset to the delivery version.  
  
For safety's sake, the system asks you to enter the configuration protection password in order to ensure that you have not mistakenly selected this command instead of the `Boot-system` command. If no password has been assigned, you must press Enter a second time.

Upload-system

This option starts a firmware upload (refer to chapter 'How to set up new software').  
  
The flash ROM technology permits flexible and service-friendly handling of the system software by allowing different firmware versions to be read in. It also allows devices can be retrofitted for all future options.