

ELSA LANCOM™ Business

Manuale

© 1999 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 nei termini previsti 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 consentiti senza previa autorizzazione scritta di ELSA. Ci si riserva il diritto di apportare quelle modifiche che possono derivare dal 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.

Marchi

Windows®, Windows NT® e Microsoft® sono marchi registrati di Microsoft, Corp.

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

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

Aachen, novembre 1999

Qualche parola di presentazione

Vi ringraziamo per la fiducia accordataci

Con il *ELSA LANCOM Business* avete scelto un router con cui si possono collegare reti locali o singole workstation con altre reti tramite connessioni ISDN.

I massimi requisiti di qualità in fase di produzione e un severo controllo finale costituiscono la base per l'alto livello del prodotto e il presupposto per una qualità costante dei prodotti ELSA.

Documentazione

La documentazione allegata è costituita da:

- Guida all'installazione
Installazione hardware ed esempi di configurazione
- Manuale
Descrizione dettagliata delle funzioni e delle modalità operative del router
- Documentazione elettronica (su CD)
Manuale di riferimento per consultazione, descrizione completa dei menu

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, i nostri servizi online (server Internet www.elsa.com) sono disponibili 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 (FAQ). Driver aggiornati, firmware, tool e manuali sono disponibili in ogni momento per essere scaricati.

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

Contenuto

Introduzione	1
Che cosa fa un router?	1
Che cosa offre un <i>ELSA LANCOM Business</i> ?	3
Si alza il sipario sul <i>ELSA LANCOM Business</i>	8
L'apparecchio si presenta così.....	8
Nodo o hub?	10
Conformità CE	10
Modalità di configurazione	13
Molte strade portano a <i>ELSA LANCOM</i>	13
La via diretta: outband.....	13
Prerequisiti per la configurazione outband.....	14
Configurazione outband con <i>ELSA LANconfig</i>	14
Configurazione outband con emulatore di terminale	14
La via comoda: inband	15
Prerequisiti per la configurazione inband.....	15
Alternativa: Gestione indirizzi con il server DHCP	15
Avviare la configurazione inband tramite <i>ELSA LANconfig</i>	15
Avviare la configurazione inband tramite Telnet.....	16
L'accesso remoto: configurazione tramite accesso remoto	16
Quello che serve per la configurazione remota	17
Come si prepara la configurazione remota.....	17
Il primo collegamento remoto con accesso remoto (<i>ELSA LANconfig</i>)....	17
Il primo collegamento remoto con un PPP client e Telnet.....	17
Limitazione della configurazione remota.....	18
Comandi per la configurazione	20
Nuovo firmware con FirmSafe	21
FirmSafe funziona così.....	21
Un nuovo software si carica così.....	22
Configurazione con SNMP	24
Generalità.....	24
Accesso alle tabelle e ai parametri tramite SNMP.....	24
La Management Information Base (MIB).....	26
Che cosa succede sulla linea?	28
Documentazioni trace	28
<i>ELSA LANmonitor</i>	30

Funzioni e modalità	33
Sicurezza per la configurazione	33
Protezione con password	34
Il blocco del login	34
Controllo degli accessi tramite TCP/IP	34
Sicurezza per la LAN	35
Il controllo	35
La chiamata di risposta	36
Come nascondersi: mascheratura IP (NAT, PAT)	37
Gestione degli addebiti	37
Limitazione della connessione in base agli addebiti	38
Limitazione della connessione in base al tempo	38
Impostazioni nel modulo addebiti	39
Connessioni ISDN	39
Name-list	40
Impostazioni di interfaccia	41
Impostazioni di interfaccia router	41
Impostazioni di interfaccia <i>LANCAPi</i>	42
Lista layer	42
Lista RoundRobin	43
Lista canali	44
Lista PPP	44
Script	45
Accettazione di chiamate	45
Lista dei numeri	46
Connessioni fisse e backup	46
La connessione fissa si imposta così	47
Accesso tramite GSM	49
Point-to-point protocol	50
Il protocollo	50
La lista PPP	52
Tutto o.k.? Controllo della linea con LCP	53
Assegnazione degli indirizzi IP tramite PPP	53
Funzioni di richiamata	54
Chiamata di risposta rapida secondo ELSA	57
Richiamata secondo RFC 1570 (PPP LCP extensions)	57
Raggruppamento canali con MLPPP	58
Routing IPX	60
Indirizzamento IPX	60
Informazioni sulla LAN	60
Tabella di routing IPX	61
Che cosa succede nella trasmissione dati in rete IPX?	62

Tabelle RIP e SAP	62
Tanti router qui	63
Rotte ridondanti	63
Exponential backoff.....	63
Filtro per i pacchetti IPX.....	64
Routing IP	66
Tabella di routing IP	66
Filtro per i pacchetti TCP/IP	69
Proxy ARP	70
Routing locale	70
Routing dinamico con IP-RIP	71
Mascheratura IP (NAT, PAT)	73
DNS forwarding	76
Policy based routing.....	76
Gestione indirizzi automatica con DHCP	77
Il router come server DHCP.....	77
DHCP – 'On', 'off' o 'auto'?.....	78
Gli indirizzi vengono assegnati in questo modo	78
Configurazione del router come server DHCP.....	81
DNS	84
Che cosa fa un server DNS?	84
Come si imposta il server DNS	85
NetBIOS proxy.....	87
In breve: Che cosa è il NetBIOS?	87
Trattamento dei pacchetti NetBIOS.....	88
Quali sono i presupposti indispensabili?	89
Come si connettono due reti Windows tramite ISDN	92
Come si seleziona un computer con accesso remoto.....	93
Cercato — Trovato: L'ambiente di rete.....	94
IP Pooling per gli accessi da linea commutata.....	95
Comunicazione di ufficio e <i>ELSA LANCAPI</i>	95
<i>ELSA LANCAPI</i>	96
<i>ELSA CAPI Faxmodem</i>	100
Installazione	100
Invio di fax tramite <i>ELSA CAPI Faxmodem</i>	100
Il Least-cost router	100
Workshop	107
Configurazione con <i>ELSA LANconfig</i> e l'assistenza	107
Configurazione senza assistenza	107
Quale apparecchio si utilizza?.....	108
Impostazioni opzionali.....	108
Applicazioni Internet	108

Internet per tutti i PC della LAN.....	109
Intranet con proprio Web server in Internet	113
Accoppiamenti LAN-LAN	118
Connessione di reti con il router IP	119
Connessione di reti con il router IPX.....	125
Accesso remoto	129
Accesso remoto con TCP/IP	130
Least-cost router	135

Appendice	141
Dati tecnici	141
Collegamenti dei connettori	142
Condizioni generali di garanzia dal 01.06.1998.....	143
Dichiarazione di conformità	145

Glossario	147
------------------------	------------

Indice	155
---------------------	------------

Description of the menu options	R-1
Status	R-3
Display and keyboard.....	R-4
Status/Connection	R-5
Status/Current-time	R-5
Status/Operating-time	R-5
Status/WAN-statistics.....	R-6
Status/LAN-statistics.....	R-8
Status/PPP-statistics.....	R-9
Status/IPX-statistics	R-17
Status/TCP-IP-statistics	R-22
Status/IP-router-statistics.....	R-28
Status/Config-statistics	R-30
Status/Queue-statistics	R-30
Status/Connection-statistics	R-31
Status/Info-connection	R-32
Status/Layer-connection	R-33
Status/Call-info-table	R-33
Status/Remote-statistics	R-34
Status/S0-bus	R-35
Status/Channel-statistics	R-35
Status/Time-statistics.....	R-36
Status/LCR-statistics	R-37
Status/Delete-values	R-37
Setup	R-37
Setup/WAN-module	R-38

Setup/LAN-module	R-48
Setup/IPX-module	R-49
Setup/TCP-IP-module	R-57
Setup/IP-router-module	R-61
Setup/SNMP-module	R-69
Setup/DHCP-module	R-70
Setup/NetBIOS-module	R-72
Setup/Config-module	R-74
Setup/LANCAPI-module	R-76
Setup/LCR-module	R-77
Setup/DNS-module	R-78
Setup/Time-module	R-79
Firmware	R-80
Other	R-82
Novell SAP Numbers	83
TCP/IP Ports	87
.....	89
ELSA LANCOM Business Internal	91
Script Processing	91
General	91
The Script List	92
CompuServe Select	92
Online Trace Outputs	93
General	93
Control of Trace Outputs	94
Examples for Control of Trace Outputs	95
Supported Protocols and Functions	95
Policy Based Routing	105
General	105
Examples	106

Introduzione

Con gli odierni mezzi delle moderne comunicazioni le applicazioni Internet e Intranet diventano sempre più importanti per le aziende di diversi settori. I servizi online vengono utilizzati sempre di più per utilizzi professionali. Le filiali sono collegate per realizzare una rapida comunicazione tra le differenti sedi, e anche il telelavoro acquista un'importanza sempre maggiore.

Tutte queste applicazioni rendono più attraente che mai l'impiego delle soluzioni router ISDN. I router ISDN di ELSA collegano le reti locali con Internet e nelle piccole e medie aziende realizzano la centrale di comunicazione, attraverso cui si possono eseguire funzioni come fax e segreteria telefonica.

Inoltre i router connettono le reti locali con altre LAN (Local Area Network) e consentono l'accesso ai dati aziendali tramite accesso remoto.

Che cosa fa un router?

Con un router si collegano reti locali (LAN) e PC singoli creando una Wide Area Network (WAN). Ciascun computer di questa WAN può accedere, a seconda della propria abilitazione, ai computer e ai 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 ai siti del World Wide Web.

Ma i router possono fare anche di più. Attraverso una speciale interfaccia, la *ELSA LANCAPI*, le moderne funzioni di comunicazione di ufficio come fax, segreteria telefonica, online banking ecc. possono essere rese disponibili in tutta la rete locale. 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.

Il router viene collegato alla rete locale come un normale PC. Quindi tutti i dati che passano attraverso il cablaggio della rete arrivano anche al router. Esso decide autonomamente se i dati devono essere trasferiti a un'altra rete. Se necessario, 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, trasferimento file 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 la 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 commutate, 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 sede. Naturalmente anche in caso di accesso remoto un *ELSA LANCOM* provvede alla protezione dei dati aziendali: La funzione richiamata tramite nomi registrati e numeri d'utenza 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 di *LANCAPi*.

LANCAPI è una speciale forma di interfaccia CAPI-2.0, che può essere utilizzata da programmi applicativi come *ELSA-RVS-COM* o *ELSA-ZOC* per accedere al router.

■ Nodi di accesso commutato per provider Internet

Con le quattro connessioni S_0 disponibili, e quindi con otto canali B, un *ELSA LANCOM Business* è anche conveniente come unit di accesso commutato per provider. Con la funzione di IP Pooling, anche la gestione di molte stazioni remote che possono chiamare il router può essere realizzata comodamente.

Che cosa offre un *ELSA LANCOM Business*?

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

Facile installazione

- Collegare *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. Un *ELSA LANCOM Business* viene collegato tramite connessione 10/100Base-TX a (Fast-)Ethernet.

Connessione WAN

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

Raggruppamento di canali e compressione

Sulla linea ISDN l'apparecchio supporta il raggruppamento di canali statico e dinamico tramite MLPPP e BACP. Con *ELSA LANCOM Business 4100* si possono raggruppare fino a otto canali. Con la compressione dati Stac (hi/fn) si può realizzare un aumento della velocità di trasmissione dati fino al 400%.

Gestione multicanale

Con *ELSA LANCOM Business 4100* sono disponibili quattro connessioni ISDN, e quindi in totale otto canali B. Per ciascuna connessione si può definire la sequenza con cui i canali devono essere utilizzati. Quindi per es. si possono tenere determinati canali riservati per gli accessi RAS o abilitare solo determinati canali per l'accesso Internet.

Display di stato

Un display e spie LED sul pannello anteriore e posteriore del router ISDN consentono di controllare le connessioni ISDN e Ethernet e le connessioni di linea attuali e quindi facilitano la diagnosi in caso di possibili anomalie di sistema.

ELSA LANmonitor

Lo stato del router può essere controllato non solo sui LED. Per gli utenti di sistemi operativi Windows esiste una possibilità supplementare. Con il *LANmonitor* si hanno sempre sullo schermo le informazioni di stato di *ELSA LANCOM*. Per ciascuna periferica della rete locale il *LANmonitor* visualizza le informazioni più importanti, per es.:

- Stato di connessione per ogni canale B
- Nome della controparte collegata
- Modulo da cui è connessa la periferica (router, *LANCAP*)
- Durata della connessione e velocità di trasmissione
- Estratti delle statistiche della periferica (per es. informazioni sulla negoziazione PPP)

Inoltre il *LANmonitor* consente di registrare e memorizzare i messaggi sul PC per impieghi successivi.

Statistiche

L'ampia disponibilità di dati statistici permette di tenere il router sotto controllo. In tali dati si possono trovare per es. tutte le informazioni sulle connessioni stabilite e con esse ottimizzare la configurazione del router ISDN.

Controllo degli addebiti

Attivando le « Informazioni di addebito durante la connessione » nella rete ISDN (secondo AOCD) si possono definire le unità a pagamento 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 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 più conveniente. Si definisce prima il provider che offre le tariffe più convenienti per le proprie necessità, e il router seleziona automaticamente per ciascuna connessione (indifferentemente se via router o via *LANCAP*) 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.

Configurazione con *ELSA LANconfig*

L'impostazione e l'adattamento del router 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 sistema operativi possono utilizzare Telnet o un qualunque emulatore di 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.

L'installazione assistita incorporata aiuta a mettere in funzione gli apparecchi in pochi passi.

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 d'utenza (CLIP) anche una funzione di richiamata, che consente solo il collegamento alla linea verso utenze telefoniche prestabilite. Il filtro firewall e la mascheratura IP completano il sistema di sicurezza. Inoltre il blocco del login impedisce gli « attacchi di forza bruta » e impedisce l'accesso al router dopo un numero definibile di tentativi di login con password sbagliata.

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 speciale caratteristica del router di ELSA, per situazioni in cui nessuno può o deve occuparsi localmente dell'impostazione, è la possibilità di configurazione remota attraverso la rete di 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 inaccessibile a chiamanti non autorizzati.

Aggiornamenti Software

Per rimanere sempre nelle condizioni più aggiornate in campo software, i router posseggono 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. un errore di trasmissione), viene automaticamente ripristinata la precedente versione pronta per il servizio.

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 collegate alla 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 (Fax classe 1) che, come interfaccia tra *ELSA LANCAPI* e l'applicazione, consente l'impiego di programmi fax standard con un *ELSA LANCOM Business*.

DHCP

ELSA LANCOM Business dispone delle funzioni di 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 *ELSA LANCOM Business* può anche stabilire autonomamente tutti gli indirizzi della rete e assegnarli alle periferiche in rete.

NetBIOS proxy

I router *ELSA* sono specialmente predisposti per l'accoppiamento di reti peer-to-peer Microsoft. Attraverso il routing integrato di pacchetti IP NetBIOS, l'accoppiamento di due reti Windows 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, il router risponde in modo locale alle richieste per computer conosciuti ed evita di stabilire la connessione senza necessità.

Server DNS

ELSA LANCOM Business dispone delle funzioni di un server DNS. In questo modo si possono stabilire collegamenti tra indirizzi IP e nomi di computer o di reti, in modo da poter assegnare l'instradamento corretto alle richieste di nomi di computer conosciuti.

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

Come ulteriore funzione, 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.

Collegamento tramite GSM

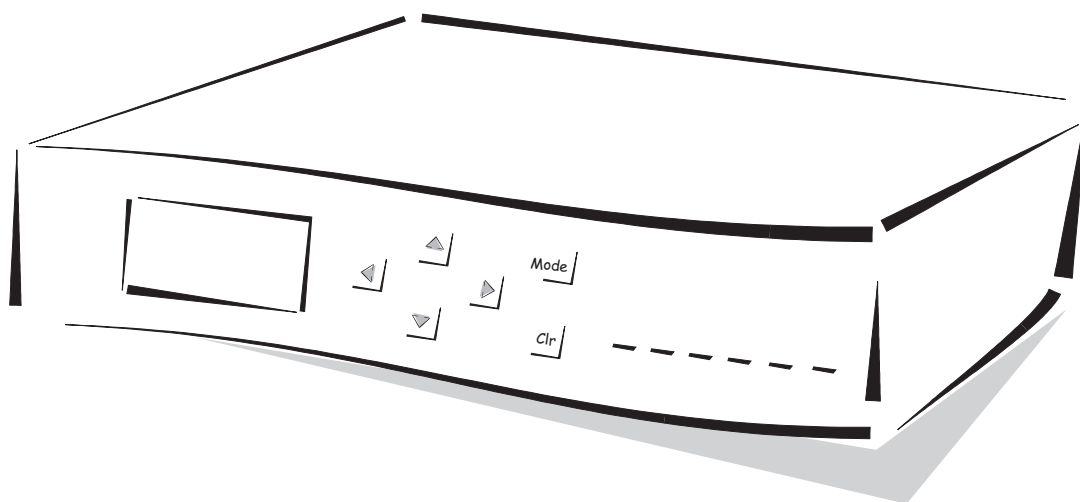
ELSA LANCOM Business consente anche il collegamento tramite telefoni mobili secondo lo standard GSM. In tale circostanza il router riconosce la chiamata tramite il protocollo V.110 e imposta automaticamente il layer utilizzato per questo tipo di trasmissione. Quindi gli accessi RAS tramite GSM e tramite ISDN possono utilizzare lo stesso layer.

Si alza il sipario sul *ELSA LANCOM Business*

In questo capitolo viene presentato l'hardware dell'apparecchio. Sono trattati significato degli elementi di visualizzazione e possibilità di connessione.

L'apparecchio si presenta così

Per prima cosa vogliamo presentare il router. Sul lato anteriore si trovano gli elementi di visualizzazione e di comando: un display, alcuni tasti e spie (LED).



Il display mostra i diversi stati operativi e i messaggi dell'apparecchio. Gli stati operativi e i messaggi vengono visualizzati secondo tre diversi tipi di rappresentazione. Con i tasti si seleziona il tipo di rappresentazione, si confermano i messaggi ed eventualmente si sfogliano le visualizzazioni a più righe. La funzione esatta dei singoli tasti nei diversi stati operativi del *ELSA LANCOM* è descritta nel capitolo 'Possibilità di configurazione'.

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 lampeggiante, oppure l'apparecchio entra in servizio e il LED rimane costantemente acceso.

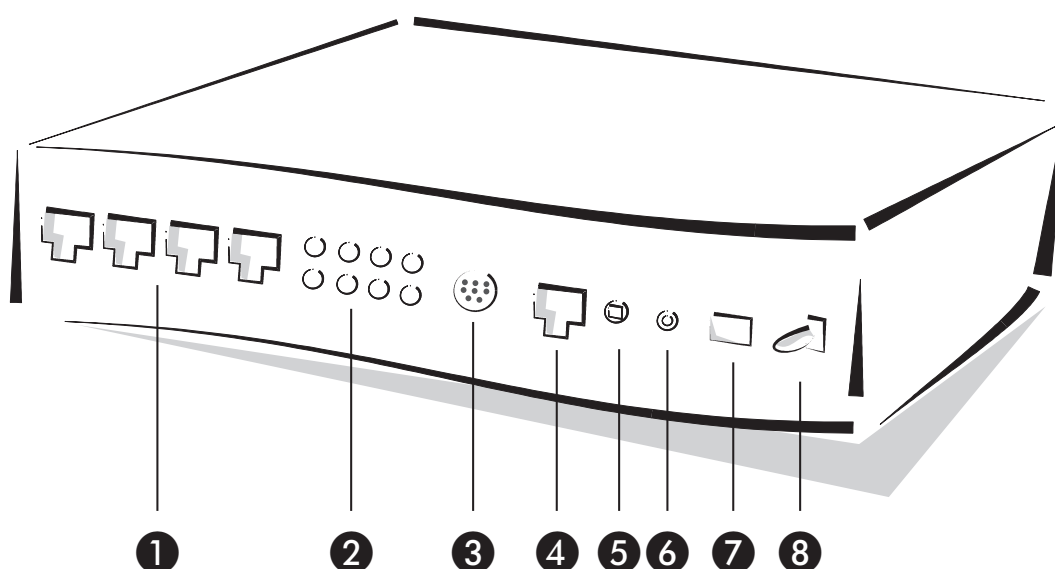
off		Apparecchio disinserito, ma non senza tensione
rosso	1 x breve	Bootstrap (verifica e caricamento) iniziato
rosso	lampeggiante	Visualizzazione di un errore di bootstrap (codificato con codice lampeggiante)
rosso		Apparecchio pronto per il servizio
rosso	interr.	Messaggio di errore o una protezione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

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 100Mbit

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



- ❶ Quattro connessioni ISDN-S₀ (ELSA LANCOM Business 4100)
- ❷ LED di stato per le quattro connessioni S₀:

Stato S ₀	off	Bus non attivato
	lampeggia rapidamente	Bus attivato con canale D, nessuna TEI Canale D riconosciuto, bus non attivato
	verde	Bus attivato con canale D, TEI assegnata
S ₀ Line	off	Nessuna chiamata, nessuna connessione
	lampeggia lentamente (1x al sec., in totale da 2 a 3x)	Chiamata in arrivo, tuttavia il router non è coinvolto o il router stabilisce autonomamente una connessione
	lampeggia rapidamente (3x al sec.)	Chiamata in arrivo, il router è coinvolto ma non ha (ancora) accettato
	giallo	La connessione viene/è stabilita

- 3 Interfaccia di configurazione V.24
- 4 10/100Base-TX per reti 10 Mbit o reti 100Mbit
- 5 Commutatore node/hub
- 6 Pulsante di reset, effettua un reset hardware o ripristina l'apparecchio allo stato di fornitura (premendo per ca. 5 secondi).
- 7 Connessione per l'alimentatore
- 8 Interruttore On/Off

Nodo o hub?

Quando si connette alla rete fare attenzione alla posizione del commutatore node/hub:

- Nello stato di fornitura il commutatore si trova in posizione 'Node'. In questa posizione l'apparecchio si comporta come un nodo di una rete. In questa condizione può essere connesso solo a un hub, non direttamente alla scheda di rete di un computer.
- Se non si vuole collegare l'apparecchio a un hub, ma direttamente a una workstation, portare il commutatore in posizione 'Hub'. In questa posizione, le linee per l'invio e la ricezione dei dati vengono incrociate.

Si può controllare la corretta posizione del commutatore node/hub con l'ausilio del link-status LED (Link).



Conformità CE

Questo dispositivo è stato testato e soddisfa in condizioni di funzionamento regolari ai requisiti di protezione secondo le direttive del Consiglio della Comunità Europea per l'armonizzazione delle leggi degli Stati membri relative alla tollerabilità elettromagnetica (89/336/CEE) corrispondente alla norma EN 55022 classe B ed EN 50082-1.



In caso di utilizzo non secondo destinazione o di impiego dell'apparecchio in vicinanza di trasmettenti molto forti si possono verificare mancanze di funzionamento temporanee dell'apparecchio.

Questi requisiti garantiscono una adeguata protezione contro disturbi di ricezione in aree abitative. L'apparecchio produce e utilizza segnali della banda di frequenza di Radio e Televisione e può irradiarle. Qualora l'apparecchio non venga installato e non funzioni conformemente alle indicazioni fornite, può determinare disturbi nella ricezione. Non è tuttavia possibile garantire che un'installazione corretta escluda completamente fenomeni di disturbo durante la ricezione. Nel caso in cui l'apparecchio causi fenomeni di disturbo alla ricezione di radio e televisione (questo può essere verificato spegnendo

temporaneamente l'apparecchio), si consiglia di tentare di eliminare il disturbo adottando una delle seguenti misure:

- Modificare la direzione o la posizione dell'antenna di ricezione.
- Aumentare la distanza tra l'apparecchio e il televisore o la radio.
- Collegare l'apparecchio ad un altro circuito di alimentazione rispetto al televisore o alla radio.
- Rivolgersi al proprio rivenditore o ad un esperto tecnico radiotelevisivo.

Modalità di configurazione

Gli *ELSA LANCOM Business* vengono sempre forniti con un software aggiornato, in cui sono già predisposte alcune impostazioni.

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 ELSA ha preparato un nuovo firmware con nuove prestazioni, si trovano le istruzioni per caricare il nuovo software.

Molte strade portano a *ELSA LANCOM*

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

- Tramite l'interfaccia di configurazione (interfaccia Config) sul pannello posteriore del router (denominato anche outband)
- 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 guasta. La configurazione remota dipende anche 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*.

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.



Prerequisiti per la configurazione outband

Apparecchiatura necessaria:

- Un computer con Windows 95, Windows 98 o Windows NT 4.0 e il programma di configurazione *ELSA LANconfig*
o
Un computer con qualunque sistema operativo ed un emulatore 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 (la porta COM del PC all'interfaccia di configurazione del router).

Configurazione outband con *ELSA LANconfig*

Avviare *ELSA LANconfig* per es. dalla barra di avvio di Windows con **Avvio ► Programmi ► ELSA lan ► 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 **Periferica ► Trova ► Trova su tutte le interfacce**. *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 strumenti di configurazione. Selezionare uno dei wizard proposti, e rispondere semplicemente alle domande. Alla fine *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.

Configurazione outband con emulatore di terminale

Se l'emulatore di terminale è avviato, premere alcune volte 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'.

La via comoda: inband

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

Prerequisiti per la configurazione inband

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 192.110.130.1, è possibile raggiungere il router con l'indirizzo 192.110.130.254.

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.

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. Quando viene utilizzato il server DHCP, è possibile fare impostare automaticamente tutti gli indirizzi IP della rete, compreso quello dello stesso router (vedere anche il capitolo 'Assegnazione automatica degli indirizzi con DHCP').

Avviare la configurazione inband tramite *ELSA LANconfig*

Dopo l'installazione (facendo doppio clic su 'autorun.exe') si richiama lo strumento di configurazione *ELSA LANconfig* per es. dalla barra di avvio di Windows con **Avvio ► Programmi ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* cerca automaticamente nella rete locale le periferiche *ELSA LANCOM*. Se nella rete locale viene trovata una periferica non ancora configurata, *ELSA LANconfig* avvia autonomamente il settaggio assistito.

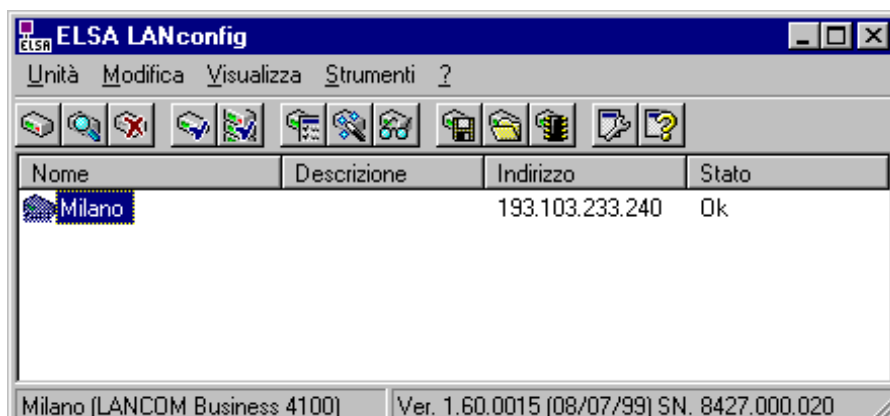
Selezionare il wizard proposto, e rispondere semplicemente alle domande. Alla fine il router è impostato per il compito selezionato.

Per avviare manualmente la ricerca di un nuovo router, 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.



Facendo doppio clic sulla periferica evidenziata, cliccando sul pulsante **Configura** o sull'articolo a 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 l'help online. 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.

Avviare la configurazione inband tramite Telnet

Tramite Telnet si avvia la configurazione inband per es. con il comando:

```
telnet 10.1.80.125
```

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

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

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.

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*

Come si prepara la configurazione remota

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

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 utilizzato per 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 *ELSA LANconfig* stabilisce una connessione tramite accesso remoto.

Il primo collegamento remoto con un PPP client e Telnet

- ① Stabilire con il PPP client una connessione mediante *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. *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 *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 *ELSA LANCOM* tramite accesso remoto esattamente come tutte le altre periferiche.

Limitazione della configurazione remota

La connessione PPP di una qualunque controparte al router si realizza ovviamente 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 l'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 nel campo di configurazione 'Gestione' sulla scheda di registro 'Sicurezza'.
- 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'.

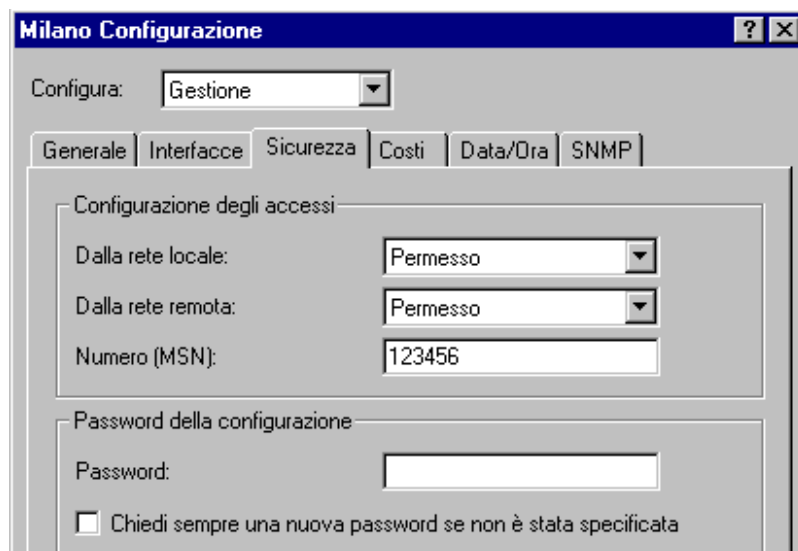


- ③ Introdurre come numero telefonico nel campo 'Configurazione degli accessi' un MSN o EAZ del proprio collegamento ISDN, che non sia utilizzato per il router, per LANCAP/ o le porte a/b.

Immettere in alternativa il seguente comando:

```
set /Setup/Config-module/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.

Comandi per la configurazione

Quando si utilizza Telnet (inband) o un emulatore di terminale (outband) per la configurazione del router si introducono i comandi e le indicazioni di percorso nel modo già noto per il DOS o per UNIX.

Per separare le voci in un percorso si introduce una barra obliqua inversa. I comandi e le voci delle tabelle non devono essere scritti completamente, è sufficiente una abbreviazione univoca.

Nella configurazione dei router vengono visualizzate ed eventualmente modificate le voci per i gruppi MENU, VALORE, TABELLA, TABINFO, AZIONE e INFO. A questo scopo si possono utilizzare i seguenti comandi:

Questo comando ha il seguente significato per es.:
? o help	Richiama i testi di aiuto.	-
dir, list, ll, ls <MENU>, <VALORE> o <TABELLA>	Visualizza il contenuto di MENU, VALORE o TABELLA.	dir/status/wan-statistics visualizza la statistica WAN attuale.
cd <MENU> o <TABELLA>	Passa nel MENU o nella TABELLA indicati.	cd setup/tcp-ip-module (abbreviato cd se/tc) passa nel modulo TCP/IP.
set <VALORE>	Il VALORE si imposta così.	set ip-adress 192.110.120.140 imposta un nuovo indirizzo IP.
	Nelle righe delle tabelle si introducono tutte le voci separate da spazi. Un * lascia la voce inalterata.	set /setup/name MILANO assegna all'apparecchio il nome 'MILANO'
set <VALORE> ?	Mostra quali valori possono essere introdotti.	
del <VALORE>	Cancella una riga da una tabella.	del /se/wan/nam/MILANO Cancella la voce per la controparte MILANO
do <AZIONE> (parametri)	Esegue l'AZIONE, eventualmente con i parametri indicati.	do /firmware/firmware-upload avvia lo scarico di un nuovo firmware.
passwd	Consente di introdurre una nuova password. A questo scopo si deve introdurre prima la vecchia password, se presente. Poi si deve introdurre la nuova password due volte di seguito confermando ogni volta con  .	
repeat <sec> <AZIONE>	Ripete l'AZIONE dopo il numero di secondi indicato. Qualunque tasto interrompe la ripetizione.	repeat 3 dir/status/wan-statistics visualizza ogni 3 secondi la statistica WAN attuale.
time	Imposta l'ora e la data di sistema.	time 24.12.1998 18:00:00

Questo comando ha il seguente significato	... per es.:
language <lingua>	Imposta la lingua per l'attuale sessione di configurazione.	Le lingue supportate sono attualmente Inglese (language english) Tedesco (language deutsch)
exit, quit, x	Si esce dalla configurazione.	

I testi introdotti contenenti spazi vengono accettati solo tra virgolette, per es. `set /se/snmp/admin "Un amministratore"`.

Le voci di testo (valori singoli e in tabelle) vengono cancellate nel modo seguente:

```
set /se/snmp/admin " "
```

Nuovo firmware con FirmSafe

Il software dei router di 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!

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 come 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 evitare 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, il router attende per altri cinque minuti che un login venga eseguito con successo via outband o inband (Telnet). 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 router 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. Il router 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.

Un nuovo software si carica così

Per il firmware upload (così si definisce il caricamento del software) esistono diverse vie:

- Strumento di configurazione *ELSA LANconfig* (raccomandato)
- Emulatori di 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



Nello strumento di configurazione *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 manualmente. 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 *Telnet* 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, che per es. si trova nel file 'LC_1000U.130', in un router 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
```



*Questo comando invia il file corrispondente al router utilizzando il parametro **writelflash**. 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 verifica un errore (errore di scrittura nella flash ROM, errore di trasferimento TFTP e simili) la connessione TFTP viene interrotta per segnalare il problema all'operatore. In questo caso l'apparecchio non si riavvia, ma continua ad operare con il firmware esistente fino al successivo spegnimento/accensione. Quindi l'operatore ha per es. la possibilità di salvare la configurazione dell'apparecchio.

Se si spegne l'apparecchio durante un upload TFTP, esso può essere configurato solo in modo locale, vale a dire attraverso l'interfaccia outband. Quando viene riacceso, l'apparecchio attende un firmware upload tramite l'interfaccia seriale.



Pertanto fare attenzione ad eseguire il firmware upload solo attraverso una connessione sicura (stabile).

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 indirizzo 10.0.0.1
- `tftp 10.0.0.1 get dir/status/verb file2` : Salva le informazioni di connessione attuali nel file2

Configurazione con SNMP

Generalità

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. Nel linguaggio comune questa posizione viene denominata « Manager », mentre le periferiche vengono denominate « Agent ». La struttura consentita per lo scambio di informazioni SNMP è relativamente semplice. Un'applicazione Manager ha accesso sulla rete a tutte le periferiche e servizi con capacità SNMP (gli agent). I diritti di accesso vengono regolati tramite « Communities ».

Come mostrato nella seguente tabella, il SNMP v.1 consente solo un set di comandi limitato:

Comando	Destinazione/sorgente	Funzione
GetRequest	Manager – Agent	richiama un'informazione dall'agent
GetNextRequest	Manager – Agent	richiama l'informazione successiva nel MIB dall'agent
SetRequest	Manager – Agent	modifica un'impostazione presso l'agent
GetResponse	Agent – Manager	restituisce al manager il valore richiesto
Trap	Agent – Manager	segnala un errore o uno stato speciale

Con l'ausilio di questi comandi le periferiche con capacità SNMP di una rete possono essere monitorate e configurate in modo centralizzato. Le capacità SNMP dell'agent vengono definite nelle cosiddette MIB = Management Information Bases.

Nel firmware dei router di ELSA è implementato un agent per SNMP V.1 (secondo RFC 1157). Viene supportata una parte delle MIB-2 e una MIB privata, allegata al prodotto come file separato. Per gestire completamente un router tramite SNMP, questa MIB deve essere caricata e tradotta da un manager SNMP (per es. HP-OpenView). Poi tutti i menu e i parametri della configurazione diventano disponibili in uno specifico ramo dell'albero di configurazione management SNMP:

iso/org/dod/internet/private/enterprises/elsa/isdn-devices/isdn-router/...
o 1.3.6.1.4.1.2356.400.1...

Accesso alle tabelle e ai parametri tramite SNMP

Tutte le tabelle e i parametri possono essere letti ed eventualmente modificati tramite l'interfaccia SNMP. Nella MIB si specificano le variabili che hanno lo stato 'read-only' o

'read-write'. Nei manager SNMP reperibili sul mercato i due stati 'read-only' e 'read-write' di regola sono evidenziati a colori.

Protezione di accesso sotto SNMP v.1

L'accesso agli oggetti SNMP avviene attraverso le cosiddette communities. Una community è essenzialmente una password, con cui si può regolamentare l'accesso a determinate classi di informazioni. Nel router con la community 'public' si può accedere in lettura a tutti i parametri e tabelle. Con questa community non si possono attivare accessi di scrittura.

Se si devono scrivere dati tramite SNMP, si deve utilizzare come community la password dell'apparecchio. Se per un router non è stata immessa una password, in linea di principio non è consentito **alcun** accesso di scrittura tramite SNMP.

Per accedere a un router tramite SNMP le impostazioni sotto 'Setup/Config module' vengono valutate nel modo seguente:

Voce	Valore	Significato
Password-required	On	L'accesso tramite la community 'public' è interdetto.
Password-required	Off	L'accesso tramite la community 'public' è consentito solo con diritti di lettura. Se la password viene indicata come community, possono essere effettuate tutte le azioni.
LAN/WAN-Config	Off	Ogni accesso tramite LAN/WAN è interdetto.
LAN/WAN-Config	On	L'accesso tramite la community 'public' è consentito solo con diritti di lettura. Se la password viene indicata come community, possono essere effettuate tutte le azioni.
LAN/WAN-Config	Lettura	L'accesso sia tramite la community 'public' che con password è read-only.

In caso di tentativo di accesso fallito, se è stato attivato il meccanismo trap, una trap 'Authentication Failed' viene attivata e inviata al/ai manager nella tabella trap SNMP.

Il meccanismo community in SNMP v.1 è comunque un diritto di accesso molto limitato, poiché i dati, i MIB-ID e le community vengono inviati all'interno delle richieste e delle risposte senza codifica nel blocco di dati UDP.

Cancellazione di righe di tabelle con SNMP

SNMP non mette a disposizione alcuno speciale meccanismo di cancellazione. Pertanto è necessario servirsi di un artificio per cancellare le voci dalle tabelle o per inserire nuove righe nelle tabelle.

Se si deve cancellare una riga, si deve modificare al valore attuale l'indice di tale riga, vale a dire il valore nella prima colonna.

- Esempio: Nella seguente tabella di routing si deve cancellare la riga n. 3.

Indirizzo IP	Maschera di rete IP	Nome del router	Distanza
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.240.0.0	0.0.0.0	0
10.0.0.0	255.0.0.0	ROBERT	0
224.0.0.0	224.0.0.0	0.0.0.0	0

Tramite il manager si modifica la voce '10.0.0.0' (quindi il primo elemento della terza riga) al suo valore attuale, e quindi a '10.0.0.0' e si invia il comando Set. Il SetRequest SNMP contiene la voce per modificare il primo elemento della terza riga a '10.0.0.0'. Il software SNMP riconosce questa assegnazione ridondante dell'indice e la interpreta come comando di cancellazione.

Aggiunta di righe di tabelle con SNMP

Se si deve aggiungere una riga in una tabella, si deve modificare l'indice di una qualunque riga già esistente al nuovo valore della nuova riga. La riga utilizzata come sorgente per la modifica rimane invariata.

Messaggi di errore tramite trap SNMP

Tramite il meccanismo di trap SNMP possono essere inviati messaggi di errore o di avvertimento a una posizione di management. L'agent SNMP contenuto nel router consente di inviare trap a un massimo di 20 manager SNMP. Gli indirizzi IP di tali manager vengono configurati nel menu di configurazione sotto `/setup/SNMP-module/IP-Trap-Table`. L'invio può essere attivato e disattivato in generale con il pulsante `/setup/SNMP-module/Send-Traps`.

SNMP e *ELSA LANmonitor*

Le tre voci `/setup/SNMP-module/...Register-monitor`, `.../Delete-monitor` e `.../Monitor-table` sono coinvolte solo per la registrazione automatica del *LANmonitor* e non hanno alcun altro significato per l'utente. Esse vengono visualizzate nel menu solo a scopo di controllo.

La Management Information Base (MIB)

Per consentire ai sistemi di management SNMP l'accesso alla configurazione di *ELSA LANCOM*, deve essere fornita con l'apparecchio una rappresentazione testuale della struttura di configurazione (la cosiddetta MIB privata). La sintassi di questa MIB è conforme a ASN.1 (Abstract Syntax Notation One, ISO 8824).

Di regola nel pacchetto di programmi del software management SNMP è contenuto un cosiddetto MIB compiler. Questo compiler traduce il file MIB in una forma utilizzabile dal manager.

L'attuale MIB ELSA è reperibile sia come allegato al prodotto su CD che sui servizi ELSA online.

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.

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. Particolare interessante: Gli errori da rintracciare possono essere trovati sia nella configurazione del proprio *ELSA LANCOM* 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.

Avviamento di trace

Trace viene richiamato secondo la seguente sintassi:

```
trace [code] [parameters]
```

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	Negoziazione del protocollo ELSA
PPP	Negoziazione del protocollo PPP



Questo parametro in collegamento con trace genera la seguente visualizzazione:
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 IPX NetBIOS
IP-router	Routing IP
IP-RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
Script	Negoziazione script
IP-masquerading	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-Tr., 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.



Le istruzioni per l'interpretazione delle documentazioni trace si possono trovare nella parte di riferimento del Manuale.

ELSA LANmonitor

Con *ELSA LANmonitor* si può disporre di un piccolo tool di monitoraggio, con cui in ambiente Windows si possono avere sempre sullo schermo le informazioni più importanti sullo stato del 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 il software di configurazione *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 'ELSA 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 sul collegamento con l'Internet provider.

- 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 ► ELSAlan ► 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 **Opzioni ► Strumenti Unità Monitor**.

- ③ *ELSA LANmonitor* crea automaticamente una nuova voce nella lista delle periferiche e visualizza prima lo stato dei canali B. Avviare il browser Internet e richiamare una qualunque pagina Web. Ora si può vedere in *ELSA LANmonitor* come viene stabilita la connessione su un canale e quale controparte viene chiamata. 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.
- 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 *LANmonitor* in forma di file, selezionare nel menu 'Visualizza' le 'Opzioni' e passare alla scheda di registro 'Registrazione'. Attivare la protocollazione e impostare se *LANmonitor* deve creare un file di protocollo giornalmente, mensilmente o continuamente.

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
- Connessioni fisse e procedure di backup
- Collegamento GSM
- Supporto PPP
- Routing IPX
- Routing IP
- Server DHCP
- Server DNS
- NetBIOS proxy
- IP pooling
- *ELSA LANCAPI*
- Controllo ora
- Least-cost router

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

Nel workshop si possono trovare esempi dettagliati di configurazione.

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

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 utenti della rete.

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

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`.

Il blocco del login

La configurazione del *ELSA LANCOM Business* è protetta mediante un blocco del login contro gli « attacchi brute force ». Si possono impostare sia il numero massimo consentito di tentativi di login sbagliati che la durata del blocco.

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`)

Controllo degli accessi tramite TCP/IP

Con una speciale lista di filtro può essere limitato l'accesso tramite TCP/IP alle funzioni interne degli apparecchi. Si definiscono come funzioni interne le sessioni 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`.

Sicurezza per la LAN

Certo non si può consentire che un qualunque estraneo possa semplicemente vedere o modificare i dati contenuti nel server aziendale. Un *ELSA LANCOM Business* offre diverse possibilità per limitare l'accesso dall'esterno:

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

Il controllo

L'« Identifier » che deve essere utilizzato per riconoscere il chiamante viene impostato nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Accettazione chiamate' oppure nel menu /Setup/WAN-module/Protect. Si hanno le seguenti possibilità di selezione:

- Tutte: 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 o nella lista dei nomi.

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

Controllo del nome

Nelle connessioni tramite PPP può essere trasmesso anche il nome della controparte.

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.

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: Inoltre qui si può richiedere una protezione valida specialmente per questo

protocollo come PAP (Password Authentication Protocol) o CHAP (Challenge Handshake Authentication Protocol). Si tratta di una forma di protezione che il vostro apparecchio impone agli utenti remoti.



Le procedure di sicurezza PAP o CHAP naturalmente non si applicano per es. se con il ELSA LANCOM si chiama 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 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 telefonico del chiamante, già prima che la connessione venga stabilita (CLI – Calling Line Identifier).

Se il numero telefonico 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 in *ELSA LANCOM* è stata definita una protezione tramite il numero, tutte le chiamate da controparti con numero telefonico sconosciuto vengono respinte.

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

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 telefonico.

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

- Il router può respingere la richiesta di chiamata di risposta.
- Può richiamare un numero telefonico prestabilito.
- Il numero telefonico 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 telefonico 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 (brevettata). Questa accelera notevolmente la procedura di chiamata di risposta.

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 (masquerading) 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 della 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-module/IP-routing-table`.

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

Gestione degli addebiti

La proprietà del router di stabilire autonomamente la connessione con tutte le controparti richieste e di chiuderla alla fine della trasmissione consente all'utente di accedere molto comodamente a Internet o a computer e reti remoti. Nella trasmissione dati tramite linee commutate ISDN tuttavia si possono presentare in conseguenza di una configurazione non corretta del router (per es. nella configurazione del filtro) o di un eccessivo uso del servizio (per es. navigazione prolungata in Internet) costi telefonici molto alti.

Limitazione della connessione in base agli addebiti

Per limitare tali costi, il software offre già da molto tempo la possibilità di limitare gli addebiti disponibili per un determinato periodo. Per es. nello stato di default si possono usare al massimo 830 unità a pagamento alla settimana. Quando questo limite è stato raggiunto, il router non consente di stabilire ulteriori connessioni.



*Il monitoraggio addebiti del router può essere utilizzato al meglio quando sono attivate le « informazioni di addebito **durante** la connessione » sulla rete ISDN (come 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!

Limitazione della connessione in base al tempo

Tuttavia questo meccanismo non interviene se sul collegamento ISDN non vengono trasmesse informazioni di addebito. 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 limitare comunque i costi telefonici, la durata massima della connessione può anche essere comandata con l'ausilio del tempo. A questo scopo viene definito analogamente al budget addebiti un budget di tempo per un periodo. Per es. nello stato di default si possono stabilire connessioni attive per un massimo di 210 minuti alla settimana.



Se viene raggiunto uno dei due limiti, tutte le connessioni aperte stabilite dal router vengono chiuse automaticamente. 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 non vengono rilevate.

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 sessioni 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-units, Minutes-budget
Unità oppure minuti online massimi di un periodo di monitoraggio
- Spare-units, Spare-minutes
Unità oppure minuti online disponibili per il periodo corrente
- Router-units, Router-minutes
Unità oppure minuti online 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.

Connessioni ISDN

La comunicazione dati tra due periferiche ISDN si realizza tramite connessioni ISDN. In linea di principio queste connessioni possono essere connessioni a su linea commutata 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 eventualmente 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.

Le seguenti sezioni presentano sommariamente le liste e i parametri in esse contenuti, mostrano la correlazione con altre liste e parametri e come questi vengono configurati nel software.

Name-list

La lista dei nomi si trova in *ELSA LANconfig* nella sezione di configurazione 'Comunicazione' sulla scheda di registro 'Siti remoti' o nelle sedute Telnet o di terminale nella posizione `/Setup/WAN-module/Name-list`.

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 telefonico 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 telefonici, immettere gli altri numeri telefonici nella lista round robin.

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

- B?-DT

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

Impostazioni di interfaccia

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

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 per la connessione fissa.
- Prefisso
Numero che deve essere selezionato prima del numero telefonico per le chiamate in uscita, per es. il numero identificativo del centralino nel caso di impianti interni.

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 sessioni 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 telefonici (MSN/EAZ)
Il router reagisce a questi numeri telefonici nelle chiamate in arrivo. Più numeri telefonici vengono separati da punto e virgola. Se non si immettono i numeri telefonici, il router reagisce a tutti i numeri telefonici.

Il primo numero telefonico immesso viene trasmesso alla controparte in caso di stabilimento attivo della connessione. Se non si immettono i numeri telefonici, 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 telefonico
Attivare questa opzione se il proprio numero telefonico non deve essere indicato alla controparte durante lo stabilimento attivo della connessione del router.



Questa funzione deve essere supportata dal gestore della rete.

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 telefonici (MSN/EAZ)
La *LANCAPi* reagisce a questi numeri telefonici nelle chiamate in arrivo. Più numeri telefonici vengono separati da punto e virgola. Se non si immettono i numeri telefonici, il router reagisce a tutti i numeri telefonici.
- 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 telefonico
Normalmente durante lo stabilimento attivo della connessione tramite la *LANCAPi* viene trasmesso il numero telefonico impostato nell'applicazione CAPI. Se tale numero telefonico manca o non è valido, la *LANCAPi* non trasmette alcun numero telefonico. Con questa opzione si può stabilire che, in caso di mancanza del numero telefonico dell'applicazione CAPI, al posto di questo venga trasmesso il primo numero presente nel campo 'Numeri d'telefonico'.

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 Scripts è necessaria una voce aggiuntiva nella lista Scripts.
- Layer 2
Protocollo layer 2 per la connessione.
- Opzioni
Attiva come opzione la compressione dei dati e il raggruppamento di canali. Questa opzione diventa attiva solo se viene supportata dai protocolli layer 2 e layer 3.
- Layer 1
Protocollo layer 1 per la connessione. Viene riconosciuto in parte automaticamente nelle chiamate in arrivo.

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/Round robin-list`.

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

- Sito remoto
Nome della controparte definito per primo nella lista dei nomi.
- Round robin
Ulteriori numeri d'telefonico per tale controparte. Più numeri d'telefonico 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.

Lista canali

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

Nella lista canali si stabilisce quanti canali B devono essere utilizzati al minimo o al massimo per la connessione, secondo quale sequenza vengono stabiliti i canali e quanti canali devono essere utilizzati per una connessione fissa o eventualmente come linea di backup tramite connessioni a selezione.

- Sito remoto

Nome della controparte definito per primo nella lista dei nomi.

- Almeno

Numero minimo di canali che devono essere stabiliti per la connessione.

Se si indica più di un canale, si realizza un raggruppamento di canali statico per questa connessione. Il layer utilizzato deve essere impostato per il raggruppamento di canali nelle opzioni layer 2.

- Al massimo

Numero massimo di canali che devono essere stabiliti per la connessione.

Se si indica un numero di canali massimo maggiore di quello minimo, si realizza un raggruppamento di canali dinamico per questa connessione. Il layer utilizzato deve essere impostato per il raggruppamento di canali nelle opzioni layer 2.

- Sequenza

La sequenza con cui i canali devono essere stabiliti viene indicata secondo la sintassi [Interfaccia]-[Canale];[Interfaccia]-[Canale] ecc.

- Backup

Numero dei canali che devono essere stabiliti per una connessione fissa tramite linee a selezione se la connessione fissa è guasta.

Lista PPP

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

Nella lista PPP si definiscono per una connessione i parametri aggiuntivi, che utilizzano PPP nel layer di comunicazione su layer 3.

- Sito remoto

Nome della controparte definito per primo nella lista dei nomi.

- Nome utente
Nome utente che viene utilizzato per la chiamata della controparte.
- Password
Password che viene utilizzata per la chiamata della controparte.
- IP, NetBIOS, IPX
Protocolli che possono essere trasmessi tramite questa connessione.
- Auth.
Procedura di autenticazione che il router deve richiedere alla controparte.
- Tempo, Tentativi, Conf., Fail., Term.
Parametri di comportamento della connessione che qui non vengono descritti in dettaglio.

Script

La lista Script si trova in *ELSA LANconfig* nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Protocolli' o nelle sessioni 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.

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.

■ Per nome

Tutte le chiamate vengono accettate inizialmente. Nella negoziazione 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 telefonico della controparte viene trasmesso.

■ Per nome o numero

La chiamata viene accettata se uno dei due controlli ha successo.

Lista dei numeri

La lista dei numeri si trova in *ELSA LANconfig* nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Accettazione chiamate' o nelle sessioni 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.

■ Numero di telefono

Numero telefonico che viene trasmesso dalla controparte chiamante (eventualmente incl. numero prefisso 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.

Connessioni fisse e backup

Se si opera in modo permanente tramite la connessione ISDN, o è necessario un accesso ripetuto a brevi distanze, può essere conveniente l'impiego di una connessione ISDN fissa. Poiché nelle connessioni fisse il canale D non è necessario per la trasmissione dati, ma la disponibilità del canale di comando viene comunque addebitata, le connessioni fisse senza canale D presentano il migliore rapporto prezzo/prestazioni.

Se un canale è sufficiente nel medio termine, si dovrebbe scegliere la D64S. Se la velocità di trasmissione di un singolo canale non è sufficiente, si dovrebbe prendere in considerazione l'allestimento di una D64S2. Per le connessioni con due diverse controparti, utilizzare due D64S. Nel seguito questa combinazione viene anche definita D64SY:

Connessione fissa	Tipo
D64S	Un canale B, nessun canale D per una controparte
D64S2	Due canali B, nessun canale D per una controparte
D64SY	Due canali B, nessun canale D per due controparti diverse

Tutte le tre varianti vengono impostate nella tabella di interfaccia del router come connessione fissa Gruppo 0. Le varianti si distinguono per il « flag YV. » nella tabella di interfaccia, per la voce 'Opzioni layer 2' nella lista layer e per le voci nella lista canali.

La connessione fissa si imposta così

Per predisporre il router a operare sulle diverse connessioni fisse sono necessarie le seguenti impostazioni.

Impostazioni nella tabella di interfaccia

- Nella tabella di interfaccia si immette il protocollo **Grp0**.
- Per le connessioni con una controparte il **flag YV.** deve avere il valore **Off**, per le connessioni con due diverse controparti il valore **On**.
- Nel layer usato, per le connessioni con un canale B si può immettere come opzione layer 2 **compr.**

Per le connessioni con due canali B verso una controparte si immette **raggruppamento** ed eventualmente **compr.**

Per le connessioni con due canali B con controparti diverse si può immettere **compr.**

Impostazioni nella lista canali

Nella lista canali si stabilisce quali canali devono essere utilizzati per la connessione fissa. L'indicazione dei canali e la loro sequenza deve essere impostata allo stesso modo sui due lati della connessione. Inoltre indicare qui (allo stesso modo per i due lati della connessione) quanti canali devono essere impiegati eventualmente per il backup.

Device-name	Min	Max	Sequenza	Backup
FVG0	2	2	1-1;1-2	0

Impostazioni nella lista dei nomi

Quando si utilizza una connessione fissa gruppo 0, dopo l'attivazione gli apparecchi si mettono automaticamente in linea e stabiliscono una connessione con il layer di default.

Se si deve utilizzare un altro layer, il meccanismo dial backup o un raggruppamento dinamico tramite linee a selezione, la controparte deve essere presente nella lista dei nomi.

Device-name	Dialup-remote	B1-HZ	B2-HZ	WAN-layer	Chiamata di risposta
FVG0	1234	20	0	PPPHDLC	Off

Il numero telefonico viene utilizzato per stabilire tramite connessioni a selezione altri canali che devono essere raggruppati con la connessione fissa in modo dinamico. Gli altri numeri d'telefonico eventualmente necessari possono essere immessi nella lista round robin.

Se la connessione fissa non è disponibile a causa di disturbi e anche le eventuali connessioni a selezione raggruppate in modo dinamico sono state interrotte a causa di una riduzione temporanea della trasmissione dati, i numeri d'telefonico immessi vengono utilizzati per stabilire le connessioni di backup.

Impostazioni nella lista layer

Una connessione fissa gruppo 0 viene stabilita inizialmente sempre con la controparte di default, vale a dire con il layer indicato nella controparte di default. Se non è disponibile nessuna controparte di default o in questa non è indicato nessun layer, la connessione viene stabilita con il layer indicato nella lista layer come DEFAULT. Se anche in questa non è registrata una voce di DEFAULT, la connessione viene stabilita con le seguenti impostazioni di layer.

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	Trans	PPP	Trans	nessuno	HDLC64K

Esempio: D64S2, raggruppamento dinamico (un canale), nessun backup

Nella lista dei nomi si assegna alla connessione fissa il layer 'MLHDLC' e si indica il numero telefonico per la linea a selezione dinamica:

Device-name	Dialup-remote	B1-HZ	B2-HZ	WAN-layer	Chiamata di risposta
FVG0	123456	20	20	MLHDLC	Off

Nella lista canali si immette il numero di canali richiesto e si definiscono i canali che devono essere utilizzati. Non viene indicato nessun canale di backup.

Device-name	Min	Max	Sequenza	Backup
FVG0	2	3	1-1;1-2;2-1	0

Esempio: D64S2, raggruppamento dinamico (un canale), backup (un canale)

La voce nella lista dei nomi rimane la stessa. Nella lista canali si immette un canale di backup.

Device-name	Min	Max	Sequenza	Backup
FVG0	2	3	1-1;1-2;2-1	1

Esempio: D64S2, nessun raggruppamento, backup (due canali)

La voce nella lista dei nomi rimane la stessa. Nella lista canali si immette un canale di backup.

Device-name	Min	Max	Sequenza	Backup
FVG0	2	3	1-1;1-2	2

Accesso tramite GSM

ELSA LANCOM Business, con il suo grande numero di canali B disponibili è idealmente adatto come nodo di accesso (remote access server) per piccole e medie aziende. Per consentire l'accesso alla rete aziendale anche ai collaboratori in servizio esterno, il router supporta anche il protocollo V.110 e quindi consente il collegamento da notebook tramite telefoni mobili GSM.

L'accesso tramite GSM viene predisposto come un normale accesso remoto, per es. tramite la comoda assistenza di *ELSA LANconfig*. Poi si deve solo adattare il layer utilizzato al corrispondente protocollo.

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	Trans	APPP	Trans	nessuna o comp.	V.110 9600



L'impiego di servizi dati tramite telefono mobile GSM non è incluso nel contratto standard di tutti i provider ed eventualmente deve essere abilitato con addebito. Alcuni provider distinguono anche l'abilitazione per le chiamate dati in uscita e in arrivo!

Point-to-point protocol

I router di ELSA supportano anche il point-to-point protocol (PPP). PPP è un concetto riassuntivo per una intera serie di protocolli WAN che facilitano la cooperazione di router di diversi produttori, poiché questo protocollo viene supportato da quasi tutti i produttori.

Proprio perché il PPP non può essere assegnato a una determinata modalità dei router, e naturalmente anche in conseguenza della grande importanza di questa famiglia di protocolli, le funzioni degli apparecchi correlate con il PPP vengono trattate qui in una sezione a parte.

Il protocollo

Che cosa è il PPP?

Il protocollo point-to-point protocol è stato sviluppato specialmente per connessioni in rete tramite canali seriali e si è affermato come standard per le connessioni tra router. Esso realizza le seguenti funzioni:

- Protezione con password secondo PAP o CHAP
- Funzioni di richiamata
- Trattamento tramite la connessione stabilita dei protocolli di rete da utilizzare (per es. IP o IPX). Vengono anche trattati i parametri necessari per questi protocolli come per es. gli indirizzi IP/IPX. Questa negoziazione si svolge tramite i protocolli IPCP e IPXCP (IP Control Protocol e IPX Control Protocol).
- Controllo della connessione con il LCP (Link Control Protocol)
- Raggruppamento di più canali (multilink PPP)

Per le connessioni router, PPP è lo standard per la comunicazione tra periferiche oppure il software di connessione WAN di produttori diversi. Per garantire per quanto possibile una trasmissione dati efficiente, la negoziazione per i parametri di connessione e l'accordo su un denominatore comune avvengono tramite protocolli di controllo standardizzati (LCP, IPCP, IPXCP, CCP), che sono contenuti nel PPP.

Per che cosa si utilizza il PPP?

Il protocollo point-to-point protocol viene impiegato nelle seguenti applicazioni:

- Per motivi di compatibilità per es. nelle comunicazioni con router remoti
- Accesso remoto di workstation remote con interfacce ISDN
- Accesso a Internet (con trasferimento di indirizzi)

Il PPP implementato nel *ELSA LANCOM* può essere utilizzato in modo sincrono o asincrono sia attraverso una connessione HDLC trasparente che attraverso una connessione X.75.

Le fasi di una negoziazione PPP

Per stabilire una connessione tramite PPP si comincia sempre con una negoziazione sui parametri che devono essere utilizzati per la connessione. Questa negoziazione si svolge in quattro fasi, la cui conoscenza è importante per la configurazione e la ricerca difetti.

■ Fase Establish

Dopo che una connessione è stata stabilita tramite la parte di comunicazione dati, comincia la negoziazione sui parametri di connessione tramite LCP.

Si stabilisce se anche la controparte è pronta a usare il PPP, la dimensione dei pacchetti e il protocollo di autenticazione (PAP, CHAP o nessuno). Successivamente il LCP passa nello stato 'Opened'.

■ Fase Authenticate

Se necessario, vengono scambiate le password. In caso di autenticazione mediante PAP la password viene trasmessa solo una volta. Quando si usa il CHAP una password codificata viene inviata periodicamente a intervalli regolabili.

Eventualmente in questa fase viene anche contrattata una richiamata tramite CBCP (Callback Control Protocol).

■ Fase Network

Nel *ELSA LANCOM* sono implementati i protocolli IPCP e IPXCP.

Dopo che la password è stata trasmessa con successo possono essere stabiliti i layer di rete IPCP e/o IPXCP.

Se la negoziazione sui parametri si è svolta con successo per almeno uno dei layer di rete, possono essere trasmessi dai moduli router pacchetti IP e/o IPX sulla linea (logica) aperta.

■ Fase Terminate

Nell'ultima fase la linea viene chiusa, se sono stabilite le connessioni logiche per tutti i protocolli.

La negoziazione PPP nel *ELSA LANCOM*

Lo svolgimento di una negoziazione PPP viene protocollata nelle statistiche PPP degli apparecchi e in caso di errore può essere controllato con l'ausilio dei pacchetti di protocollo ivi enumerati dettagliatamente.

Un'ulteriore possibilità di analisi è offerta dalle stampe trace PPP. Con il comando

```
trace + ppp
```

si può avviare nell'ambito di una sessione terminale la stampa dei frame di protocollo PPP scambiati. Se questa sessione terminale è protocollata in un log file, dopo l'interruzione della connessione si può eseguire un'analisi dettagliata.

La lista PPP

Nella lista PPP per ciascuna controparte che entra in contatto con la propria rete è possibile stabilire una specifica definizione della negoziazione PPP. 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.

La lista PPP può registrare 64 voci, che contengono i seguenti valori:

In questa colonna della lista PPP si introducono i seguenti valori:
Sito remoto	Nome della controparte, con cui questa si presenta al router
Nome utente	Procedura per la sicurezza della connessione PPP('PAP', 'CHAP' o 'nessuna'). Il proprio router richiede alla controparte di rispettare questa procedura! Non all'inverso. Pertanto la sicurezza secondo 'PAP' o 'CHAP' non si presenta nelle connessioni con provider di servizi Internet, che normalmente non vogliono trasmettere alcuna password. Per tali connessioni selezionare 'nessuna' sicurezza.
Password	Password che viene trasmessa dal router alla controparte (se richiesta). * nella lista indicano che è registrata una voce.
Tempo	Tempo tra due controlli della connessione con LCP. Questo tempo viene introdotto in multipli di 10 secondi (quindi per es. 2 per 20 sec.). Contemporaneamente il tempo tra due controlli della connessione secondo CHAP. Questo tempo viene introdotto in minuti. Per controparti con Windows 95, Windows 98 o Windows NT il tempo deve essere impostato su '0'!
Tentativi	Numero delle ripetizioni per i tentativi di controllo. Con più ripetizioni si esclude l'influenza di disturbi di linea a breve termine. La linea viene chiusa solo se tutti i tentativi rimangono senza successo. L'intervallo di tempo tra due ripetizioni è 1/10 del tempo tra due controlli. Contemporaneamente il numero delle « Configure Requests », che il router invia al massimo prima di sopporre un disturbo di linea e di chiudere la connessione.
Conf, Fail, Term	Con questi parametri si influisce sul modo di operare del PPP. I parametri sono definiti nel RFC 1661 e non vengono descritti ulteriormente qui. Se non si riesce a stabilire nessuna connessione PPP, trovare in questo RFC in relazione con le statistiche PPP del router le indicazioni per eliminare l'anomalia. In generale le impostazioni di default sono sufficienti. Questi parametri possono essere modificati solo tramite SNMP o TFTP (con il programma di configurazione <i>ELSA LANconfig</i> !)
Username	Nome con cui il router si presenta alla controparte. Se non è registrata nessuna voce, viene utilizzato il nome della periferica del router.
Diritti	Protocolli di rete che devono essere instradati tramite questa connessione: IP, IPX, NTB (NetBIOS). NetBIOS richiede sempre uno degli altri due protocolli.

Tutto o.k.? Controllo della linea con LCP

Quando si stabilisce la connessione tramite PPP le periferiche partecipanti negoziano un comportamento comune durante la trasmissione dati. Esse decidono per es. prima se con le impostazioni della procedura di sicurezza, nomi e password si può stabilire una connessione.

Se la connessione è stabilita, con l'ausilio del LCP si può controllare continuamente l'affidabilità della linea. All'interno del protocollo questo avviene con la LCP echo request e la rispettiva LCP echo reply. La LCP echo request è una richiesta in forma di pacchetto di dati, che viene trasmessa alla controparte insieme ai dati utili veri e propri. Se a questa richiesta viene data una risposta valida (LCP echo reply), la connessione è affidabile e stabile. Per un controllo permanente della connessione questa richiesta viene ripetuta a determinati intervalli.

Che cosa succede se la risposta non arriva? Prima vengono effettuate alcune ripetizioni della richiesta, per escludere disturbi di linea a breve termine. Se tutte queste ripetizioni rimangono senza risposta, la linea viene chiusa e si cerca un percorso sostitutivo. Questo può essere trovato per es. sotto forma di linea di backup.

Durante l'accesso remoto di single workstation con Windows 95, Windows 98 o Windows NT si raccomanda di disattivare le richieste LCP regolari, poiché questi sistemi operativi non rispondono alle LCP echo request.

Il comportamento per le richieste LCP viene impostato nella lista PPP per ciascuna connessione. Con le voci nei campi 'Tempo' e 'Tent.' si stabilisce con quali intervalli deve essere inviata la richiesta LCP e quante ripetizioni devono essere effettuate in caso di mancata risposta, prima che la linea venga considerata come guasta. Con un tempo '0' e '0' ripetizioni si disattivano completamente le LCP request.

Assegnazione degli indirizzi IP tramite PPP

Per la connessione di computer che impiegano TCP/IP come protocollo di rete, tutti i partecipanti devono avere un indirizzo IP valido e univoco. Se una controparte non possiede un proprio indirizzo IP (per es. la singola workstation di un telelavoratore), il *ELSA LANCOM* può assegnare ad essa un indirizzo IP per la durata della connessione e in questo modo consentire la comunicazione.

Questo tipo di assegnazione dell'indirizzo viene effettuato durante la negoziazione PPP e solo per le connessioni tramite la WAN. L'assegnazione degli indirizzi mediante DHCP viene utilizzata invece all'interno di una rete locale.

L'assegnazione di un indirizzo IP è possibile solo se ELSA LANCOM riesce ad identificare la controparte attraverso il numero telefonico o il nome quando arriva la chiamata, e quindi l'autenticazione ha avuto successo.



■ Esempio: accesso remoto

L'assegnazione dell'indirizzo diventa possibile con una speciale voce nella 'tabella di routing...' IP. Oltre all'indirizzo IP che deve essere assegnato alla controparte dal campo 'Nome del router', si indica come maschera di rete 255.255.255.255. In questo caso il nome del router è il nome con cui la controparte si deve presentare al *ELSA LANCOM*.

Oltre all'indirizzo IP, con questa configurazione vengono trasferiti alla controparte anche gli indirizzi dei server DNS e NBNS (Domain Name Server e NetBIOS Name Server) compresi gli indirizzi dei backup server dedotti dalle voci presenti nel modulo TCP/IP.

Affinché il tutto possa funzionare, naturalmente la controparte deve anche essere impostata in modo da ricevere l'indirizzo IP e il nome dei server (DNS e NBNS) da *ELSA LANCOM*. Questo si realizza per es. nella rete di accesso remoto di Windows con le voci nelle 'Impostazioni TCP' sotto 'Indirizzo IP' oppure 'Configurazione DNS'. Vengono attivate le opzioni 'Indirizzo IP assegnato dal server' e 'Nome indirizzo del server assegnato dal server'.

■ Esempio: accesso a Internet

Se attraverso *ELSA LANCOM* viene realizzato l'accesso a Internet per una rete locale, l'assegnazione degli indirizzi IP può seguire il percorso inverso. In questo caso sono possibili configurazioni in cui lo stesso *ELSA LANCOM* non possiede un indirizzo IP valido in Internet e se ne fa assegnare uno dal provider Internet per la durata della connessione. Oltre all'indirizzo IP, *ELSA LANCOM* riceve durante la negoziazione PPP anche informazioni sul server DNS del provider.

Nella rete locale *ELSA LANCOM* è conosciuto solo con il proprio indirizzo Intranet valido internamente. Tutte le workstation della rete locale possono quindi accedere allo stesso account Internet e anche per es. raggiungere il server DNS.

Gli indirizzi assegnati possono essere visualizzati dagli utenti Windows sul *LANmonitor*. Oltre al nome della controparte collegata si trova l'indirizzo IP attuale e gli indirizzi dei server DNS e NBNS. Vengono anche visualizzate opzioni come il raggruppamento canali o la durata della connessione.



ELSA LANmonitor viene normalmente installato automaticamente durante l'installazione di ELSA LANconfig. Si può trovare una descrizione di ELSA LANmonitor nel capitolo 'Possibilità di configurazione' nella sezione 'Che cosa succede sulla linea'.

Funzioni di richiamata

Gli *ELSA LANCOM* supportano oltre alla richiamata tramite il canale D e la richiamata tramite il protocollo ELSA anche la richiamata CBCP specificata da Microsoft e la richiamata tramite PPP secondo RFC 1570 (PPP LCP Extensions). Esiste inoltre la possibilità di una richiamata particolarmente rapida tramite una procedura sviluppata da ELSA.

I PC con Windows 95, Windows 98 o Windows NT possono essere richiamati solo tramite il CBCP. Affinché nel *ELSA LANCOM* sia possibile anche un controllo del numero telefonico, sono disponibili nella lista dei nomi per la richiamata i seguenti valori:

Con questa voce si imposta la richiamata in questo modo:
Off	Nessuna richiamata.
Auto (non in Windows 95, Windows 98 o Windows NT, v. sotto)	Se la controparte viene trovata nella lista dei numeri, viene richiamata. A questo scopo la chiamata viene prima respinta e poi richiamata, appena il canale ritorna libero (durata ca. 8 secondi). Se la controparte non viene trovata nella lista dei numeri, si suppone prima che si tratti della controparte di DEFAULT, e la richiamata viene effettuata durante la negoziazione del protocollo. Questo comporta un addebito di un'unità.
Nome	Prima di una richiamata viene sempre effettuata una negoziazione di protocollo, anche se la controparte è stata trovata nella lista dei numeri (per es. per i computer con Windows che selezionano la periferica). Questo comporta un addebito di un'unità.
ELSA	Se la controparte viene trovata nella lista dei numeri, viene effettuata la chiamata di risposta rapida, cioè <i>ELSA LANCOM</i> invia uno speciale segnale alla controparte e poi richiama immediatamente, se il canale ritorna libero. Dopo ca. 2 secondi si realizza la connessione. Se la controparte non accetta la chiamata subito dopo il segnale, dopo due secondi si ritorna alla normale procedura di richiamata (di nuovo durata ca. 8 secondi). Questa procedura è disponibile solo su connessioni DSS1.
Looser	Si utilizza l'opzione 'Looser' se si attende una richiamata dalla controparte. Questa impostazione assolve contemporaneamente a due compiti. Per un verso provvede che una connessione stabilita venga ritirata se arriva una chiamata proprio dalla controparte chiamata, per l'altro verso con questa impostazione si attiva la funzione per poter reagire alla procedura di chiamata di risposta rapida. Questo significa che per utilizzare la chiamata di risposta rapida il chiamante si deve trovare in modalità 'Looser', mentre presso il chiamato la richiamata deve essere impostata su 'ELSA'.



L'impostazione 'Nome' offre la massima sicurezza, se è configurata una voce sia nella lista dei numeri che nella lista PPP. L'impostazione 'ELSA' consente il metodo di richiamata più rapido tra due router ELSA.

*Per controparti Windows **deve** essere selezionata l'impostazione 'Nome'.*

Richiamata secondo Microsoft CBCP

Il protocollo Microsoft CBCP consente diversi modi per determinare il numero di richiamata:

- Il chiamato non richiama.
- Il chiamato consente al chiamante di indicare il numero di richiamata.
- Il chiamato conosce il numero di richiamata e richiama **solo** questo.

Tramite CBCP è possibile accettare una connessione da un PC Windows 95, Windows 98 o Windows NT a *ELSA LANCOM* e lasciarsi richiamare da questo. Le tre impostazioni

possibili vengono selezionate tramite la voce richiamata e la voce numero telefonico nella lista dei nomi.

Lista dei nomi - Nuovo elemento

Nome: REMOTE01

Numero di telefono: 123456

Breve pausa di tempo: 20 secondi

Breve pausa di tempo (bundle): 20 secondi

Nome del livello: PPP

Richiamo automatico:

- ☒ nessun richiamo
- ☐ Richiamo sito remoto
- ☐ Richiamo sito remoto(procedura rapida)
- ☐ Richiamo sito remoto dopo la verifica del nome
- ☐ Attendi il richiamo dal sito remoto

OK Annulla

Nessun richiamo

Per questa impostazione la voce richiamata deve avere il valore 'Off' durante la configurazione tramite programma terminale o Telnet.

Numero di richiamata selezionato

La controparte viene richiamata dopo il controllo del nome. Per questa impostazione la voce richiamata deve avere il valore 'Nome', nella lista dei nomi non deve essere indicato **nessun** numero telefonico.

Dopo l'autenticazione in Windows 95 compare la seguente finestra di dialogo, in cui l'utente può indicare il proprio numero telefonico:

Convenience Callback

You may supply a callback location to connect to PPP_LANCOM. Enter a phone number where PPP_LANCOM can call you back.

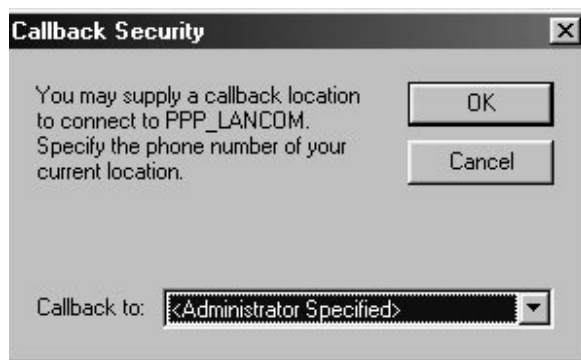
OK Cancel

Location:

Numero di richiamata stabilito da *ELSA LANCOM*

La controparte viene richiamata dopo il controllo del nome. Per questa impostazione la voce richiamata della corrispondente controparte deve avere il valore 'Nome', e nella lista dei nomi deve essere indicato **un** numero telefonico.

Dopo l'autenticazione in Windows 95 compare il seguente messaggio, che l'utente può solo confermare:



La richiamata a una workstation Windows 95, Windows 98 o Windows NT avviene ca. 15 secondi dopo che la connessione è stata interrotta. Questo tempo non può essere abbreviato, poiché è determinato da Windows.

Chiamata di risposta rapida secondo *ELSA*

Se due *ELSA LANCOM* comunicano tra loro e uno deve essere richiamato, è indicata la chiamata di risposta rapida secondo la procedura specifica *ELSA*.

- Il chiamante che vorrebbe essere richiamato imposta nella lista dei nomi 'Attendere la richiamata della controparte' ('Looser' in caso di configurazione tramite programma terminale o Telnet).
- Il richiamante seleziona 'Richiamare la controparte (procedura rapida)' nella lista dei nomi e imposta il numero telefonico ('*ELSA*').

Richiamata secondo RFC 1570 (PPP LCP extensions)

Secondo RFC 1570 esistono cinque possibilità per richiedere una richiamata. Tutte le vengono accettate dal *ELSA LANCOM*. Per tutte le varianti si procede allo stesso modo:

Dopo l'autenticazione della controparte *ELSA LANCOM* interrompe la connessione e la richiama dopo tre secondi.

Raggruppamento canali con MLPPP

Se si stabilisce una connessione ISDN con una controparte con capacità PPP, si possono utilizzare procedure che accelerano la trasmissione dei dati: Si possono comprimere i dati e/o utilizzare più canali B per la trasmissione (raggruppamento di canali).

La connessione con raggruppamento canali si distingue dalle « normali » connessioni per il fatto che non si usa un solo canale ma più canali B in parallelo per la trasmissione dei dati.

Per il raggruppamento canali si utilizza MLPPP (multilink PPP). Naturalmente questa procedura è solo disponibile se si utilizza PPP come protocollo di canale B. MLPPP è consigliabile per es. per l'accesso a Internet tramite provider che impiegano nei loro nodi di selezione anche controparti con capacità MLPPP.

■ Raggruppamento canali statico

Se viene stabilita una connessione con raggruppamento di canali statico, il router tenta immediatamente di stabilire i canali B indicati come 'minimi' nella lista canali. Vengono usati i canali indicati nella lista canali o canali liberi qualunque.

■ Raggruppamento canali dinamico

In una connessione con raggruppamento di canali dinamico il router stabilisce prima solo canali B indicati come 'minimi' nella lista canali e comincia la trasmissione dati. Se durante la connessione riscontra che la velocità di trasmissione per un certo periodo risulta superiore a un determinato valore limite, esso tenta di attivare altri canali, fino a quando viene raggiunto il numero indicato come 'massimo' nella lista canali. Anche in questo caso vengono usati i canali indicati nella lista canali o canali liberi qualunque.

Se i canali dinamici sono stabiliti e la velocità di trasmissione ritorna sotto la soglia, il router attende ancora il tempo di attesa B2 impostato e poi richiude automaticamente i canali. Le unità a pagamento iniziate vengono utilizzate, se le informazioni di addebito vengono comunicate durante la connessione. Quindi il router utilizza i canali dinamici solo se e nella misura in cui ne ha bisogno effettivamente!

Il raggruppamento canali si configura nel modo seguente:

La configurazione del raggruppamento canali per una connessione è composta da tre impostazioni:

- ① Creare nella lista dei nomi una voce per la connessione che deve utilizzare il raggruppamento canali. Selezionare un layer che nelle opzioni layer 2 ha impostato il raggruppamento.
 - **compr.** dopo la procedura di compressione LZS (Stac) il volume dei dati si riduce, se i dati non erano già stati compressi in precedenza. Questa procedura viene

supportata anche da router di altri produttori e da interfacce ISDN sotto i sistemi operativi Windows.

- **Raggruppamento** utilizza più canali B per una connessione. Il tipo di raggruppamento di canali viene impostato attraverso la configurazione delle opzioni layer 2 nella lista di layer, dei tempi di attesa nella lista dei nomi e della voce per la connessione Y nella tabella di interfaccia e della voce nella tabella canali.
 - **bnd+compr** utilizza entrambi (compressione e raggruppamento canali) e quindi consente la velocità di trasmissione massima possibile.
- ② Impostare anche nella lista dei nomi i tempi di attesa per questa connessione. Seguire le seguenti regole:
- Il tempo di attesa B1 dovrebbe essere scelto, secondo il caso di applicazione, tanto grande da non interrompere la connessione troppo presto a causa di una breve mancanza di pacchetti. In base all'esperienza i valori tra 60 e 180 secondi rappresentano una buona base per l'inizio, e poi possono essere successivamente adattati.
 - Il tempo di attesa B2 determina dopo quanto tempo i canali dinamici vengono interrotti se la velocità di trasmissione è inferiore al valore limite.
- ③ Stabilire nella lista canali quanti canali devono essere utilizzati per la connessione. Inoltre si può definire qui quali canali possono essere presi in considerazione, e quindi per es. tenere liberi determinato canali per la selezione tramite RAS.
- La voce nella lista canali determina se si tratta di un raggruppamento di canali statico o dinamico (vedere sopra). Con più di un canale minimo il raggruppamento diventa statico, con più canali massimi rispetto a quelli minimi si predispone la possibilità di un raggruppamento di canali dinamico.
- ④ Definire nella lista di interfaccia con la voce per la connessione Y che cosa deve succedere se durante una connessione in corso con raggruppamento di canali viene comunicata la richiesta di una ulteriore connessione verso un'altra controparte, ma non ci sono più canali B liberi.
- Connessione Y **On**: Il router interrompe il raggruppamento di canali su questa interfaccia per stabilire la connessione con l'altra controparte. Se il canale ritorna libero, il raggruppamento canali riprende automaticamente questo canale (nel raggruppamento statico sempre, in quello dinamico solo se necessario).
 - Connessione Y **Off**: Il router mantiene il raggruppamento di canali su questa interfaccia, l'altra connessione deve tentare su un'altra interfaccia o attendere, se nessuna delle interfacce con raggruppamento di canali attivo consente l'interruzione di un canale.

Routing IPX

Il router IPX trasmette i dati da reti che utilizzano come protocollo di rete IPX/SPX (per es. le reti Novell). Con l'introduzione nella tabella di routing IPX una rete remota viene notificata ai computer della rete locale. Nella tabella di routing possono essere introdotte fino a 16 reti diverse.

Indirizzamento IPX

Un indirizzo completo in una rete IPX è costituito da tre parti: un numero di rete, l'indirizzo MAC della scheda di rete e il numero di socket:

- Il numero di rete può essere scelto liberamente. Tuttavia esso deve essere univoco su tutte le reti IPX raggiungibili, in modo da garantire una corretta assegnazione.
- L'indirizzo MAC è definito in modo fisso per ciascun componente della rete. Solo in casi eccezionali viene usato all'interno della rete anche un altro indirizzo.
- Per colloquiare non solo con un computer, ma anche con uno specifico servizio su tale computer, una rete IPX utilizza i numeri di socket. Con questo vengono identificati in modo univoco i diversi servizi.

Informazioni sulla LAN

Se in una sede diventano necessarie più reti LAN distinte, queste non devono avere necessariamente anche cablaggi separati. Diverse reti logiche possono condividere lo stesso cavo. Affinché i dati delle diverse reti non si disturbino tra loro e una rete rimanga invisibile alle altre, esse utilizzano formati diversi per i pacchetti Ethernet. Questi formati vengono determinati dal binding, che è collegato a un numero di rete univoco sul cavo.

Affinché anche il router sappia a quale rete appartiene, è necessario comunicare ad esso il numero di rete e il rispettivo binding. Se si lascia l'indirizzo di rete sull'impostazione standard '00000000', il router determina autonomamente l'indirizzo di rete e il binding. A questo scopo esso ricerca sul cavo collegato la rete da cui riceve la maggior parte delle replies SAP.

Tabella di routing IPX

Nella tabella di routing IPX si definisce quali controparti (e quindi quali altri router o computer) sono raggiungibili per la rete locale, e si indicano alcuni parametri per la connessione. La tabella con un massimo di 16 voci ha la seguente struttura:

Sito remoto	Rete	Binding	Propagato	Backoff
FILIALE01	00000245	802.3	Rotta	On
FILIALE02	00000320	SNAP	Filt.	On
CENTRALE	00000420	802.2	Filt.	Off

■ Sito remoto:

Nome della controparte, come è indicato come nome della periferica nel corrispondente router della controparte.

■ Rete:

Indirizzo della WAN. Questo non è l'indirizzo della rete di destinazione, ma un terzo indirizzo, che rappresenta la rete tra le due reti da connettere. Vale quanto segue:

Indirizzo LAN 1 \neq Indirizzo WAN 1 = Indirizzo WAN 2 \neq Indirizzo LAN 2 \neq Indirizzo LAN 1

■ Binding:

Viene impostato il binding Ethernet che deve essere utilizzato sulla WAN. Questa diventa attiva solo se il layer per questa connessione supporta la Ethernet-Encapsulation. Se la voce manca, si assume 802.3.

■ Propagato:

Filtro per i pacchetti IPX del tipo 20 (NetBIOS Propagated Frames). Il sistema Network Basic Input/Output è stato sviluppato originalmente per IBM e viene utilizzato in forma modificata anche da Microsoft. Questo protocollo rende disponibili nei layer 3 e 4 del modello OSI servizi come suddivisione del nome, assicurazione dati e corretta sequenza dei pacchetti (protocollo assicurato). I pacchetti NetBIOS presentano uno speciale tipo di pacchetto e socket (pacchetti propagated). NetBIOS viene utilizzato in prima linea per lo scambio di dati tra le stazioni di una rete locale (LAN).

Con l'impostazione del 'filtro', questi pacchetti IPX possono essere esclusi dalla trasmissione o instradati. Con l'impostazione della 'Rotta' i pacchetti vengono trasmessi se è stabilita una connessione con la corrispondente controparte o è ancora disponibile un canale libero per stabilire un'ulteriore connessione. Se tutte le linee sono occupate con altre controparti, i propagated frame vengono respinti.

■ Backoff:

Il router IPX utilizza uno speciale algoritmo (exponential backoff), per ridurre al minimo i costi di connessione in caso di configurazioni sbagliate.

Se nella rete della controparte non è disponibile un server (per es. durante Accesso remoto di una workstation), la funzione backoff dovrebbe essere disattivata (vedere anche 'Exponential backoff').

L'impostazione di default è 'On'.

Che cosa succede nella trasmissione dati in rete IPX?

Se una periferica si presenta in una rete IPX, essa invia prima una richiesta secondo il Service Advertising Protocol (SAP) si presenta al più vicino server raggiungibile (Get Nearest Server Request) in rete con il num. '00000000'. Se in questa rete esiste un router o un server, questo risponde alla richiesta e comunica il corretto numero di rete.

Inoltre i server inviano regolarmente informazioni sui servizi offerti e sulle altre reti che essi possono raggiungere. A questo scopo essi utilizzano degli speciali pacchetti di dati secondo il Service Advertising Protocol oppure Routing Information Protocol (RIP).

Se il router IPX è completamente configurato e viene attivato, esso stabilisce prima delle connessioni con tutte le controparti raggiungibili tramite le tabelle di routing e poi scambia con tali reti informazioni SAP e RIP. Il router memorizza questi dati nelle sue tabelle SAP e RIP interne.

Tabelle RIP e SAP

Le informazioni RIP e SAP compaiono nelle corrispondenti tabelle in ordine alfabetico. Le RIP sono ordinate solo secondo la rete, le SAP prima secondo il tipo di servizio, poi secondo il nome del server.

Con ciascun nuovo pacchetto RIP oppure SAP le tabelle RIP e SAP vengono aggiornate. Affinché vengano offerti solo servizi (SAP) che sono anche raggiungibili (RIP), il router accoglie nella propria tabella solo le informazioni SAP per cui esiste anche la corrispondente voce RIP. Oltre alle informazioni su rotte e servizi raggiungibili le voci delle tabelle riportano per es. anche quanti router devono essere passati lungo il percorso (hops) o quanto tempo impiega un pacchetto di dati per arrivare alla rete di destinazione (tic = ca. 1/18 di secondo). Se attraverso le informazioni RIP per es. vengono offerte più rotte per una rete di destinazione, il router sceglie in base alle tabelle il percorso con meno tics e con il minimo hop-count e memorizza solo questa rotta.

Le tabelle RIP possono accogliere 64 voci, le tabelle SAP 128 voci. Se ogni nuovo pacchetto aggiorna le tabelle, naturalmente in qualche momento le vecchie voci debbono scomparire. A questo scopo le voci sono sottoposte a un invecchiamento artificiale. Per tutte le voci delle tabelle RIP/SAP che sono state apprese tramite scambio di dati locali, l'età viene incrementata di uno ogni 60 secondi. Un nuovo pacchetto RIP oppure SAP per

una voce azzera la sua l'età. Dopo un'età impostabile da 1 a 60 la rotta o il servizio vengono definiti come irraggiungibili (Down). Quando è trascorso il doppio di questo tempo, la voce viene rimossa. Inoltre quando viene stabilita una connessione tutte le informazioni RIP e SAP che interessano tale controparte vengono cancellate dalle tabelle e sostituite da nuove informazioni.

Tanti router qui ...

Se in una rete si desidera connettere contemporaneamente più controparti di quanti siano i canali B disponibili, è arrivato il momento per un secondo (terzo ...) router. Per assicurare una cooperazione senza problemi tra fratelli e che la rete trovi effettivamente sempre una controparte, in tutti i router vengono riportate le stesse voci della 'tabella di routing'. Per mezzo di pacchetti RIP, ad ogni router vengono comunicate le stesse informazioni di routing, ma con tic e hop count più alti (attivare `Setup/IPX-module/LAN-config/RIP-SAP-scal.`). In questo modo queste rotte vengono contrassegnate quasi come riserve, se sull'apparecchio chiamato sono occupati tutti i canali.

Rotte ridondanti

Se un router riceve con un pacchetto RIP informazioni su rotte con gli stessi tic e hop-count delle proprie rotte (rotte ridondanti), naturalmente non deve notificare queste rotte al mittente. Esso quindi invia queste rotte solo ai router che non hanno propagato la rotta. Questa procedura viene definita split horizon.

Se comunque risulta necessario notificare rotte ridondanti nella rete locale, si può usare la funzione 'Propagazione Loop' (`SETUP/IPX-module/LAN-Config/LOOP-PROP.`). Le rotte apprese in questo modo vengono contrassegnate come 'LOOP' nella tabella RIP. Poiché la propagazione di rotte ridondanti non è vietata dalle specifiche Novell, ma comunque dovrebbe essere ridotta al minimo, l'impostazione di default è 'Off'.

Exponential backoff

Per ottenere le informazioni di routing sulle controparti IPX necessarie per il servizio (informazioni RIP e SAP), dopo l'attivazione il router IPX della periferica tenta di stabilire le corrispondenti connessioni. Se questo non risulta possibile, eventualmente a causa di un errore di configurazione del router IPX, l'algoritmo exponential backoff evita che la connessione venga stabilita continuamente e quindi consente di risparmiare sugli addebiti.

Se un primo tentativo di connessione con una controparte non ha successo, il router tenta di raggiungere di nuovo la controparte dopo un tempo di attesa continuamente crescente. Il tempo di attesa viene determinato nel modo seguente:

- La prima selezione avviene dopo $10 + x$ secondi. x è un numero tra 0 e 10.
- Il secondo tentativo viene avviato $10 + x$ secondi dopo il fallimento del primo tentativo. x rappresenta ora un numero tra 0 e 20 secondi.
- Il valore superiore per x viene raddoppiato per ogni nuovo tentativo. Dopo il 16. tentativo senza successo il router rinuncia definitivamente. In conseguenza del continuo aumento del tempo di attesa dopo 16 tentativi è trascorso al massimo un giorno.

Se tutti i tentativi di selezione della controparte rimangono senza successo, la rotta viene bloccata. Solo una modifica della voce nella tabella di routing può ristabilire i tentativi di connessione.



Il tempo rimanente fino alla successiva selezione e il numero dei tentativi di connessione possono essere ricavati dalle statistiche di rete (Status / IPX-statistics / IPX-router-statistics / Networks).

Filtro per i pacchetti IPX

Attraverso le voci della tabella di routing si determina quali altre reti sono raggiungibili. Queste reti sono raggiungibili anche per i pacchetti di dati che non sono necessari nella rete della controparte. Questi pacchetti comportano anche che vengano stabilite connessioni non necessarie e costano denaro.

Pertanto si devono introdurre opportuni filtri. Per poter escludere o almeno limitare la trasmissione su WAN per es. dei pacchetti di dati che servono solo alla comunicazione interna delle reti:

■ Propagated frames

Questi speciali pacchetti di dati utilizzano protocolli che non possono essere instradati. Per poter partecipare comunque al routing comune, questi dati vengono incapsulati in normali pacchetti IPX e inviati come broadcast.

Talvolta si desidera non instradare questi pacchetti. Pertanto per questo tipo di pacchetti è possibile impostare esplicitamente se deve essere instradato oppure filtrato.

■ Filtro socket

Ciascun pacchetto di dati in una rete IPX riceve oltre agli indirizzi di destinazione e di sorgente anche socket di destinazione e di sorgente. I socket definiscono i processi a cui sono destinati i dati del pacchetto.

Per i socket della rete locale e delle reti remote esiste sempre una corrispondente tabella di filtro, che contiene i filtri con cui possono essere esclusi dalla

trasmissione singoli socket di destinazione o interi gruppi. Alcuni socket, che notoriamente causano connessioni non desiderate, sono già inseriti come default nella tabella di filtro socket.

■ Informazioni RIP e SAP

Attraverso le RIP un router comunica agli altri router secondo il principio Split-Horizon tutte le rotte note (percorsi verso altre reti). Queste sono le voci della propria tabella di routing ed anche tutte le rotte che il router ha appreso da altri router. Esso apprende sia dai router delle reti locali che dalle reti remote. Esso registra tutte le informazioni di routing disponibili nella propria tabella RIP interna.

Nelle informazioni SAP i server offrono i loro servizi. I diversi servizi vengono rappresentati con numeri nelle informazioni SAP. Ciascun servizio (per es. server di file o server di stampa) possiede un numero univoco. Il router accoglie le informazioni sui servizi disponibili nella tabella SAP interna e registra quale servizio è disponibile in quale rete e a quale indirizzo MAC. Esso apprende anche se il servizio offerto si trova nella rete locale o in una rete remota, e quindi può propagare il servizio senza stabilire la connessione.



Nel modulo IPX (setup/IPX-module/RIP-config oppure SAP-config) dei router si possono visualizzare le tabelle RIP e SAP con i valori aggiornati.

Naturalmente le informazioni RIP e SAP sono molto importanti per la comunicazione delle periferiche di una rete, pertanto esistono diverse possibilità per impostare la trasmissione di questi pacchetti:

- Con una tabella di filtro LAN e WAN il router può essere indirizzato a non accogliere nella tabella RIP o SAP interna le informazioni sulle rotte per determinate reti oppure su determinati servizi. Pertanto le rotte interessate non vengono utilizzate e non vengono nemmeno propagate, i servizi non vengono offerti nella propria rete.
- I pacchetti RIP e SAP senza filtro vengono sempre trasmessi. Essi occupano in ogni caso una parte della linea di connessione.
- I pacchetti RIP e SAP vengono inviati solo se hanno causato una modifica delle informazioni.
- Le RIP e SAP possono essere trasmesse a intervalli regolari impostabili. Normalmente le informazioni vengono inviate a intervalli di un minuto. Con l'impostazione del tempo questo intervallo può essere allungato fino a 60 minuti.
- Il trattamento più economico dei pacchetti RIP e SAP trasmette le informazioni una volta sola, quando una connessione è già stabilita.

■ Watchdogs IPX e SPX:

Con questi pacchetti di dati i server annunciano, per es. nelle workstation, se sono ancora attivi o se eventualmente possono essere disattivati. Affinché questi pacchetti « Sei ancora sveglio? » per i computer di una rete remota non stabiliscano

continuamente la connessione, si può impostare la risposta a queste richieste nel modo seguente:

- I watchdogs IPX rimangono completamente senza risposta. Dopo il tempo impostato dal server i computer vengono disattivati.
- I watchdogs IPX e SPX possono ricevere una risposta locale. Questa procedura viene definita spoofing. Il router risponde al posto del computer interrogato, che naturalmente non viene mai disattivato. Ha anche senso l'impostazione di un tempo nel server, dopo il quale le corrispondenti periferiche vengono disattivate in ogni caso.
- Naturalmente i watchdogs IPX e SPX possono anche essere instradati normalmente, ma in tale caso causano spesso che venga stabilita una connessione.



Ulteriori istruzioni su IPX, sul router IPX e sui rispettivi parametri si possono trovare nel capitolo 'Setup/IPX module' Manuale di riferimento.

Routing IP

Un router IP opera tra reti che utilizzano TCP/IP come protocollo di rete. Vengono trasmessi solo i dati i cui indirizzi di destinazione sono inseriti nella tabella di routing. In questo capitolo si apprende come è costruita la tabella di routing IP in un router ELSA e con quali altre funzioni viene supportato il routing IP.

Tabella di routing IP

Nella tabella di routing IP si comunica al router a quale controparte (quindi a quale altro router o computer) deve inviare i dati per determinati indirizzi IP o gruppi di indirizzi IP. Una siffatta indicazione viene anche definita « rotta », poiché con essa si descrive il percorso dei pacchetti di dati. Poiché queste indicazioni vengono effettuate in proprio e rimangono invariate fino a quando non vengono modificate o cancellate, questa procedura viene anche definita « routing statico ». Contrapposto a questo naturalmente esiste anche un « routing dinamico ». In questo i router si scambiano autonomamente tra loro informazioni sulle rotte e le rinnovano in continuazione. La tabella di routing statico può accogliere fino a 64 voci, la tabella dinamica 128. Quando è attivato IP-RIP il router IP considera entrambe le tabelle.

Inoltre nella tabella di routing IP si comunica al router quanto è lungo il percorso su questa rotta, in modo che, in cooperazione con IP-RIP in caso di più rotte verso la stessa destinazione possa essere scelta quella più conveniente. L'impostazione fondamentale della distanza verso un altro router è 2, vale a dire che il router ISDN è raggiungibile direttamente. Tutte le periferiche raggiungibili localmente, e quindi gli altri router o workstation nella stessa LAN, che sono connessi tramite proxy ARP vengono indicati con distanza 0. Indicando in modo mirato una distanza più alta (fino a 14) si abbassa la

« qualità » di tale rotta. Tali rotte « peggiori » devono essere utilizzate solo quando non si può trovare un'altra rotta verso la corrispondente controparte.

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-module/IP-routing-table. Per es. una tabella di routing IP si presenta così:

Indirizzo IP	Maschera di rete IP	Nome del router	Distanza	Mascheratura
192.168.120.0	255.255.255.0	MILANO	2	On
192.168.125.0	255.255.255.0	ROMA	3	Off
192.168.130.0	255.255.255.0	191.168.140.123	0	Statico

Che cosa significano le singole voci della lista?

■ **Indirizzo IP e maschera di rete IP**

Questo è l'indirizzo della rete di destinazione, a cui possono essere inviati i pacchetto di dati, con la rispettiva maschera di rete. Usando la maschera di rete e l'indirizzo IP di destinazione dei pacchetti di dati in arrivo il router controlla se il pacchetto appartiene alla rete.

■ **Nome del router**

Il router trasmette a questa controparte i pacchetti di dati corrispondenti all'indirizzo IP e alla maschera di rete. Se la controparte è un router di un'altra rete o una singola workstation, in questo punto c'è un nome. Se il proprio router non può raggiungere la controparte, in questo punto c'è l'indirizzo IP di un altro router che conosce il percorso fino alla rete di destinazione.

■ **Distanza**

Numero dei router che si trovano tra il proprio e la destinazione. Nelle connessioni a lunga distanza questo valore viene spesso fatto corrispondere ai costi di trasmissione e utilizzato per distinguere tra percorsi di trasmissione convenienti e cari. I valori di distanza indicati vengono propagati nel modo seguente:

- Mentre viene stabilita una connessione verso una rete di destinazione, tutte le reti raggiungibili tramite questa connessione vengono propagate con distanza 1.
- Tutte le reti non connesse vengono propagate con la distanza indicata nella tabella di routing (comunque almeno con distanza 2), se non è ancora disponibile un canale di trasmissione libero.
- Se non esiste più un canale libero, le restanti reti vengono propagate con distanza 16 (= unreachable).
- Un'eccezione è costituita dalle controparti connesse tramite proxy ARP. Questi « proxy hosts » non vengono propagati.

■ **Mascheratura**

Con l'opzione 'Masquerading' nella tabella di routing si informa il router su quale indirizzo IP deve essere utilizzato per il trasferimento dei pacchetti.

- 'off': Non viene effettuata alcuna mascheratura.
- 'on': Con questa impostazione si richiede al provider di assegnare un qualunque indirizzo IP valido in Internet che si intende utilizzare per la connessione con mascheratura.
- 'stat.': Con questa impostazione si richiede al provider di assegnare un determinato indirizzo, indicato come indirizzo IP nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Generale' oppure nel menu /Setup/TCP-IP-module. Questo indirizzo deve essere utilizzato nel seguito per la connessione e la mascheratura.

Ulteriori informazioni sul si possono trovare nella sezione 'Mascheratura IP'.

■ **Le seguenti voci hanno un significato speciale:**

- Indirizzo IP 255.255.255.255 con maschera di rete 0.0.0.0: Questa è la rotta di default. Tutti i pacchetti di dati che non possono essere instradati attraverso altre voci di routing, vengono trasmessi alla controparte indicata in questo punto.
- Maschera di rete 255.255.255.255: Le voci con maschera di rete completamente piena spesso caratterizzano solo singole workstation (accesso remoto), non reti. Qualche volta può anche essere indicata una rete che, attraverso la mascheratura IP è visibile dall'esterno solo con un indirizzo IP.
- Nome del router 0.0.0.0: Rotte di esclusione. I pacchetti di dati per queste « rotte di esclusione » vengono respinti e non trasferiti. Con queste per es. si escludono dalla trasmissione le rotte vietate in Internet (Privat Address Spaces, per es. 10.0.0.0).

Esempi con spiegazioni:

Indirizzo IP	Maschera di rete IP	Nome del router	Dist.	Accade quanto segue:
192.168.1.9	255.255.255.255	SERVIZIO ESTERNO	2	La controparte SERVIZIO ESTERNO può essere raggiunta sotto l'indirizzo IP 192.168.1.9.
192.168.120.0	255.255.255.0	ROUTER01	2	Tutti i pacchetti di dati con gli indirizzi IP di destinazione 192.168.120.x vengono trasmessi al ROUTER01.
192.168.125.0	255.255.255.0	ROUTER02	3	Tutti i pacchetti di dati con gli indirizzi IP di destinazione 192.168.125.x vengono trasmessi al ROUTER02.

Indirizzo IP	Maschera di rete IP	Nome del router	Dist.	Accade quanto segue:
192.168.130.0	255.255.255.0	192.168.140.123	0	Tutti i pacchetti di dati con gli indirizzi IP di destinazione 192.168.130.x vengono trasmessi al router con indirizzo IP 192.168.140.123.
10.0.0.0	255.0.0.0	0.0.0.0	0	Esclude la trasmissione di tutti i pacchetti di dati delle reti a 10.
255.255.255.255	0.0.0.0	CENTRALE	2	Tutti i pacchetti di dati che non possono essere assegnati attraverso le voci precedenti, vengono trasmessi alla controparte CENTRALE.



Anche la sequenza delle voci è importante: Queste vengono eseguite dall'alto verso il basso! Il router classifica le voci autonomamente: Prima secondo le maschere di rete, con la più grande in alto. Poi secondo gli indirizzi IP, con il più piccolo in alto. In questo modo la voce 'CENTRALE' viene posta proprio alla fine della lista. Con questa voce nel punto più alto della lista il router invierebbe nella rete della centrale tutti (!) i pacchetti di dati che non appartengono alla propria rete.

Filtro per i pacchetti TCP/IP

Con le voci della tabella di routing si può stabilire con precisione quali pacchetti di dati devono essere trasmessi. Inoltre, con la voce '0.0.0.0' nel campo 'Router' si possono respingere interi gruppo di indirizzi IP.

Qualche volta si desidera limitare ulteriormente la trasmissione dei dati. A questo scopo si usa la proprietà di TCP/IP di inviare con un pacchetto di dati oltre agli indirizzi IP della sorgente e della destinazione anche i numeri di porta per la destinazione e la sorgente. La porta di destinazione in un pacchetto di dati indica il servizio della rete TCP/IP che deve essere indirizzato. Le porte di destinazione per i diversi servizi della rete TCP/IP sono definiti in modo fisso (vedere anche 'Porte TCP/IP' Manuale di riferimento). Le porte sorgenti invece vengono scelte liberamente all'interno di determinati intervalli.

Il router può leggere le porte di destinazione e sorgenti dei pacchetti di dati che usano TCP o UDP come protocollo. Da queste porte può poi ricavare lo scopo previsto per i dati. In questo modo si possono per es. riconoscere gli accessi FTP o le sessioni Telnet. Con l'ausilio della corrispondente tabella di filtro si può stabilire che determinati dati non devono essere trasmessi dalla LAN alla controparte. Allo stesso modo naturalmente possono essere bloccati anche i dati per determinate porte dalla WAN in direzione delle LAN. Oltre alla definizione dei gruppi di porte e dei rispettivi protocolli, nelle tabelle di filtro si può anche stabilire tramite il tipo di filtro se i pacchetti di dati interessati non devono essere trasmessi mai oppure solo se non devono causare una connessione (e quindi essere trasmessi soltanto con una connessione già stabilita).

Nel router IP ci sono due tabelle di filtro separate per i pacchetti che provengono dalla LAN e i pacchetti che provengono dalla WAN. Queste tabelle di filtro si trovano in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Filtraggio' oppure nel menu /Setup/IP-router-table/WAN-filter-table oppure LAN-filter-table.

Proxy ARP

Una particolarità del router IP è costituita dalla possibilità del proxy ARP. « Proxy » è un termine inglese e significa « rappresentante ». Questo rappresentante viene impiegato quando la trasmissione dati verso indirizzi IP deve avvenire nella stessa rete logica del mittente, ma l'indirizzo di destinazione non può essere raggiunto tramite un router. Per es. questo è il caso del collegamento di singole workstation (telelavoratori) tramite TCP/IP alla rete aziendale. Il telelavoratore ha un indirizzo IP che si trova nella stessa rete locale logica di tutti gli altri computer della LAN. Normalmente un pacchetto di dati dalla LAN al telelavoratore cercherebbe solo un ricevente locale, ma non lo troverebbe.

Per utilizzare questa funzione, l'opzione 'Proxy ARP attivo' deve essere attivata (in LANconfig nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Router' oppure nel menu /Setup/IP-router-module per altre possibilità di configurazione).

Con la seguente voce della tabella di routing il router diventa rappresentante del telelavoratore:

Indirizzo IP	Maschera di rete IP	Nome del router	Distanza	Mascheratura IP
192.168.110.123	255.255.255.255	Teleworker01	0	spento

Siccome il router risponde a una ARP request per il computer Proxy con il proprio indirizzo MAC, gli host Proxy in un pacchetto RIP non vengono propagati. Nella tabella di routing la distanza viene posta a '0', per evidenziare ciò.

Il router ora risponde alla richiesta di indirizzo MAC per l'indirizzo IP 192.168.110.123 con il proprio indirizzo MAC. In questo modo tutti i pacchetti per il telelavoratore della LAN vengono inviati automaticamente al router, che trasmette i dati al computer sull'altro lato della connessione.

Routing locale

Si conosce già il seguente comportamento delle workstation di una rete locale: se il computer desidera inviare un pacchetto di dati a un indirizzo IP che non si trova nella propria rete, esso cerca un router che lo possa aiutare. Normalmente questo router viene specificato nel sistema operativo attraverso la voce come router standard o gateway. Se in una rete esistono più router, spesso può essere specificato un solo router standard,



che deve raggiungere tutti gli indirizzi IP sconosciuti alla workstation. Tuttavia talvolta questo stesso router standard non può raggiungere direttamente la rete di destinazione, ma conosce un altro router che conosce questa destinazione.

Come si può aiutare la workstation?

Come standard il router invia al computer una risposta con l'indirizzo del router che conosce la rotta per la rete di destinazione (questa risposta viene definita ICMP redirect). La workstation accetta questo indirizzo e invia immediatamente il pacchetto di dati all'altro router.

Purtroppo alcuni computer non possono operare con i ICMP redirect. Per poter recapitare comunque i pacchetti di dati, si utilizza il routing locale (in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Routing' oppure nel menu */Setup/IP-router-module/Local-routing*). In questo modo si indica al router di inviare il pacchetto di dati all'altro router. Oltre a questo il router non invia altri ICMP-Redirect.

In linea di principio si tratta di una cosa notevole, comunque il routing locale dovrebbe essere utilizzato solo in « caso di emergenza », poiché questa funzione comporta un raddoppio di tutti i pacchetti di dati verso la rete desiderata. I dati vengono inviati prima al router standard e da questo a sua volta al router interessato.

Routing dinamico con IP-RIP

Oltre alla tabella di routing statica, i router di ELSA dispongono anche di una tabella di routing dinamica con un massimo di 128 voci. Questa tabella, a differenza da quella statica, non deve essere compilata, questo viene effettuato dallo stesso router. A questo scopo esso utilizza il Routing Information Protocol (RIP). Con questo protocollo tutti i router di una rete locale, che operano con RIP, si scambiano informazioni relative alle rotte raggiungibili.

Quali informazioni vengono propagate tramite IP-RIP?

Un router comunica nelle informazioni IP-RIP agli altri router della rete le rotte che trova nella propria tabella statica. Non vengono considerate le seguenti voci:

- Rotte che vengono respinte con l'impostazione router '0.0.0.0'.
- Rotte che indicano altri router della rete locale.
- Rotte che collegano singoli computer alla LAN tramite Proxy ARP.

Le voci della tabella di routing statica vengono introdotte manualmente, tuttavia queste informazioni cambiano secondo la situazione di connessione del router e con esse anche i pacchetti RIP inviati.

- Quando il router ha stabilito una connessione con una controparte, trasferisce tutte le reti raggiungibili con questa rotta nelle RIP con distanza '1'. In questo modo gli altri router della LAN vengono informati del fatto che con questo router può essere utilizzata una connessione esistente con questa controparte. In questo modo si può

evitare di stabilire ulteriori connessioni a selezione dei router ed eventualmente si possono ridurre i costi di connessione.

- Se inoltre in questo router non si può stabilire un'ulteriore connessione verso un'altra controparte, tutte le altre rotte vengono trasferite con distanza '16' nel RIP. Il '16' significa « Al momento questa rotta non è raggiungibile ». Il fatto che un router non possa stabilire altre connessioni oltre a quella esistente può derivare da una delle seguenti cause:
 - Su tutti gli altri canali è stata già stabilita un'altra connessione (anche tramite LANCAPI o le porte a/b).
 - La connessione esistente utilizza tutti i canali B (raggruppamento di canali).



Per utilizzare questa funzione, l'opzione 'IP-RIP' deve essere attivata (in ELSA LANconfig nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Routing' oppure nel menu Setup/ IP-Router-module per altre possibilità di configurazione).

I router con capacità RIP inviano i pacchetti RIP ogni 30 secondi circa. Il router è impostato per l'invio e la ricezione di RIP solo quando ha un indirizzo IP univoco. Nell'impostazione fondamentale con l'indirizzo IP XXX.XXX.XXX.254 il modulo IP-RIP è disattivato.

Quali informazioni riceve il router dai pacchetti IP-RIP ricevuti?

Se il router riceve pacchetti IP-RIP, li incorpora nella propria tabella di routing IP dinamica, e questa si presenta così:

Indirizzo IP	Maschera di rete IP	Tempo	Distanza	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

Che cosa significano queste voci?

L'indirizzo e IP e la maschera di rete definiscono la rete di destinazione, la distanza viene ricavata dalle informazioni RIP, l'ultima colonna indica il router che ha comunicato questa rotta. Rimane il 'Tempo'. Con questo la tabella dinamica indica da quanto tempo esiste la corrispondente rotta. Il valore indicato in questa colonna vale come moltiplicatore per l'intervallo con cui arrivano i pacchetti RIP, un '1' significa circa 30 secondi, un '5' sta per circa 2,5 minuti ecc. Se arriva una nuova informazione su una rotta, questa naturalmente viene considerata direttamente raggiungibile e riceve il tempo '1'. Dopo che il corrispondente tempo è trascorso il valore in questa colonna viene automaticamente aumentato. Dopo 3,5 minuti la distanza viene impostata a '16' (rotta non raggiungibile), dopo 5,5 minuti la rotta viene cancellata.

Se ora il router riceve un pacchetto IP-RIP, deve decidere se registrare o meno nella propria tabella dinamica le rotte contenute in questo. A tale scopo esso procede nel modo seguente:

- Se la rotta non è ancora presente nella tabella, le incorpora nella tabella (se in questa c'è posto).
- La rotta è già presente nella tabella con il tempo '5' o '6'. La nuova rotta viene utilizzata se presenta una distanza uguale o migliore.
- Se la rotta è già presente nella tabella con tempo da '7' a '10', quindi ha la distanza '16'. La nuova rotta viene utilizzata in ogni caso.
- La rotta è ancora nella tabella. La nuova rotta proviene dallo stesso router che ha indicato anche tale rotta, ma ha una distanza peggiore rispetto alla voce già presente. Se un router notifica il peggioramento della propria tabella di routing statica (per es. a causa della chiusura di una connessione la distanza aumenta da '1' a '2'), il router gli crede e accoglie la voce peggiorata nella propria tabella dinamica.



*I pacchetti RIP dalla WAN non vengono considerati e vengono immediatamente respinti!
I pacchetti RIP dalla LAN vengono valutati e non vengono trasmessi nella LAN!*

Cooperazione: Tabella statica e dinamica

Dalla tabella statica e dinamica il router calcola la tabella di routing IP vera e propria, con cui determina il percorso per i pacchetti di dati. A tale scopo accoglie, oltre alle rotte della propria tabella statica, le rotte della tabella dinamica che non conosce e che presentano una distanza minore della propria rotta (statica).

Router senza supporto IP-RIP

Talvolta sono presenti nella rete locale anche router che non supportano il Routing Information Protocol. Questi router non possono riconoscere i pacchetti RIP e li trattano come normali pacchetti broadcast o multicast. Se in questo router è registrata la rotta standard per un router remoto, con i RIP vengono stabilite continuamente connessioni. Per evitare ciò, si può introdurre la porta RIP nella tabella di filtro.

Scalata mediante IP-RIP

Se si usano più router in una rete locale con IP-RIP, i router della rete locale possono essere rappresentati all'esterno come un unico grande router. Questa procedura viene anche definita « Scalata ». Attraverso un continuo scambio di informazioni tra i router diventa quindi disponibile un router che in linea di principio può disporre di un numero qualunque di percorsi di trasmissione.

Mascheratura IP (NAT, PAT)

Un problema continuamente crescente in Internet è la limitazione degli indirizzi IP disponibili e di validità generale. Inoltre l'assegnazione di indirizzi IP fissi per Internet

tramite il Network Information Center (NIC) è una soluzione costosa. Che cosa può essere più attraente di suddividere un indirizzo IP tra più computer?

La soluzione si chiama mascheratura IP. Con questa procedura, solo un router della LAN compare con un indirizzo IP in Internet. Questo indirizzo IP viene assegnato al router per es. in modo fisso dal NIC o temporaneo da un provider Internet. Tutti gli altri computer della rete si « nascondono » dietro questo unico indirizzo IP. Oltre all'utile effetto di risparmio, la mascheratura IP rappresenta anche una protezione molto efficace contro gli accessi da Internet alla rete locale.

Due indirizzi per il router

Nella mascheratura si scontrano nel router due esigenze contrastanti: Per un verso esso deve avere un indirizzo IP valido nella rete locale, in modo che sia raggiungibile dalla LAN, per un altro verso esso deve avere un indirizzo Internet valido. Poiché questi due indirizzi in linea di principio non possono stare in una rete logica, c'è una sola possibilità: Ci vogliono due indirizzi IP. Il router riceve un indirizzo **Internet** e un indirizzo **intranet**, naturalmente ciascuno con adatta maschera di rete. Con l'opzione 'Mascheratura' nella tabella di routing si informa il router su quale dei due indirizzi deve essere utilizzato per il trasferimento dei pacchetti. Se un determinato indirizzo viene richiesto dal provider, esistono due possibilità di assegnazione dell'indirizzo:

- Il provider indica al router l'indirizzo desiderato. La maschera di rete determina quanti computer sono mascherati dietro il router.
 - Indirizzo IP con maschera di rete completamente piena '255.255.255.255': Questo è il proprio, unico indirizzo IP registrato dal NIC. Tutti gli altri computer della rete non hanno un indirizzo valido in Internet e vengono mascherati dietro l'indirizzo del router.
 - Indirizzo IP con maschera di rete non completamente piena, per es. '255.255.255.248': Si hanno più indirizzi IP registrati, uno dei quali viene assegnato al router. Gli altri indirizzi IP vengono assegnati a periferiche in Intranet, che quindi possono accedere a Internet tramite connessioni non mascherate. Comunque le altre periferiche possono essere collegate a Internet tramite connessioni mascherate.
- Il provider indica al router un altro indirizzo. Allora **tutti** i computer della rete locale vengono mascherati dietro l'indirizzo assegnato.

Come funziona la mascheratura IP?

La mascheratura usa la proprietà di trasmissione dati tramite TCP/IP in cui vengono utilizzati oltre agli indirizzi della sorgente e della destinazione anche i numeri di porta per la sorgente e la destinazione. Se il router ora riceve un pacchetto di dati da trasmettere, annota in una tabella interna l'indirizzo IP e la porta del mittente. Poi esso assegna al pacchetto il proprio indirizzo IP e un qualunque nuovo numero di porta. Esso annota nella tabella anche questa nuova porta e trasmette il pacchetto con i nuovi valori.



La risposta a questo pacchetto arriva all'indirizzo IP del router con il nuovo numero di porta del mittente. Usando la voce registrata nella tabella interna il router può assegnare questa risposta al mittente originale.

Nelle statistiche del router si possono visualizzare queste tabelle (vedere anche 'Stato' nel Manuale di riferimento).

Mascheratura semplice e inverso

Questa mascheratura funziona in entrambe le direzioni: Se un computer della LAN invia un pacchetto in Internet, la rete locale viene mascherata dietro l'indirizzo IP del router (mascheratura semplice).

Se all'inverso un computer di Internet invia un pacchetto per es. a un server FTP in Intranet, a questo computer sembra come se il router fosse il server FTP. Tramite la voce nella tabella di servizio, il router conosce l'indirizzo Intranet del server (in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Mascheratura' oppure nel menu `Setup/IP-router-module/Masquerading/Service-table`). Il pacchetto viene trasferito a questo computer. Tutti i pacchetti che arrivano nella rete locale dal server FTP (risposte del server), vengono nascosti dietro l'indirizzo IP del router.

Una piccola differenza:

- L'accesso dall'esterno a un servizio (porta) in Intranet deve essere prima definito indicando un numero di porta. In una tabella di servizio viene indicata la porta di destinazione con l'indirizzo Intranet per es. del server FTP.
- Durante l'accesso da Intranet a Internet invece l'introduzione in tabella delle informazioni per porta e indirizzo IP viene effettuata dallo stesso router.

La corrispondente tabella può accogliere al massimo 2048 voci, e quindi consentire **contemporaneamente** 2048 trasmissioni tra la rete mascherata e quella non mascherata.

Dopo un tempo definibile, il router suppone che la voce non sia più necessaria e la cancella autonomamente dalla tabella.

Quali protocolli possono essere trasmessi con mascheratura IP?

Naturalmente solo quelli che comunicano anche attraverso porte. I protocolli che operano senza numeri di porta o utilizzano porte sopra IP in modello OSI, non possono essere mascherati senza uno speciale trattamento.

Nella versione attuale il router effettua una mascheratura per i seguenti protocolli:

- FTP
- TCP
- UDP
- ICMP

DNS forwarding

Durante l'accesso a Internet normalmente non vengono utilizzati indirizzi IP per raggiungere un server ma piuttosto nomi. Chi conosce l'indirizzo che si nasconde dietro 'www.domain.com'? Il server DNS!

DNS significa Domain Name Service e definisce l'assegnazione di nomi di dominio (come domain.com) ai corrispondenti indirizzi IP. Naturalmente queste informazioni devono essere curate continuamente e tenute sempre disponibili su scala mondiale. A questo scopo esistono server DNS, che presentano lunghe tabelle con indirizzi IP e nomi di dominio.

Se un computer desidera chiamare da Intranet una homepage, invia prima una request DNS: « Quale indirizzo IP corrisponde a www.domain.com? » Se il router nelle workstation è indicato come un server DNS, questa richiesta viene trattata nel modo seguente:

- Il router cerca prima nelle proprie impostazioni se è registrato un server DNS (in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Indirizzi' oppure nel menu /Setup/TCP-IP-module). Se lo trova, stabilisce una connessione con tale server e raccoglie l'informazione desiderata.
- Se nessun server DNS è registrato nel router, esso tenta di raggiungere su una connessione PPP eventualmente esistente (per es. con il provider Internet) un server DNS, e raccoglie da questo l'assegnazione dell'indirizzo IP al nome. Naturalmente questo ha successo solo se durante la negoziazione PPP l'indirizzo di un server DNS è stato trasferito al router.
- Se non esiste alcuna connessione, viene stabilita la rotta di default e con questa viene ricercato il server DNS.

Con questa procedura non è necessario conoscere l'indirizzo di un server DNS. La registrazione dell'indirizzo intranet del router come server DNS nelle workstation non è sufficiente per l'assegnazione dei nomi. Inoltre l'indirizzo del server DNS viene aggiornato automaticamente. Se per es. il provider che comunica questo indirizzo rinomina il server DNS, oppure si passa ad un altro provider, il router riceve sempre le informazioni aggiornate.

Policy based routing

Si definisce policy based routing la procedura per cui determinati pacchetti di dati vengono trattati in modo preferenziale. A questo scopo viene valutato uno speciale campo all'interno dei pacchetti di dati IP, il campo type-of-service (TOS). Questo trattamento preferenziale di alcuni pacchetti di dati serve per es. a facilitare la configurazione del router attraverso la WAN, se contemporaneamente devono essere trasmessi molti dati.



Ulteriori informazioni sul policy based routing si possono trovare nella 'Descrizione dei punti di menu' nel Manuale di riferimento.

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). Con questo protocollo un server DHCP in una rete TCP/IP può assegnare dinamicamente gli indirizzi necessari alle singole stazioni.

Il router come server DHCP

Il router può gestire come server DHCP gli indirizzi 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 router completamente non configurato di ELSA può addirittura definire autonomamente in modalità DHCP automode gli indirizzi IP per se stesso e per i computer della rete.

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

DHCP – 'On', 'off' o 'auto'?

Il server DHCP nei router di ELSA 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 il router 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 il router cerca di attivarsi nella rete locale dopo altri server DHCP (si riconosce dalla breve accensione del LED Tx dopo l'attivazione).
 - 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 router 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 server è attivo o disattivo.

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

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 assegnato può essere prelevato dal pool di indirizzi impostato (dall'indirizzo iniziale all'indirizzo finale del pool di indirizzi). 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'. 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 nella rete. In questo stato il server DHCP assegna agli altri computer della rete solo l'indirizzo IP e la sua 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 router 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 (sequenza come per l'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

Il router assegna sempre al computer richiedente il proprio indirizzo IP come indirizzo di gateway.

Se necessario, questa assegnazione può essere sovrascritta 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 di 6000 minuti, 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 deve utilizzare parametri diversi da quelli ad esso assegnati (per es. un'altra gateway standard), questo deve essere impostato direttamente sulla workstation. 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 del router 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 effettuato la richiesta iniziale. 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.

Configurazione del router come server DHCP

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

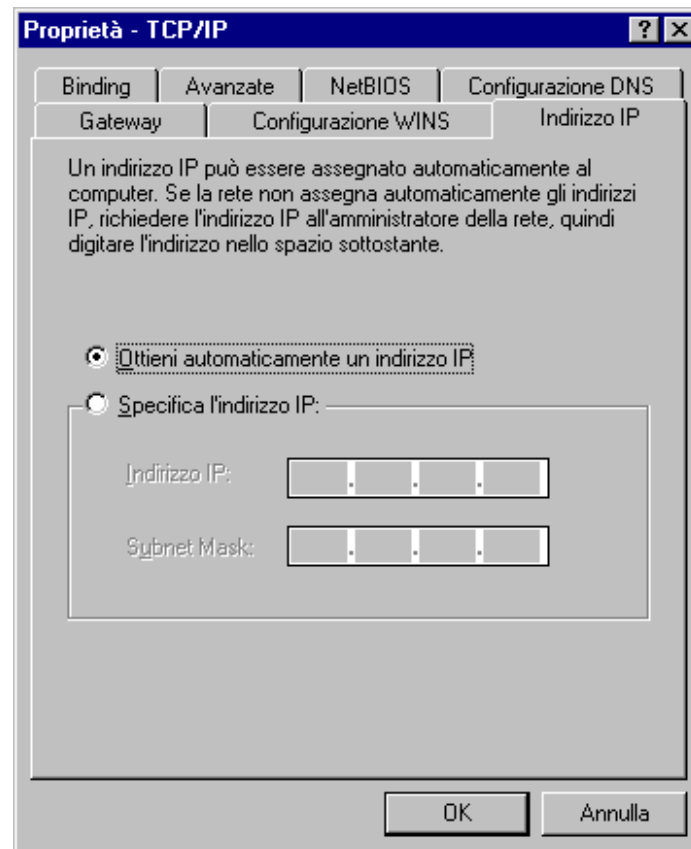
- Una rete non è stata ancora creata, oppure la rete locale esistente non utilizza un TCP/IP. Con il server DHCP del router si possono assegnare in un solo colpo gli indirizzi IP a tutti i computer della rete e allo stesso router.
- Esiste già una rete con TCP/IP, ma senza server DHCP e si vuole passare 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 il router non configurato alla propria rete locale tramite il cavo di rete. Se si collega l'apparecchio a un hub, il commutatore node/hub si deve trovare 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 router 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 aprire la finestra di configurazione delle caratteristiche di rete per es. in ambiente Windows 95 con **Avvio ► Impostazioni ► Pannello di controllo ► 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 router.



Nel workshop si apprende come si può installare un protocollo di rete per es. in ambiente Windows 95 o Windows NT. Nella Guida all'installazione si trovano istruzioni per l'installazione di ELSA LANconfig.

- ④ Installare *ELSA LANconfig* su uno dei computer della rete.
- ⑤ Avviare *ELSA LANconfig* dal gruppo di programmi 'ELSAIlan'. 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, selezionare l'opzione 'Tutto impostato automaticamente' in questo wizard, e premere nella finestra seguente 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.

Il wizard assegna al router l'indirizzo IP introdotto con la rispettiva maschera di rete. Dall'indirizzo IP l'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).

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 servizio è necessario per la comunicazione in Internet, per es. per poter rispondere a una richiesta come 'www.elsa.com' con il corrispondente indirizzo IP. Ma anche nell'ambito di una rete locale o di un accoppiamento tra LAN ha senso poter assegnare in modo univoco gli indirizzi IP della LAN ai nomi dei computer.

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 in *ELSA LANCOM Business*:

- Un *ELSA LANCOM Business* 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 Business* inoltre conosce i nomi dei computer e gli indirizzi IP delle altre reti NetBIOS collegate. Inoltre anche i computer con indirizzo IP fisso si registrano nella tabella NetBIOS e quindi sono conosciuti con nome e indirizzo IP.
- Il server DNS in *ELSA LANCOM Business* 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.

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.

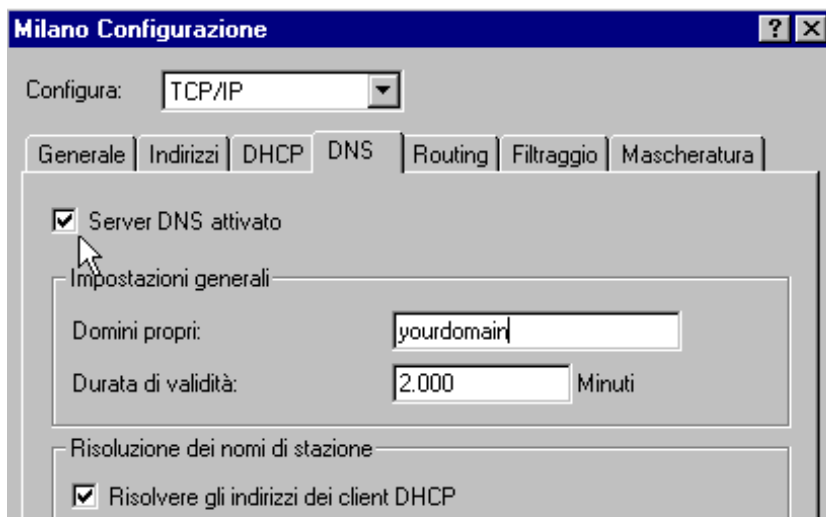
```
set setup/DNS-module/operating on
```

- 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.

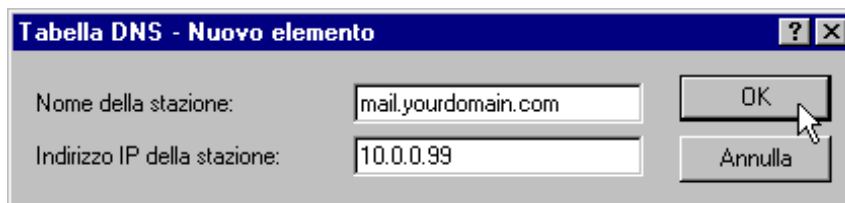
```
set setup/DNS-module/dhcp-usage yes
set setup/DNS-module/NetBIOS-usage yes
```



- 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 sono noti,
- 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 remoto e si vuole raggiungere attraverso il router il mail server della sede (Nome: mail.yourdomain.com, IP: 10.0.0.99), introdurre:

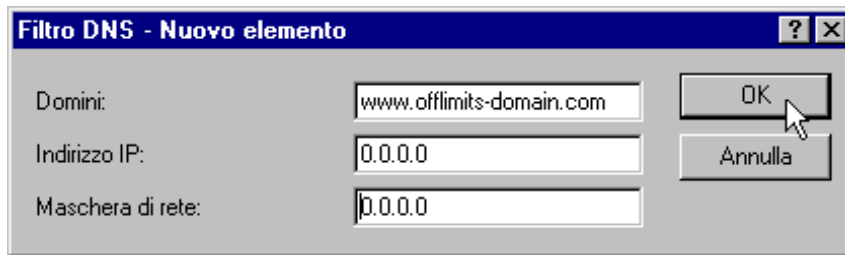


```
cd setup/DNS-module/DNS-table
set mail.yourdomain.com 10.0.0.99
```

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 sede, 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 DE, introdurre:

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



La hit list delle statistiche DNS riporta i 64 nomi richiesti più frequentemente, 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.

NetBIOS proxy

Funzionando come NetBIOS proxy un *ELSA LANCOM Business* 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 sezione descrive il funzionamento di NetBIOS proxy in generale e la configurazione del router e dei computer per la interconnessione di reti Windows.

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 Business* 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.

Trattamento dei pacchetti NetBIOS

Il comportamento molto verboso dei computer Windows può causare forti addebiti in una connessione su linee ISDN, poiché ciascun pacchetto NetBIOS con informazioni sul nome causa automaticamente lo stabilimento della connessione (per es. con ISP già collegato). Con siffatti pacchetti la linea rimane continuamente collegata 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 Business* 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),

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.

Per evitare che le richieste per computer che non si trovano nella propria LAN e neanche nelle controparti NetBIOS 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.

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 Business su IP!

Il routing dei pacchetti NetBIOS nel *ELSA LANCOM Business*, 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 si 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

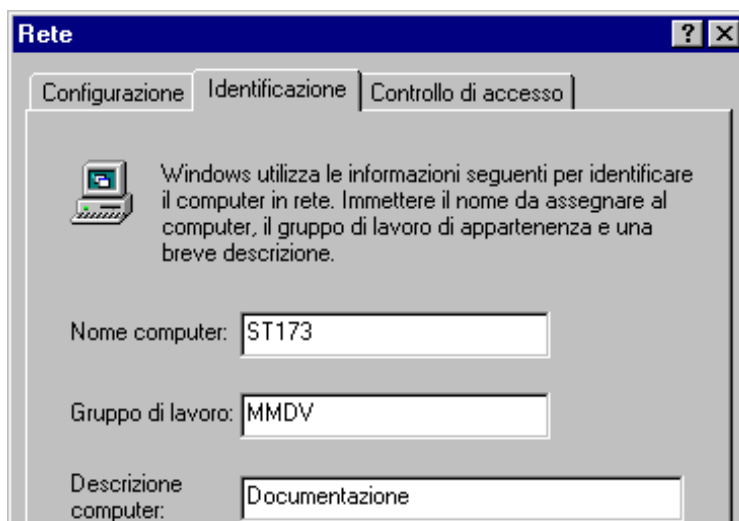
L'abilitazione di file e stampanti consente di abilitare unità disco o stampanti per altri utenti della rete Windows.

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.

■ Condivisione di file e stampanti

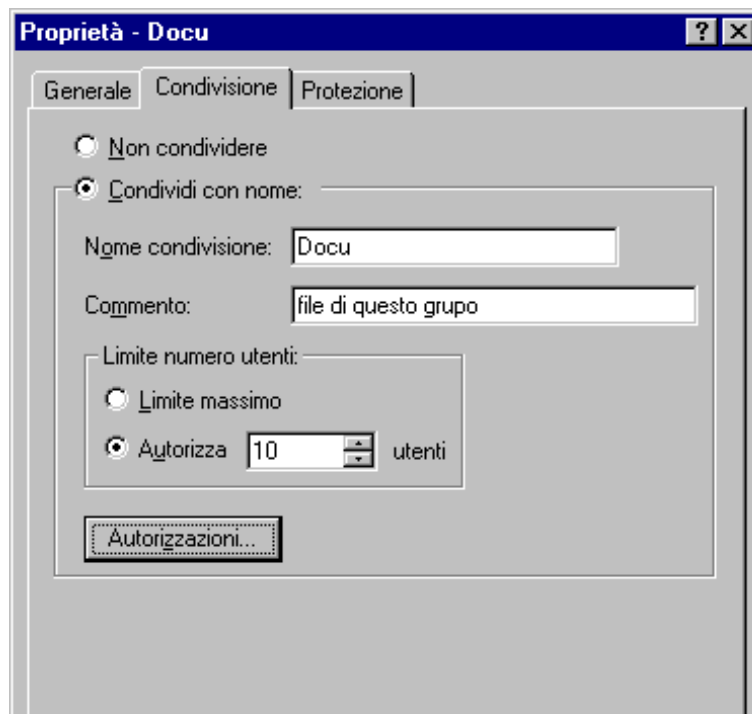
Dopo l'installazione, controllare se è attivata la condivisione di file e stampanti. A questo scopo cliccare su **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► Condivisione di file e stampanti**. Selezionare se gli altri utenti della rete

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.

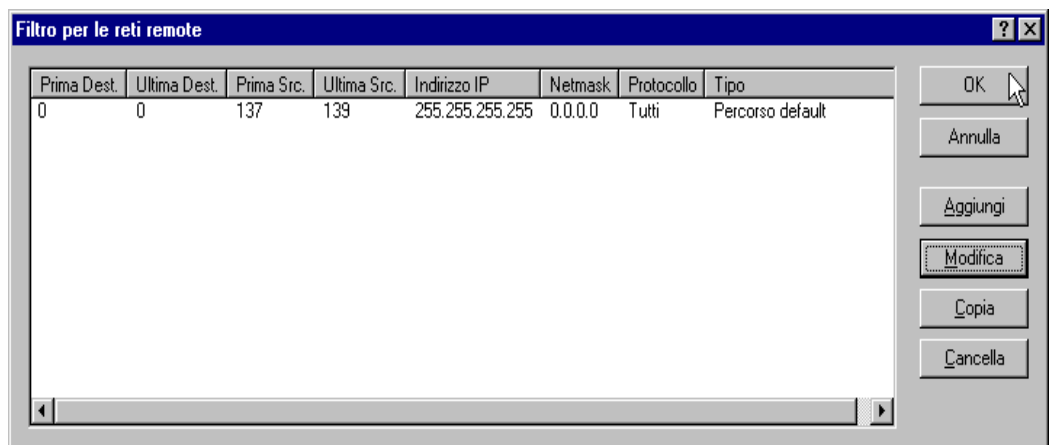


Si può controllare facilmente se le impostazioni nella rete Windows sono corrette: Il proprio computer deve essere visualizzato nell'ambiente di rete con il rispettivo nome.

Come si connettono due reti Windows tramite ISDN

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:



- 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'.



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. In caso di accesso a macchine Windows NT si deve introdurre manualmente il corrispondente dominio/gruppo di lavoro.

- 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.

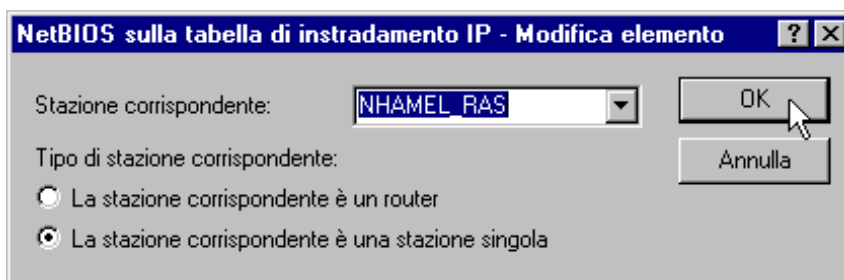
```
cd /Setup/NetBIOS-module  
set operating on
```

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.

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 Business* 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 Business* (vedere 'Come si connettono due reti Windows tramite ISDN').
- 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.

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, in *ELSA LANCOM Business* è disponibile una lista con tali nomi di computer. Tramite Telnet con

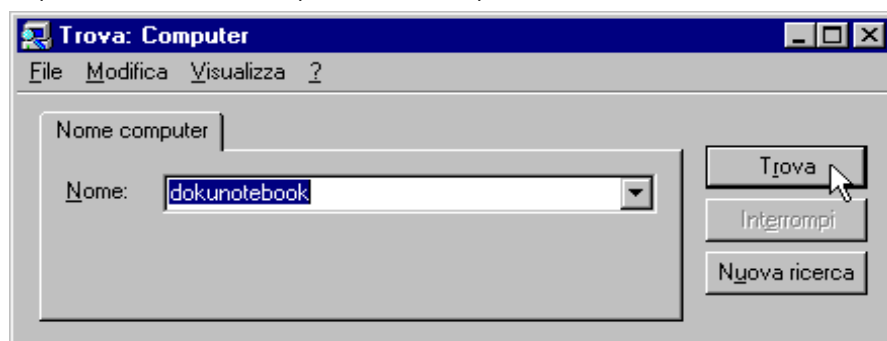
```
dir /Setup/NetBIOS-module/Host-list
```

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	192.168.100.162	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:

- Sul lato del nodo di selezione non è disponibile alcun server in cui si possano scegliere i computer disponibili della rete Windows della 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 Business*.

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.

IP Pooling per gli accessi da linea commutata

ELSA LANCOM Business con il suo grande numero di canali B disponibili è idealmente adatto come nodo di accessi remoto (remote access server) per piccole e medie aziende. Per evitare di dover creare una propria rotta per ciascun accesso da linea commutata, il router dispone di un pool di indirizzi IP, dal quale viene assegnato alla controparte che effettua la selezione un indirizzo IP valido per la LAN per la durata della connessione.

Le impostazioni per il pool di indirizzi IP si trovano in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Indirizzi' o nelle sedute Telnet o di terminale nella posizione `/Setup/IP-router-module`.

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.

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 ISDN. Con la LANCAPI il PC instrada il fax attraverso la rete a un ELSA LANCOM Business, e questo stabilisce la connessione con il destinatario tramite ISDN.

L'impostazione dinamica della LANCAPI consente anche una facile scalabilità dei percorsi di comunicazione. Se per gestire i compiti risultano necessari più canali B, viene semplicemente installato in rete un altro ELSA LANCOM Business. Tutti gli apparecchi della rete locale si ripartiscono il lavoro da svolgere.

Si noti: Tutte le applicazioni che operano attraverso la LANCAPI utilizzano connessioni ISDN dirette e non girano attraverso il router dell'apparecchio. Pertanto la funzione Firewall e le funzioni di monitoraggio addebiti vengono disattivate!



Installazione del LANCAPI client

La LANCAPI è costituita da due componenti, un server (in ELSA LANCOM Business) 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 Business* 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 Business* 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.



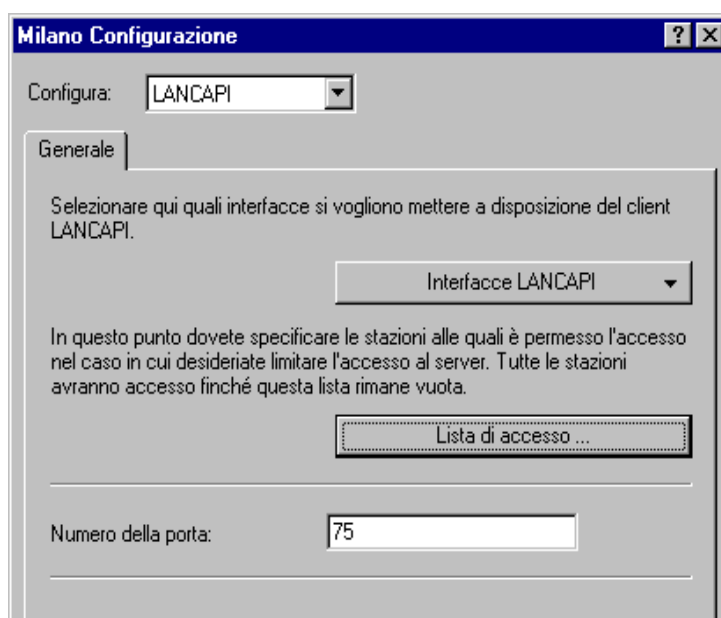
Impostazione del *LANCAPi* server

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

- A quali numeri telefonici 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'.

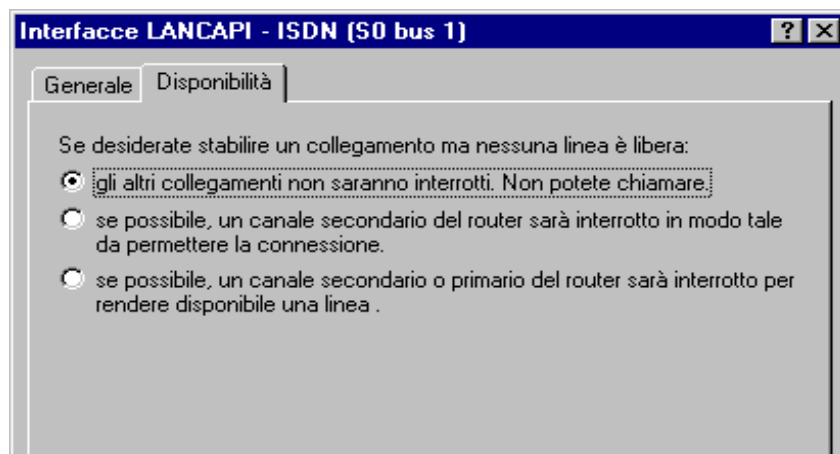


- ② Attivare il *LANCAPi* server, o consentire 'solo chiamate in uscita'. In questo caso la *LANCAPi* non reagisce alle chiamate in arrivo e non può essere impiegata per es. per ricevere messaggi fax. Per es. consentire solo le chiamate in uscita se per la *ELSA LANCAPi* non si dispone di un numero telefonico 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 telefonici possono essere separati da punto e virgola. Se non si introduce alcun numero telefonico, 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 telefonici 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* su diverse workstation indicare di volta in volta i vari numeri telefonici, ai quali il programma deve reagire.

Passare alla scheda registro 'Opzioni'. In questa si definisce come si comporta un *ELSA LANCOM Business* 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.
- 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 *LANCAPI* selezionare la voce 'ISDN WAN Line 1'.

ELSA CAPI Faxmodem

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

Installazione

ELSA CAPI Faxmodem viene può essere installato tramite il CD-Setup. Installare *ELSA CAPI Faxmodem* sempre insieme con la *ELSA LANCAPI* attuale. Dopo il riavvio, *ELSA CAPI Faxmodem* è disponibile nel sistema, per es. in ambiente Windows 95 o Windows 98 tramite **Avvio ► Pannello di controllo ► Modem**.

Invio di fax tramite *ELSA CAPI Faxmodem*

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.

Il least-cost router

Da quando c'è stata la liberalizzazione del mercato telefonico in Europa gli utenti di servizi di comunicazione posso 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 si utilizza 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 questo gruppo di cifre che identificano la 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 eventualmente 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 Business* 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.

Il Least-cost router di *ELSA LANCOM* opera in questo modo

Il LCR analizza le cifre selezionate per es. dal router o dalla *LANCAPI*.

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 telefonico 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 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. 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
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 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 Business*. A questo scopo ci sono diverse regole:
- Le possibilità di risparmio univoche possono essere introdotte direttamente:
 - '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. (per es. della rete della Telecom Italia). 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 gestore.
- Esaminare le diverse zone tariffarie. I prefissi per le diverse zone possono essere visualizzati per es. in www.risparmio-telefonico.it o www.lcr-italia.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. Indirizzi come per es. 'www.risparmio-telefonico.it' informano sui prezzi aggiornati per tutte le

connessioni immaginabili. Con queste informazioni si può passare a nutrire 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 di *ELSA LANCOM Business* 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 in *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 LRC secondo necessità per le seguenti modalità:
 - Router
 - 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 Least Cost**, 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 delle **Festività nazionali**. Introdurre ciascun giorno festivo con la data completa (GG.MM.AAAA).
- ⑤ Controllare l'orologio interno dell'apparecchio (compresa la data), in modo che il LCR possa attivare gli instradamenti all'ora giusta (vedere anche nel seguito, 'L'ora per la selezione').



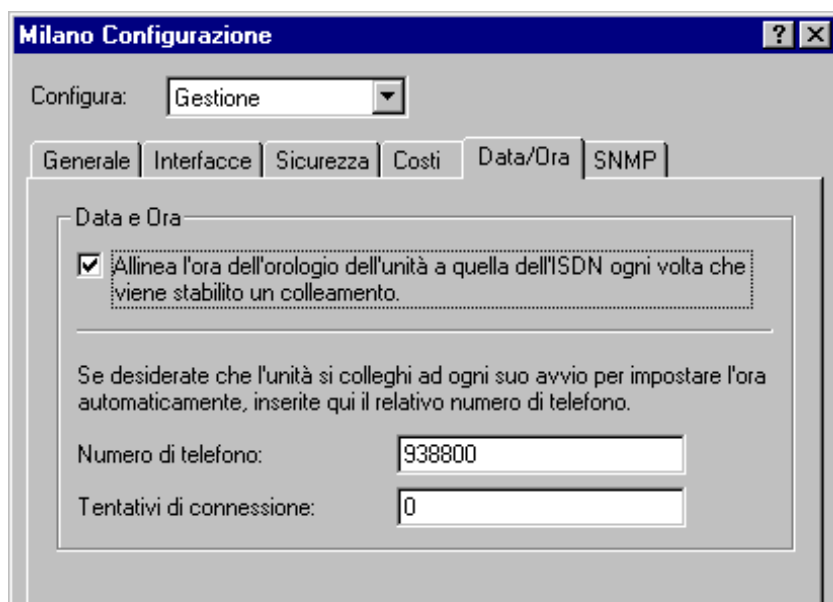
*Costruire la tabella LCR per passi, e controllare ogni volta il risultato. A questo scopo aprire per es. ELSA LANmonitor e avviare attraverso ELSA LANCAPI connessioni verso controparti che dovrebbero essere smistate in base alla tabella. In base al numero telefonico selezionato si può facilmente vedere 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 connessioni corrette, naturalmente l'orologio interno del *ELSA LANCOM Business* 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 telefonico 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!

Workshop

Negli esempi delle seguenti sezioni verrà mostrato come ottenere il massimo dal router.

Per tutte le configurazioni si parte da un apparecchio nello stato di fornitura. Quindi, se si vuole eseguire completamente un esempio, eventualmente riportare il router alla configurazione iniziale con un reset di sistema.

In questa sezione si fa la conoscenza coi i segni e i simboli utilizzati.

Il nostro team di sviluppo è continuamente all'opera per aggiungere nuove funzioni al software e per rendere sempre più comodo l'impiego con *ELSA LANconfig*. Pertanto è possibile che le foto delle schermate workshop si presentino in modo leggermente diverso rispetto allo stato attuale del software, tuttavia questo non modifica la funzionalità dei menu.

Le impostazioni fondamentali, come per es. l'indicazione dei propri numeri telefonici, si presentano ripetutamente in tutti gli esempi, in modo che ciascuna singola sezione costituisca una descrizione completa. Pertanto vengono qui descritte anche impostazioni eventualmente non necessarie per la funzione base.





Configurazione con *ELSA LANconfig* e l'assistenza

Nelle sezioni contrassegnate con questo segno, viene mostrato come si effettuano in modo rapido e comodo le configurazioni in ambiente Windows con *ELSA LANconfig* e la sua assistenza.



Configurazione senza assistenza

Nelle istruzioni passo per passo si trovano informazioni precise sui menu in cui vengono effettuate le impostazioni, sia con *ELSA LANconfig* che tramite una connessione Telnet o di terminale.




	Setup/WAN-module	
	Interfaccia	S0 DSS1 0 123456 123456

I valori indicati possono essere immessi direttamente in una sessione di configurazione, per es.

```
cd setup/WAN-module/Interface-list  
set S0 DSS1 123456 123456
```

Ulteriori informazioni sulla configurazione con Telnet o emulatori di terminale si trovano nel capitolo 'Possibilità di configurazione'.

I seguenti simboli si ritrovano nelle istruzioni passo per passo:

	Menu	Indica un sottomenu
	Valore	Indica un valore che può essere modificato
	Tabella	Indica una tabella le cui voci possono essere modificate.

Quale apparecchio si utilizza?

Le operazioni descritte nel workshop possono essere avviate con diversi modelli della famiglia *ELSA LANCOM*. Le limitazioni riferite a determinati modelli vengono indicate con corrispondenti simboli accanto al testo.

Tutte le descrizioni valgono per router con un bus (interfaccia) S_0 , e quindi con 2 canali 2 B. Per gli apparecchi con più bus S_0 (per es. *ELSA LANCOM Business 4100*) eventualmente le impostazioni devono essere trasmesse alle altre interfacce e canali.

Impostazioni opzionali



Questo simbolo indica le impostazioni opzionali, che non sono strettamente necessarie per la funzione specifica dell'esempio di configurazione. Fanno parte di queste per es. le impostazioni di filtri, che escludono dalla trasmissione speciali pacchetti di dati o i meccanismi di protezione, che limitano l'accesso all'apparecchio.

Applicazioni Internet

Nella prima sezione sull'impiego pratico degli apparecchi presentiamo le applicazioni in collegamento con Internet.

Il primo esempio descrive la rete locale di una azienda, che deve essere connessa con Internet tramite un router. Tutte le workstation della LAN ricevono l'accesso ai servizi e alle possibilità di Internet tramite un account presso un provider. Ma allo stesso tempo in questa applicazione il router, con la funzione firewall, deve anche proteggere la rete locale contro l'accesso dall'esterno e rendere inaccessibili le workstation al di fuori di Internet.

Nel secondo esempio l'azienda vorrebbe non solo utilizzare i servizi di Internet come partecipante passivo, ma anche predisporre in modo attivo un proprio servizio di informazioni. A questo scopo viene installato nella rete locale aziendale un Web server, che viene collegato con il provider tramite una connessione fissa. Naturalmente questo server deve essere raggiungibile da Internet, tutti gli altri computer della rete devono rimanere protetti dalla funzione firewall.

Internet per tutti i PC della LAN

La motivazione

Molte aziende vorrebbero connettere ad Internet tutti i computer della rete locale. Tuttavia, in alcuni casi finora c'erano due motivi in contrario:

- Account esclusivi diversi per ciascun computer presso un Internet Service Provider (ISP) o addirittura l'acquisto di indirizzi IP registrati, validi in Internet nella maggior parte dei casi sono troppo cari. A ciò si aggiunge l'impegno richiesto per l'allestimento e la manutenzione dei singoli accessi a Internet.
- Un'ulteriore fonte di preoccupazione in caso di connessione dei singoli computer alla WWW è l'insicurezza, il timore che in questo modo si spalanchino le porte di accesso alla rete aziendale.

Il router risolve entrambi i problemi con una sola funzione: la mascheratura IP. In breve avviene quanto segue:

Il router è l'unica periferica della LAN che possiede indirizzo IP valido in Internet. Questo può essere assegnato per es. in modo dinamico tramite PPP dal provider Internet durante la selezione (come con tin.it, AOL ecc.). I computer della rete utilizzano gli indirizzi di uno speciale gruppo di indirizzi protetto (per es. indirizzi « 10 »). Attraverso la mascheratura IP tutta la rete locale viene « nascosta » dietro un indirizzo IP registrato del router.

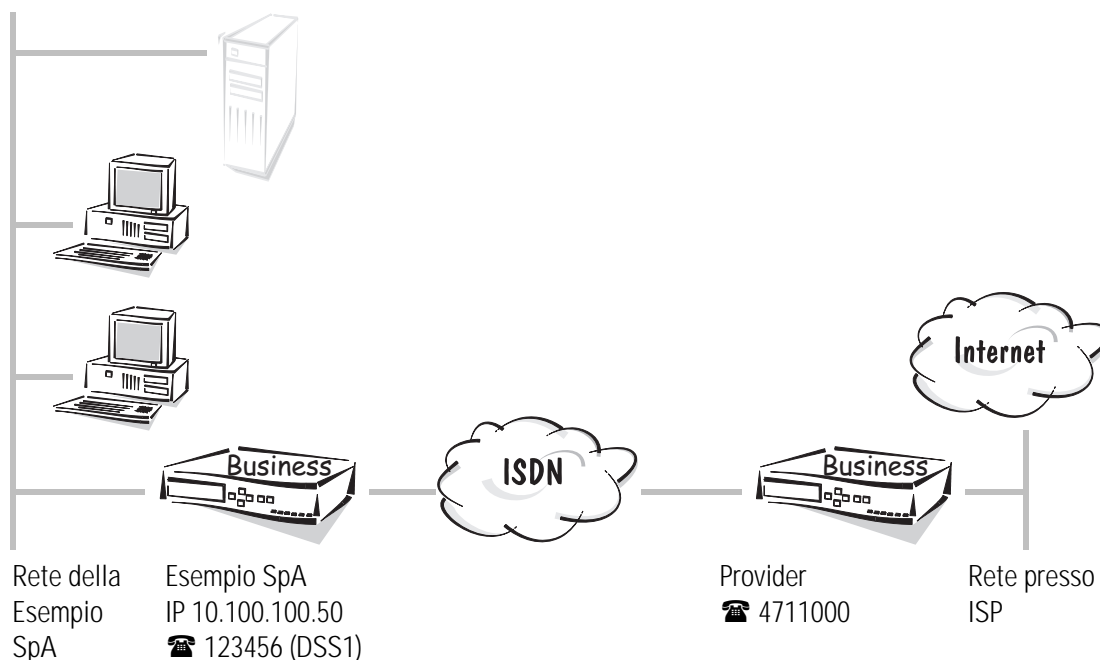
Questa procedura presenta molti vantaggi:

- La mascheratura IP rende semplice l'accesso a Internet.
Si deve configurare un solo un apparecchio. E inoltre si ha l'aiuto del settaggio assistito di *ELSA LANconfig*.
- La mascheratura IP rende conveniente l'accesso a Internet.
Tutti i computer della rete locale possono utilizzare verso l'esterno l'indirizzo IP del router e quindi avere accesso a Internet. In questo modo, per molti utenti è necessario un solo account presso il provider. Inoltre il router gestisce autonomamente la linea ISDN e stabilisce la connessione con il provider solo quando devono essere effettivamente trasmessi dati.
- La mascheratura IP rende sicuro l'accesso a Internet.
I computer della rete locale non sono visibili dall'esterno. In Internet è noto solo l'indirizzo IP del router. Un accesso alla rete locale dall'esterno è impossibile, la mascheratura IP agisce come un efficace firewall e separa Internet da intranet. Inoltre il router è l'unica interfaccia verso Internet, ed è più facile da controllare rispetto a molti singoli apparecchi sulle workstation.

Il caso preso come esempio

Da un lato c'è la rete locale di un'azienda con alcune workstation e un router su una connessione Euro ISDN. In questa rete ci può essere un server, ma non è necessario.

Dall'altro lato c'è una rete presso il provider di servizi Internet con un router ISDN come nodo di selezione per gli utenti. Questo nodo di selezione vorrebbe essere chiamato con PPP e richiede una sicurezza secondo 'CHAP'. I dati richiesti per l'accesso sono il nome utente 'WEB_USER' e la password 'Navigare'.



La seguente tabella mostra l'assegnazione di tutti i dati importanti, come vengono utilizzati nell'esempio. Si raccomanda di creare una siffatta tabella per ogni applicazione. Essa supporta il lavoro durante la configurazione, durante la ricerca difetti e in caso di richieste al supporto.

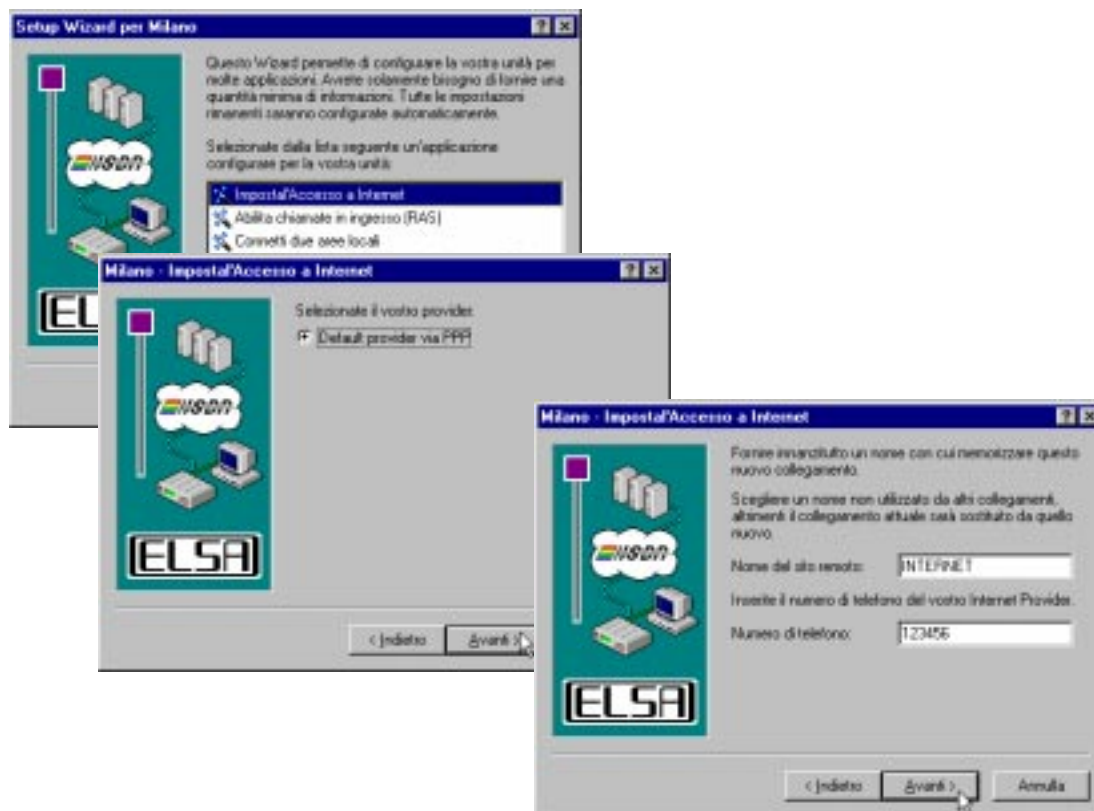
	Rete locale della Esempio SpA	Rete locale del provider
Indirizzo IP della LAN	10.100.100.0	
Indirizzo IP del router	10.100.100.50	
Maschera di rete IP	255.255.255.0	
Nome della periferica	Esempio SpA	Provider
Dialup-remote	123456	4711000



Internet molto semplice con **ELSA LANconfig** e i wizard

Per la configurazione di *ELSA LANCOM* per l'accesso a Internet, in *ELSA LANconfig* sono disponibili diversi wizard, che si incaricano di eseguire tutte le impostazioni necessarie nel software *ELSA LANCOM*. Dopo aver avviato il wizard, selezionare (automaticamente o con **Strumenti ► Setup Wizard**) il wizard desiderato. In questo esempio non abbiamo scelto uno dei grandi servizi online, ma un altro ISP, che offre nodi di selezione tramite PPP. Quindi selezionare la voce 'Internet tramite PPP'. L'assistenza chiede i pochi dati

necessari e successivamente fornisce informazioni su quello che rimane da impostare sulle workstation.



Passo per passo: Quali impostazioni si effettuano nel router?

- ① Prima immettere nella tabella di interfaccia router il numero telefonico per le chiamate in arrivo e in uscita (campo di configurazione 'Comunicazione', registro 'Generale'):

```
cd /setup/WAN-module/Router-interface-list
S0-1 123456 ON 0 OFF
```

Quando si immettono più numeri telefonici, per le chiamate in uscita viene utilizzato il primo numero.



Con l'impostazione dell'opzione 'Connessione Y' si definisce se tramite il secondo canale B può essere stabilita contemporaneamente una connessione con un'altra controparte.

- ② Una nuova voce nella lista dei nomi (campo di configurazione 'Comunicazione', registro 'Siti remoti') con la denominazione della controparte e i rispettivi numeri telefonici e la selezione del layer predefinito 'PPPHDL' (senza chiamata di risposta) consente al router dell'azienda di chiamare il router del ISP:

```
cd setup/WAN-module/Name-list
set Provider 4711000 * * PPPHDL OFF
```

- ③ Nella lista PPP si immette il nome utente e la password che vengono trasmessi durante la selezione della controparte. Poiché solo l'ISP richiede il nome e la password, ma non viceversa, la negoziazione PPP da questo lato non ha 'nessuna' sicurezza.

```
cd Setup/WAN-module/PPP-list/Default
set Provider no surfing * * WEB_USER IP
```

La password 'Navigare' viene rimpiazzata da alcuni * durante l'immissione! Gli altri * in questa voce indicano o valori che devono essere accettati senza modifica.



Notare che nel nome utente e nella password vengono distinti i caratteri maiuscoli e minuscoli.

- ④ Adesso rimangono da chiarire solo gli indirizzi. Affinché il router possa essere trovato nella propria rete TCP/IP, ha bisogno di un indirizzo IP libero di intranet. Esso lo riceve con l'immissione dell'indirizzo intranet con la rispettiva maschera di rete (campo di configurazione 'TCP/IP', registro 'Generale').

```
cd Setup/TCP-IP-module
set Intranet IP address 10.100.100.50
set Intranet netmask 255.255.255.0
set operating on
```



Le voci per l'indirizzo IP e la maschera di rete IP rimangono libere, poiché il router in questo esempio riceve l'indirizzo IP in modo dinamico dal ISP. Se invece sono disponibili indirizzi IP registrati, validi in Internet, qui dovrebbe essere immesso uno di questi con la rispettiva maschera di rete (vedere anche 'Intranet con proprio Web server in Internet').

- ⑤ Con le impostazioni fatte fino a questo punto il router è diventato in pratica una parte costituente di Internet, però i computer della LAN non possono ancora navigare. Per ottenere questo, creare una voce nella tabella di routing (campo di configurazione 'TCP/IP', registro 'Routing'), mediante la quale tutti i pacchetti per indirizzi non raggiungibili localmente vengono instradati in Internet (rotta di DEFAULT).

```
cd Setup/IP-router-module
set IP-routing-table 255.255.255.255 0.0.0.0 Provider
2 ON
```

La rotta con indirizzo IP '255.255.255.255' con maschera di rete '0.0.0.0' riceve tutti i pacchetti che non possono essere recapitati localmente. 'Provider' è la denominazione della controparte a cui devono essere inviati i corrispondenti dati. La controparte può essere raggiunta direttamente dal router, pertanto la distanza è posta a '2'. Con l'opzione 'ON' per la mascheratura IP tutti i computer della LAN vengono nascosti dietro l'indirizzo del router e non compaiono in Internet.

- ⑥ Adesso attivare il router IP, e il router è pronto per la WWW.

```
cd Setup/IP-router-module  
set operating on
```

- ⑦ Che cosa rimane da fare? Naturalmente anche i computer della LAN devono sapere che *ELSA LANCOM* è il centralino per Internet. A questo scopo l'indirizzo intranet del router viene indicato come gateway di default e server DNS per le workstation.



Quando il router viene usato come server DHCP, queste impostazioni possono essere effettuate automaticamente (vedere 'Server DHCP').

Il risultato

Se uno dei collaboratori dalla sua workstation avvia un browser e immette un'indirizzo Web (per es. ELSA), tramite il server DNS registrato nel sistema operativo (nel presente caso tramite il router) si tenta di determinare il rispettivo indirizzo IP. Il router in qualità di gateway Internet trasferisce questa richiesta al server DNS del ISP, che finalmente determina l'indirizzo IP per questo nome (per es. 168.192.156.100) e lo restituisce alla workstation tramite il router. Poiché questo indirizzo non si trova nella rete locale, il router invia in Internet tutti i pacchetti per questo indirizzo IP tramite la rotta di default.

Intranet con proprio Web server in Internet

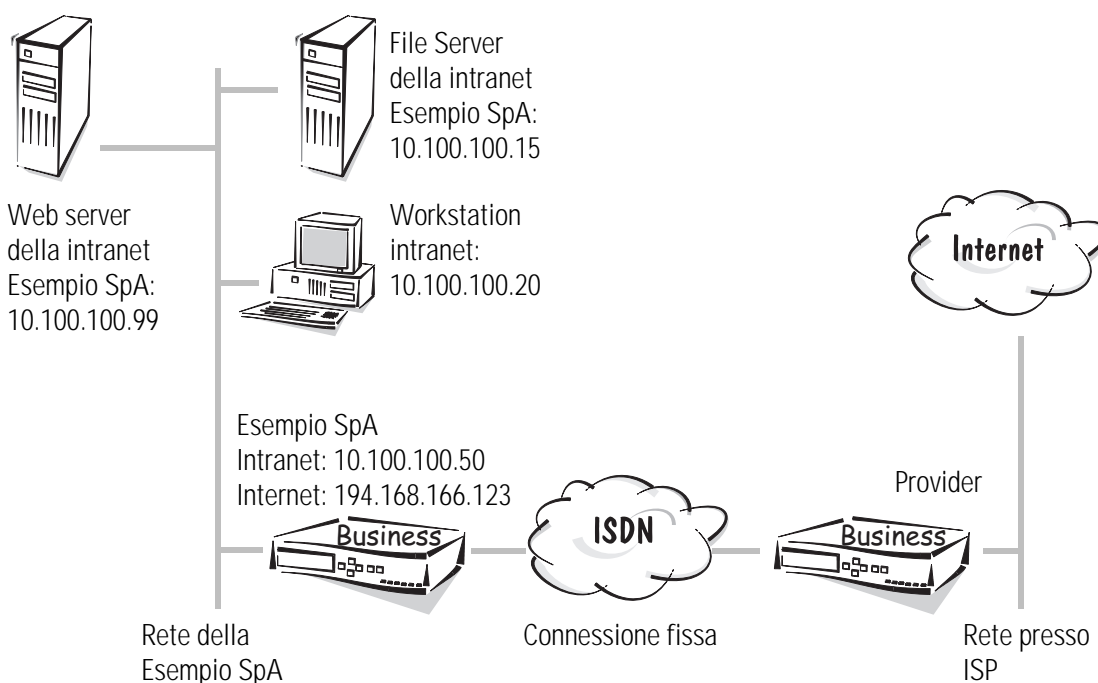
La motivazione

Nell'esempio 'Internet per tutti i PC della LAN' si è visto come una rete TCP/IP completa può essere collegata a Internet tramite un router (con mascheratura IP).

Nel seguente esempio alla LAN della Esempio SpA viene aggiunto un proprio Web server, che deve essere raggiungibile da Internet. A questo scopo, oltre all'account presso l'ISP è necessario un indirizzo IP fisso. Questo indirizzo IP registrato viene assegnato al router. Il router si incarica della conversione dall'indirizzo registrato all'indirizzo intranet del Web server. In questo modo il Web server diventa visibile in Internet all'indirizzo registrato (mascheratura IP inversa). Tutti gli altri computer della rete locale rimangono nascosti come in precedenza.

Il caso preso come esempio

Da un lato c'è la rete locale della Esempio SpA con alcune workstation e un router su una connessione Euro ISDN. In tale rete, oltre ai server locali è presente anche un Web server.



Dall'altro lato c'è la rete presso il provider servizi Internet. Per la connessione a tale rete, in linea di principio esistono due diverse possibilità normali:

- Se il Web server è molto frequentato, forse è opportuna una linea dedicata (connessione fissa) con il provider (per es. D64S con un canale B senza canale D). In questo caso, installare un secondo router presso l'ISP e configurare i due apparecchi per la connessione fissa utilizzata.
- Se non è necessaria una connessione fissa, è sufficiente anche un router nella propria rete locale. Affinché non vengano attribuiti addebiti all'ISP per la connessione al proprio Web server, impostare il router per la chiamata di risposta al provider.

Nella seconda possibilità, per ogni accesso al proprio sito Web vengono stabilite connessioni con l'ISP, che causano costi sul conto telefonico. Poiché questi addebiti non possono essere controllati (se non con l'impiego di budget addebiti, che in questo caso non hanno senso), in questo esempio si preferisce la prima variante.

La seguente tabella mostra l'assegnazione di tutti i dati importanti, come vengono utilizzati nell'esempio. Si raccomanda di creare una siffatta tabella per ogni applicazione.

Essa supporta il lavoro durante la configurazione, durante la ricerca difetti e in caso di richieste al supporto.

	Rete locale della Esempio SpA	Rete locale del provider
Indirizzo IP del router	194.168.166.123	
Maschera di rete IP del router	255.255.255.255	
Indirizzo intranet della LAN	10.100.100.0	
Indirizzo intranet del router	10.100.100.50	
Indirizzo intranet del Web server	10.100.100.99	
Maschera di rete intranet	255.255.255.0	
Nome della periferica	Esempio SpA	Provider



Connessione fissa: Quali impostazioni si effettuano nel router?

Le impostazioni dei due apparecchi sono molto simili. Partendo dall'impostazione del router della Esempio SpA vengono indicate le eventualmente differenze per il router del provider.

- ① Prima impostare il router nella tabella di interfaccia per l'impiego di una connessione fissa secondo D64S (campo di configurazione 'Gestione', registro 'Interfacce'):

```
cd Setup/WAN-module/Interface-list
set S0-1 GRP0 1
```

Il canale B utilizzato deve essere lo stesso in entrambi i router!

- ② Già con queste impostazioni i due router possono stabilire autonomamente una connessione, se sono collegati alla connessione fissa e attivati. In tale condizione essi utilizzano automaticamente il layer 'DEFAULT'.

Affinché la connessione fissa utilizzi un altro layer, creare un nuovo layer secondo le proprie esigenze nella lista layer e impostarlo nella lista layer (campo di configurazione 'Comunicazione', registro 'Generale') di entrambi gli apparecchi, per es. con protocollo 'PPP' e compressione:

```
cd Setup/WAN-module/Layer-list
set FVG0 TRANS PPP TRANS compr. HDLC64K
```

- ③ Una nuova voce nella lista dei nomi (campo di configurazione 'Comunicazione', registro 'Siti remoti') con la denominazione della controparte e il layer da utilizzare consente a uno dei router di stabilire la connessione con le corrette impostazioni. Non è necessario immettere un numero telefonico:

```
cd Setup/WAN-module/Name-list
set connessione fissa * 0 0 FVG0 Off
```

I tempi di attesa vengono impostati a '0', poiché altrimenti si possono verificare ritardi a causa di tentativi di stabilimento della connessione non necessari.

- ④ Nella lista canali si stabilisce quali canali devono essere utilizzati per la connessione fissa. L'indicazione dei canali e la loro sequenza deve essere impostata allo stesso modo sui due lati della connessione. Inoltre immettere qui (anche uguale su entrambi i lati della connessione) quanti canali eventualmente devono essere utilizzati per il backup (campo di configurazione 'Comunicazione', registro 'Siti remoti'):

```
cd Setup/WAN-module/Channel-list
set connessione fissa 1 1 1-1 0
```

- ⑤ Affinché i nomi della lista dei nomi dei router vengano trasmessi e riconosciuti, assegnare opportunamente il nome all'apparecchio (campo di configurazione 'Comunicazione', registro 'Generale'):

```
cd Setup
set Name Esempio SpA
```

- ⑥ Adesso rimangono da chiarire solo gli indirizzi IP. Affinché il router della Esempio SpA possa essere trovato nella propria rete TCP/IP, ha bisogno di un indirizzo IP libero di intranet. Esso lo riceve con l'immissione dell'indirizzo intranet con la rispettiva maschera di rete (campo di configurazione 'TCP/IP', registro 'Generale'). Inoltre esso riceve, come definito, l'indirizzo IP registrato incl. la maschera di rete. Affinché queste impostazioni diventino efficaci, attivare il modulo TCP/IP.

```
cd /Setup/TCP-IP-module
set IP-address 194.168.166.123
set IP-netmask 255.255.255.255
set Intranet address 10.100.100.50
set Intranet netmask 255.255.255.0
set operating on
```

L'altro router riceve analogamente un indirizzo IP fisso e (se si usa la mascheratura IP) un indirizzo intranet del gruppo di indirizzi del ISP.

- ⑦ Con l'immissione degli indirizzi IP il router della Esempio SpA è diventato in pratica una parte costituente di Internet, però i computer della LAN non possono ancora navigare. Per aprire Internet ai propri collaboratori, creare una voce nella tabella di routing (campo di configurazione 'TCP/IP', registro 'Routing'), mediante la quale tutti i pacchetti per indirizzi non raggiungibili localmente vengono instradati in Internet (rotta di DEFAULT).

```
cd Setup/IP-router-module
```

```
set IP-routing-table 255.255.255.255 0.0.0.0
connessione fissa 2 ON
```

La rotta con indirizzo IP '255.255.255.255' con maschera di rete '0.0.0.0' riceve tutti i pacchetti che non possono essere recapitati localmente. 'Provider' è la denominazione della controparte a cui devono essere inviati i corrispondenti dati. La controparte può essere raggiunta direttamente dal router della Esempio SpA, pertanto la distanza è posta a '2'. Con l'opzione 'ON' per la mascheratura IP tutti i computer della LAN vengono nascosti dietro l'indirizzo del router e non compaiono in Internet.

- ⑧ Anche il router del ISP deve ricevere una voce nella tabella di routing. Tale rotta contiene l'indirizzo IP registrato del router della Esempio SpA e il nome della controparte. Per questa rotta il 'Mascheratura IP' rimane disattivato, poiché in questa direzione si deve instradare e non mascherare.

```
cd Setup/IP-router-module
```

```
set IP-routing-table 194.168.166.123 255.255.255.255
Esempio SpA 2 Off
```

Poiché questo indirizzo IP si trova nel proprio gruppo di indirizzi del provider, la funzione 'Proxy-ARP' deve essere attivata:

```
cd /Setup/IP-router-module
```

```
set Proxy-ARP On
```

- ⑨ Il Web server diventa visibile in Internet tramite una voce nella tabella di servizio nell'apparecchio della Esempio SpA (campo di configurazione 'TCP/IP', registro 'Mascheratura'):

```
cd /Setup/IP-Router-module/Masquerading/Service-table
set 80 10.100.100.99
```

L'indicazione del valore '80' indica che il servizio visibile verso l'esterno è HTTP (WWW), l'indirizzo '10.100.100.99' seleziona come Web server il computer con questo speciale indirizzo intranet.

Una lista con ulteriori servizi si trova nel capitolo 'Porte TCP/IP'.

- ⑩ Adesso attivare il router IP (campo di configurazione 'TCP/IP', registro 'Routing'), e il router è pronto per WWW.

```
cd /Setup/IP-router-module
```

```
set operating on
```

- ⑪ Che cosa rimane da fare? Naturalmente anche i computer della LAN devono sapere che il router è il centralino per Internet. A questo scopo l'indirizzo intranet del router



viene indicato come gateway di default per le workstation. Inoltre viene notificato come server DNS l'indirizzo IP del corrispondente server del ISP.



Quando il router viene usato come server DHCP, queste impostazioni possono essere effettuate automaticamente (vedere 'Server DHCP').

Il provider di servizi Internet deve inoltre provvedere affinché il Web server venga immesso nel proprio server DNS con l'indirizzo IP registrato e il nome dei domini, per es. 'www.esempiospa.it'.

Il risultato

L'obiettivo delle impostazioni era la possibilità di scambio dati con Internet in due direzioni: Richieste dalla rete locale verso Internet e inversamente richieste da Internet verso il Web server della rete locale. Questo è stato realizzato:

■ Internet per i collaboratori:

Se uno dei collaboratori dalla sua workstation avvia un browser e immette un'indirizzo Web (per es. ELSA), tramite il server DNS registrato nel sistema operativo si tenta di determinare il rispettivo indirizzo IP. Il router in qualità di gateway Internet trasferisce questa richiesta al server DNS del ISP, che finalmente determina l'indirizzo IP per questo nome (per es. 168.192.156.100) e lo restituisce alla workstation tramite il router. Poiché questo indirizzo non si trova nella rete locale, esso invia in Internet tutti i pacchetti per questo indirizzo IP tramite la rotta di default.

■ Sito Web dell'azienda in Internet

Se un utente Internet in una qualunque parte del mondo avvia il proprio browser e immette l'indirizzo Web (per es. www.esempiospa.it), il suo computer riceve tramite il server DNS l'indirizzo IP del router dell'azienda (194.168.166.123). Successivamente il computer dell'utente Web può comunicare direttamente con il router con questo indirizzo IP. Il router converte automaticamente le richieste per la porta 80 (WWW) all'indirizzo intranet del Web server e quindi consente l'accesso al sito Web dell'azienda.

Naturalmente si possono offrire in Internet anche altri servizi come FTP e Gopher, ampliando in modo corrispondente la tabella di servizio. Con l'ausilio della tabella di servizio si può impostare liberamente se per i diversi servizi si deve usare uno o più server.

Accoppiamenti LAN-LAN

Se gli affari della Esempro SpA vanno proprio bene, può venire il momento di aprire una succursale o una filiale estera. Naturalmente anche la filiale avrà la propria rete locale e vorrà mantenersi aggiornata.

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

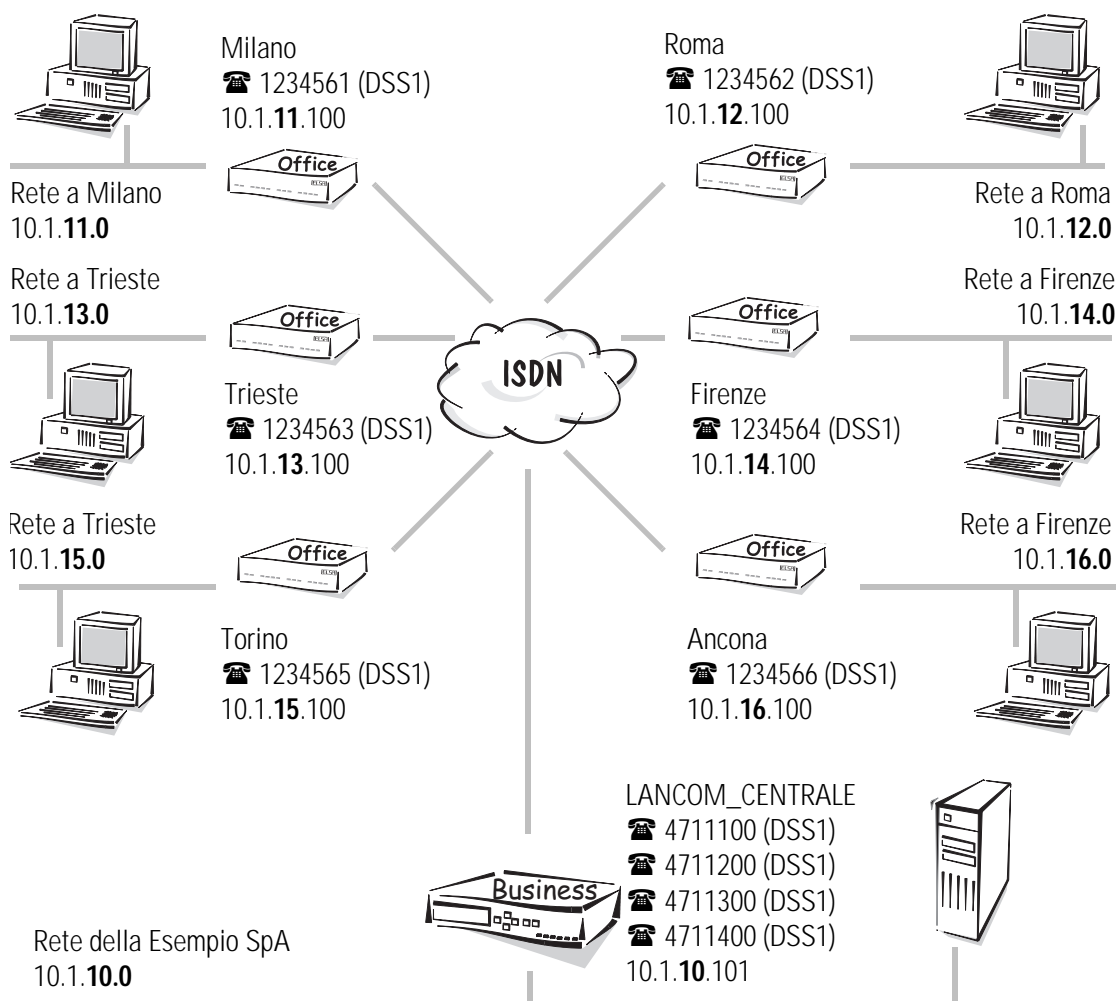
Connessione di reti con il router IP

La motivazione

Con il router IP si possono connettere reti che si basano sul protocollo di rete TCP/IP. A differenza dell'accesso a Internet tramite mascheratura IP ('Internet per tutti i PC della LAN'), nell'accoppiamento di reti tramite il router IP **tutti** gli indirizzi IP delle reti partecipanti diventano visibili nelle altre reti collegate, non solo quello del router.

Il caso preso come esempio

In questo caso la sede possiede sei filiali. In ciascuna delle filiali c'è un « piccolo » router, che viene collegato tramite linee a selezione ISDN a un *ELSA LANCOM Business* nella centrale.



La seguente tabella mostra l'assegnazione di nomi di apparecchi, indirizzi e numeri telefonici, come vengono utilizzati nell'esempio:

Rete	Esempio SpA	Milano	Roma	Trieste	Firenze	Torino	Ancona
Indirizzo IP della LAN	10.1.10.0	10.1.11.0	10.1.12.0	10.1.13.0	10.1.14.0	10.1.15.0	10.1.16.0
Indirizzi IP dei router	10.1.10.101	10.1.11.100	10.1.12.100	10.1.13.100	10.1.14.100	10.1.15.100	10.1.16.100
Maschera di rete IP	255.255.255.0						
Nome della periferica	Esempio_SpA	Milano	Roma	Trieste	Firenze	Torino	Ancona
Numeri telefonici	4711100 4711200 4711300 4711400	1234561	1234562	1234563	1234564	1234565	1234566



Routing IP molto semplice con *ELSA LANconfig* e i wizard

Per la configurazione dell'accoppiamento LAN è disponibile in *ELSA LANconfig* un wizard che si incarica di tutte le impostazioni del software necessarie e tiene conto di tutte le particolarità delle reti TCP/IP. Dopo aver avviato il wizard (automaticamente o con **Opzioni ► Settaggio assistito**), selezionare la voce 'Accoppiamento di due reti locali'. L'assistenza richiede brevemente i dati necessari – tra cui anche il protocollo di rete utilizzato – e poi fornisce informazioni su quello che rimane da impostare nelle workstation.

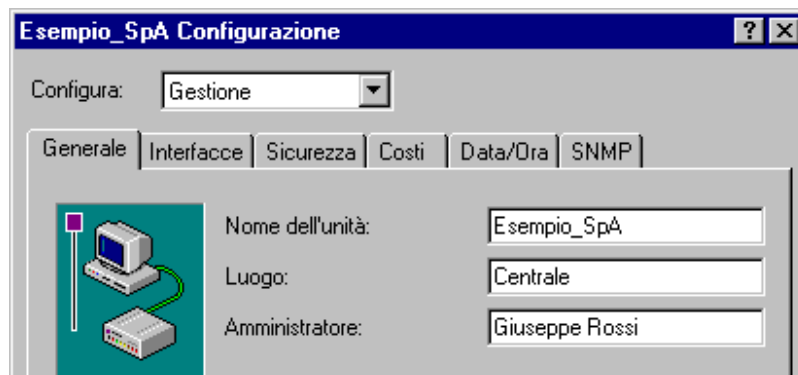
Poiché in questo esempio si vogliono accoppiare più reti, eseguire il wizard sul router della sede una volta per ciascuna delle reti da collegare. Il wizard viene utilizzato una volta anche in ciascuno dei router delle filiali.



Passo per passo: Quali impostazioni si effettuano nei router?

In linea di principio le impostazioni sono uguali per tutti i router. Nei seguenti passi di configurazione viene mostrato esattamente, a partire dal router della centrale, quello che deve essere impostato allo stesso modo, e vengono date informazioni sulle differenze negli altri router.

- ① Affinché i nomi utilizzati nella lista dei nomi vengano trasmessi e riconosciuti anche dai router, assegnare opportunamente il nome all'apparecchio (campo di configurazione 'Gestione', registro 'Generale'):

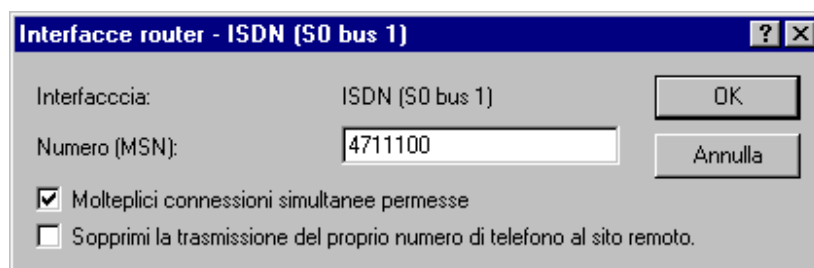


In caso di configurazione con altri ausili, il nome dell'apparecchio si imposta direttamente nel menu 'Setup':

```
set /Setup/Name Esempio_SpA
```

Gli apparecchi delle filiali ricevono corrispondentemente i nomi da 'Milano' a 'Ancona'.

- ② Poi immettere i **propri** numeri telefonici del router della sede (campo di configurazione 'Comunicazione', registro 'Generale'):



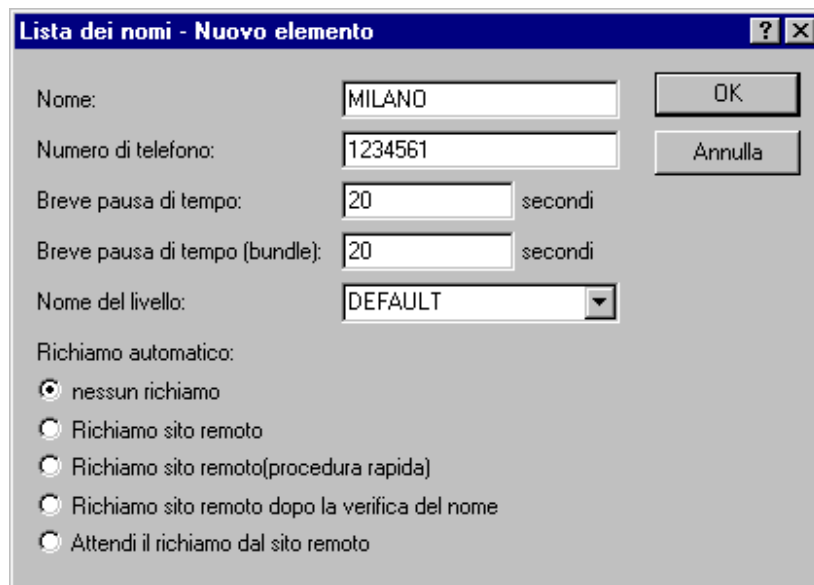
```
cd /Setup/WAN-module/Router-interface-list
```

```
set s0-1 4711100 On No
```

Le altre interfacce e apparecchi ricevono i loro numeri telefonici in modo corrispondente.

- ③ Nuove voci nella lista dei nomi (campo di configurazione 'Comunicazione', registro 'Siti remoti') con la denominazione della controparte e i rispettivi numeri telefonici, e la selezione di un layer presente in tutti i router (in questo caso per es. il layer predefinito DEFAULT) consentono al router della centrale di chiamare i router delle altre reti. Ciascuna connessione viene interrotta con i valori standard per i tempi di attesa B1 e B2, se per 20 secondi sulla linea non viene trasmesso nessun dato.

Ciascuna rete deve accollarsi i propri costi telefonici, pertanto la voce chiamata di risposta rimane su OFF:



Lista dei nomi - Nuovo elemento

Nome: MILANO OK

Numero di telefono: 1234561 Annulla

Breve pausa di tempo: 20 secondi

Breve pausa di tempo (bundle): 20 secondi

Nome del livello: DEFAULT

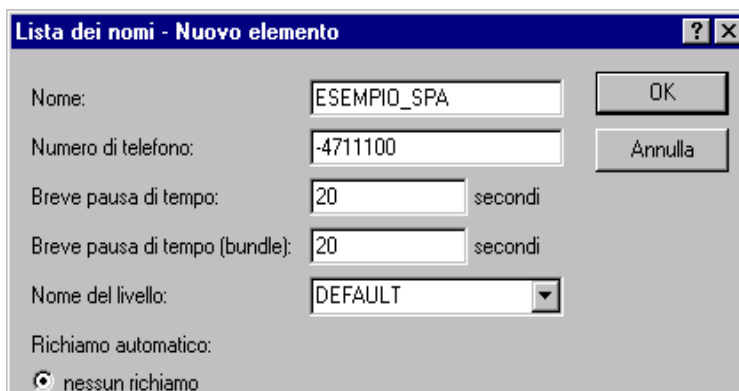
Richiamo automatico:

- ☒ nessun richiamo
- ☐ Richiamo sito remoto
- ☐ Richiamo sito remoto(procedura rapida)
- ☐ Richiamo sito remoto dopo la verifica del nome
- ☐ Attendi il richiamo dal sito remoto

```
cd /Setup/WAN-module/Name-list
```

```
set Milano 1234561 * * DEFAULT OFF
```

Gli altri apparecchi immettono solo il router 'Esempio_SpA' e il numero telefonico della corrispondente interfaccia. Il trattino prima del numero telefonico segnala che nella lista RoundRobin sono presenti altri numeri telefonici per questa rete.



Lista dei nomi - Nuovo elemento

Nome: ESEMPIO_SPA OK

Numero di telefono: -4711100 Annulla

Breve pausa di tempo: 20 secondi

Breve pausa di tempo (bundle): 20 secondi

Nome del livello: DEFAULT

Richiamo automatico:

- ☒ nessun richiamo

- ④ Con la lista RoundRobin si prosegue allo stesso modo. Nei router delle filiali si immettono i numeri telefonici delle altre interfacce del router della centrale, che non sono stati immessi in precedenza nella lista dei nomi.

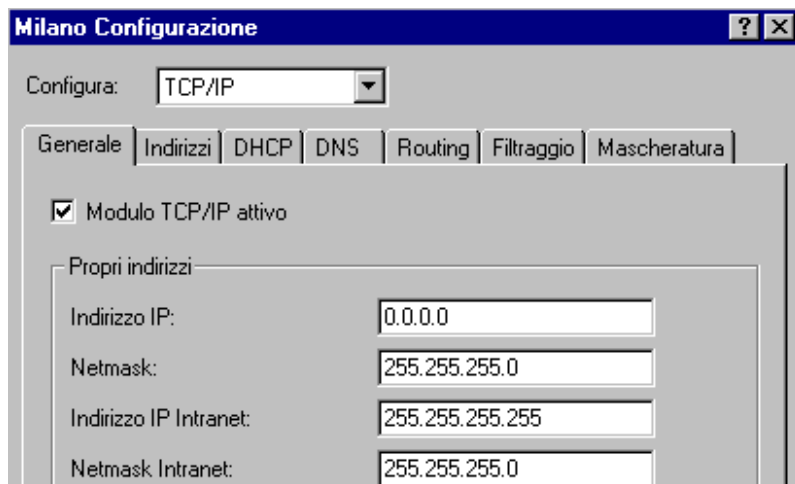
```
cd /Setup/WAN-module/RoundRobin-list
set Esempio_SpA 4711200 last
```

- ⑤ Se le connessioni verso le reti delle filiali devono usare solo determinati canali B, in modo da tenere liberi gli altri canali per es. per accessi a selezione tramite RAS, immettere nella lista canali del router della centrale per ciascuna controparte una voce che definisce i canali consentiti.

```
cd /Setup/WAN-module/Channel-list
set MILANO 1 2 2-1;2-2 0
```

- ⑥ Adesso rimangono da chiarire solo gli indirizzi. Affinché gli apparecchi vengano trovati nelle proprie reti TCP/IP, ciascuno ha bisogno di un indirizzo IP intranet libero. Essi lo ricevono con l'immissione dell'indirizzo intranet con la rispettiva maschera di

rete (campo di configurazione 'TCP/IP', registro 'Generale'). Affinché queste impostazioni diventino efficaci, attivare il modulo TCP/IP.



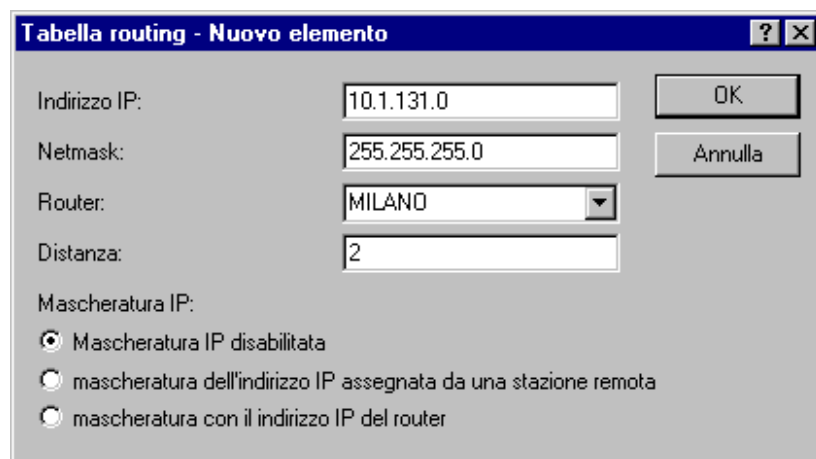
```
cd /Setup/TCP-IP-module/RoundRobin-list
```

```
set Intranet address 10.1.130.101
```

```
set Intranet netmask 255.255.255.0
```

I router delle filiali ricevono gli indirizzi IP da 10.131.1.100 a 10.136.1.100, tutti con la maschera di rete 255.255.255.0, come rappresentato in figura e nel sommario.

- ⑦ Quali indirizzi IP devono instradare i router verso quale destinazione? Nella tabella di routing del router della centrale si indicano gli indirizzi IP e le maschere di rete di tutte le filiali con le rispettive controparti (senza mascheratura IP!):



Alla fine attivare il router IP, e il primo *ELSA LANCOM* è pronto per la connessione con le altre reti.

```
cd /Setup/IP-router-module/IP-routing-table
```

```
set 10.1.131.0 255.255.255.0 Milano 2 Off
```

```
cd /Setup/IP-router-module
```

```
set operating on
```

Ciascuno dei router delle filiali riceve una voce per la sede. In questo modo tutte le connessioni delle filiali tra loro vengono instradate attraverso il router della sede.



Come alternativa le filiali possono anche comunicare direttamente tra loro. A questo scopo ricevono prima nella lista dei nomi le stesse voci come il router della sede. Inoltre esse ricevono nella tabella di routing le stesse voci come gli apparecchi della sede, dove la voce di routing per la propria rete viene rimpiazzata dalla voce per la rete della sede.

- ⑧ Che cosa rimane da fare? Naturalmente anche i computer della LAN devono sapere che il router è il centralino per le altre reti. A questo scopo l'indirizzo intranet del router viene indicato come gateway di default per le workstation e per i server.



Quando il router viene usato come server DHCP, queste impostazioni possono essere effettuate automaticamente (vedere 'Server DHCP').

Il risultato

Durante l'accesso di un computer di una filiale alla rete della sede esiste la possibilità di smistamento su un'altra interfaccia tramite la voce della lista round robin, se quella selezionata per prima è occupata.

Connessione di reti con il router IPX

La motivazione

Con il router IPX si possono connettere reti che si basano sul protocollo di rete IPX/SPX. Per es. si può collegare la sede di un'azienda con le reti di più filiali.

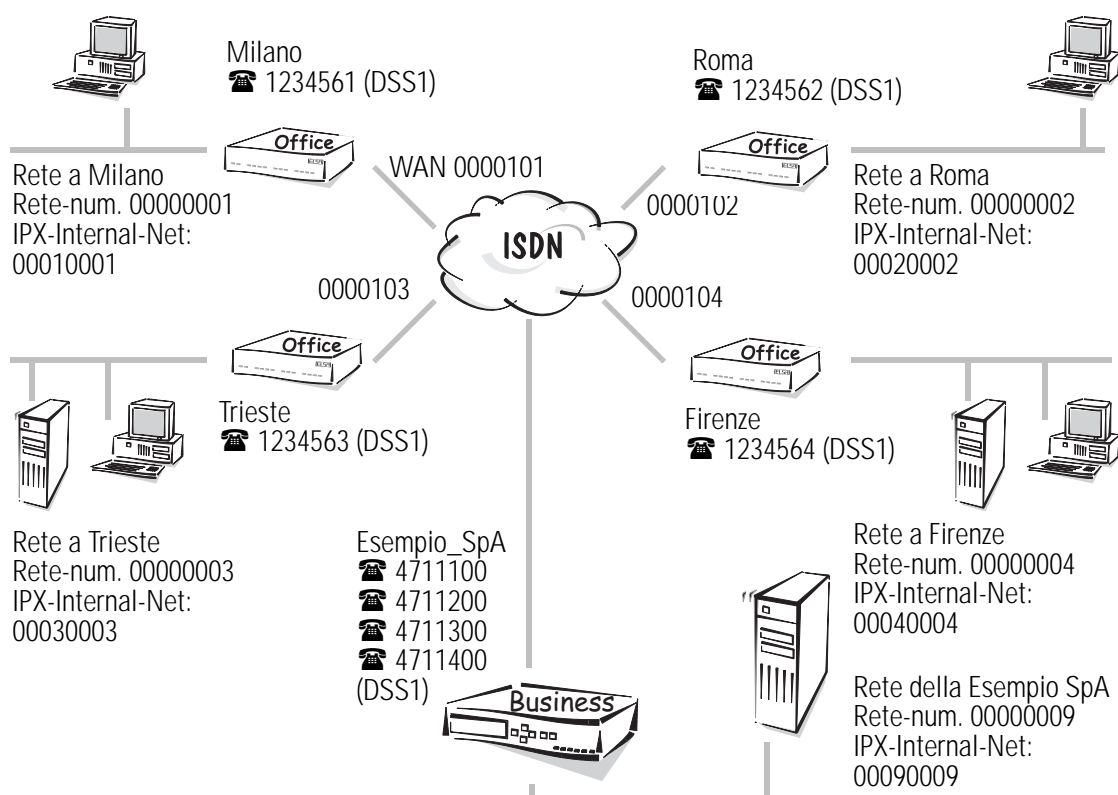
Il caso preso come esempio

In questo caso la sede centrale possiede quattro filiali. In ciascuna delle filiali c'è un « piccolo » router, che viene collegato tramite linee a selezione ISDN a un *ELSA LANCOM Business* nella centrale.

La seguente tabella mostra l'assegnazione di nomi di apparecchi, indirizzi e numeri telefonici, come vengono utilizzati nell'esempio:

Rete	LAN della Esempio SpA	LAN Milano	LAN Roma	LAN Trieste	LAN Firenze
Indirizzo di rete	00000009	00000001	00000002	00000003	00000004
IPX-Internal-Net	00090009	00010001	00020002	00030003	00040004
Binding	802.3	SNAP	SNAP	802.3	802.3

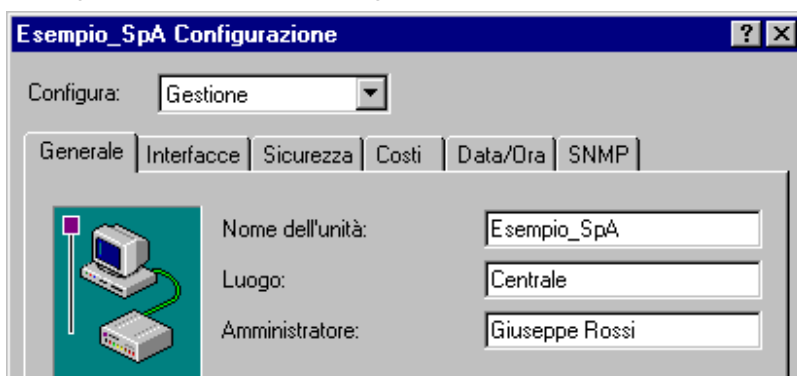
Nome della periferica	Esempio_SpA	Milano	Roma	Trieste	Firenze
Dialup-remote	4711100 4711200 4711300 4711400	1234561	1234562	1234563	1234564
Reti WAN		00000101	00000102	00000103	00000104



Passo per passo: Quali impostazioni si effettuano nei router?

Nei seguenti passi di configurazione vengono mostrate esattamente le impostazioni a partire dal router della centrale, e vengono date informazioni sulle differenze negli altri router.

- ① Affinché i nomi utilizzati nella lista dei nomi vengano trasmessi e riconosciuti anche dai router, assegnare opportunamente il nome all'apparecchio (campo di configurazione 'Gestione', registro 'Generale'):



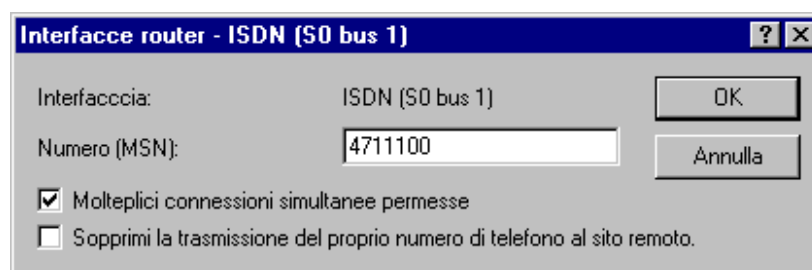
In caso di configurazione con altri ausili, il nome dell'apparecchio si imposta direttamente nel menu 'Setup':

```
cd Setup
```

```
set Name Esempio_SpA
```

I router delle filiali ricevono corrispondentemente i nomi 'Milano', 'Roma', 'Trieste' e 'Firenze'.

- ② Poi immettere il **proprio** numero telefonico del router della centrale (campo di configurazione 'Comunicazione', registro 'Generale'):



```
cd setup/WAN-module/Router-interface-list
```

```
S0-1 4711100
```

```
S0-2 4711200
```

```
S0-3 4711300
```

```
S0-4 4711400
```

Gli altri apparecchi ricevono in modo corrispondente i propri numeri telefonici (1234561, 1234562, 1234563 e 1234564).

- ③ Nuove voci nella lista dei nomi (campo di configurazione 'Comunicazione', registro 'Siti remoti') con la denominazione della controparte e i rispettivi numeri telefonici, e la selezione di un layer presente in tutti i router (in questo caso per es. il layer predefinito DEFAULT) consentono al router della centrale di chiamare i router delle

altre reti delle filiali. Ciascuna rete deve accollarsi i propri costi telefonici, pertanto la voce chiamata di risposta rimane su OFF:

```
cd Setup/WAN-module/Name-list
set Milano 1234561 * * DEFAULT OFF
set Roma 1234562 * * DEFAULT OFF
set Trieste 1234563 * * DEFAULT OFF
set Firenze 1234564 * * DEFAULT OFF
```

I router delle filiali immettono solo il router 'Esempio_SpA' e il numero telefonico di una delle interfacce del router della centrale.

- ④ Adesso rimangono da chiarire solo gli indirizzi. Affinché il router possa distinguere la propria LAN dalle altre LAN e dalla WAN, immettere l'indirizzo di rete e il binding per la rete della Esempio SpA (campo di configurazione 'IPX', registro 'Generale'):

```
Setup/IPX-module/LAN-config
set Network 00000009
set Binding 802.3
```



La rete della sede centrale ha un server. Se non si conosce il numero di rete, questo può essere determinato automaticamente impostando '00000000' come numero di rete. Anche il binding può essere determinato automaticamente. Poiché il router seleziona sempre la rete in cui viene scambiata la maggior parte delle informazioni RIP/SAP, questa procedura è conveniente per es. quando solo una rete logica viene utilizzata sul circuito Ethernet.

Anche per gli apparecchi delle filiali di Trieste e Firenze immettere i rispettivi indirizzi di rete con il binding 'Auto'.

```
cd /Setup/IPX-module/LAN-config
set network 00000003 oppure 00000004
set binding Auto
```

Per le reti delle filiali di Milano e di Roma si deve sempre indicare esplicitamente il binding, per es. 'SNAP', e il numero di rete, poiché in tali reti non c'è un server:

```
cd /Setup/IPX-module/LAN-config
set network 00000001 and 00000002
set Binding SNAP
```

- ⑤ Verso quale destinazione devono instradare gli apparecchi? Nella tabella di routing (campo di configurazione 'IPX', registro 'Routing') indicare le controparti con un **proprio** indirizzo di rete per la WAN (non delle altre LAN!) . Per il router della rete della centrale le voci della tabella si presentano così:

```
cd /Setup/IPX-module/WAN-config/Routing-table
set Milano 00000101 802.3 Route Off
set Roma 00000102 802.3 Route Off
set Trieste 00000103 802.3 Route On
set Firenze 00000104 802.3 Route On
```

Oltre al nome di periferica del router della rete della controparte, ciascuna voce della tabella di routing riceve un proprio indirizzo WAN. Indirizzo di rete della WAN su cui viene utilizzato il binding '802.3'. Poiché, visto dalla rete della centrale, per le controparti a Trieste e a Firenze è presente un server, viene attivato il meccanismo 'exponential backoff'.



Ulteriori informazioni sulla funzione del meccanismo 'exponential backoff' si possono trovare in 'Exponential backoff'.

Per la rete della filiale di Milano per es. la voce si presenta così:

```
cd /Setup/IPX-module/WAN-config/Routing-table
set Esempio_SpA 00000101 802.3 Route On
```

L'indirizzo di rete della WAN coincide sempre con la voce per la rete della filiale nel router della centrale. Come binding sulla WAN viene sempre utilizzato '802.3'. Poiché, visto dalle reti delle filiali, per la controparte è sempre presente un server, viene attivato il meccanismo 'exponential backoff'.

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 il router 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.

Accesso remoto con TCP/IP

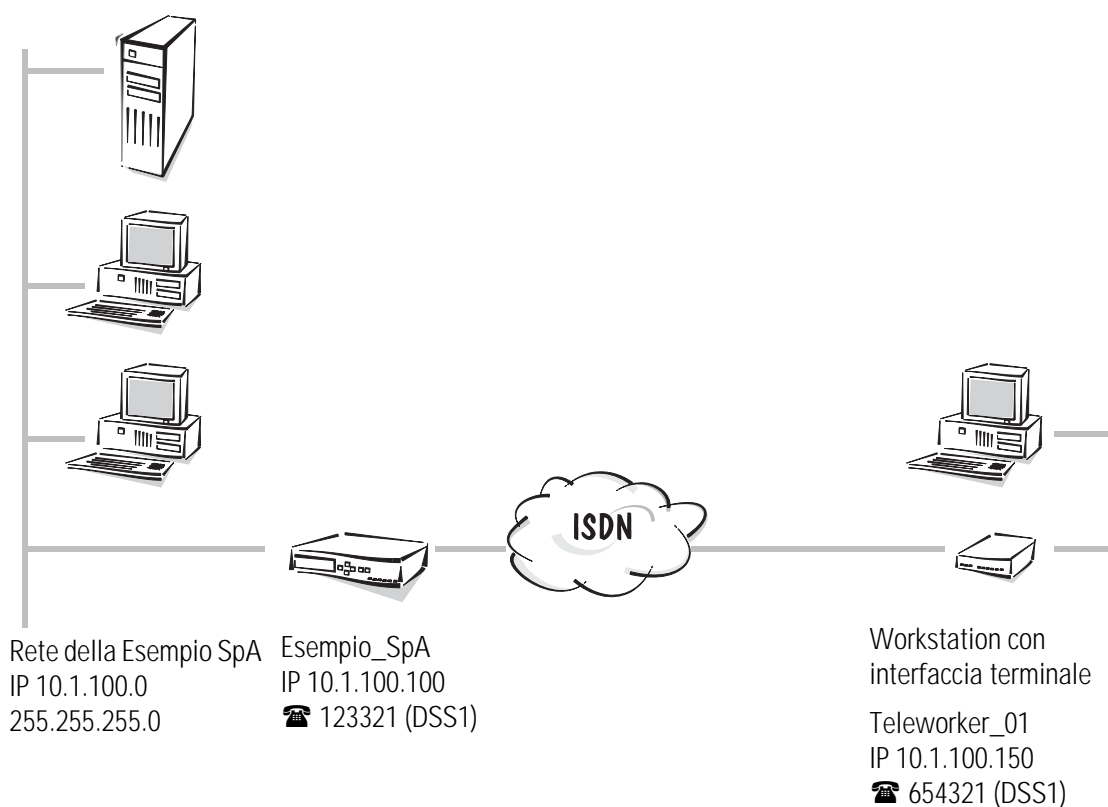
La motivazione

Un'azienda occupa alcuni collaboratori che non sono presenti in azienda ogni giorno, ma svolgono un servizio esterno o sono telelavoratori. Comunque, dal loro computer essi devono avere accesso alla rete locale (intranet) dell'azienda, in modo da poter scambiare dati e informazioni (per es. posta elettronica). Come protocollo per la trasmissione dati si usa PPP, poiché questo è gestito da tutte le normali periferiche e sistemi operativi. Per ridurre l'impegno nella gestione degli accessi a selezione, gli indirizzi IP vengono assegnati tramite IP Pooling.

Il caso preso come esempio

I collaboratori che partecipano all'accesso remoto hanno a casa una workstation con un'interfaccia ISDN o una scheda ISDN. Alcuni collaboratori in servizio esterno possono anche selezionare la rete aziendale con un Notebook tramite telefono mobile GSM.

Sui computer remoti è installato un client PPP, in questo caso l'Accesso remoto di Windows con il protocollo TCP/IP. Affinché i lavoratori in servizio esterno possano accedere alle reti Windows anche con abilitazione di file e stampanti, deve essere anche supportato il routing di pacchetti NetBIOS. Nella LAN dell'azienda c'è un *ELSA LANCOM Business*, che in caso di necessità può richiamare la workstation.



Accesso remoto molto semplice con *ELSA LANconfig* e i wizard

Per la configurazione degli accessi a selezione è disponibile in *ELSA LANconfig* un wizard che si incarica di tutte le impostazioni del software necessarie e tiene conto di tutte le particolarità delle reti TCP/IP. Dopo aver avviato l'assistenza (automaticamente o con **Opzioni ► Settaggio assistito**), selezionare la voce 'Impostazione accesso a selezione (RAS)'. Il wizard richiede brevemente i dati necessari, tra cui anche il protocollo di rete utilizzato.



Passo per passo: Quali impostazioni si effettuano nel router?

- ① Prima immettere nella tabella di interfaccia router il **proprio** numero telefonico per le chiamate in arrivo e in uscita (campo di configurazione 'Comunicazione', registro 'Generale'):

```
cd /Setup/WAN-module/Router-interface-list
set S0-1 123321 ON
```

Quando si immettono più numeri telefonici, per le chiamate in uscita viene utilizzato il primo numero.



In questo caso viene attivata l'opzione 'Connessione Y', in modo che siano possibili anche connessioni contemporanee con due diversi telelavoratori.

- ② L'accesso remoto deve essere anche possibile senza controllo dei numeri telefonici in arrivo, poiché i collaboratori in servizio esterno talvolta chiedono di accedere alla

rete aziendale da località diverse. Pertanto non si può realizzare l'assegnazione di un layer con impiego del PPP con riconoscimento del numero telefonico. Controllare i valori del layer di 'DEFAULT', ed eventualmente impostare tale layer sui valori richiesti:

```
cd /Setup/WAN-module/Layer-list
set DEFAULT trans PPP trans none HDLC64K
```

In questo modo, qualunque chiamante che non può essere assegnato tramite la lista dei numeri viene accolto immediatamente con una negoziazione PPP.

Se il router riscontra che la controparte chiama tramite GSM, vengono utilizzate automaticamente le impostazioni di protocollo `Trans APPP Trans nessun v.110 9600`, per consentire lo stabilimento della connessione.

- ③ Per la chiamata di risposta verso telefoni mobili GSM dopo è necessario un layer impostato sulla connessione tramite il protocollo V.110:

```
cd /Setup/WAN-module/Layer-list
set RAS_GSM Trans APPP Trans none 0 comp. V.110 9600
```

- ④ La voce nella lista dei nomi per ciascuna controparte RAS con la denominazione della controparte, il layer ('DEFAULT' o 'RAS_GSM') e l'opzione di chiamata di risposta 'Nome' consente a *ELSA LANCOM* di richiamare il computer del collaboratore in servizio esterno. In tale circostanza è obbligata la negoziazione di protocollo tramite PPP, il numero telefonico per la chiamata di risposta rimane libero nella lista dei nomi e può essere definito dallo stesso collaboratore in servizio esterno. Se un lavoratore in servizio esterno chiama in alternativa tramite ISDN e GSM, per tale collaboratore si devono creare due voci nella lista dei nomi.

```
cd /Setup/WAN-module/Name-list
set Tele_01_ISDN * * * DEFAULT Name
set Tele_01_GSM * * * RAS_GSM Name
set Tele_02 * * * DEFAULT Name
```

- ⑤ Nella lista canali si può definire quanti canali devono essere utilizzati per un accesso a selezione e come opzione i canali da usare. In caso di accesso tramite ISDN deve essere consentito il raggruppamento di due canali. In caso di selezione GSM è disponibile solo un canale su un'altra interfaccia:

```
cd Setup/WAN-module/Channel-list
set Tele_01_ISDN 1 2 1-1;1-2 0
set Tele_01_GSM 1 1 2-1 0
set Tele_02 1 2 1-1;1-2 0
```

- ⑥ Poiché per l'accesso dei computer remoti si utilizza il PPP, si può definire nella lista PPP il nome utente (per es. Campione) e la password (per es. remote) per la

controparte 'Teleworker_01'. Come procedura di sicurezza si utilizza il PAP e si consente il routing di pacchetti IP e NetBIOS tramite tale connessione:

```
cd /Setup/WAN-module/PPP-list  
Tele_01_ISDN PAP Remote 0 0 Tele_01 IP+NTB  
Tele_01_GSM PAP Remote 0 0 Tele_01 IP+NTB
```

Come nome utente si può assegnare lo stesso valore anche alle due voci per ISDN e GSM. Quindi il corrispondente collaboratore si può presentare sempre con lo stesso nome. Dopo l'immissione, la password « Remote » viene rimpiazzata da un *!



Notare che nel nome utente e nella password vengono distinti i caratteri maiuscoli e minuscoli.

- ⑦ Per il routing dei pacchetti NetBIOS è necessaria anche una voce nella tabella NetBIOS. Con questa si comunica al router che con tale controparte possono essere scambiate informazioni NetBIOS e che si tratta di una singola workstation, che quindi non deve essere chiamata direttamente:

```
cd /Setup/NetBIOS-module/Remote-table  
Tele_01_ISDN Workstation  
Tele_01_GSM Workstation
```

- ⑧ Adesso rimangono da chiarire solo gli indirizzi. Affinché il router possa essere trovato nella propria rete TCP/IP, ha bisogno di un indirizzo IP libero della rete aziendale. Esso lo riceve con l'immissione dell'indirizzo intranet con la rispettiva maschera di rete:

```
cd /Setup/TCP-IP-module  
set Intranet address 10.1.100.100  
set Intranet netmask 255.255.255.0
```

- ⑨ E l'indirizzo IP del computer chiamante? Questo viene assegnato in modo dinamico da un pool di indirizzo IP per la durata della connessione. A questo si definisce solo l'inizio e la fine del gruppo di indirizzi. Pertanto la voce nella tabella di routing IP diventa superflua:

```
cd /Setup/IP-router-module  
set Start-WAN-Pool 10.1.100.110  
set End-WAN-Pool 10.1.100.120
```

- ⑩ Affinché il router possa instradare i dati per un computer remoto con un indirizzo della propria rete logica, deve essere attivato il proxy ARP.

```
cd /Setup/IP-router-module  
set Proxy-ARP On
```

- ⑪ Adesso attivare il router IP, e il router è pronto per la selezione di collaboratori in servizio esterno.

```
cd /Setup/IP-router-module  
set operating on
```

- ⑫ Che cosa rimane da fare? La workstation del collaboratore in servizio esterno deve essere ancora impostata in modo che anche da parte sua sia possibile l'accesso alla rete aziendale. A questo scopo sono necessarie le seguenti impostazioni, che vengono presentate qui solo in breve:

- Accesso remoto correttamente impostato
- TCP/IP installato e collegato all'interfaccia di accesso remoto
- Nuova connessione di accesso remoto con il numero telefonico del router
- Interfaccia terminale o scheda ISDN impostati su PPPHDLC
- PPP selezionato come tipo di server di accesso remoto, 'Attivazione compressione software' e 'Richiesta identificativo codificato' disattivati
- TCP/IP selezionato come protocollo di rete
- Assegnazione di indirizzo IP e di indirizzo server nomi attivata, 'Compressione intestazione IP' disattivata

Che cosa si è ottenuto?

Il collaboratore sulla workstation remota ora può stabilire la connessione con la rete aziendale tramite Accesso remoto. In tale circostanza egli indica il nome utente definito nella lista PPP e la rispettiva password.

Successivamente egli può accedere ai server e alle reti Windows della rete TCP/IP. Questi Server possono essere trovati per es. con tre clic su **Avvio ► Trova ► Computer** nella barra di avvio Windows.

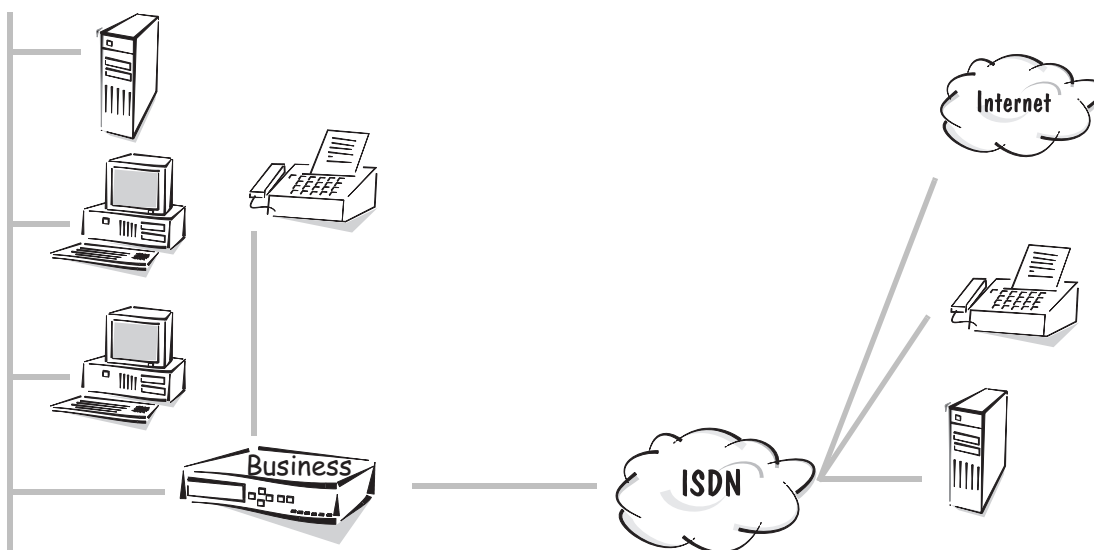
Least-cost router

In questo capitolo viene mostrato sulla base di un esempio come si possono risparmiare molti addebiti utilizzando il Least-cost router.

Dopo l'impostazione, ogni volta che si stabilisce una comunicazione il least-cost router cerca automaticamente il provider con le condizioni più favorevoli e tenta di stabilire la connessione tramite tale rete.

Esempio:

Come esempio viene considerato qui un piccolo studio di ingegneria (una sede distaccata di un ufficio di pianificazione più grande) con due posti di lavoro. Entrambi i posti di lavoro hanno un telefono, inoltre c'è un apparecchio fax e una segreteria telefonica.



I due collaboratori di questo ufficio utilizzano le seguenti funzioni di *ELSA LANCOM Business*:

- L'accesso a Internet tramite un provider configurato in un lampo con *ELSA LANconfig* e la sua assistenza. Per questo si utilizza il router IP.
- Lo scambio dati con la centrale avviene tramite un accoppiamento LAN-LAN con le funzioni del router IPX.
- Per spedire i messaggi fax direttamente dal PC viene utilizzato *ELSA-RVS-COM* tramite la *LANCAPI*.

Naturalmente l'ufficio preso come esempio in questo capitolo vorrebbe anche realizzare le sue connessioni per l'invio di fax, per l'accesso a Internet e per lo scambio dati con la sede centrale nel modo più conveniente possibile. A questo scopo si utilizza il least-cost router, che cerca automaticamente ad ogni selezione la connessione più conveniente. Le informazioni sulle tariffe applicate si ottengono per es. da giornali, da opuscoli o da Internet.

L'ufficio preso come esempio si trova ad Milano ed ha una connessione telefonica della Telecom Italia. Le seguenti voci per il least-cost router vengono impostate in base a queste circostanze locali e alle informazioni fornite da Internet su zone e tariffe.



Si noti che tali voci non possono assolutamente essere trasferite ad altre situazioni, esse servono solo come esempio.



Impostazione del least-cost router con *ELSA LANconfig*

Con i seguenti passi si rende il *ELSA LANCOM Business* attento ai prezzi:

- ① Aprire la configurazione dell'apparecchio in *ELSA LANconfig* facendo doppio clic sulla voce nella lista delle periferiche, e passare nel campo di configurazione 'Least-cost router'.
- ② Attivare nella scheda di registro 'Generale' la funzione del LCR per tutte le modalità presentate. Poiché l'ufficio non richiede un monitoraggio addebiti, l'impiego del LCR anche per i moduli router non è critico.
- ③ Modificare la tabella dei giorni festivi sulla scheda di registro 'Orari e festività nazionali'.
 - Immettere prima i giorni festivi che si ripetono ogni anno indicando giorno e mese, ma senza anno. Queste voci vengono impostate automaticamente per ogni anno.
 - Poi immettere i giorni festivi variabili indicando giorno e mese e anno, possibilmente per i prossimi due, tre anni.
- ④ Poi si entra nel cuore della faccenda: Le voci della tabella LCR. Per alcune voci ci sono più numero identificativi di rete. Questi vengono selezionati in successione se i numeri precedenti sono occupati. Affinché venga stabilita sempre in breve tempo una connessione, per tutte le voci viene attivato il trasferimento automatico alla propria società telefonica (in questo caso la Telecom Italia).
- ⑤ Prima si considerano le chiamate interurbane. Con questa voce si inoltrano tutte le chiamate interurbane a un altro provider, in base all'ora:

Prefisso	Numero identificativo di rete Call-by-Call	Giorni	Ora	Trasferimento
0	1055	Lu-Ve	0:00–1:59	Sì
0	1088	Lu-Ve	2:00–4:59	Sì
0	1073	Lu-Ve	5:00–7:59	Sì
0	1077	Lu-Ve	8:00–8:59	Sì
0	1055	Lu-Ve	9:00–17:59	Sì
0	1055	Lu-Ve	18:00–23:59	Sì

Prefisso	Numero identificativo di rete Call-by-Call	Giorni	Ora	Trasferimento
0	1073	Sa, Do, giorni festivi	0:00–7:59	Sì
0	1055	Sa, Do, giorni festivi	8:00–8:59	Sì
0	1077;1088	Sa, Do, giorni festivi	8:00–20:59	Sì
0	1088	Sa, Do, giorni festivi	21:00–23:59	Sì

- ⑥ Le chiamate internazionali sono relativamente rare. Pertanto in questo esempio viene considerata valida solo una voce per tutte le chiamate internazionali:

Prefisso	Numero identificativo di rete Call-by-Call	Giorni	Ora	Trasferimento
00	1073;1077	tutti i giorni	0:00–23:59	Sì

- ⑦ Alcune reti urbane in vicinanza della sede possono essere raggiunte con un prefisso, ma con tariffa urbana. Queste non devono essere inoltrate come le altre chiamate interurbane, e quindi vengono « recuperate » abilitando il loro numero identificativo di rete. L'ufficio preso come esempio si trova ad Milano. I collaboratori hanno appreso da Internet quali reti urbane rientrano ancora nella zona vicina, e pertanto si aggiungono le seguenti voci:

Prefisso	Numero identificativo di rete Call-by-Call	Giorni	Ora	Trasferimento
0240		tutti i giorni	0:00–23:59	Sì
0246		tutti i giorni	0:00–23:59	Sì
0241		tutti i giorni	0:00–23:59	Sì
0242		tutti i giorni	0:00–23:59	Sì
0243		tutti i giorni	0:00–23:59	Sì
0245		tutti i giorni	0:00–23:59	Sì
0244		tutti i giorni	0:00–23:59	Sì
0232		tutti i giorni	0:00–23:59	Sì
0231		tutti i giorni	0:00–23:59	Sì
0238		tutti i giorni	0:00–23:59	Sì
0239		tutti i giorni	0:00–23:59	Sì
0257		tutti i giorni	0:00–23:59	Sì

Prefisso	Numero identificativo di rete Call-by-Call	Giorni	Ora	Trasferimento
0258		tutti i giorni	0:00–23:59	Sì
0287		tutti i giorni	0:00–23:59	Sì
0288		tutti i giorni	0:00–23:59	Sì
0289		tutti i giorni	0:00–23:59	Sì
0271		tutti i giorni	0:00–23:59	Sì
0273		tutti i giorni	0:00–23:59	Sì

Una volta creata la prima voce, la si può semplicemente copiare e poi cambiare ogni volta solo il prefisso.

- ⑧ Anche alcuni speciali numeri telefonici possono essere sottratti all'inoltro, per es. i '0130', '0180', '0190' e '0800':

Prefisso	Numero identificativo di rete Call-by-Call	Giorni	Ora	Trasferimento
01		tutti i giorni	0:00–23:59	Sì
0800		tutti i giorni	0:00–23:59	Sì

- ⑨ Finito! In questo modo il least-cost router è stato impostato con grande precisione. Inizialmente controllare il funzionamento del LCR con *ELSA LANmonitor*, e alla fine del mese dare un'occhiata al conto telefonico. Eventualmente con l'ausilio del sommario delle telefonate di può trovare qualche altro prefisso da immettere nella tabella LCR.



Least-cost router passo per passo

Se non si può utilizzare il tool di configurazione *ELSA LANconfig*, lo stesso risultato si ottiene eseguendo l'impostazione tramite Telnet (o un emulatore di terminale) con i seguenti comandi:

Menu	Parametro	Nota o valore
Setup/LCR module	Uso del router	Attivazione del modulo LCR per le singole modalità.
	Uso della LANCAPI	
	Esempio	'set router on' 'set lanapi on' 'set ab-port on'
Setup/LCR-module/ tabella tempi	Indice	Indice corrente per i voci della tabella.
	Prefisso	Prefisso che deve essere inoltrato.

Menu	Parametro	Nota o valore
	Giorni	Validità della voce per giorni feriali e festivi rappresentata con una maschera a 8-bit: Il bit 0 rappresenta il Lunedì, il bit 7 i giorni festivi. Quindi la voce '31' rappresenta tutti i giorni feriali, '192' le domeniche e i giorni festivi.
	Inizio	Ora di inizio della validità della voce nei giorni definiti.
	Fine	Ora finale della validità della voce nei giorni definiti.
	Lista dei numeri	Numero identificativo di rete del provider Call-by-Call.
	Trasferimento	Trasferimento automatico alla propria società telefonica, se tutti i numeri Call-by-Call sono occupati.
	Esempio	'set 1 02 31 1:00 11:59 01030;01090;01070 On' inoltra tutte le conversazioni interurbane nella regione '02' tra l'una e le dodici al provider con numero identificativo di rete '01030'. Se questo è occupato, si tenta con i numeri identificativi di rete '01090' e '01070'. Se anche questi non sono disponibili, la connessione viene stabilita tramite la normale società telefonica.

Creare tutte le voci necessarie seguendo questo campione, e orientarsi sulle tabelle dell'impostazione tramite *ELSA LANconfig*.

Appendice

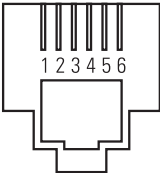
In questa appendice, oltre ai dati tecnici si trovano tra l'altro i collegamenti dei connettori, e le condizioni generali di garanzia.

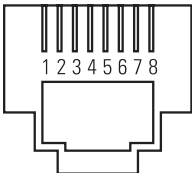
Dati tecnici

Modalità di funzionamento:	Router IP, router IPX, server CAPI, server DHCP; Least Cost Router per connessioni router e CAPI, possibile funzionamento contemporaneo di tutte le modalità di funzionamento
Connessione LAN:	Ethernet IEEE 802.3, 10/100Base-TX (RJ45, Node/Hub, Switch), auto-sense, funzionamento Full-Duplex
Protocolli di rete:	Router IP: IP, TCP, ICMP, ARP, RIP-1, RIP-2, PROXY ARP, DHCP Router IPX: RIP, SAP, Novell NetBIOS, Novell-Burst-Mode
Possibilità di filtro:	Router IP: filtraggio di porta TCP, UDP, filtro di rete sorgente e di rete destinazione Router IPX: RIP, SAP, watchdog IPX e SPX, sockets, propagated packets
Spoofing:	Router IPX: RIP e SAP packets; Watchdog IPX e SPX, Novell NetBIOS, keep-alive-packets
Interfaccia ISDN:	Connessione: Bus ISDN-S0, configurazione punto-a-punto e punto-a-più punti, I.430 canale D: 1TR6, Euro-ISDN (DSS1), auto-sense, connessioni fisse gruppo 0 (D64S, D64S2, D64SY) canale B: PPP (asinc./sinc.), MLPPP, X.75, HDLC, V.110, CAPI 2.0 tramite ELSA LANCAPI, compressione dati Stac
Server CAPI:	CAPI 2.0 virtuale per sistemi operativi Windows, driver NDIS-WAN, Standard 1
Controllo di linea:	Chiamata di risposta automatica con o senza stabilimento della connessione; line-on-demand (raggruppamento di canali dinamico), short-hold-modus, selezione RoundRobin, fast call back, dial backup per connessione fisse
Protezione addebiti:	Possibilità di definire il numero max. di unità a pagamento in un intervallo di tempo prestabilito
Funzioni security e firewall:	Valutazione del numero d'utenza della controparte; PAP e CHAP, meccanismi di autenticazione in PPP; chiamata di risposta Firewall automatica tramite CLIP, PPP o protocollo ELSA; possibilità di filtro in modalità IP, IPX e Bridge; protezione della configurazione tramite liste di accesso e password, registrazione delle ultime informazioni sulla connessione, mascheratura IP, codifica in preparazione
Mascheratura IP:	(NAT/PAT) conversione di indirizzo IP e di porta tramite un indirizzo IP, assegnazione statica/dinamica degli indirizzi IP tramite PPP, mascheratura di TCP, UDP, ICMP, FTP; DNS forwarding; mascheratura inversa per servizi IP da Intranet
Management:	Via LAN, ISDN (telemanutenzione) o V.24, software di management ELSA LANconfig e ELSA LANmonitor per Windows, configurazione tramite SNMP v.1, TFTP, possibile Telnet o terminale
Sicurezza di esercizio:	Watchdog hardware, autotest regolari, concetto FirmSafe per aggiornamento remoto del software

Statistiche:	Contatori di pacchetti LAN e WAN, contatori di errori, connessioni, tempo e addebiti
Display/comando:	Display LCD e tastiera, LED di stato LAN e WAN
Alimentazione elettrica:	12 V c.a. con alimentatore a spina per 230 V, 12 VA
Condizioni ambiente:	Temperatura: 5..40°C, umidità dell'aria: 0..80%, senza condensa
Costruzione e dimensioni:	Robusto involucro metallico, connessioni sul lato posteriore; dimensioni 230 x 38 x 228 mm (L x H x P)
Materiale fornito:	Accessori: Alimentatore, cavo di connessione ISDN, cavo per interfaccia outband, cavo twisted-pair (CAT-5), documentazione dettagliata e CD-ROM <i>ELSA LANCOM</i> Software: <i>ELSA LANconfig</i> , <i>ELSA LANmonitor</i> , <i>ELSA LANCAPI</i> , client TFTP, software di comunicazione per uffici <i>ELSA-RVS-COM</i> , emulatore di terminale <i>ELSA-ZOC</i> , software per telemanutenzione LapLink per Windows, T-Online, CompuServe
Autorizzazioni:	Per Germania, Svizzera e tutti i paesi EU in preparazione
Servizio e garanzia:	Garanzia di 6 anni
Supporto:	Tramite hotline e Internet

Collegamenti dei connettori

Connettore	RJ11-Pin	Linea
 porte a/b – RJ11	1	libero
	2	libero
	3	a
	4	b
	5	libero
	6	libero

Connettore	RJ45-Pin	Linea	IAE
 ISDN – RJ45	1	libero	libero
	2	libero	libero
	3	T+	2a
	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	libero	libero
	8	libero	libero

Condizioni generali di garanzia dal 01.06.1998

La ELSA AG fornisce questa garanzia 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'eventualmente 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 a colori 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 Svolgimento

- 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 di andata e ritorno fino 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 e 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 utilizzo

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.

Dichiarazione 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 Business
Product Name:	
EG-Baumusterprüfbescheinigungs Nr.: D801080L	
Registration No.:	
Benannte Stelle:	CETECOM ICT Services GmbH
Notified Body:	C 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/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: 1992 Teil 2: 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, 8th February 1999

i.V. Peter Wieninger
Bereichsleiter Entwicklung
VP Engineering

Glossario

- **10BaseT** – wisted Pair; versione di connessione 10 Mbit-Ethernet; connessione di rete con connettore tipo RJ45.
- **10BaseT** – Twisted Pair; versione di connessione 10 Mbit-Ethernet; connessione di rete con connettore tipo RJ45.
- **10Base2** – Thin Ethernet; Cheapernet; versione di connessione 10Mbit-Ethernet; connessione di rete con connettore tipo BNC.
- **10Base5** – Thick Ethernet; versione di connessione 10 Mbit-Ethernet; connessione di rete con connettore tipo AUI o Sub-D 15 poli.
- **100BaseTX** – Twisted Pair; versione di connessione 100 Mbit-Fast-Ethernet; connessione di rete con connettore tipo RJ45.
- **Accesso base** – Connessione utente ISDN con due →canali base (ciascuno da 64.000 bps) e un canale di segnalazione (16.000 bps). L'interfaccia dell'accesso base con l'utente è l'interfaccia →S₀.
- **ARP** – Adress Resolution Protocol è un protocollo della →famiglia di protocolli TCP/IP. Con ARP gli indirizzi IP vengono riprodotti secondo i rispettivi indirizzi MAC.
- **AUI** – Attachment Unit Interface = Interfaccia per connessioni di rete generali.
- **BNC** – Tecnica di connessione comune per Cheapernet (Thin-Ethernet). Questa connessione viene anche definita T-BASE2. Per il collegamento di apparecchi con prese BNC si deve usare un connettore a T.
- **Bridge** – Un Bridge (ponte) è una connessione due reti con la stessa struttura layer-2 nel →modello OSI. Un siffatto bridge può essere costituito da due apparecchi collegati tra loro con una linea di trasmissione dati. Questa configurazione viene definita remote-bridge.
- **Broadcast** – I broadcast sono speciali pacchetti di dati, indirizzati a tutte le stazioni pronte a riceverli. Nelle reti Ethernet questi pacchetti di dati sono caratterizzati dall'indirizzo di destinazione FFh FFh FFh FFh FFh FFh (vale a dire a tutti).
- **Burst Mode** – Burst Mode è uno speciale tipo di trasporto dei pacchetti di dati nelle reti Novell, in cui più pacchetti di dati vengono trasmessi in successione senza conferma di ricevuta.
- **Canale B** – Canale di trasmissione dati in ISDN (64 Kbit); un accesso base ISDN possiede 1 canale D e 2 canali B.
- **Canale di comando** – Canale di segnalazione ISDN (anche →canale D), per la trasmissione di informazioni di comando (per es. la segnalazione di una chiamata in arrivo o simile) tra connessione ISDN e centralino con una capacità di trasmissione di 16.000 bps negli →accessi base oppure 64.000 bps negli →accessi multiplex primari. Viene anche definito canale D.
- **CEPT** – Conférence Européenne des Postes et des Télécommunications = conferenza europea per la definizione di norme per la telecomunicazione.
- **Client** – Client = workstation. Un client è un utente di uno dei →servizi offerti da un server.

- **CLIP** – Caller Line Identification Parameter = numero d'utenza del chiamante, che può essere trasmesso in ISDN.
- **Compressione dati** – Metodo per ridurre il volume di dati da trasmettere; con la compressione dati si può aumentare la velocità di trasmissione su una linea (procedure note: V.42bis, Stac, MPPC).
- **Compressione Stac** – Procedura di compressione dei dati.
- **Configurazione outband** – Nella configurazione Outband, o anche configurazione out-of-band, lo scambio dati con l'apparecchio da configurare avviene tramite un'interfaccia seriale V.24. La connessione di configurazione rimane anche in caso di disturbi alla connessione di rete.
- **Connessione di linea S₀** – Interfaccia dell'accesso base con l'utente. Questa interfaccia è costituita da un bus a cui possono essere connessi fino a otto terminali ISDN. Su questo bus possono essere installate fino a 12 prese.
- **Connessione Y** – Connessione contemporanea con due differenti controparti ciascuna su un canale B della stessa connessione di linea ISDN-S₀.
- **D-channel dump** – Canale di segnalazione in ISDN (selezione, trasmissione del numero d'utenza, informazioni di addebito, stabilimento e interruzione); un accesso base ISDN possiede 1 canale D e 2 canali B.
- **DNS** – Domain Name Server. Definisce un server che mette a disposizione un servizio nomi per ciascun computer di un →dominio. Con una richiesta a questo server, un'altra macchina che conosce solo il nome simbolico della destinazione può conoscere il rispettivo indirizzo IP.
- **Dominio** – (ingl. Domain) Si definisce dominio un gruppo di reti logicamente delimitato, per es. reti aziendali o provider Internet.
- **DSS1** – Euro-ISDN definito dalla →ETSI; attualmente il più comune protocollo canale D in ISDN.
- **EAZ** – La EAZ = cifra di selezione di terminale serve nel protocollo 1TR6 a distinguere i diversi terminali collegati allo stesso →accesso base ISDN. Questa cifra viene aggiunta dal chiamante come ultima cifra del numero d'utenza.
- **ETSI** – European Telecommunications Standards Institute = Istituto Europeo per gli Standard di Telecomunicazione. Questo ente di normalizzazione ha sviluppato uno standard europeo per il protocollo canale D (DSS1).
- **Firewall** – Meccanismi di protezione per una rete Intranet contro l'accesso dall'esterno; *ELSA LANCOM* supporta i meccanismi firewall mascheratura IP, filtro di porta, lista di accesso.
- **Flash ROM** – Una flash ROM è una memoria non volatile cancellabile e riscrivibile elettricamente. Le flash ROMs vengono impiegate spesso negli apparecchi il cui firmware può essere aggiornato tramite update.
- **Gateway** – Componente della rete che su un layer del → modello OSI consente l'accesso ad altri componenti di rete (per es. in Windows 95 sul layer 3).
- **HDLC** – High Level Data Link Control. Formato di un pacchetto di dati che viene assicurato tramite un calcolo CRC.
- **HOPS** – Numero dei router tramite i quali viene stabilito un collegamento di rete.

- **Hub** – Componente della rete; distributore; collettore; anche per la conversione da un tipo di connessione a un altro; un ingresso di rete – più uscite di rete per una distribuzione a stella.
- **Indirizzo IP** – 1. parte dell'indirizzo con cui un componente della rete viene identificato nella rete TCP/IP.
- **Indirizzo IPX** – È costituito da →node ID, indirizzo di rete IPX e socket; serve a definire in modo univoco un componente della rete all'interno di una rete IPX.
- **Interfaccia V.24** – Interfaccia seriale; per es. interfaccia per la connessione di un modem; *ELSA LANCOM* possiede un'interfaccia V.24, per consentire la selezione analogica anche con un modem connesso.
- **Internet** – Internet è una riunione di tutte le reti collegate tra loro tramite →TCP/IP.
- **Intranet** – Dominio; rete, per es. limitata solo alla propria azienda e che consente solo in modo regolato l'accesso dall'esterno o verso l'esterno.
- **IP** – Internet Protocol è un'ampia famiglia di protocolli sviluppata all'inizio degli anni settanta dal DoD (Department of Defence) per il collegamento di Wide Area Network eterogenee.
- **IPX** – Internet Packet eXchange = un protocollo di trasporto definito dalla Novell per la trasmissione di dati attraverso una rete. Su un PC questo protocollo viene realizzato dal driver IPX.COM oppure dalla →VLM-Shell.
- **IPX-watchdog** – Pacchetti che vengono inviati dal server a determinati intervalli di tempo per controllare una workstation. Se una workstation non risponde, viene automaticamente staccata.
- **ISDN** – Integrated Services Digital Network = rete di telecomunicazione digitale integrata per servizi.
- **ISO** – International Standardization Organization. L'ISO è un'organizzazione internazionale che coordina lo sviluppo di norme su scala mondiale – per tutti i campi – e che provvede alla loro pubblicazione. Suoi membri sono gli istituti di normalizzazione nazionali come per es. DIN (Germania), ANSI (USA), BSI (Gran Bretagna) o AFNOR (Francia).
- **ITU-T** – Settore di standardizzazione per le telecomunicazioni della International Telecommunications Union (ITU) si occupa della standardizzazione dei servizi dati e telefonici. Le raccomandazioni ITU-T della Serie V riguardano tra l'altro la trasmissione dati sulla rete telefonica. ITU-T è l'organizzazione erede del CCITT (Comité Consultatif International Télégraphique et Téléphonique).
- **LAN** – Local Area Network (rete locale). Secondo →l'ISO, una rete locale è una rete collocata entro confini territoriali ed è sotto il controllo dell'utente per la trasmissione seriale di informazioni tra i suoi elementi indipendenti, accoppiati tra loro. Una rete locale è quindi una rete fortemente delimitata nello spazio, che normalmente è installata entro di un edificio o della sede di un'azienda.
- **Layer** – strato, livello (v. modello OSI); strato all'interno di una connessione stabilita in modo modulare tra due sistemi in comunicazione.
- **Linea fissa** – Una linea fissa è una connessione fissa (stabile) tra due partecipanti, che può essere utilizzata esclusivamente dai due partecipanti.
- **Line-on-demand** – Stabilimento della connessione su richiesta. In *ELSA LANCOM*, il

contenuto dei pacchetti ricevuti dalla LAN decide sullo stabilimento di una connessione.

- **MAC** – Media Access Control = comando di accesso al mezzo. Definizione →ISO per il sottolivello del layer 2 del modello ISO. Nelle reti Ethernet, gli indirizzi di sorgente e di destinazione e il tipo di protocollo rientrano nei dati di layer MAC.
- **Maschera di rete IP** – 2. parte dell'indirizzo con cui un componente della rete viene identificato nella rete TCP/IP.
- **Mascheratura IP** – Single IP Address; Port Address Translation; procedura per il collegamento di una rete Intranet (più workstation) a Internet tramite un solo indirizzo IP; *ELSA LANCOM* supporta questa procedura.
- **MPPC** – Microsoft Point to Point Compression; procedura di compressione dati (attualmente non supportata da *ELSA LANCOM*).
- **MPR** – Multi Protocol Router; router (come *ELSA LANCOM Business 4100*) capace di instradare più protocolli.
- **MSN** – Multiple Subscriber Number = numero d'utenza multipla. Nel protocollo DSS1 possono essere assegnati dal centralino interessato più numeri d'utenza a una connessione ISDN. In genere si tratta di tre numeri, in ogni caso non più di otto. Mediante questi numeri è possibile, analogamente a quanto accade per il protocollo 1TR6, collegare in particolare determinati apparecchi terminali all'interfaccia S₀ attraverso cifre EAZ. A differenza delle EAZ impostate, che vengono attaccati ai numeri d'utenza effettivi, il MSN può essere costituito da un massimo di 16 cifre.
- **Multicast** – I multicast sono speciali pacchetti di dati, indirizzati a tutte le stazioni di un gruppo pronte a riceverli.
- **Multilink PPP** – MLPPP; procedura per il raggruppamento di canali con PPP; (*ELSA LANCOM* attualmente non la supporta).
- **NBNS** – Net BIOS Name Server. Definisce un server che mette a disposizione un servizio nomi per ciascun computer di un →dominio. Con una richiesta a questo server, un'altra macchina che conosce solo il nome simbolico della destinazione può conoscere il rispettivo indirizzo.
- **NETX** – NETX = NetWare-Shell. Questo programma rappresenta un'interfaccia tra i programmi di applicazione e il sistema operativo di rete Novell.
- **Node** – Node = nodo. Si definisce node un apparecchio collegato alla rete che riceve o invia dati. Questi possono essere singoli *ELSA LANCOM*, computer, server o stampanti, che possono essere chiamati da più partecipanti alla rete.
- **Node ID** – Indirizzo MAC.
- **Novell** – Produttore del sistema operativo di rete Novell NetWare.
- **OSI** – Open System Interconnection = sistemi aperti di comunicazione. Modello di riferimento per reti sviluppato dal →ISO (International Standardization Organization) per la definizione degli standard di interfaccia tra produttori di computer nel campo dei requisiti hardware e software.
- **Pacchetto di dati** – Un pacchetto di dati contiene un numero di caratteri prescritto dalla rete (comandi) per la trasmissione dati.
- **Ping** – Comando tramite ICMP; simile al ping (eco-scandaglio) dei sommergibili, con questo

comando si determina la distanza di un componente nella rete TCP/IP.

- **PPP** – Point to Point Protocol; famiglia di protocolli (LCP, IPCP, IPXCP, CBCP, ECP, CCP ecc.); protocollo per la negoziazione sui parametri di connessione in una connessione punto-a-punto tra componenti della rete (per es. chiamata di risposta, protocollo di rete, compressione).

- **Protocollo** – Per lo stabilimento e la sicurezza delle connessioni (rete, ISDN, tipi di connessione analogica); dialogo tra componenti connessi.

- **Proxy ARP** – Con proxy ARP si ottiene che le stazioni, che normalmente sono connesse direttamente a una rete locale TCP/IP e pertanto posseggono un indirizzo IP locale adatto, siano raggiungibili anche tramite un router (quindi tramite una connessione WAN). Il router si presenta come apparecchio remoto in una richiesta ARP nella rete locale, quindi rinuncia al proprio indirizzo MAC. Successivamente esso può ricevere i pacchetti di dati e inviarli al sito remoto.

- **Raggruppamento di canali** – Raggruppamento dei due canali B di ISDN in una connessione logica, per raddoppiare la velocità di trasmissione.

- **Raggruppamento di canali dinamico** – Bandwidth-on-Demand; secondo necessità la larghezza di banda viene aumentata con l'aggiunta automatica del 2. (o più) canale B.

- **Rete** – Una rete è un sistema multiutente e multifunzione di un gruppo di sistemi informatici e di terminali per l'impiego in comune di informazioni e risorse, collegati tra loro tramite linee di comunicazione.

- **Rete Ethernet** – Una rete Ethernet è un →sistema di bus con →accesso CSMA/CD e

→trasmissione su banda base. Nel 1979 questa rete locale è stata sviluppata dalle compagnie DEC, Intel e Xerox. Essendo una delle prime →LAN è diventata uno standard di fatto ed è stata accettata come standard dal IEEE (Institute of Electrical and Electronics Engineers) (Norma 802.3). La trasmissione avviene su linee coassiali, twisted pair, fibre ottiche o altri mezzi di trasmissione a 10 Mbit al secondo.

- **RIP** – Routing Information Protocol; serve nelle reti (qui Netware-IPX) per diffondere le informazioni per router.

- **RoundRobin** – Una procedura per la selezione di una controparte logica (per es. centrale aziendale) tramite diversi numeri d'utenza su apparecchi diversi. In essa, se la controparte standard è occupata, si passa automaticamente ad altre controparti libere.

- **Router** – Un router è un apparecchio per la connessione due reti con la stessa struttura layer-3 nel →modello OSI. Un siffatto router può essere costituito da due apparecchi collegati tra loro con una linea di trasmissione dati. Questa costellazione viene definita anche remote-router.

- **RTS** – Request to Send = attivare la trasmissione.

- **SAP** – Service Advertising Protocol. Viene utilizzato per diffondere i servizi nelle reti NetWare.

- **Server** – Un server offre dei servizi che vengono presi in considerazione da un →client. Molti sistemi operativi di rete presentano un'architettura client-server, vale a dire che uno speciale computer molto potente opera come server, da cui un gran numero di client (workstation) ricevono dati e programmi.

- **Short-hold modus** – Una connessione viene interrotta dopo un tempo prestabilito, se non devono essere più trasmessi dati. In questo modo si può ottenere che la connessione rimanga attiva per un certo tempo fino a quando non vengono più trasmessi dati.
- **SNMP** – Simple Network Management Protocol; protocollo normalizzato per il management di componenti della rete; vantaggio: Controllo di diversi componenti della rete tramite un'unica superficie (per es. HP-Openview o Cabletron-Spectrum); indipendente dal produttore; *ELSA LANCOM* supporta SNMP, versione 1.
- **Socket** – Numero identificativo che definisce il servizio per cui un pacchetto di dati viene inviato.
- **Soluzione stand-alone** – *ELSA LANCOM Business 4100* è una siffatta soluzione stand-alone, poiché per l'accoppiamento tra reti non è necessario installare alcun computer aggiuntivo o installare un software aggiuntivo su un server, come nel caso dei normali router, vale a dire si tratta di un componente della rete distinto.
- **Spoofing** – Lo spoofing è un metodo impiegato per evitare costi di connessione non necessari. In esso le richieste dal lato LAN ricevono risposta direttamente dal router, senza stabilire una connessione per l'invio di dati alla controparte.
- **SPV** – Connessione semipermanente = connessione a selezione predisposta. Una connessione semipermanente viene attualmente offerta per il protocollo →1TR6 e può essere allestita tra due connessioni ISDN qualsiasi. L'allestimento viene realizzato per ciascun canale B separatamente. Appena la connessione semipermanente è attiva, l'addebito non avviene più in base al tempo, ma secondo una tariffa mensile complessiva. In questo modo in taluni casi si può risparmiare sugli addebiti.
- **SPX** – Internet Packet eXchange = un protocollo definito dalla Novell per la trasmissione sicura di dati attraverso una rete. Su un PC questo protocollo viene realizzato dal driver NETX.COM (o simile).
- **SPX-watchdog** – Pacchetti che vengono inviati dal server a determinati intervalli di tempo per controllare una connessione SPX.
- **TCP/IP** – Transmission Control Protocol/Internet Protocol. Un'ampia famiglia di protocolli sviluppata all'inizio degli anni settanta dal DoD (Department of Defence) per il collegamento di Wide Area Network eterogenee. I due fondamenti di questa famiglia di protocolli sono l'IP, che implementa il layer 3 del →modello OSI e il suo analogo TCP per il quarto layer.
- **Telnet** – Telnet è un protocollo della →famiglia di protocolli TCP/IP. Esso consente l'accesso remoto da una workstation a un altro sistema informatico che si trova in rete. Il protocollo Telnet utilizza per la trasmissione dati il →protocollo TCP, poiché esso richiede una comunicazione bidirezionale assicurata. In questo modo un terminale virtuale sul server Telnet viene messo a disposizione di un client Telnet.
- **TFTP** – Trivial File Transfer Protocol; semplice protocollo per la trasmissione di un file (per es. firmware upload, salvataggio/ripristino della configurazione).
- **TICS** – Unità di tempo di sistema del *ELSA LANCOM*.
- **Transceiver** – Transceiver = convertitore di segnali. Un transceiver è un apparecchio che

converte un formato di segnale di ingresso in un altro formato di uscita.

■ **Trasmissione asincrona** – Nella

trasmissione seriale dei dati è necessaria una procedura per realizzare la coordinazione tra trasmittente e ricevente, in modo da consentire al ricevente di riconoscere l'inizio e la fine di un carattere trasmesso. Per questa strutturazione, nella trasmissione asincrona ciascun byte da trasmettere viene marcato con uno start bit e uno o due stop bit. Specialmente nell'ambito dei microcomputer, questa procedura start-stop è uno dei sistemi di trasmissione utilizzati di frequente, poiché è relativamente semplice da realizzare, a differenza della trasmissione sincrona.

■ **Trasmissione sincrona** – La trasmissione sincrona, come la →trasmissione asincrona, è una procedura per realizzare la coordinazione tra trasmittente e ricevente. In questo formato di trasmissione dati, a differenza della trasmissione asincrona, la coordinazione non viene realizzata tramite start bit e stop bit per un carattere completo, ma tramite impulsi di sincronizzazione per ciascun singolo bit. Pertanto, poiché non si devono trasmettere start bit e stop bit aggiuntivi, la trasmissione sincrona è più veloce, ma la realizzazione tecnica è sostanzialmente più impegnativa.

■ **UDP** – User Datagram Protocol = contribuisce alla trasmissione dati di determinati servizi nelle reti IP, tuttavia a differenza del TCP non realizza una trasmissione dati assicurata.

■ **UNIX** – UNIX è un sistema operativo sviluppato dalla AT&T per potenti microcomputer, computer e grandi calcolatori.

■ **V.42bis** – Raccomandazione del →ITU-T per la compressione dei dati nell'ambito di un traffico di dati.

■ **V.110** – Raccomandazione del →ITU-T per l'adattamento dei traffici di dati seriali asincroni e sincroni al bit rate ISDN di 64 Kbit al secondo per la trasmissione su →canale B ISDN (viene anche denominato I.463).

■ **VLM** – Virtual Loadable Module = Questo programma rappresenta l'interfaccia tra i programmi di applicazione e il sistema operativo di rete Novell.

■ **WAN** – Wide Area Network = reti ad ampio raggio per dati come per es. le connessioni tramite apparecchi ISDN.

■ **Workstation** – Denominazione per un computer per posto di lavoro.

■ **X.75** – Raccomandazione del →ITU-T per la trasmissione assicurata di dati con formato di trasmissione HDLC su →canale B ISDN.

■ **XModem** – XModem è un →protocollo di trasmissione con riconoscimento automatico e correzione degli errori. La trasmissione dei dati avviene in blocchi con dimensione di 128 Byte. Se viene riconosciuto un errore di trasmissione, il blocco difettoso viene inviato di nuovo. XModem è uno dei protocolli più usati su scala mondiale. Esso viene supportato da molti emulatori di terminale standard, tuttavia la sua efficienza è stata superata da protocolli più moderni, come Zmodem.

Indice

■ Numerics

10/100Base-TX	10
100Base-T	R-48
1TR6	3, R-40
802.2	R-50
802.3	R-50

■ A

Abilitazione di file e stampanti	90
Access-list	R-59
Accesso a Internet	54
Accesso a selezione	95
Accesso remoto	2, 13, 16, 36, 54, 88, 130
Accesso remoto con TCP/IP	130
Accoppiamenti LAN-LAN	118
Adattatore	14
Addebiti	38, 88
Address pool	R-70
Address ranges	R-62
Aggiornamenti software	6
Aging-minute(s)	R-54, R-56
Ambiente di rete	94
AOCD	4, 38
Applicazioni Internet	108
APPP	R-44
ARP cache	R-60
ARP-aging-minute(s)	R-60
Assegnazione degli indirizzi	15
Asynchronous PPP	R-44
Autenticazione	56
Auth.	R-45
Automode	77

■ B

Backoff	R-53
BACP	3
B-channel protocols	R-43
Binding	R-50
Blocco	34
Blocco dei domini	87
Blocco del login	34

Boot system	R-82
Budget di tempo	38
Buffers	R-48

■ C

Cache	R-60
Call numbers	R-46
Callback	R-41, R-46, R-48
Callback options	R-42
Call-by-call	100, 101, R-77
Calling Line Identification Restriction	R-40
Canale B	31
stato di connessione	4
Canale D	36
CAPI Faxmodem	100
Caricamento del software	21
Cavo ISDN	3
CBCP	55
CE	10
Challenge Handshake Authentication Protocol	36, R-45
Channel bundling	R-44
CHAP	36, R-45
Charge	R-42
Charges	R-50, R-55
Charging information	R-41
Charging unit	R-41
Chiamata di risposta	35, 36
Fast call back	37
Cifra identificativa di rete	100
CLI	36, R-46
Client per reti Windows	90
CLIP	5
CLIR	R-40
Collegamento remoto	17
Comando priorità	99
Common ISDN Application Programming Interface	95
Communities	24
Commutatore node/hub	10

Compatibility	R-43
Compressione	3
Compressione dati LZS	58
Compressione dati Stac	3
Compuserve	91
Compuserve select	92
Computer	84
Computer raggiungibili	94
Comunicazione di ufficio	95
Condivisione	91
Config-aging-minute(s)	R-75
Configuration options	R-74
Configurazione	5
comandi	20
procedure	13
SNMP	24
Configurazione degli accessi	18
Configurazione dell'accesso Internet	109
Configurazione inband	13
Configurazione outband	13, 14
Configurazione punto-a-più punti	3
Configurazione punto-a-punto	3
Configurazione remota	6, 13
Configurazione WINS	80
Connect	R-47
Connection time-outs	R-41
Connector	R-48
Connessione fissa	108, 114
Connessione impianto	3
Connessione in rete	1
Connessione LAN	3
Connessione multipla	3
Connessione PPP	13, 18
Connessione router di reti Windows	87
Connessione WAN	3
Connessione Y	59
Connessioni	9
Connessioni fisse	2, 119
impostazione	47
Control outputs	93
Controllo in arrivo	34
Controllo ora	5
Controparti NetBIOS	88

Conversazione urbana	102
Conversazioni internazionali	101
Conversazioni interurbane	101
Costi telefonici alti	37

D

D64S	47
D64S2	47
D64SY	47
Data compression	R-44
Dati tecnici	141
DDI numbers	R-43
Default Layer	18
Default route	R-63
Definizione di nomi e gruppi	90
Destination network	R-61
Destination port	R-63
Device names	R-41
DHCP	7, 77, R-70
DHCP automode	77
DHCP per scomposizione WINS	80
DHCP server	R-70
Dial prefix	R-42
Dialup-remote	R-41
Disconnect	R-47
Display	4, 8
Display canali	31
Display di stato	4
Distanza di una rotta	67
DNS	76, 84, R-59
DNS forwarding	76, R-60
DNS queries	R-64
DNS-backup-IP-address	R-60
Documentazioni Trace	28
Domain Name Service	76, 84
Domini	84
Driver fax	6, 100
DSS1	3, R-40
Dst-address	R-64
Dst-netmask	R-64
Durata della connessione	4
Dynamic assignment of the IP address ..	R-61
Dynamic bundling	R-41

Dynamic Host Configuration Protocol	77
Dynamic IP routing table	R-67
Dynamic short-hold	R-41

■ **E**

<i>ELSA CAPI Faxmodem</i>	6
<i>ELSA-RVS-COM</i>	3
<i>ELSA-ZOC</i>	3
E-mail	2
Emulatore di terminale	5
Encaps	R-43
End-address-pool	R-70
Ethernet	3, R-43
10/100Base-T	3
Fast-Ethernet	3
Ethernet packet format	R-50
EuroFileTransfer	6
Exponential backoff	R-53

■ **F**

Fast call back	37
Fast callback procedure	R-42
Fast-Ethernet	3
10/100Base-T	3
Fax	1, 2, 6, 100
Fax classe 1	6, 100
Faxmodem	6
<i>LANCAPI</i>	100
Filtri	35
Filtro IP	89
Filtro socket	64
Firewall	5, 108
Firewall function	R-64
FirmSafe	6, 21, R-81
Firmware	6, R-80
Firmware upload	22
con <i>LANconfig</i>	22
con programma di terminale	22
con TFTP	23
Forza bruta	5
Funzione di monitoraggio addebiti	96
Funzione di richiamata	5
Funzione firewall	37, 96
Funzioni di sicurezza	2

Fuori tempo	58
-------------------	----

■ **G**

Gateway	37, 77, 80
Gestione degli addebiti	37
Gestione indirizzi	77
Gestione multicanale	4
Gestori di rete	100
Giorni feriali	101
Giorni festivi	101
Group table	R-73
Gruppi di nomi	88
Gruppo	88
GSM	7

■ **H**

HDLC packets	R-44
HDLC56K	R-44
HDLC64K	R-44
Host table	R-73
Hub	10
Hyperterminal	14

■ **I**

ICMP	R-64, R-66, R-68
Identification	R-38
Identificativi	91
Identificazione	90
Identificazione del chiamante	35
Inband	13, 15
con Telnet	16
presupposti	15
Indirizzamento IPX	60
Indirizzi IP	7
Indirizzi IP registrati	109
Indirizzo finale	78
Indirizzo iniziale	78
Indirizzo Internet	74
Indirizzo Intranet	74
Indirizzo IP	15, 31, 37, 53
Indirizzo IP fisso	113
Informazioni di addebito	4, 38, 58
Informazioni sul nome	88
Installazione	3

- Installazione del Web Server in Internet . 113
- Interfacce 9
- Interfaccia CAPI 95
- Interfaccia di configurazione 13
- Interfaccia di configurazione V.24 10
- Interfaccia S₀ 3
- Interfaccia seriale 13, 23
- Interface list R-39
- Internet 2, 37
- Internet Account 108
- Intranet R-58
- Intranet-mask R-58
- Inverse masquerading R-67
- IP R-66
- IP address R-58
- IP broadcast R-66
- IP header R-65
- IP masquerading R-61, R-67
- IP multicast R-66
- IP pooling 3, 95
- IP netmask R-58
- IP routing
 - Filtro 69
- IP routing table R-61
- IPX router R-49
- IPX routing
 - propagazione Loop 63
- IPX watchdog R-50
- ISDN layers R-43
- ISDN time R-5
- **K**
 - Key R-45
- **L**
 - LANCAPi 1, 3, 6, 17, 95, R-76
 - LANCAPi Client 96
 - LANCAPi Server 98
 - LAN-Coll 9
 - LANconfig 5, 13, 15, 17, 22, 30
 - wizard 15
 - LAN-configuration R-75
 - LAN-filter-table R-54, R-56, R-63
 - Langner open ISDN config
 - wizard 15
 - Language R-75
 - LAN-Link 9
 - LANmonitor 4, 26, 30, 104
 - LAN-Rx 9
 - LAN-Tx 9
 - Layer name R-41, R-43
 - LCP echo reply 53
 - LCP echo request 53
 - LCR 5, 38, 101, R-77
 - Leased-line connection R-43
 - Least-cost router
 - Caduta automatica 103
 - Modalità 103
 - Monitoraggio addebiti 103
 - Least-cost router 100, 103
 - Least-cost routing 5, 38
 - LED 8
 - Limitazione degli addebiti 37
 - Limitazione dei costi 38
 - Limitazione della connessione 38
 - Limitazione della connessione in base
 - al tempo 38
 - Line management 2, 119
 - Linee a selezione 2, 119
 - Linee a selezione ISDN 37
 - Link-status LED 10
 - Lista di accesso IP 15
 - Lista layer 48
 - Lista PPP 35
 - Local-routing R-51, R-65
 - Location R-38
 - Lock-minutes R-75
 - Login 21
 - Log-in block R-75
 - Login-errors R-75
 - LOOP-propagate R-52
 - Looser R-42
 - **M**
 - MAC address R-48
 - Mail Server 86
 - Management Information Base 26

Manager	26
Manual connection	R-47
Mascheratura IP	2, 5, 35, 37, 109
Mascheratura IP inversa	113
Masquerading	R-58, R-61, R-67
Masquerading IP	73
masquerading semplice	75
protocolli supportati	75
Masquerading table	R-68
Maximum number of simultaneous connections	R-75
Meccanismi di filtro	2, 119
Meccanismo di forwarding DNS	85
Memoria flash ROM	6, 21
Messaggi	8
MIB	24
MLPPP	3, 58
Modalità	33
Modem operation	R-44
Monitoraggio	30
Multilink PPP	50
Multilink-PPP	58

N

Name	R-38
Name server	R-59
Name verification	R-46
Name-list	R-41
Nameserver NetBIOS	88
NAT	35, 37, 73
NBNS	88, R-60
NBNS-backup	R-60
Negoziazione PPP	18
Nessuna informazione di addebito	38
NetBIOS	7, 85, R-51
Accesso remoto	93
Accoppiamento LAN-LAN	92
Controparte	92
Filtri IP	92
Protocollo di rete	89
TCP/IP	89
NetBIOS name server	R-60
NetBIOS propagated frames	R-52

NetBIOS-Proxy	87
NetWare server	R-50
Network	R-50
Network address	R-52
Network connection	R-48
Network Information Center	74
Networking Windows	94
NIC	74
Node	10
Node-ID	R-49
Nodi di selezione	3
Nome del router	67
Nome utente	18, 36, 52
Nomi	88
Nomi dei computer	88
Nomi di computer	84
Nomi di rete	84
Novell	R-52
NT domain	R-72
Number	R-41
Number list	R-46
Numeri speciali	102
Numero telefonico di configurazione	19
Numero di porta	75

O

Online banking	1
Operating	R-49, R-58, R-61
Opzioni	99
Ora	101, 104
Ora del giorno	101
Ora della rete ISDN	104
Ora ISDN	5
Orologio interno	104
Other	R-82
Outband	13
prerequisiti	14

P

PAP	36, R-45
Password	19, 31, 35, 36, 52, R-59
Password Authentication Protocol	36, R-45
Password-required	R-75
PAT	35, 37, 73

Periodo	38
Periodo di validità	77, 80
Point-to-point protocol	R-44
Policy Based Routing	105
Pool di indirizzi	78, 83, 95
Pool di indirizzi IP	95
Porta	98
Porte NetBIOS	89
Possibilità di risparmio nelle telefonate ..	102
Power	8
PPP	5, 6, 31, 36, 58, R-44, R-46
Assegnazione degli indirizzi IP	53
Controllo della linea con LCP	53
Funzioni di richiamata	54
PPP Client	13, 17
PPP LCP extensions	57
PPP negotiation	R-58
Prefisso	100, 101
Preselezione	100
Procedura di sicurezza	36
Procedure di compressione dati	
LZS	58
Programma di terminale	14
Programmi di fax standard	100
Prohibited address ranges	R-62
Propagated Frames	64, R-52
Protect	R-46
Protezione con password	5, 34
Protezione di accesso	5, 35
per nome	35
per numero	35
tutte	35
Protocollo di canale B	36
Protocollo V.110	7
Provider	100
Provider Internet	1
Proxy	7
Proxy ARP	R-61, R-62, R-65

■ **R**

R1-mask	R-67
Raggruppamento canali dinamico	58
Raggruppamento canali statico	58
Raggruppamento di canali	3, 58
dinamico	3
statico	3
Registered IP address	R-58
Regolazione automatica dell'ora	104
Remote access	R-53, R-65
Remote station verifications	R-45
Remote-table	R-72
Reset system	R-82
Rete 100 Mbit	10
Rete urbana	102
Rete Windows	80, 87
Reti NetBIOS	85
Reti peer-to-peer	7
Reti TCP/IP	84
Reti Windows	7
Ricerca difetti	30
Ricerche online	2
Richiamata	2
Riconoscimento del numero telefonico	5
RIP	62, R-66
RIP-SAP-scaling	R-51
RIP-type	R-66
Risorse abilitate	91
Rotte di esclusione	68
RoundRobin list	R-42, R-43
Routes/FRM	R-54
Routing	88
Routing dinamico	66
Routing Information Protocol	62
Routing IP	
FTP	69
Telnet	69
Routing IPX	
Backoff	62
Binding	60, 61
Controparte	61
Exponential backoff	63
Filtro	64
Hops	62
Propagate	61
Rete	61
Tabelle RIP e SAP	62

Tic 62
 Routing-table R-52

S

SAP 62, R-55
 SAP numbers 83
 SAP services R-56
 Scaling R-51
 Scope ID R-72
 Scopes 88
 Script list R-46
 Script processing 91
 Security procedure R-45
 Segreteria telefonica 1, 2
 Semipermanent leased-line connection R-42
 Server DHCP 7, 15, 77, 84
 Configurazione 81
 Server DNS 7, 77, 79, 84
 Informazioni disponibili 85
 Lista di filtro 87
 Meccanismo di filtro 85
 Server information R-55
 Server list R-74
 Server NBNS 77, 79, 80
 Server WINS 88
 Server/FRM R-56
 Service Advertising Protocol 62
 Service information R-56
 Service table R-67
 Servizi online 15
 Servizio 84
 Setup
 DHCP-module R-70
 IP-router-module R-61
 IPX-module R-49
 LAN-module R-48
 TCP-IP-module R-57
 WAN-module R-38
 Setup Wizard 14
 Short-hold R-41
 Sicurezza 33, 35, 37, 109
 Simboli 108
 Single User Access 37

Sito remoto 52
 Smistamento 101
 SNAP R-50
 SNMP 24, R-69
 Agent 24
 Manager 24
 MIB 24
 Società telefonica 102
 Socket-filter R-53
 Source port R-64
 Spare-heap-blocks R-49
 Special dialing characters R-41, R-42
 Speed R-44
 Spie LED 4
 Split horizon 63
 Spoofing R-55, R-57
 SPX-watchdog R-51
 Stabilimento della connessione 88
 Stac 58, R-44
 Start-address-pool R-70
 Stati operativi 8
 Static bundling R-41
 Static IP address R-61
 Statistiche 4
 Status R-3
 Call-info-table R-33, R-34, R-36, R-37
 Config-statistics R-30
 Connection-state R-5
 Connection-statistics R-31
 Delete values R-37
 Info-connection R-32
 IP-router-statistics R-28
 IPX-statistics R-17
 LAN-statistics R-8
 Layer-connection R-33
 Operating time R-5
 PPP-statistics R-9
 Queue-statistics R-30
 S₀-bus R-35
 TCP-IP-statistics R-22
 WAN-statistics R-6
 Struttura tariffaria 102
 Supported Protocols and Functions 95

Suppresses the outgoing MSN	R-40
System-administrator	R-69
System-location	R-69

■ **T**

Tabella di interfaccia	47
Tabella di routing	
Mascheratura IP	68
Voci speciali	68
Tabella di routing IP	66
Tabella di routing IPX	61
Tabella LCR	101
Tabelle RIP	62
Tabelle SAP	62
Table-ARP	R-60
Table-RIP	R-53, R-67
Table-SAP	R-55
Tariffa urbana	102
Tariffe	100
Tasti	8
TCP	R-64, R-68
TCP max. connections	R-60
TCP/IP	15, 66
TCP-aging-minute(s)	R-60
Telelavoro	2, 130
Telephone company	R-77
Teleworkers	R-65
Telix	14
Telnet	5, 17
Telnet server	R-59
Tempo di attesa	58
Tentativi di login	34
TFTP	15
TFTP server	R-59
Time	R-5, R-45, R-79
Timeout	R-71
Tipo di accesso	91
TOS	R-66, 105
Trace	
avvio	28
chiave e parametri	28
esempi	30
Trace editions	

SCRPT	105
Trace Outputs	93
Trace outputs	
ARP	103
control	94
DHCP	104
Error	97
examples	95
ICMP	103
IP-RIP	102
IP-Rt.	101
IPX watchdogs	100
IPX-NetBIOS	101
IPX-Rt.	98
PPP	97
RIP	99
SAP	99
SCRPT	104
Source	97
SPX watchdogs	101
Time	96
Trap	26
Trap-IP	R-69
Traps-active	R-69
Trasferimento file	2
Trasmissione dati	58
Trasmissione dati in rete IPX	62
Trasmissione di fax	100
Trunk seizure	R-42
Type-of-service	76, R-65

■ **U**

UDP	R-64, R-68
Ufficio a casa	2, 129
Unità a pagamento	38, 58
Upload	6, 21
Upload-system	R-82
Username	52, R-45

■ **V**

Velocità di trasmissione	4, 31, 58
Verification attempt	R-45
Version-table	R-80

■ **W**

WAN-configuration	R-75
WAN-filter-table	R-54, R-56, R-64
WAN-update-minute(s)	R-55, R-57
Watchdog	65, R-50
Watchdogs IPX	65
Watchdogs SPX	65
Web server	108, 113
Wildcard	87
Windows Internet Name Service Server ...	88
WWW	37

■ **X**

X.75 data protection	R-44
X.75 secured format	R-44
XModem	23

■ **Y**

Y connections	R-40
---------------------	------

■ **Z**

Zona tariffaria	102
-----------------------	-----

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		Status
	Name		Connection
	WAN-module		Current-time
	Charges-module		Operating-time
	LAN-module		WAN-statistics
	IPX-module		LAN-statistics
	TCP-IP-module		PPP-statistics
	IP-router-module		IPX-statistics
	SNMP-module		TCP-IP-statistics
	DHCP-module		IP-router-statistics
	NetBIOS-module		Config-statistics
	Config-module		Queue-statistics
	LANCAPI-module		Conn.-statistics
	LCR-module		Info-connection
	DNS module		Layer-connection
	Time-module		Call-info-table
	Firmware		Remote-statistics
	Version-table		S ₀ -bus
	Table-firmsafe		Channel-statistics
	Mode-firmsafe		Time-statistics
	Timeout-firmsafe		LCR-statistics
	Test-firmware		Delete-values
	Firmware-upload		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 ₀ -bus		Status of the S ₀ 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 S₀ 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:

Ifc	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:

Ifc	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:

Ifc	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:

Ifc	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:

Ifc	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:

Ifc	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	0	Number of data packets received
LAN-tx-packets	0	Number of data packets sent
LAN-rx-errors	0	Number of data packets incorrectly received
LAN-tx-errors	0	Number of data packets incorrectly sent
LAN-stack-errors	0	Number of packets without a suitable receive module (bridge/router)
LAN-NIC-errors	0	Number of data packets discarded by the NIC
LAN-heap-packets	0	Number of buffers available
LAN-queue-packets	0	Number of buffers in use
LAN-queue-errors	0	Number of packets discarded due to a lack of buffers
LAN-collisions	0	Number of collisions during a send procedure
Link-active	0	Display of correct Ethernet connection (data transfer possible). Corresponds to the 'Link' LED on the device.
Negotiation done	0	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: 10B-TX: 10 MBit, half-duplex FD10B-TX: 10 MBit, full-duplex 100B-TX: 100 MBit, half-duplex FD100B-TX: 100 MBit, full-duplex 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 AUTHENTICAT , NETWORK and TERMINATE .
LCP	Status of the 'Link Control Protocol' subprotocol. The possible values are: Initial , Starting , Stopping , Stopped , Closing , Closed , ReqSent , AckRcvd , AckSent and Opened .
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	M aximum R eceive U nit designates the maximum packet size that the remote station can receive
ACCM	A synchronous C ontrol C haracter M 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 'ffffffff' 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
Refreshes		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. The possible values are: Init , Setup WAN , Ready , Dial , Incoming call , Protocol , Connection , Callback , Bundle and Reserved . The Bundle status is indicated in the display <i>ELSA LANCOM Business 4100</i> by the addition of a "I2" in columns 15 and 16 of the associated display line. Bundle 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. Reserved 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: Active (active call establishment = dialing) Passive (passive call establishment = call acceptance) CB (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 ₀	5678	1234	HDLC64K	2
OT; 00:20:46	S ₀	4321	1234	HDLC64K	1
OT; 00:19:47	S ₀	4321	1234	HDLC64K	1
OT; 00:11:33	S ₀	5678	1234	HDLC64K	1
OT; 00:01:13	S ₀	4321	1234	HDLC64K	2
OT; 00:01:02	S ₀	4321	1234	HDLC64K	1
OT; 00:00:06	S ₀	5678	1234	HDLC64K	1

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. 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
0T; 00:20:57	LONDON	Active	Ch01	50	5
0T; 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: Active – the connection was actively established by the device Pas. – The device received a call 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/S₀-bus

This option allows you to display the current status of the S₀ interface. The statistics have the following layout:

/S ₀ -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 ₀ -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	T erminal E quipment I 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 ₀ -1-ERR	00000000	Router	active	0000	0241123456	00000000	3	0		
S ₀ -1-B1	00000000	a/b	active	0000	0241123457	00000000	2	20		
S ₀ -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 Business* 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: 'ISDN' for time taken from the ISDN, 'Manual' for the manual setting of the time with the 'time' command, '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 Business* 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		ELSA LANCAPI 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 ₀ 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: Auto : automatic detection of the D-channel protocol DSS1 : Euro-ISDN 1TR6 : National ISDN GRP0 : Leased-line connection group 0 P2P-DSS1 : Point-to-point connection
LL-B-chan.	B-channel settings for a leased-line connection. The possible values are: none : Leased-line connection not assigned to a specific channel. 1 or 2 : Leased-line connection operates over the assigned B channel. 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>On: 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>LANCAPI</i>.</p> <p>Off: 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>Yes: Activate CLIR, do not send MSN.</p> <p>No: 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 ₀ bus. Syntax: [<BusNo>-<ChannelNo>][:<BusNo>-<ChannelNo>]... Possible values: 1 to 4 for the busses, 1 or 2 for the channel. If no entry has been made, a random channel on a random bus will be used. 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. 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 Device Name column, you can enter an original remote station name, which you must then assign to the relevant remote station via the Name option in the Setup 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. If no data is being transmitted when this time expires, the connection on this channel is released (default: 20). 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). 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 (not applicable to Windows 9x or 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. Syntax: F[channel:][subscriber number] The channel and subscriber number are both optional. In the case of several leased lines, the channel specifies the B channel to be used. 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 Head column, the following entries are possible: Last: The next connection to be established will begin with the DDI that was successfully used for establishing the last connection (default). First: The next connection to be established will always begin with the first DDI. For a logical remote station, this field can be modified only by means of its first 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 Business*:

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
RAWHDLC	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. If an entry with the name DEFAULT 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 DEFAULT 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 Encaps 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.
	SCTrans	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. 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! 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. 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. 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. If no user name is entered, the device name serves as the user name. 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. 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
CSERVE	<>[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 and UDP	Always-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

*Type*

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.

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/ Domain	UPD	IP-address	OS- Ver	SMB- Ver	Server- type	Remote station	Time- 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-(EAS-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/LANCAPI-module

Configuring *LANCAPI* basically involves answering two questions:

- What call numbers from the telephone network should *LANCAPI* respond to?
- Which of the computers in the local network should be able to access the telephone network via *LANCAPI*?
- Via which UDP port do the *LANCAPI* server and *LANCAPI* clients communicate?

The *LANCAPI* module has the following layout:

/LANCAPI-module		LANCAPI settings
Access-list		List of computers allowed to use the <i>LANCAPI</i>
Interface-list		Activation of the <i>LANCAPI</i> for the various interfaces and specification of the various subscriber numbers to which the <i>LANCAPI</i> should respond.
Priority-list		Priority for the <i>LANCAPI</i> versus router connections
UDP-port		UDP port for communication between the <i>LANCAPI</i> server and clients

Access-list This option allows you to limit the circle of computers permitted to use the *LANCAPI*. This table can have a maximum of 16 entries. If the table is empty, all computers can access the *LANCAPI*.

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>LANCAPI</i> operation is permitted on this interface for outgoing calls, incoming and outgoing calls (On) or whether <i>LANCAPI</i> operation is disabled completely (Off).
EAZ-MSN(s)	Enter the EAZs or MSNs on which the <i>LANCAPI</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>LANCAPI</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 *LANCAPI* 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		Activate LCR for the router modules, On or Off
Lancapi-usage		Activate LCR for the <i>LANCAPI</i> , On or Off
Timetable		Call forwarding table
Celebration-day-table		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. 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. 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: On, Off
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.

Ifc	Module	Version	Serial-number
Ifc	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.

Novell SAP Numbers

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

Decimal	Hexa-decimal	SAP description
75	004b	Btrieve VAP/NLM 5.0
76	004c	Netware SQL VAP/NLM Server
77	004d	Xtree Network Version Netware XTree
80	0050	Btrieve VAP 4.11
82	0052	QuickLink (Cubix)
83	0053	Print Queue User
88	0058	Multipoint X.25 Eicon Router
96	0060	STLB/NLM
100	0064	ARCserve
102	0066	ARCserve 3.0
114	0072	WAN Copy Utility
122	007a	TES-Netware for VMS
146	0092	WATCOM Debugger or Emerald Tape Backup Server
149	0095	DDA OBGYN
152	0098	Netware Access Server (Asynchronous gateway)
154	009a	Netware for VMS II or Named Pipe Server
155	009b	Netware Access Server
158	009e	Portable Netware Server or SunLink NVT161
161	00a1	Powerchute APC UPS NLM
170	00aa	LAWserve
172	00ac	Compaq IDA Status Monitor
256	0100	PIPE STAIL
258	0102	LAN Protect Bindery
259	0103	Oracle DataBase Server
263	0107	Netware 386 or RSPX Remote Console
271	010f	Novell SNA Gateway
273	0111	Test Server
274	0112	Print Server (HP)
276	0114	CSA MUX (f/Communications Executive)

Decimal	Hexa-decimal	SAP description
277	0115	CSA LCA (f/Communications Executive)
278	0116	CSA CM (f/Communications Executive)
279	0117	CSA SMA (f/Communications Executive)
280	0118	CSA DBA (f/Communications Executive)
281	0119	CSA NMA (f/Communications Executive)
282	011a	CSA SSA (f/Communications Executive)
283	011b	CSA STATUS (f/Communications Executive)
286	011e	CSA APPC (f/Communications Executive)
294	0126	SNA TEST SSA Profile
298	012a	CSA TRACE(f/Communications Executive)
299	012b	Netware for SAA
301	012e	IKARUS virus scan utility
304	0130	Communications Executive
307	0133	NNS Domain Server or Netware Naming Services Domain
309	0135	Netware Naming Services Profile
311	0137	Netware 386 Print Queue or NNS Print Queue
321	0141	LAN Spool Server (Vap, Intel)
338	0152	IRMLAN Gateway
340	0154	Named Pipe Server
358	0166	NetWare Management
360	0168	Intel PICKIT Comm Server or Intel CAS Talk Server
371	0173	Compaq
372	0174	Compaq SNMP Agent
373	0175	Compaq
384	0180	XTree Server or XTree Tools
394	018A	NASI services broadcast server (Novell)
432	01b0	GARP Gateway (net research)

Decimal	Hexa-decimal	SAP description
433	01b1	Binview (Lan Support Group)
447	01bf	Intel LanDesk Manager
458	01ca	AXTEC
459	01cb	Shiva NetModem/E
460	01cc	Shiva LanRover/E
461	01cd	Shiva LanRover/T
462	01ce	Shiva Universal
472	01d8	Castelle FAXPress Server
474	01da	Castelle LANPress Print Server
476	01dc	Castille FAX/Xerox 7033 Fax Server/Excel Lan Fax
496	01f0	LEGATO
501	01f5	LEGATO
563	0233	NMS Agent or Netware Management Agent
567	0237	NMS IPX Discovery or LANtern Read/Write Channel
568	0238	NMS IP Discovery or LANtern Trap/Alarm Channel
570	023a	LABtern
572	023c	MAVERICK
575	023f	Used by eleven various Novell Servers / Novell SMDR
590	024e	Netware Connect
591	024f	NASI server broadcast (Cisco)
618	026a	Network Management (NMS) Service Console
619	026b	Time Synchronization Server (Netware 4.x)
632	0278	Directory Server (Netware 4.x)
640	0280	Novell File and Printer Sharing Service for PC
989	03dd	Banyan ENS for Netware Client NLM
772	0304	Novell SAA Gateway
776	0308	COM or VERMED 1
778	030a	Galacticomm's Worldgroup Server

Decimal	Hexa-decimal	SAP description
780	030c	Intel Netport 2 or HP JetDirect or HP Quicksilver
800	0320	Attachmate Gateway
807	0327	Microsoft Diagnostics
808	0328	WATCOM SQL server
821	0335	MultiTech Systems Multi-synch Comm Server
835	0343	Xylogics Remote Access Server or LAN Modem
853	0355	Arcada Backup Exec
858	0358	MSLCD1
865	0361	NETINELO
894	037e	Twelve Novell file servers in the PC3M family
895	037f	VirusSafe Notify
902	0386	HP Bridge
903	0387	HP Hub
916	0394	NetWare SAA Gateway
923	039b	Lotus Notes
951	03b7	Certus Anti Virus NLM
964	03c4	ARCserve 4.0 (Cheyenne)
967	03c7	LANspool 3.5 (Intel)
983	03d7	Lexmark printer server (type 4033-011)
984	03d8	Lexmark XLE printer server (type 4033-301)
990	03de	Gupta Sequel Base Server or NetWare SQL
993	03e1	Univel Unixware
996	03e4	Univel Unixware
1020	03fc	Intel Netport
1021	03fd	Print SErver Queue
1196	04ac	On-Time Scheduler NLM
1034	040A	IpServer Running on a Novell Server
1037	040D	LVERRMAN Running on a Novell Server
1038	040E	LVLIC Running on a Novell Server
1044	0414	Kyocera

Decimal	Hexa-decimal	SAP description
1065	0429	Site Lock Virus (Brightworks)
1074	0432	UFHELP R
1075	0433	Synoptics 281x Advanced SNMP Agent
1092	0444	Microsoft NT SNA Server
1096	0448	Oracle
1100	044c	ARCserve 5.01
1111	0457	Canon GP55 Running on a Canon GP55 network printer
1114	045a	QMS Printers
1115	045b	Dell SCSI Array (DSA) Monitor
1169	0491	NetBlazer Modems
1200	04b0	CD-Net (Meridian)
1299	0513	Emulux NQA Something from Emulux
1312	0520	Site Lock Checks
1321	0529	Site Lock Checks (Brightworks)
1325	052d	Citrix OS/2 App Server
1343	0535	Tektronix
1344	0536	Milan
1387	056b	IBM 8235 modem server
1388	056c	Shiva LanRover/E PLUS
1389	056d	Shiva LanRover/T PLUS
1408	0580	McAfee's NetShield anti-virus
1466	05BA	Compatible Systems Routers
	05B8	NLM to workstation communication (Revelation Software)
	0606	JCWatermark Imaging
1569	0621	IBM AntiVirus NLM
1600	0640	Microsoft Gateway Services for NetWare
1614	064e	Microsoft Internet Information Server
1900	076C	Xerox
1947	079b	Shiva LanRover/E 115
1958	079c	Shiva LanRover/T 115

Deci- mal	Hexa- decimal	SAP description
1972	07B4	Cubix WorldDesk
	07c2	Quarterdeck IWare Connect V2.x NLM
	07c1	Quarterdeck IWare Connect V3.x NLM
2084	0824	Shiva LanRover Access Switch/E
2154	086a	ISSC collector NLMs
2175	087f	ISSC DAS agent for AIX
2857	0b29	Site Lock
3113	0c29	Site Lock Applications
3116	0c2c	Licensing Server
9088	2380	LAI Site Lock
9100	238c	Meeting Maker
18440	4808	Site Lock Server or Site Lock Metering VAP/NLM
21845	5555	Site Lock User
25362	6312	Tapeware
28416	6f00	Rabbit Gateway (3270)
30467	7703	MODEM??
32770	8002	NetPort Printers (Intel) or LANport
32776	8008	WordPerfect Network Version
34238	85BE	Cisco Enhanced Interior Routing Protocol (EIGRP)
34952	8888	WordPerfect Network Version or Quick Network Management
36864	9000	McAfee's NetShield anti-virus
38404	9604	?? CSA-NT_MON
46760	b6a8	Ocean Isle Reachout Remote Control
61727	f11f	Site Lock Metering VAP/NLM
61951	f1ff	Site Lock
62723	f503	Microsoft SQL Server
63749	f905	IBM Time and Place/2 application
64507	fbfb	TopCall III fax server
65535	ffff	Any Service or Wildcard

TCP/IP Ports

Capab.	Port no.	Protocol
echo	7	tcp
echo	7	udp
discard	9	tcp
discard	9	udp
systat	11	tcp
systat	11	tcp
daytime	13	tcp
daytime	13	udp
netstat	15	tcp
qotd	17	tcp
qotd	17	udp
chargen	19	tcp
chargen	19	udp
ftp-data	20	tcp
ftp	21	tcp
telnet	23	tcp
smtp	25	tcp
time	37	tcp
time	37	udp
rlp	39	udp
name	42	tcp
name	42	udp
whois	43	tcp
domain	53	tcp
domain	53	udp
nameserver	53	tcp
nameserver	53	udp
mtp	57	tcp
bootp	67	udp
tftp	69	udp
rje	77	tcp
finger	79	tcp
www	80	tcp

Capab.	Port no.	Protocol
www	80	udp
link	87	tcp
supdup	95	tcp
hostnames	101	tcp
iso-tsap	102	tcp
dictionary	103	tcp
x400	103	tcp
x400-snd	104	tcp
csnet-ns	105	tcp
pop	109	tcp
pop2	109	tcp
pop3	110	tcp
portmap	111	tcp
portmap	111	udp
sunrpc	111	tcp
sunrpc	111	udp
auth	113	tcp
sftp	115	tcp
path	117	tcp
uucp-path	117	tcp
nntp	119	tcp
ntp	123	udp
nbname	137	udp
nbdatagram	138	udp
nbssession	139	tcp
NeWS	144	tcp
sgmp	153	udp
tcprepo	158	tcp
snmp	161	udp
snmp-trap	162	udp
print-srv	170	tcp
vmnet	175	tcp
load	315	udp
vmnet0	400	tcp

Capab.	Port no.	Protocol
sytek	500	udp
biff	512	udp
exec	512	tcp
login	513	tcp
who	513	udp
shell	514	tcp
syslog	514	udp
printer	515	tcp
talk	517	udp
ntalk	518	udp
efs	520	tcp
route	520	udp
timed	525	udp
tempo	526	tcp
courier	530	tcp
conference	531	tcp
rxd-control	531	udp
netnews	532	tcp
netwall	533	udp
uucp	540	tcp
klogin	543	tcp
kshell	544	tcp
new-rwho	550	udp
remotefs	556	tcp
rmonitor	560	udp
monitor	561	udp
garcon	600	tcp
maitrd	601	tcp
busboy	602	tcp
acctmaster	700	udp
acctslave	701	udp
acct	702	udp
acctlogin	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctslave2	706	udp

Capab.	Port no.	Protocol
acctdisk	707	udp
kerberos	750	tcp
kerberos	750	udp
kerberos_master	751	tcp
kerberos_master	751	udp
passwd_server	752	udp
userreg_server	753	udp
krb_prop	754	tcp
erlogin	888	tcp
kpop	1109	tcp
phone	1167	udp
ingreslock	1524	tcp
maze	1666	udp
nfs	2049	udp
knetd	2053	tcp
eklogin	2105	tcp
rmt	5555	tcp
mtb	5556	tcp
man	9535	tcp
w	9536	tcp
mantst	9537	tcp
bnews	10000	tcp
rscs0	10000	udp
queue	10001	tcp
rscs1	10001	udp
poker	10002	tcp
rscs2	10002	udp
gateway	10003	tcp
rscs3	10003	udp
remp	10004	tcp
rscs4	10004	udp
rscs5	10005	udp
rscs6	10006	udp
rscs7	10007	udp
rscs8	10008	udp
rscs9	10009	udp
rscsa	10010	udp

Capab.	Port no.	Protocol
rscsb	10011	udp
qmaster	10012	tcp
qmaster	10012	udp

ELSA LANCOM Business internal

This chapter provides information on the internal functions of the router. It is not always necessary in day-to-day work with the ISDN routers but can be very useful to specialists in specific situations.

Script processing

General

Some Internet service providers (e.g. CompuServe) run a script-controlled login procedure before a PPP negotiation. To enable the establishment of such a connection, a simple script process is implemented in the *ELSA LANCOM*.

A script can include the following elements:

Element	Description
<>	Send the included text with a carriage return at the end.
[]	Wait until the included text has been received. The text may be upper or lower case. It is sufficient to enter an unambiguous subtext.
\$U	Send the user name (from the PPP table) with a carriage return at the end.
\$P	Send the password (from the PPP table) with a carriage return at the end.
\$C	End of the script.

As previously noted in the overview, the user name and password are taken from the PPP table if there is an appropriate entry there. If there is no user name in the PPP table, the device name of the *ELSA LANCOM* is forwarded as the user name.

Once the script is complete, a PPP negotiation is started or the login procedure is concluded.

The layer 3 entry in the layer list is used to define whether a PPP negotiation is started after the script has been processed. There are three possible entries:

SCPPP	A synchronous PPP negotiation is started once the script has been processed.
SCAPPP	An asynchronous PPP negotiation is started once the script has been processed.
SCTTRANS	The logical connection to the remote station exists once the script has been processed. There is no more protocol negotiation.

The script list

Scripts are entered in a script list table provided for that purpose. This table is in the /Setup/WAN-module and has the following structure:

Device name	Script
CSERVE	<>[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, another entry similar to the RoundRobin list for the logical remote station may be added. The syntax for this is: Device name followed by '#' and a number. The entries are processed from top to bottom.

Example:

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

In the *ELSA LANconfig* the script list is on the 'Communication' tab.

CompuServe select

The settings required for selection on the CompuServe network via X.75, asynchronous PPP and script control with an example.

Layer list:

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
CSERVE	TRANS	SCAPPP	X.75LAPB	none	HDLC64K

Name list:

Device name	Dialup-remote	B1-DT	B2-DT	WAN-layer	Callback
CSERVE	0021194260	60	60	CSERVE	Off

PPP list:

Device name	Authent.	Key	Time	Rep.	User-name
CSERVE	none	*	0	0	xxxxxx,xxxx/PPP:CISPPP

The CompuServe account is to be entered for xxxxxx,xxxx.

Script list:

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

The script elements have the following meaning:

Element	Meaning
<>	Start script on the remote station by sending a carriage return.
[Host]	Wait for the answer from the CompuServe node. At some point the 'Host Name' will appear in the answer.
<CIS>	Send 'CIS' followed by a carriage return.
[User]	Wait for the answer. CompuServe requests the 'User ID'.
\$U	Send the user name. For CompuServe this consists of the CompuServe User ID with attached '/PPP:CISPPP'. The user name is taken from the PPP table and sent to the remote station with a final carriage return.
[Password]	Wait for the password query.
\$P	Send the password followed by a carriage return. The password will be taken from the PPP table.
[PPP]	Wait for the connect message from the remote station.
\$C	The script is fully processed. The asynchronous PPP negotiation (SCAPPP) in the layer list is started.

Online trace outputs

General

With so-called 'online trace outputs' (control outputs) the user can receive information on internal processes of a working *ELSA LANCOM*. Such information can aid in finding erroneous configurations easily and securely, both from *ELSA LANCOM* and from other devices connected with an *ELSA LANCOM*.

The online trace outputs can be flexibly administered for individual protocols and functions in the firmware and individual configuration sessions. With session-based "Trace Profiles" only the trace information activated within a session is displayed.

The online trace outputs are controlled by a newly implemented command in the remote configuration, which is evaluated by the command interpreter and gives a direct acknowledgment of the settings that have been made to the user. Changes to these settings are effective immediately and generate or suppress the corresponding outputs directly.

The online trace outputs are displayed by the remote configuration with a time delay with respect to the actual event. The time stamp that is optionally displayed reflects the time of the output, but not the time of the actual event. There is usually not a substantial difference between these times; however, this point should always be considered when analyzing the outputs.

All displays within the online trace outputs are shown in plain text so far as possible. Because analysis of network protocols cannot completely avoid showing numerical parameters and a trace system only makes sense when the information displayed is also understood, exact descriptions of the trace information will be given below for all protocols and functions.

If displays are activated for a protocol, the next output will overwrite the current system prompt; every additional output will be preceded by a <Return> <LineFeed>. If the user presses a key, the entire buffered input will be shown again with the current system prompt. The user therefore receives visual feedback and inputs need not to be entered "blind".

Control of trace outputs

Trace outputs are controlled by command line in the usual way. For this purpose, the remote configuration has the command `trace` added; this has the following command syntax:

trace [key] [parameter] ...[parameter]	Shows or influences the status of the trace outputs of individual protocols or functions.
Key	<code>?</code> display a help page <code>+</code> activate the trace outputs <code>-</code> deactivate the trace outputs <code>#</code> toggle the trace outputs (toggle) <code>(no)</code> status display
Parameter	Symbolic protocol or function name.

Keys and parameters must be separated by spaces. The keys are recognized by the command interpreter only if they are unambiguous, i.e. they consist of one of the characters listed above with no prefix or suffix. For the input of the symbolic protocol or function name the input of an unambiguous prefix is sufficient, as usual.

Any number of keys and parameters may be entered in a command line, limited only by the size of the line input buffer. The parameters are processed corresponding to the last

preceding key. If a key is not entered prior to the parameters, the status of that trace function (ON or OFF) is output.

It should also be noted that the command line is processed from left to right. Therefore, the trace output of a parameter can be activated and deactivated several times in one line, because it is toggled from the input buffer while the token is being read (see also examples).

In addition to activating online trace outputs, the preset output of the system time and the protocol names may be activated or deactivated via the key words "Time" and "Source". Without these two displays every trace output is shortened to 21 characters.

Examples for control of trace outputs

The table below is intended to show some practical examples of how the command for the trace outputs can be used:

Input	Effect
trace	Output of all protocols that can be generated in the trace outputs configuration session, and the status of the outputs (ON, OFF).
trace + all	Activates all trace outputs in the current session.
trace + protocol display	Activates all connection structural protocols and the display outputs.
trace + all - icmp	Activates all trace outputs, but deactivates outputs from the ICMP protocol.
trace ppp elsa	Shows the status of the PPP and ELSA trace outputs.
trace # ipx-rt display	Toggles the trace outputs of the IPX router and the display outputs.
trace - time	Deactivates the operating time display before the actual output.

Supported protocols and functions

The following symbolic names for protocol stacks are supported:

Status	Display status messages via connections
Error	Display error messages via connections
PPP	Display PPP protocol negotiation
SCRPT	Display script negotiation
IPX-Rt.	Display IPX routing
RIP	Display IPX routing information protocol
SAP	Display IPX service advertising protocol
IPX-Wd.	Display IPX watchdog spoofing
SPX-Wd.	Display SPX watchdog spoofing

NetBIOS	Display IPX NetBIOS administration
IP-Rt.	Display IP routing
IP-RIP	Display IP routing information protocol
ICMP	Display Internet control message protocol
IP-MASQ	Display procedures in masquerading module
ARP	Display address resolution protocol
DHCP	Display Dynamic Host Configuration Protocols (only <i>LANCOM Office-Router</i>)
Packet dump	Display of the 64 bytes of a packet in hexadecimal format (only <i>LANCOM Office-Router</i>)

In addition to these parameters there are also the following "group parameters" (parameters for a specific type of protocol), with whose aid the online trace outputs for a complete, logically connected protocol family can be activated or deactivated:

All	Display all online trace outputs
Display	Display 'status' and 'error'
Protocol	Display 'ELSA', 'PPP' and 'SCRPT'
TCP-IP	Display 'IP-Rt.', 'IP-RIP', 'ICMP', 'ARP' and 'IP-MASQ'
IPX-SPX	Display 'IPX-Rt.', 'RIP', 'SAP', 'IPX-Wd.', 'SPX-Wd.' and 'NetBIOS'

Finally, still more parameters are recognized with which the display format of the trace outputs can be influenced:

Time	Display the system time as a prefix
Source	Display the generating protocol as a prefix

Every trace output is shortened to 21 characters by switching off the prefix outputs 'time' and 'source'. The output of the prefixes is activated by default.

Prefix output 'time'

By activating the prefix output 'time' every trace output has the system time (at the time the output is generated) in the following form as a prefix:

- Format: [days]d; _[hours]:[Minutes]:[Seconds]_
- Example:
12t; 07:23:15

corresponds to the system time of twelve days, seven hours, twenty-three minutes and fifteen seconds.

Prefix output 'source'

Activation of the prefix output 'source' shows a trace output of the symbolic name of the protocol that caused this trace output. The display is always 9 characters (if necessary by filling spaces).

- Example: ICMP

ie the following trace output was caused by the ICMP protocol.

Online trace 'status'

The outputs under 'status' describe status changes on a WAN interface (at present only the internal S_0 terminal). They are displayed in the following format:

- Format: [Interface] [Status]

- Example:

Ch01: Dial 8700

On the first B channel of the internal S_0 terminal the call number 8700 is dialed.

Online trace 'error'

The outputs under 'error' describe errors that have occurred on a WAN interface. They are displayed in the following format:

- Format: [Interface] [Error]

- Example:

Ch01: No response

The remote station dialed did not react to the call.

Online trace 'PPP'

The point-to-point protocol consists of a collection of subprotocols, of which *ELSA LANCOM* detects and manages the following:

LCP	The link control protocol
PAP	The password authentication protocol
CHAP	The challenge-handshake protocol
IPXCP	The IPX control protocol
IPCP	The IP protocol

These PPP subprotocols are addressed directly in specific phases during a protocol negotiation. The link control protocol is negotiated within the ESTABLISH phase; at this time only LCP packets are permitted within the PPP. If an authentication is negotiated by the LCP, PPP switches into the AUTHENTICATE phase; LCP, PAP and CHAP packets may be transmitted from this point. After the end of the (optional) authentication PPP

switches to the NETWORK phase; LCP, authentication and network control protocol packets (such as IPXCP and IPCP) may be transmitted in any combination from now on. To terminate a PPP connection it switches into the TERMINATE phase where once again only LCP packets are permitted. Once the connection has been terminated, PPP is in the DEAD phase. It will switch into the ESTABLISH phase only when a new connection is established. Every PPP phase change is displayed in the form

Change Phase to [New phase]

approximately as below

Change Phase to AUTHENTICAT

Received and sent packets, important parameters and options with completed actions are displayed for all PPP subprotocols listed above. A received frame is always displayed in the following format:

- Format: [Interface] Rx [Protocol] [Packet type] [Packet type] [Length of packet]

- Example:

Ch01: Rx IPXCP ConfReq ID=00 Length=22

In the above example a configure request for the IPX control protocol with the ID 00 and a length of 22 bytes has been received on the first B channel. If a packet cannot be assigned to any of the five subprotocols, this message appears:

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

- Example:

Ch01: Rx Unknown Protocol 8029

A Packet with the protocol ID 8029 (= Appletalk control protocol) has been received.

Online trace 'IPX-Rt.'

The outputs under 'IPX-Rt.' describe the processing of IPX frames by the IPX router. They are displayed in the following format:

- Format: [Source interface] [IPX target address] [IPX source address] [Target / Action]

- Example:

Internal Rx

DstAddr: 00000002 ffffffff 0453

SrcAddr: 00000002 00a057123456 0453

WAN-Tx Peer: ELSA.SUP.TEST

The IPX router has received a frame from an internal process (in this case from the entity of the routing information protocol) whose target address is assigned to a logical remote station (ELSA.SUP.TEST) and therefore is sent to a WAN interface.

LAN RX

DstAddr: 00000001 ffffffff 0455

SrcAddr: 00000001 0123456789ab 0455

Filter

The IPX router has received a NetBIOS frame (IPX-socket 455) from the local network, which is to be forwarded as broadcast ffffffff to all stations in network 00000001. Because a filter has been set on the socket, the frame is rejected by the router.

Online trace 'RIP'

The outputs under 'RIP' describe the processing of IPX routing information protocol frames by the RIP process of the IPX router. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit/Action] [Source node address] [Frame type] [Para.] [Network address] [Hops] [Tics] [Action] ... [Network address] [Hops] [Tics] [Action]

- Example:

LAN-Rx node: 0000c0123456 Req: 00000002

An RIP request for the IPX network 00000002 is received from the local network. The RIP request was sent from the IPX node 0000c0123456.

- Example:

LAN-Rx node: 00a057123456 Resp

Route: 00000002 Hops: 0001 Tics: 0002 Up

An RIP response (routing information protocol response) was received from the local network (generated by the IPX node 00a057123456). With this response route 00000002, with a hop distance (number of interim stations) of 1 and a tic distance of 2, is entered as available again in the RIP table.

LAN update

The RIP process sends all required routing information to the local network.

Online trace 'SAP'

The outputs under 'SAP' describe the processing of IPX service advertising protocol frames by the SAP process of the IPX router. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit/Action] [Source node address] [Frame type] [Para.] [Service type] [Server name] [Action] ... [Service type] [Server name] [Action]

- Example:

LAN-Rx node: 00a057123456 response

0004 FS_development up

```

0107 FS_development up
023f FS_development up
0511 FS_development up change
030c 08000912345678CGNP-development filtered

```

An SAP response was received (sent by the IPX node 00a057123456) by the local network. With this response the servers 'FS_development' (file server), 'FS_development' (NetWare 386 server), 'FS_development' (DNS server) and 'FS_development' (time sync server) are recorded as available again in the SAP table. In this case the status of the time sync server 'FS_development' has changed in the SAP table (i.e. the server was previously not available). The last displayed server is a print server; because this server type is set with a SAP filter, it is not recorded in the SAP table but is rejected.

LAN trigger

Because of a received SAP response a status change in the SAP table has occurred, which is immediately reported in the local network by the SAP process; the change can therefore only have occurred because of the WAN's evaluation of a SAP response.

LAN age

The SAP process of the router "ages" all server/services forwarded from the local network minute by minute. After a period that can be adjusted a SAP entry is deleted (Setup/IPX-module/SAP-configuration/Aging-minutes)

Online trace 'IPX watchdogs'

The outputs under 'IPX-Wd.' describe the processing of so-called 'IPX watchdog' packets. These are packets that are sent at regular intervals from a Novell server to a workstation to verify the connection to this workstation. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit] [Source address] [Target address] [Action]
- Example:

```
LAN RX
```

```
DstAddr: 12345678 00a057654321 0451
```

```
SrcAddr: 00000002 00a057123456 0451
```

```
SpooF
```

The *ELSA LANCOM* has received an IPX watchdog from the node 00a057123456, which was intended for checking a remote workstation. Because the remote network with the workstation is active, the IPX watchdog is answered locally by *ELSA LANCOM* to avoid establishing a connection unnecessarily. Alternatively the following displays for actions will appear:

- **Route:** The IPX watchdog is forwarded (establishes a connection)
- **Filter:** The IPX watchdog is rejected and not answered
- **Dst Net DOWN Error:** The IPX watchdog target network is not available.

Online trace 'SPX watchdogs'

The processing of 'SPX watchdog' packets by the outputs under SPX-Wd. is described analogous to the trace outputs for IPX watchdogs. These are packets sent by a Novell server at regular intervals to the workstation to check an SPX connection (e.g. R-console). The trace outputs are displayed as follows:

- Format: [Source interface] [Receive/Transmit] [Source address] [Target address] [Action]

therefore completely analogous to the displays of the IPX watchdog packets.

Online trace 'IPX-NetBIOS'

The outputs under NetBIOS describe the processing of IPX NetBIOS and IPX propagated packets. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit] [Source address] [Target address] [Action]
- Example:

```

LAN RX
DstAddr: 12345678 00a057654321 0455
SrcAddr: 00000002 00a057123456 0455
Route
```

Online trace 'IP-Rt.'

The outputs under 'IP-Rt.' describe the processing of IP frames by the IP router. They are displayed in the following format:

- Format: [Source interface] [IP target address] [IP source address] [Protocol] [Target port] [Source port] [Type of service] [Action] [Target]
- Example:

```

LAN RX
DstIP: 195.162.38.161, SrcIP: 194.162.38.162
Prot.: TCP, DstPort: 23, SrcPort: 1197, TOS: ----
Route: WAN-Tx peer: R1
```

The IP router has received a TCP packet from the computer with the IP address 194.162.38.162, which is to be sent to the computer 195.162.38.161.

The source port is 1197, the target port 23 (telnet), a bit is not set in the TOS. The field TOS may accept the following values (or a combination of them):

D---	Low delay
-T--	High throughput
--R-	High reliability
---C	Low costs

The packet is routed and the target computer can be reached under the logical remote station **R1**. Therefore, the packet is sent on a WAN interface.

LAN RX

DstIP: 195.162.38.161, SrcIP: 194.162.38.162

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

Route: WAN-Tx peer: R1

The IP router has received an ICMP packet from the computer with the IP address 194.162.38.162, which is to be sent to the computer 195.162.38.161.

Because ICMP does not know any ports, --- is output as target or source port. The field **High Reliability** is set in the TOS.

Online trace 'IP-RIP'

The outputs under 'IP-RIP' describe the processing of IP routing information protocol frames by the RIP process of the IP router. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/transmit/Action] [Source address] [RIP version] [Routing domain] [Network address] [Network mask] [Best route] [Distance] [Action] ... [Network address] [Network mask] [Best route] [Distance] [Action]

- Example:

LAN-Rx Src: 194.162.38.252

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

190.254.0.0255.255.0.0194.162.38.1623Store

195.126.38.0255.255.255.0194.162.38.1623update

255.255.255.2550.0.0.0194.162.38.1622Discard

194.162.38.0255.255.255.0194.162.38.1622Discard

An RIP-1 frame has been received from the local network. This frame contains the route to the networks 190.254.0.0, 195.126.38.0, 255.255.255.255 (DEFAULT route) and 194.162.38.0. The procedure with these routes was as follows:

Route 190.254.0.0 is saved because it is either better than the prior one or is still unknown.

Route 195.126.38.0 is processed, ie the route is unchanged, only the distance may have changed. In every case the aging timer is reset.

The DEFAULT route has been rejected because a better route is known.

The route to network 194.162.38.0 is rejected because it is a route to the local network (split horizon).

The trace outputs of received RIP frames are always done after they have been evaluated by the RIP process and network masks (RIP-1) and best route have been determined. With RIP frames that have been sent the packets are displayed as they were sent. For example, with RIP-1 frames this means that the network masks are always output as 0.0.0.0.

Online trace 'ARP'

The outputs under 'ARP' describe the processing of address resolution protocol frames by the TCP-IP module. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit/Action] [Source address] [Target address] [Target/Action]

- Example:

LAN-Rx request

SrcIP: 194.162.38.162, DstIP: 194.162.38.171

Cache update: 194.162.38.162 : 0000c0717860

Response LAN-Tx

An ARP request for the IP address 194.162.38.171 has been received from computer 194.162.38.162. The MAC address of the source computer is saved in the ARP table. In addition, the queried computer is the *ELSA LANCOM*. Then an ARP response is sent back on the LAN interface.

Online trace 'ICMP'

The outputs under 'ICMP' describe the processing of Internet control message protocol frames by the TCP-IP module. The trace outputs are displayed in the following format:

- Format [Source/Target interface] [Receive/Transmit] [Source/Target address] [Message] [Action]

- Example:

LAN RX

SrcIP: 194.162.38.162: Echo request

LAN TX

DstIP: 194.162.38.162: Echo reply

An ICMP echo request (**ping**) from computer 194.162.38.162 has been received on the LAN interface. The *ELSA LANCOM* answers this with an ICMP echo reply.

Online trace 'IP-MASQ'

The outputs under 'IP-MASQ' describe the procedures in the masquerading module. The opening and the closing of a masked connection is output. The display is in the following format:

- Format: [Open/close]: [Protocol] [IP source address] [Source port] [Mapped port] [Reason]

TCP, UDP or ICMP are possible protocols. If the protocol is ICMP, the source port gives the identifier of the request packet. The mapped port field shows how the source port has been set. The cause of a close is given in the reason field. Possible reasons are:

Timeout	The set protocol timeout is expired
TCP finish	A TCP connection was terminated normally
TCP reset	A TCP connection was interrupted because of an error in one of the machines involved
Port assigned	A 'passive' TCP connection was assigned to source port. Example: FTP in passive mode

- Examples:

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

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

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

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

Online trace 'SCRPT'

The outputs under 'SCRPT' describe the progress of a script negotiation. The display is in the following format:

- Format: [Source interface] [Receive/transmit/Error] [Text] [Action]

- Example:

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

In the above example, the password is requested by the remote station. It is returned to the remote station (hidden under a '*').

Online trace 'DHCP'

The outputs under 'DHCP' describe the procedures in the Dynamic Host Configuration Protocol. The queries from DHCP clients and the answer from the DHCP servers are then displayed in the *ELSA LANCOM*. The display is in the following format:

- Format: [DHCP Client Message] [DHCP Server Message]

Online trace 'packet dump'

The 'packet dump' online trace supplements the trace outputs, which are generated by the IP router. The first 64 bytes of a packet is output in hexadecimal format.

Policy based routing

General

The term 'policy based routing' describes the option of using additional routing methods to the standard routing procedure for IP packets (these "policies").

To make the in-band configuration easier on wide-area networks with heavy data traffic and to improve the cooperation of *ELSA LANCOM* with 'ping' and 'traceroute' mechanisms, two methods for the IP routing have been introduced. Both methods are based on the evaluation of the 'Type of Service' field in the IP header.

The 'Type of Service' field (for short TOS) describes how IP packets should preferably be treated (but need not be), i.e. it reflects the preferred processing procedure intended by the generator of this IP packet. TOS has the following structure in this context:

Bit 7, 6	Bit 5	Bit 4	Bit 3	Bit 2, 1, 0
Unused	Reliable transmission	High Throughput	Low delay	Precedence

The **R** and the **D** bit are evaluated and the behavior adapted to its circumstances by the routing methods.

A set **R** bit requires secured transmission of the associated IP packet. Packets identified as such are always transmitted over a "secured" queue corresponding to their reception sequence. In an extreme case this can result in a "normal" packet that is already in a transmission queue being removed and placed back into the heap to make room for the packet to be sent. This occurs if the maximum number of buffers for the associated connection has already been used. However, the transmission sequence between packets with a set **R** bit and 'normal' bits is not changed by this mechanism.

The secured transmission can be activated for all ICMP packets independently of the entry in the 'Type of Service' field. Because an ICMP packet identified as such is sent without changing the transmission sequence, the throughput delays of a *ELSA LANCOM* can be determined by 'ping' or 'traceroute'.

With a set **D** bit the generator requests the fastest possible forwarding of an IP packet. IP packets identified as such are transmitted over an 'urgent' queue before the send queue packets corresponding to their reception sequence. On one hand, this results in changes in the transmission sequence, because an IP packet identified as last received

is sent first. On the other hand, there is the possibility that a packet already in the send queue will be removed from it again to make room for the IP packet that is to be sent (see above).

Packets that are already in the secured or urgent queue are not rejected. If there is no longer a packet in the normal send, secured or urgent queue, no more packets can be sent. Received IP packets are therefore rejected even with the **D** or **R** bit set.

Examples

With the setting

`Setup/IP-router-module/Routing-method/IP TOS`

the 'Type of Service' field of the IP header of a received packet is evaluated as described above, ie IP packets with set **D** bit are placed in the urgent queue and packets with set **R** bit in the secured queue. All other packets are placed in the normal send queue.

This means simultaneously that any "normal" IP packets from "secured" or "urgent" packets can be removed (with maximum filling of the send queue of this connection) or changes in the packet sequence can be made.

In the 'normal' setting all IP packets are treated equally, in accordance with the routing regulations of the Internet protocol.

With the setting

`Setup/IP-router-module/Routing-method/ICMP-routing-method`
all received ICMP packets are transmitted as if they had the **R** bit in the 'Type of Service' field of the IP header. (see above)

This means that the secured transmission of ICMP packet may result in errors in other data flows. The latency period of the router is however not influenced, because the ICMP packet is taken into the send queue as the last in spite of this.

With the 'normal' setting ICMP packets are treated like all other IP packets in accordance with the routing regulations of the Internet protocol.