

ELSA LANCOM™ Wireless IL-2

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 della merce prevista nelle condizioni di vendita e di consegna.

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

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, ottobre 1999

No.: 20943/1099

Qualche parola di presentazione

Vi ringraziamo per la fiducia accordataci

Le reti radio di ELSA rappresentano un'alternativa o un'integrazione economica di reti locali collegate via cavo (LAN). Con le schede di rete radio mobili notebook e PC possono comunicare tra loro o avere accesso tramite le stazioni base a rete collegate via cavo e addirittura a reti ISDN.

La presente documentazione si rivolge agli utenti della stazione base *ELSA LANCOM Wireless IL-2*. All'inizio verrà presentata l'apparecchiatura e le sue possibilità, verrà poi fornito all'utente l'aiuto per il collegamento e l'installazione del software e verranno quindi mostrati primi esempi applicativi.

Documentazione

La documentazione allegata è costituita da:

- Manuale
Installazione hardware, descrizione delle funzioni e tipi di funzionamento e primi esempi di configurazione
- Documentazione elettronica (su CD)
Tutti i manuali della serie, fondamenti tecnici (per es. su schede di rete radio, informazioni generali sulle reti, TCP/IP ecc.), workshop con esaurienti esempi di applicazioni, riferimenti per la consultazione con descrizione completa dei manu

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 (Internet-server 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. Driver aggiornati, firmware, tool e manuali sono disponibili in ogni momento per essere scaricati.

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

Contenuti

Introduzione	1
Come opera una rete radio?	1
Che cosa offre un <i>ELSA LANCOM Wireless IL-2?</i>	4
Installazione	11
Complesso di fornitura.....	11
<i>ELSA LANCOM Wireless</i> si presenta	11
Come collegare la stazione base	13
Installazione del software	14
Configurazione di base	14
Effettuare le impostazioni di base con <i>ELSA LANconfig</i>	14
Effettuare le impostazioni di base tramite Telnet.....	16
Possibilità di configurazione	17
Onde radio o cavo: Vie per la configurazione.....	17
Presupposti.....	17
Alternativa: Gestione indirizzi con il server DHCP	17
Avviare la configurazione tramite <i>ELSA LANconfig</i>	18
Avviare la configurazione tramite Telnet.....	19
Comandi per la configurazione	19
Nuovo firmware con FirmSafe	20
FirmSafe funziona così.....	20
Un nuovo software si carica così.....	21
Configurazione con SNMP	22
Funzioni e modalità	23
Parametri per i collegamenti radio	23
Sicurezza per la configurazione	25
Protezione con password	25
Il blocco del login	25
Controllo in arrivo tramite TCP/IP	26
Sicurezza per la LAN	26
Il controllo	26
La chiamata di risposta.....	28
Come nascondersi: mascheratura IP (NAT, PAT).....	28
Gestione degli addebiti.....	28
Limitazione della connessione in base al tempo.....	29
Impostazioni nel modulo addebiti.....	29
Connessioni ISDN	29
Name-list.....	30
Impostazioni di interfaccia.....	31

Impostazioni di interfaccia router	31
Impostazioni di interfaccia <i>LANCAPi</i>	32
Lista layer	32
Lista RoundRobin	33
Lista PPP	33
Script	34
Accettazione di chiamate	34
Lista dei numeri	35
Point-to-point protocol	35
Il protocollo	36
La lista PPP	37
Tutto o.k.? Controllo della linea con LCP	38
Routing IP	39
Tabella di routing IP	39
Filtro per i pacchetti TCP/IP	40
Proxy ARP	40
Routing locale	41
Routing dinamico con IP-RIP	42
Mascheratura IP (NAT, PAT)	43
DNS forwarding	44
Policy Based Routing	45
Gestione indirizzi automatica con DHCP	45
Il server DHCP	46
DHCP – 'On', 'Off' o 'Auto'?	46
Gli indirizzi vengono assegnati in questo modo	47
Configurazione del server DHCP	50
DNS	52
Che cosa fa un server DNS?	52
Come si imposta il server DNS	53
NetBIOS-Proxy	55
In breve: Che cosa è il NetBIOS?	55
Trattamento dei pacchetti NetBIOS	56
Quali sono i presupposti indispensabili?	57
Come si connettono due reti Windows tramite ISDN	60
Come si seleziona un computer con accesso remoto	61
Cercato – trovato: L'ambiente di rete	62
Comunicazione di ufficio e <i>ELSA LANCAPi</i>	63
<i>ELSA LANCAPi</i>	63
Il Least-Cost-Router	67
Appendice	73
Dati tecnici	73
Specifiche hardware	73

Specifiche software	73
Canali radio	74
Condizioni generali di garanzia a partire dal 01.06.1998	76
Dichiarazione di conformità	78

Index	81
--------------------	-----------

Technical basics (on CD only)	R1
--	-----------

Wireless network according to the IEEE-802.11 standard	R1
Ad hoc mode	R1
Infrastructure mode	R2
Interchangeability with other devices	R3
Network technology	R4
The network and its components	R4
Connection modes	R4
Kinds of networks	R6
IP addressing	R6
IP routing and hierarchical IP addressing	R9
Expansion through local networks	R11

Description of the menu options (on CD only)	R17
---	------------

Status	R19
Status/Connection-state	R20
Status/Current-time	R20
Status/Operating-time	R20
Status/S0-bus	R20
Status/WLAN-statistics	R21
Status/WAN-statistics	R22
Status/LAN-statistics	R25
Status/PPP-statistics	R26
Status/TCP-IP-statistics	R32
Status/IP-router-statistics	R38
Status/Config-statistics	R40
Status/Queue-statistics	R41
Status/Connection-statistics	R42
Status/Info-connection	R43
Status/Layer-connection	R43
Status/Call-info-table	R44
Status/Remote-statistics	R44
Status/Channel-statistics	R45
Status/Time-statistics	R46
Status/LCR-statistics	R47
Status/PCMCIA-status	R47
Status/Delete-values	R47

Setup	R48
Setup/WAN-module	R49
Setup/LAN-module	R58
Setup/TCP-IP-module	R59
Setup/IP-router-module	R62
Setup/SNMP-module	R70
Setup/DHCP-server-module	R71
Setup/NetBIOS	R73
Setup/Config-module	R76
Setup/LANCAPI-module	R77
Setup/WLAN-module	R78
Setup/LCR-module	R79
Setup/DNS module	R80
Setup/Time-module	R82
Firmware	R82
Other	R84

Ports and protocols(on CD only) R85

Ports	R85
Protocols	R87



Introduzione

I vantaggi una LAN collegata via radio sono evidenti: Notebook e PC possono essere collocati dove necessari – grazie al collegamento senza fili i problemi per la mancanza di prese o per modifiche strutturali appartengono al passato.

Collegamenti di rete durante conferenze o presentazioni, accesso a risorse in edifici limitrofi, scambio di dati con terminali mobili e molto altro ancora... queste le comodità della LAN via radio.

In una rete collegata via cavo il ruolo centrale spetta alla stazione base. Attraverso la stazione base tutte le stazioni in rete radio possono accedere alla LAN.

Tramite il router IP integrato e l'interfaccia ISDN si collega la propria intera LAN con il mondo esterno. L'accesso a Internet per l'intera LAN o per le funzioni di ufficio come fax e segreteria telefonica in tutti i posti di lavoro sono solo alcuni dei vantaggi offerti dal router ISDN.



In alcuni paesi europei, a causa di direttive nazionali, l'utilizzo di frequenze del campo di 2,4 – 2,48 GHz è limitato o possibile solo in seguito alla concessione di un permesso. La lista delle autorizzazioni nazionali si trova in un foglio a parte fornito.

Come opera una rete radio?

In questo capitolo si conoscerà il modo di funzionamento in linea di principio di una rete radio. Vengono spiegati i termini usati e viene spiegato il montaggio e le possibilità di impiego. Informazioni tecniche dettagliate su questo argomento e su altri si trovano nella documentazione elettronica sul CD.

*Schede di rete
radio
WLAN*

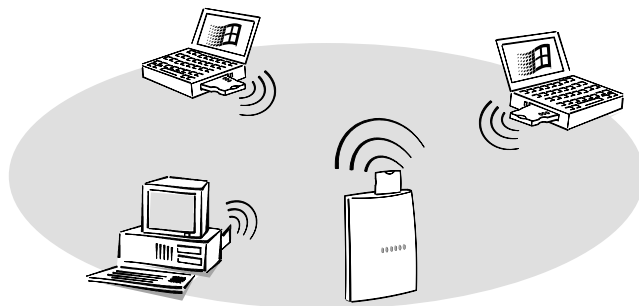
Con le schede di rete radio si collegano singoli notebook e PC in una rete locale, una **Local Area Network** (LAN). Poiché in questa LAN il cavo comunemente usato viene sostituito da un collegamento radio, queste reti radio vengono anche chiamate **Wireless Local Area Network** (WLAN).

Stazione base

La stazione base costituisce il collegamento tra la LAN e la WLAN. Da un lato disponendo di uno slot per una scheda di rete radio (*ELSA AirLancer MC-2*), e dall'altro con un normale connettore Ethernet, la stazione base trasferisce tutti i dati tra le due reti. La stazione base prolunga per così dire un cavo di rete tramite un ponte radio fino alle stazioni mobili.

Radiocellula

Il campo massimo nel quale le schede di rete radio delle stazioni mobili e le stazioni base possono raggiungersi a vicenda e scambiare dati, viene definito come radiocellula.

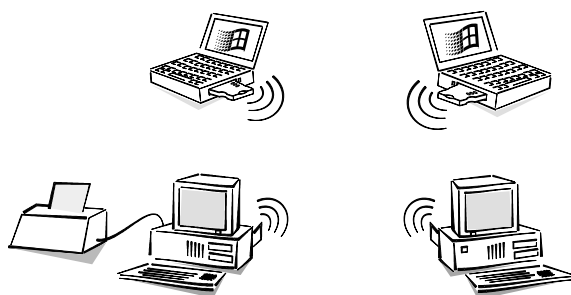


In una rete radio si hanno a disposizione tutte le funzioni di una rete a cavo: è possibile l'accesso a file, server, stampanti ecc. così come collegare stazioni mobili di un sistema di mail interno.

Con le schede di rete radio e le stazioni base di ELSA si hanno a disposizione le seguenti possibilità di impiego:

Collegamento diretto al PC

Con le schede di rete radio si collegano direttamente tra loro due o più computer. Tutti i computer di una WLAN possono comunicare l'uno con l'altro senza un hardware aggiuntivo.

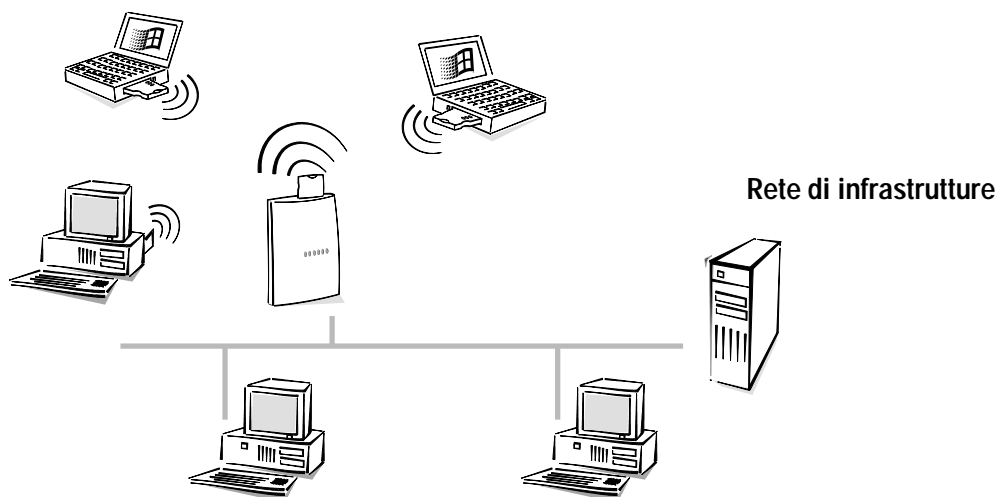
**Rete ad hoc***Peer-to-peer*

Questo impiego viene in generale anche denominato come rete peer-to-peer, nella terminologia della rete radio questo tipo di messa in rete si definisce rete ad-hoc.

Collegamento a una LAN collegata via cavo

Mediante una stazione base tutti i computer con schede di rete radio hanno accesso a una rete collegata via cavo. La stazione base serve da una parte come collegamento tra

LAN e WLAN; e dall'altra costituisce la centrale per lo scambio dati all'interno della WLAN.



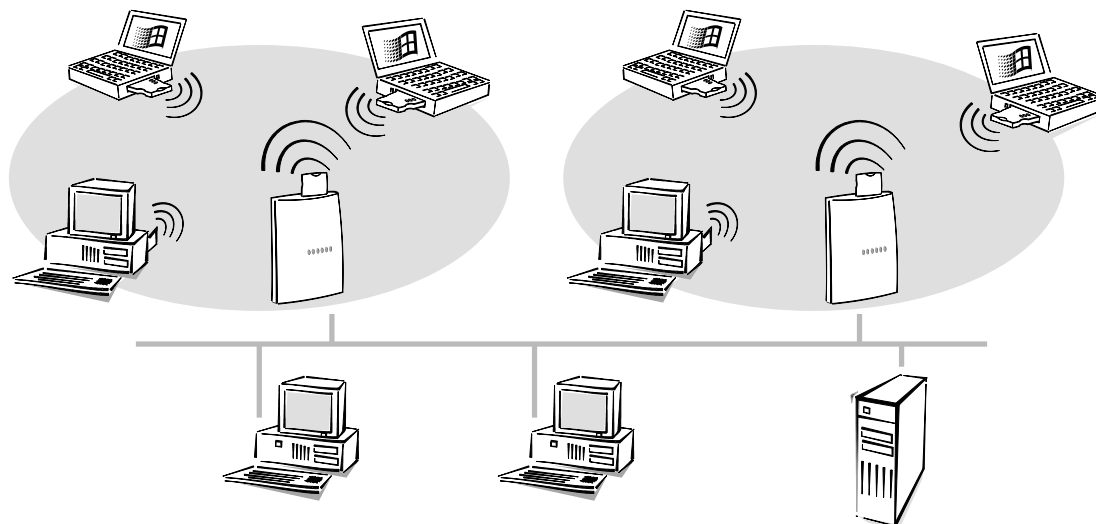
Peer-to-LAN

Una rete radio con una stazione base viene in generale chiamata anche rete peer-to-LAN, nella terminologia della rete radio questi tipo di messa in rete si definisce rete infrastruttura.

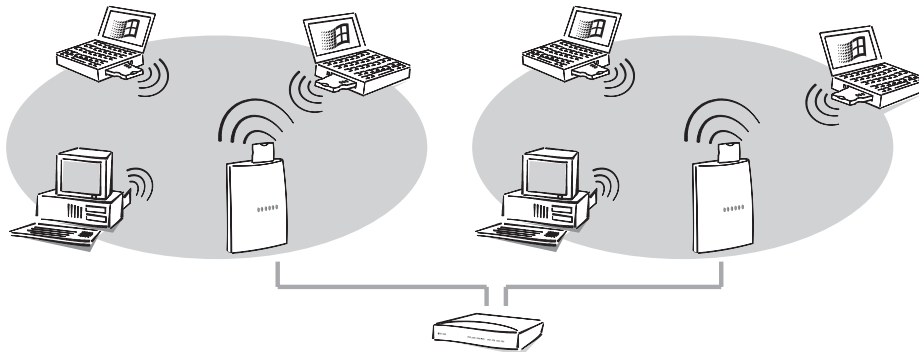
Questo tipo di rete rappresenta un'integrazione ideale delle LAN attuali. In caso di estensione di una LAN in un settore dove il cablaggio è impossibile o antieconomico, la rete infrastruttura è l'alternativa ideale.

Scalabilità

Se il raggio di azione di una radiocellula non è più sufficiente a collegare tutte le stazioni mobili in una rete radio, si possono impiegare anche più stazioni base. In tal modo il cavo di rete del LAN viene usato come ponte per il raggio di azione mancante.



Questo principio funziona anche se non esiste alcuna LAN a cavo, poiché si vuole costruire una nuova rete radio. Se le stazioni mobili non si trovano tutte all'interno del raggio di azione di una stazione base, se ne impiega una seconda. Le due stazioni base possono poi per es. venire collegate tramite un semplice cavo di rete e un hub.



Per un raggiungimento di un'elevata copertura, le radiocellule possono anche sovrapporsi. Per evitare disturbi nella rete radio, possono essere scelti per la le singole cellule canali diversi (fino a 14).

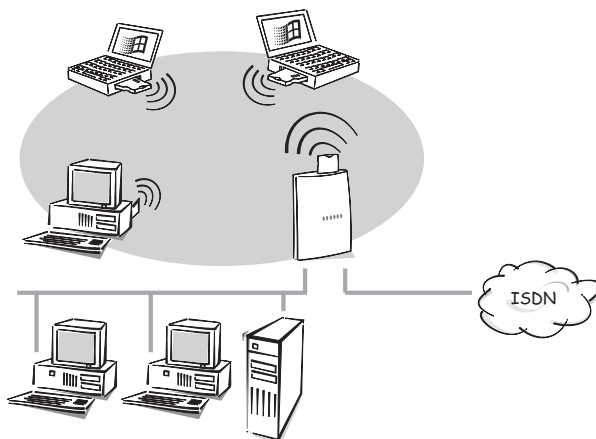
Roaming

Roaming è il passaggio trasparente tra due celle radio. Gli utenti possono passare da una cella e all'altra senza perdere la connessione di rete. Le stazioni base scambiano attraverso la rete LAN continuamente informazioni sullo stato delle stazioni radio.

Un'importante premessa al funzionamento del roaming, è che tutte le stazioni base siano connesse ad una rete Ethernet. Bridges, Switches e Repeater sono permessi, Router no!

Connessione ISDN

Una particolare funzione aggiuntiva è offerta dalla stazione base *ELSA LANCOM Wireless IL-2*. La stazione base collega tramite l'interfaccia ISDN non solo la rete radio con una LAN a cavo, bensì contemporaneamente con la rete ISDN.



Insieme con la complessità funzionale di un router IP, sono in tal modo possibile ulteriori applicazioni come l'accesso a Internet per tutti i computer nella LAN e WLAN.

Che cosa offre un *ELSA LANCOM Wireless IL-2*?

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

Facile installazione

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

Connessione LAN

Le stazioni base per rete radio di ELSA operano in Ethernet. Tramite il connettore 10Base-T e un hub o switch si collega *ELSA LANCOM Wireless* con la LAN 10 Mbit.

Connessione della rete radio

Le schede di rete radio delle stazioni base di ELSA operano secondo lo standard IEEE 802.11. Questo standard rappresenta un ampliamento delle norme IEEE già esistenti per le LAN, delle quali IEEE 802.3 per Ethernet è la più nota.

Per la trasmissione dati senza fili, si possono impiegare in linea di principio diversi metodi fisici:

- Trasmissione a raggi infrarossi
- Onde radio con frequency hopping
- Onde radio con metodo DSSS (**D**irect **S**equenz **S**pread **S**pectrum)

In questo metodo impiegato anche in campo militare per accrescere la sicurezza contro le intercettazioni, prima della trasmissione i dati vengono frammentati e suddivisi in una grande banda di frequenza (spread spectrum). In tal modo si assicura un trasferimento affidabile e sicuro contro le intercettazioni.

Le schede di rete radio di ELSA impiegano il metodo DSSS. Accanto ai vantaggi della schermatura contro disturbi causati da altri trasmettitore che eventualmente usano la stessa banda di frequenza, le schede diventano anche compatibili a sistemi di altri produttori.

IEEE 802.11 permette il servizio di reti radio locali attraverso zone pubbliche e private nella banda di frequenza ISM (**I**ndustrial, **S**cientific, **M**edical: 2,4 fino a 2,483 GHz).

La massima larghezza di banda della trasmissione dati della rete radio è pari a 2 Mbit/s. Il raggio di azione della trasmissione dati è pari all'aperto a massimo 300 metri, in edifici tipicamente a ca. 30 metri.

Connessione WAN

Un *ELSA LANCOM Wireless* viene collegato all'interfaccia(e) S_0 di una connessione ISDN in configurazione punto-a-più punti (connessione multipla) o in configurazione punto-a-punto (connessione impianto). Il router riconosce automaticamente il tipo di connessione

e il protocollo canale D utilizzato. Si possono utilizzare connessioni a selezione con DSS1 o 1TR6 come pure connessioni fisse. Le connessioni fisse sono una caratteristica aggiuntiva che si può richiedere alla ELSA.

Raggruppamento di canali e compressione

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

Bridging trasparente

I pacchetti di dati dalla LAN a cavo vengono trasferiti alla rete radio e viceversa. Oltre a ciò c'è la possibilità di limitare il traffico di dati a determinati protocolli e stazioni.

Display di stato

Le spie LED sul pannello frontale della stazione base rendono possibile il controllo di connessioni ISDN e Ethernet come pure dei collegamenti a cavo correnti e facilitano in tal modo la diagnosi nel caso di possibili disturbi del sistema.

ELSA LANmonitor

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

- Stato 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 software consente di verbalizzare e memorizzare i messaggi sul PC per impieghi successivi.

Protezione 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 per ogni connessione automaticamente il gestore 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 delle apparecchiature al compito specifico desiderato, si realizza in modo rapido e comodo per mezzo del tool di configurazione in dotazione *ELSA LANconfig* per i sistemi operativi Windows. Gli utenti di altri sistema operativi utilizzano Telnet.

L'accesso all'apparecchio è possibile da WAN (via ISDN), da WLAN o LAN. In caso di configurazione da LAN o da WLAN, 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 telefonico (CLIP) anche una funzione di richiamata, che consente solo il collegamento alla linea verso utenze telefoniche prestabilite. Il filtro firewall e il mascheratura IP completano il sistema di sicurezza. Inoltre il blocco del login impedisce gli « attacchi Brute-Force » 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 della configurazione di ELSArouter, nei luoghi in cui nessuno può o deve occuparsi 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 impedito a chiamanti non autorizzati.

Software-update

Per rimanere sempre nelle condizioni più aggiornate in campo software, le periferiche 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, WLAN o attraverso WAN (ISDN).

FirmSafe

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

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

ELSA LANCAPI e ELSA CAPI Faxmodem

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

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

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

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

DHCP

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

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

NetBIOS-Proxy

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

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

Server DNS

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

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

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.

Installazione

Il presente capitolo aiuterà l'utente a creare in modo possibilmente rapido una nuova rete radio. Si vedrà prima quale sia il complesso di fornitura del prodotto e si conoscerà poi l'apparecchiatura. A questo punto viene mostrato come collegare l'apparecchiatura e come fare a metterla in servizio.

Complesso di fornitura

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

- Stazione base *ELSA LANCOM Wireless IL-2*
- Alimentatore
- Scheda di rete radio *ELSA AirLancer MC-2*
- Cavo di connessione LAN
- Cavo di collegamento ISDN
- Documentazione
- CD con *ELSA LANconfig* e altro software e documentazione elettronica

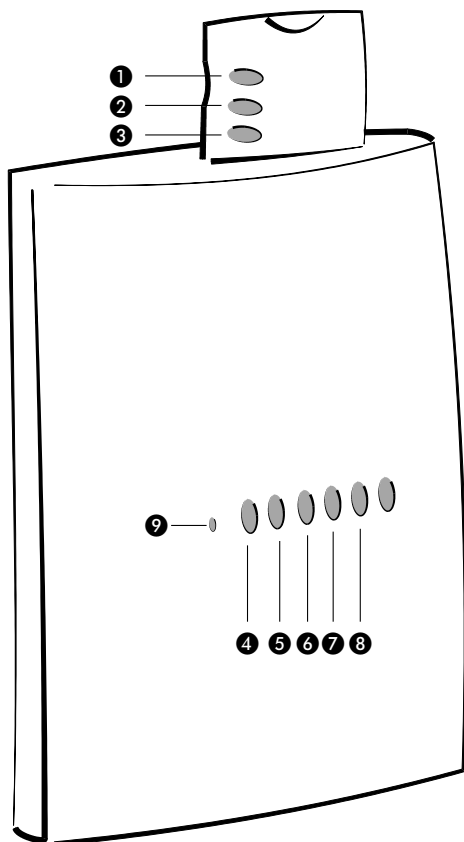
Se dovesse mancare qualcosa, rivolgersi direttamente al proprio fornitore.

ELSA LANCOM Wireless si presenta

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

LED

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



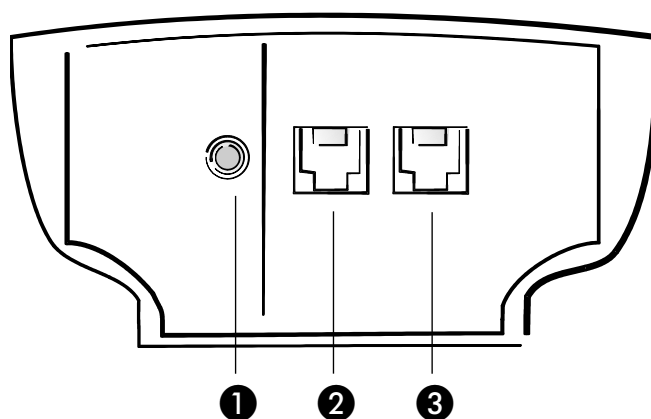
- ❶ Il LED rosso della scheda di rete radio mostra che è stabilito un collegamento tra la scheda e la stazione base.
- ❷ Il LED giallo della scheda di rete radio mostra il numero delle stazioni mobili che si sono registrate presso questa stazione base. Nel caso di tre stazioni registrate il LED lampeggia per es. tre volte consecutivamente e fa poi una pausa.
- ❸ Il LED verde della scheda di rete radio indica l'attività sulla rete radio, quindi la trasmissione e la ricezione di pacchetti di dati. Se questo LED non è acceso o se lo è in permanenza, si ha un'anomalia della scheda di rete radio.
- ❹ Il LED 'Power/Msg' della stazione base viene acceso brevemente all'attivazione dell'alimentazione. Dopo l'autotest, un errore eventualmente riscontrato viene emesso come codice a lampeggio, oppure l'apparecchio entra in servizio e il LED rimane costantemente acceso.

spento		Apparecchio disinserito, ma non senza tensione
verde	1 x breve	Bootstrap (verifica e caricamento) iniziato
verde	lampeggianti	Visualizzazione di un errore di bootstrap (codificato con codice a lampeggio)
verde		Apparecchio pronto per il servizio

- ❺ Il LED 'S₀-status' della stazione base mostra l'attività del canale D.

- ⑥ Il LED 'WAN-Channel-1' della stazione base mostra l'attività del primo canale B sull'interfaccia ISDN.
- ⑦ Il LED 'WAN-Channel-2' della stazione base mostra l'attività del secondo canale B sull'interfaccia ISDN.
- ⑧ Il tasto di reset è nascosto e può essere premuto solo con un oggetto appuntito (per es. una graffetta). Premere il tasto di reset fino a che tutti i LED si accendono, in tal modo l'apparecchiatura viene reimpostata nello stato al momento della fornitura.

Adesso ruotare il tutto e dare un'occhiata al lato inferiore. Lì si trova:



- ① Connessione per l'alimentatore
- ② Connessione di rete 10Base-T
- ③ Collegamento ISDN S₀

Come collegare la stazione base

- ① Collegare la stazione base *ELSA LANCOM Wireless IL-2* con il LAN. Innestare a tale scopo il cavo di rete fornito nel connettore 10Base-T della stazione base e in una presa di rete libera della propria rete locale (o in una presa libera di un hub della propria LAN).
- ② Collegare il router ad una rete ISDN-S₀ a più apparecchi o tramite centrale telefonica (configurazione punto-multipunto o punto-punto). Per utilizzare la protezione degli scatti e la loro statistica, è necessario richiedere presso il gestore del servizio la proprietà ISDN 'Trasmissione scatti **durante** il collegamento' (secondo AOCD).
- ③ Innestare la scheda di rete radio *ELSA AirLancer MC-2* nella stazione base. Nel farlo i LED della scheda per PC devono essere rivolti verso il davanti della stazione base.
- ④ Alimentare la stazione base tramite l'alimentatore con la tensione necessaria. Dopo un breve autotest dell'apparecchiatura, il LED 'Power/Msg' della stazione base si

accende in modo permanente. Il LED rosso della scheda di rete radio mostra che è stabilito un collegamento tra la scheda e la stazione base. Il tremolare del LED verde della scheda di rete radio, indica che questa tenta di raggiungere altre stazioni nella WLAN. Il LED 'LAN-Status' indica il corretto collegamento tra stazione base e LAN.

Installazione del software

Il software di configurazione *ELSA LANconfig* per i sistemi operativi Windows permette di impostare la propria stazione base in modo semplice e comodo per l'impiego desiderato.



I parametri per la rete radio sono impostati nello stato al momento della fornitura già in modo che nella maggior parte dei casi si può subito iniziare. Modifiche alla configurazione sono necessarie solo con particolari impieghi.

Per il servizio del software di configurazione si necessita o di un PC nella rete a cavo LAN o nella rete radio.

- ① Installare prima il protocollo di rete TCP/IP nel computer con il quale si vuole impostare la propria stazione base.
- ② Installare alla fine il software di configurazione *ELSA LANconfig*. Se il programma setup non si avvia automaticamente quando si inserisce il CD *ELSA LANCOM Wireless*, da Gestione risorse (Explorer) di Windows fare clic su 'autorun.exe' del CD e seguire le ulteriori istruzioni della routine di installazione.

Configurazione di base

Nella configurazione di base viene stabilito l'indirizzo IP per la stazione base. Viene inoltre deciso l'utilizzo del server DHCP integrato. La configurazione di base può essere fatta con *ELSA LANconfig* o con Telnet.

Effettuare le impostazione di base con *ELSA LANconfig*

Al primo avvio di *ELSA LANconfig* la stazione base nella rete TCP/IP viene riconosciuta e può essere subito configurata. Per farlo si avvia automaticamente un assistente che è di aiuto per l'impostazione di base dell'apparecchiatura o che può addirittura effettuare da solo tutte le operazioni.

- ① Avviare il nuovo software con **Start ► Programmi ► ELSAlan ► ELSA LANconfig.**



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



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

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

- ③ Scegliere l'opzione 'Desidero impostare tutto manualmente' se si ha esperienza con le reti e indirizzi IP e se è vera una delle seguenti affermazioni:
- L'utente non ha finora usato nella propria rete alcun indirizzo IP, ma adesso desidera farlo. L'utente stesso desidera però stabilire l'indirizzo IP per la stazione base e attribuirle un indirizzo qualsiasi compreso in aree di indirizzamento riservate per scopi privati, per es. '10.0.0.1' con la maschera di rete '255.255.255.0'. In tal modo s stabilisce anche contemporaneamente l'area di

indirizzamento, che poi il server DHCP userà per le altre apparecchiature della rete (a meno che il server DHCP non venga disattivato).

- L'utente ha finora già usato per i computer della LAN indirizzi IP. Assegnare alla stazione base un indirizzo libero dell'area di indirizzamento finora usata e scegliere se la stazione base debba operare come server DHCP o no.



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

- ④ Con questi pochi clic del mouse la propria stazione base è impostata definitivamente per il compito di base di rendere possibile alle stazioni mobili l'accesso ad una LAN a cavo.

Effettuare le impostazioni di tramite Telnet

Se non si desidera o non si può usare *ELSA LANconfig* (per es. poiché si dispone di un sistema operativo diverso), è possibile effettuare le impostazioni di base anche tramite un collegamento Telnet.

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

Digitare i seguenti comandi:

- ① Il collegamento Telnet lo si avvia per es. con il comando **Start ► Esegui** e digitando poi nella finestra che si è aperta `telnet 10.0.0.254`.

- ② Modificare la lingua per la configurazione con il comando:

```
set /setup/config-module/language italiano
```

- ③ Indirizzo Intranet e maschera di rete:

```
set /setup/TCP-IP-module/indirizzo Intranet 10.0.0.1
```

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

Dopo che si è modificato l'indirizzo Intranet, si deve eventualmente riavviare il router.

- ④ Disattivare eventualmente la funzione DHCP:

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



Possibilità di configurazione

Le stazioni base di ELSA vengono sempre fornite con un software aggiornato nel quale sono già presenti alcune impostazioni per l'utente.

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

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

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

Onde radio o cavo: Vie per la configurazione

Con la configurazione inband (configurazione tramite la rete) si ha accesso da ogni computer del WLAN o LAN o WAN (ISDN) alla stazione base. L'accesso può però essere limitato o bloccato del tutto dalla lista di accessi IP. Per la configurazione si utilizza Telnet (in dotazione con la maggior parte dei sistemi operativi) o 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.

Presupposti

La configurazione con Telnet o con *ELSA LANconfig* si realizza tramite TCP/IP oppure TFTP. A tale scopo nel computer usato si deve quindi installare il TCP/IP, e la propria stazione base necessita di un indirizzo IP con il quale poter accedere ad essa.

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 si ha già un computer con l'indirizzo XXX.XXX.XXX.254 nella propria rete, come prima cosa spegnerlo. Non appena si è stabilito con ELSA LANconfig o Telnet un collegamento alla stazione base, assegnarle un altro indirizzo IP libero.

Alternativa: Gestione indirizzi con il server DHCP

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



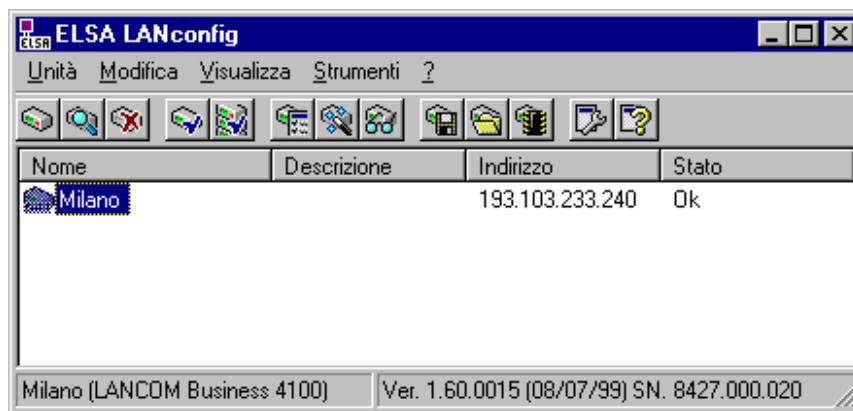
Avviare la configurazione tramite *ELSA LANconfig*

Richiamare il tool di configurazione *ELSA LANconfig* per es. dalla barra di avvio di Windows con **Start ► Programmi ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* cerca automaticamente nella rete locale le apparecchiature.



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

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



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

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

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



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

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

Avviare la configurazione tramite Telnet

Avviare tramite Telnet, per es. da un box DOS, la configurazione con il comando:

```
telnet 10.1.80.125
```

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

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


Comandi per la configurazione

Quando si utilizza Telnet o un emulatore di terminale per la configurazione 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 barretta obliqua inversa. I comandi e le voci delle tabelle non devono essere scritti completamente, è sufficiente una abbreviazione univoca.

Nella configurazione 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. Nelle righe delle tabelle si introducono tutte le voci separate da spazi. Un * lascia la voce inalterata.	set ip-adress 192.110.120.140 imposta un nuovo indirizzo IP. set /setup/home 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.

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

FirmSafe funziona così

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

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

- 'Immediato': La prima possibilità consiste nel caricare ed attivare immediatamente il nuovo firmware. Si possono presentare le seguenti situazioni:
 - Il nuovo firmware viene caricato con successo e poi funziona come voluto. Quindi tutto è a posto.

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

Un nuovo software si carica così

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

- Tool di configurazione *ELSA LANconfig* (raccomandato)
- TFTP



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

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

ELSA LANconfig



Nel tool 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. Per attivare il firmware durante il tempo di prova impostato, cliccare su **Modifica ► Gestione Firmware ► Abilitare firmware in prova**.

TFTP

Tramite TFTP un nuovo firmware può essere caricato con il comando **writeflash**. Per trasferire un nuovo firmware, che per es. si trova nel file 'LC_1000U.130', in un apparecchio con indirizzo IP 194.162.200.17, per es. sotto Windows NT introdurre il seguente comando:

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



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

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

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

- `tftp 10.0.0.1 get readconfig file1` : Legge la configurazione dall'apparecchio con indirizzo 10.0.0.1 e la salva sotto file1 nella directory corrente
- `tftp 10.0.0.1 put file1 writeconfig` : Scrive la configurazione dal file1 nell'apparecchio con 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

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

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

Funzioni e modalità

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

- Collegamenti radio
- Sicurezza per la configurazione
- Sicurezza per la LAN
- Gestione degli addebiti
- Connessioni ISDN
- Supporto PPP
- Routing IP
- Gestione indirizzi automatica con DHCP
- Server DNS
- Proxy NetBIOS
- *ELSA LANCAPI*
- Controllo ora
- Least-Cost-Router

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

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

Parametri per i collegamenti radio

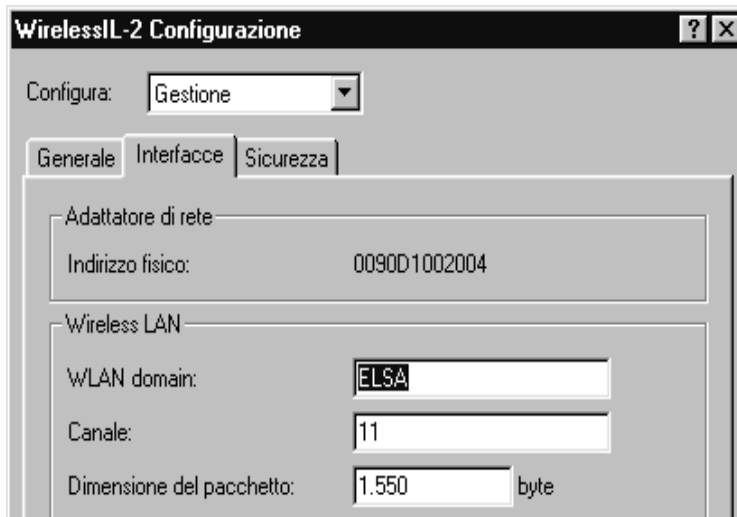
Affinché le schede di rete radio nelle stazioni mobili e nelle stazioni base si riconoscano a vicenda e possano scambiare dati, esse devono avere nei diversi parametri gli stessi valori.

Tutte le schede di rete radio (nella stazioni di base o mobili) che operano con gli stessi parametri, creano una rete radio. Con la scelta dei parametri si possono in tal modo creare in modo specifico diverse reti radio, il cui traffico di dati non si disturba a vicenda.

I parametri per le schede di rete radio nelle stazioni base per la configurazione vengono impostati tramite *ELSA LANconfig* o Telnet.

- ① Avviare *ELSA LANconfig* con **Avvio ► Programmi ► ELSA lan ► ELSA LANconfig**. *ELSA LANconfig* cerca adesso automaticamente tutte le stazioni base nel LAN e WLAN.

- ② Cliccare nella lista delle apparecchiature trovate sulla stazione base che si intende configurare. Passare nel campo di configurazione 'Gestione' sulla scheda di registro 'Interfaces'.



- ③ Impostare un nuovo valore per il dominio WLAN. Il dominio WLAN deve essere uguale in tutti i partecipanti di una rete radio.

Modificare questo valore dalla preimpostazione 'ELSA' possibilmente presto assegnandogli un altro valore qualsiasi poiché con il dominio WLAN si protegge la propria rete radio come con una password contro intrusi non autorizzati!

- ④ Impostare il canale radio per tutti i partecipanti della rete radio in modo identico. Con il canale radio si sceglie la banda di frequenza usata dalle schede di rete radio per lo scambio dati.

Con la scelta di un altro canale si possono usare in modo specifico diverse reti radio affiancate. Teoricamente si trovano a disposizione si 14 diversi canali, ma a causa della sovrapposizione di frequenza del metodo DSSS nella banda di frequenza ISM sono possibili solo tre canali senza sovrapposizione. Nel caso in cui debbano essere usate contemporaneamente più radiocellule molto vicine tra loro, bisognerebbe scegliere allora canali con la distanza quanto maggiore possibile; per es. canale 1, 7 e 14 o 3 e 13.

Prestare attenzione alla tabella nell'appendice con i canali radio ammessi nei singoli paesi.

- ⑤ Con la dimensione del pacchetto si imposta la lunghezza dei singoli pacchetti di dati da inviare tramite la rete radio. I valori possibili vanno da 600 fino a 1600 byte. I pacchetti più grandi prima del trasferimento devono essere divisi (frammentati) e poi ricostruiti presso il ricevitore (assemblati).

Pacchetti piccoli possono favorire in un ambiente disturbato migliori trasmissioni, ma il rapporto tra dati utili e la parte di informazioni gestionali di un pacchetto peggiora.

- ⑥ Utilizzate la funzione 'Roaming' se dovete gestire più stazioni radio attraverso una sola rete Ethernet comune e desiderate un passaggio uniforme da una cella radio all'altra. Attivate in questo caso il WLAN-Domain ed il canale radio di ogni stazione base coinvolta nel Roaming.
- ⑦ Modificare nell'area di configurazione 'WLAN-Bridge' se
- si accoppia per determinate stazioni mobili lo scambio dati con la LAN a cavo
 - si desidera bloccare lo scambio di pacchetti di dati con determinati protocolli.



*Nel caso in cui l'area di configurazione 'WLAN-Bridge' non è visibile, attivare nella finestra principale di ELSA LANconfig con **Visualizza ► Opzioni** la rappresentazione completa della configurazione.*

Sicurezza per la configurazione

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

Naturalmente i parametri impostati non devono essere poi modificati da persone non autorizzate. Pertanto un *ELSA LANCOM Wireless* 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 Wireless* è protetta mediante un blocco del login contro gli « attacchi Brute-Force ». Nel caso di un attacco Brute-Force, un utente non autorizzato tenta di « scassinare » la password per avere così accesso ad una rete, ad un computer o ad un'altra apparecchiatura. Per farlo per es. un computer prova automaticamente tutte le possibili combinazioni di lettere e numeri fino a che non ha trovato la password giusta.

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

Questi parametri valgono in modo globale per tutte le possibilità di configurazione (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 in arrivo tramite TCP/IP

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

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

- Filtraggio dei pacchetti di dati
- IP-mascheratura (noto anche in NAT e PAT)

Il controllo

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

- tutte: Vengono accettate le chiamate di tutte le controparti.

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

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

Controllo del nome

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 secondo PAP (Password Authentication Protocol) o CHAP (Challenge Handshake Authentication Protocol). Si tratta della protezione che il proprio apparecchio richiede alla controparte.



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

Da dove arrivano il nome e la password del chiamante?

- Se si usa il 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 nel *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 di nomi e numeri e con la scelta del protocollo si può gestire il comportamento della chiamata di risposta del proprio router :

- Il router può respingere la richiesta di chiamata di risposta.
- Può richiamare un numero 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 (in corso di brevetto). Questa accelera notevolmente la procedura di chiamata di risposta.

Come nascondersi: mascheratura IP (NAT, PAT)

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

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

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

Gestione degli addebiti

La caratteristica del router di essere in grado di stabilire collegamenti autonomamente con tutte le controparti desiderate e di terminarli alla fine del trasferimento, rende

possibile all'utente un accesso molto comodo per es. a Internet. Nel caso di trasmissione dati tramite linee soggette a costi, a causa di una configurazione errata del router (per es. nella configurazione dei filtri) o tramite utilizzo eccessivo dell'offerta (per es. un continuo surf in Internet), possono aversi costi elevati.

Limitazione della connessione in base al tempo

Per poter limitare i costi si può gestire la durata massima del collegamento agendo sul tempo. A questo scopo viene definito 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 un limite previsto viene raggiunto, tutti i collegamenti aperti del router e stabiliti dal router stesso vengono automaticamente terminati. Solo dopo che è trascorso il periodo attuale i budget vengono di nuovo abilitati e le connessioni attive sono possibili. Naturalmente l'amministratore può anche abilitare in anticipo i budget!

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

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 sessione Telnet o di terminale nella posizione */Setup/Charges-module*.



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 selezione o connessioni fisse.

I moduli router prima determinano solo la controparte a cui un pacchetto di dati deve essere trasmesso. Affinché la corrispondente connessione possa essere selezionata ed 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* nel campo di configurazione 'Comunicazione' sulla scheda di registro 'Siti remoti' o nelle sessione 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 RoundRobin.

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.

- Tempi di attesa

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

- nei canali stabiliti in modo statico per il tempo di attesa B1 non sono stati più trasmessi dati.
- nei canali stabiliti in modo dinamico per il tempo di attesa B2 la velocità di trasmissione dati è scesa sotto un valore limite prestabilito.

- WAN-layer

Il layer rappresenta un insieme di protocolli che devono essere utilizzati per questa connessione. Il layer deve essere impostato allo stesso modo sui due lati della connessione.

- Chiamata di risposta

Se il router riceve una chiamata da questa controparte, qui si può impostare come opzione di non accettare la chiamata. Invece la controparte viene richiamata con le seguenti opzioni:

- normale chiamata di risposta
- chiamata di risposta rapida secondo ELSA
- chiamata di risposta dopo il controllo del nome
- attesa della chiamata di risposta da parte della controparte secondo la procedura di chiamata di risposta rapida ELSA

Impostazioni di interfaccia

Le impostazioni di interfaccia si trovano in *ELSA LANconfig* nel campo di configurazione 'Gestione' sulla scheda di registro 'Interfacce' o nelle sessione 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 eventualmente 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 sessione 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 sessione 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 telefonici'.

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 sessione 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 'Transparente', 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 RoundRobin

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

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

■ Sito remoto

Nome della controparte definito per primo nella lista dei nomi.

■ RoundRobin

Ulteriori numeri telefonici per tale controparte. Più numeri telefonici 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 PPP

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

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

- Tutte
Vengono accettate tutte le chiamate.
- Nome
Tutte le chiamate vengono accettate inizialmente. Nella 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 di chiamate' o nelle sessione Telnet o di terminale nella posizione `/Setup/WAN-module/Number-list`.

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

- Dialup-remote
Numero telefonico che viene trasmesso dalla controparte chiamante (eventualmente incl. numero identificativo nazionale e locale).
- Sito remoto
Nome della controparte definito nella lista dei nomi. Se nella lista dei nomi è definita una chiamata di risposta, viene chiamata questa controparte.

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 (PPP) 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
- 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. Questo negoziamento avviene tramite il protocollo IPCP (IP Control Protocol).
- Controllo della connessione con il LCP (Link Control Protocol)

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 (per es. LCP, IPCP, 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 a Internet (con trasferimento di indirizzi)

Le fasi di un negoziato 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.

■ Fase Network

Se il negoziato dei parametri si è svolto con successo, dai moduli router possono essere trasmessi pacchetti IP 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 forse 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'!

In questa colonna della lista PPP si introducono i seguenti valori:
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. Tali parametri possono essere modificati solo tramite SNMP o TFTP (con <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	

Tutto o.k.? Controllo della linea con LCP

Quando si stabilisce la connessione tramite PPP le periferiche partecipanti contrattano 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.

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 disturbata. Con un tempo '0' e '0' ripetizioni si disattivano completamente le LCP request.

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 di 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.

La tabella di routing si trova in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'Routing' oppure nel menu /Setup/IP-router/IP-routing-table. Per es. una tabella di routing IP si presenta così:

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.

La rotta con l'indirizzo IP « 255.255.255.255 » e la maschera di rete « 0.0.0.0 » è quella di default. Tutti i pacchetti di dati che non possono essere inviati tramite alte voci di routing, vengono trasmessi tramite questa rotta.

■ Nome del router

Il nome del router indica cosa deve succedere con i pacchetti di dati adatti all'indirizzo IP e alla maschera di rete.

Le rotte con il nome « 0.0.0.0 » indicano rotte di esclusione. I pacchetti di dati per queste « rotte zero » vengono rigettati e non inoltrati ulteriormente. Con queste per es. si escludono dalla trasmissione le rotte vietate in Internet (Privat Address Spaces, per es. 10.0.0.0).

Se come nome di rotta viene introdotto un indirizzo IP, si tratta in questo caso di un router raggiungibile localmente che è responsabile della trasmissione dei pacchetti

di dati corrispondenti.

■ Distanza

Numero dei router che si trovano tra il proprio e la destinazione.

Esempi con spiegazioni:

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	Tutte i pacchetti di dati con gli indirizzi IP di destinazione 192.168.130.x, vengono trasmessi al router raggiungibile localmente con l'indirizzo IP 192.168.140.123.
192.168.0.0	255.255.0.0	0.0.0.0	0	Esclude la trasmissione di tutti i pacchetti di dati delle reti a 10.
172.16.0.0	255.255.0.0	0.0.0.0	0	
10.0.0.0	255.0.0.0	0.0.0.0	0	
224.0.0.0	224.0.0.0	0.0.0.0	0	

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 chiamata. 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 in determinati settori.

Il router può leggere le porte di destinazione e sorgenti dei pacchetti di dati che usano TCP o UDP come protocollo. Da queste porte si può dedurre a quale scopo questi dati sono destinati. In questo modo si possono per es. riconoscere le accessi FTP o sessione Telnet.

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 'Routing' 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	Dist.	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 LAN, 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 'Router' oppure nel menu /Setup/IP-router-module/Local-routing on). In tal modo si ordina al router nel proprio

dispositivo di inviare autonomamente il pacchetto di dati all'altro router preposto. Inoltre non vengono poi più trasmessi ICMP redirects.

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 trasmessi prima al router standard e da questo di nuovo al router effettivamente preposto nella rete locale.

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). Tramite questo protocollo tutte le apparecchiature capaci di gestire RIP, scambiano informazioni sulle 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.

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 IP e la maschera di rete indicano la rete di destinazione, la distanza indica il numero di router presenti tra trasmettitore e ricevitore, l'ultima colonna mostra il router che ha reso nota tale 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' 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.

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).

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, il mascheratura IP rappresenta anche una protezione molto efficace contro gli accessi da Internet alla rete locale.

Due indirizzi per il router

- 'off': Non viene effettuato alcun mascheratura.

Come funziona il mascheratura IP?

Il 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. Esso annota nella tabella anche questa nuova porta e trasmette il pacchetto con i nuovi valori.

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

Se all'inverso un computer di Internet invia un pacchetto per es. a un server FTP in LAN, a questo computer sembra come se il router fosse il server FTP. Tramite la voce nella tabella di servizio, il router legge dalla voce nella tabella di servizio l'indirizzo IP del server FTP nella LAN (in *ELSA LANconfig* nell'area di configurazione 'TCP/IP' nella scheda 'Masq.' o nel menù

Setup/IP-Router-module/Mascheratura/Service-table).

Il pacchetto viene trasferito a questo computer. Tutti i pacchetti che arrivano nella LAN dal server FTP (risposte del server), vengono nascosti dietro l'indirizzo IP del router.

Una piccola differenza:

- Durante l'accesso dalla LAN a Internet, l'introduzione nella tabella delle informazioni per porta e indirizzo IP viene effettuata invece dallo router stesso.

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:

- TCP (e tutti i protocolli che si basano su di esso come FTP, HTTP ecc.)
- 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 DNS-Request: « Quale indirizzo IP fa parte di www.domain.com? »

- Il router cerca prima nelle proprie impostazioni se è registrato un server DNS (nel tool di configurazione *ELSA LANconfig* nell'area di configurazione 'TCP/IP' nella scheda 'Indirizzi' o nel menù /Setup/TCP-IP-module). Se lo trova, preleva da tale server l'informazione desiderata.
- Se nessun server DNS è registrato in *ELSA LANCOM Wireless*, il router tenta di raggiungere su una connessione PPP eventualmente esistente (per es. con il provider Internet) un server DNS, e preleva 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 *ELSA LANCOM Wireless*.

Con questa procedura non è necessario conoscere l'indirizzo di un server DNS. Inoltre l'indirizzo del server DNS viene aggiornato automaticamente. Se per es. il provider che comunica questo indirizzo dovesse rinominare il server DNS, oppure se si passa ad un altro provider, la rete locale dell'utente 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). Tramite questo protocollo un server DHCP può assegnare dinamicamente in una LAN basata su TCP/IP alle singole stazioni gli indirizzi necessari.

Il server DHCP

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

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

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

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

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

DHCP – 'On', 'Off' o 'Auto'?

Il 'Server DHCP' può assumere tre diversi stati:

- 'On': Il server DHCP è attivato in modo permanente. Introducendo questo valore viene controllata la configurazione del server (validità del pool di indirizzi).
 - Se la configurazione è corretta l'apparecchio si offre come server DHCP in rete.
 - Se la configurazione non è corretta (per es. confini di pool non validi) il server DHCP si disattiva e si porta nello stato 'Off'.
- 'Off': Il server DHCP è disattivato in modo permanente.
- 'Auto': Il server si trova in modalità automatica. In questo stato l'apparecchiatura cerca dopo l'accensione nella rete locale altri server DHCP.

- Se viene trovato almeno un altro server DHCP, l'apparecchio disattiva il proprio server DHCP. In questo modo si evita tra l'altro che un apparecchio non configurato assegni dopo l'attivazione in rete indirizzi che non si trovano nella rete locale.
- Se non viene trovato nessun altro server DHCP, l'apparecchio attiva il proprio server DHCP.

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

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

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 (pool indirizzi iniziali fino a pool indirizzi finali). In questo si può introdurre qualunque indirizzo valido nella rete locale.
- Esso utilizza autonomamente l'indirizzo IP '10.0.0.254' e il pool di indirizzi '10.x.x.x' per l'assegnazione degli indirizzi IP della rete. In questo stato il server DHCP assegna agli altri computer della rete solo l'indirizzo IP e la rispettiva validità, ma non le altre informazioni.

Se ora si avvia un computer della rete che con le proprie impostazioni di rete richiede un indirizzo IP tramite DHCP, un apparecchio con modulo DHCP attivato gli offre l'assegnazione di un indirizzo. Come indirizzo IP viene prelevato dal pool un indirizzo valido. Se nel passato è già stato assegnato al computer un indirizzo IP, esso richiede proprio questo indirizzo IP, e il server DHCP tenta di assegnare di nuovo tale indirizzo, se non lo ha già assegnato a un altro computer.

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

Assegnazione della maschera di rete

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

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.

Assegnazione del server DNS e del server NBNS

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

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

Assegnazione della gateway di default

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

Se necessario, questa assegnazione può essere 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.

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

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

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

Configurazione del server DHCP

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

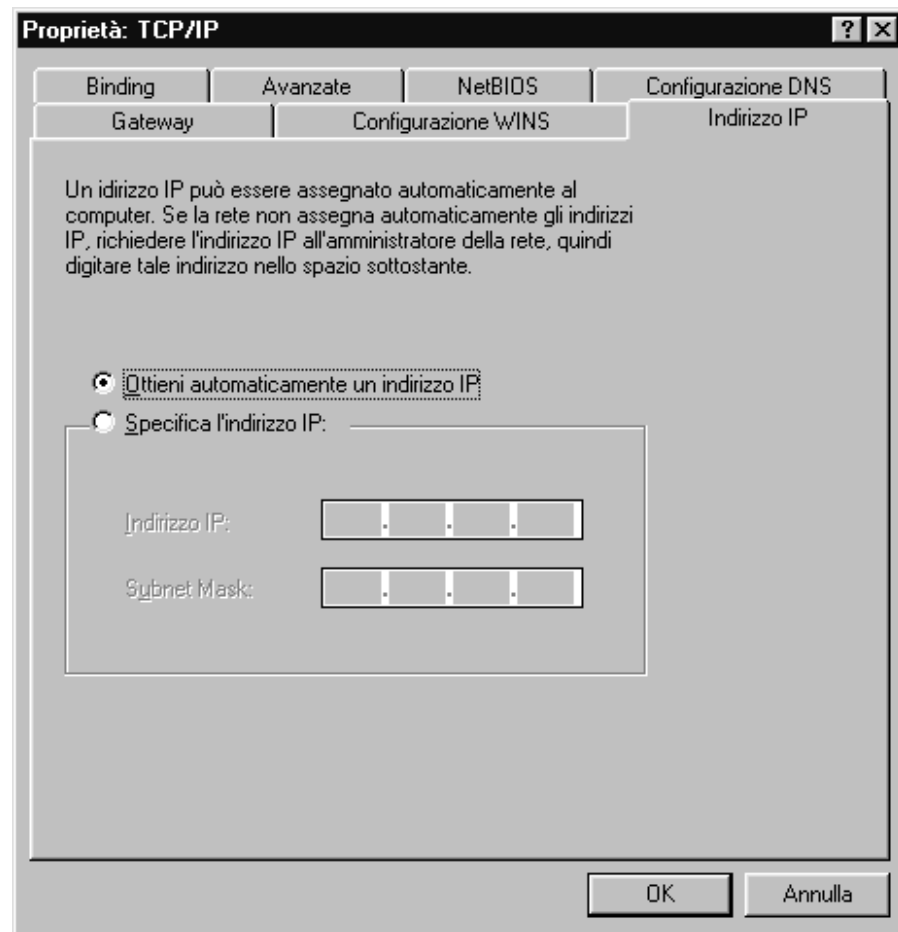
- Una rete non è stata ancora creata, oppure la rete locale esistente non utilizza un TCP/IP. Con il server DHCP della propria nuova apparecchiatura ELSA, si possono assegnare in una volta a tutti i computer della rete e all'apparecchiatura stessa indirizzi IP.
- Esiste già una rete con TCP/IP, ma senza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

Configurazione con *ELSA LANconfig* e l'assistenza

In entrambe le situazioni il tool di configurazione *ELSA LANconfig* aiuta con un assistente a effettuare le impostazioni necessarie:

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

computer richiedono automaticamente un indirizzo IP del pool di indirizzi del server DHCP.



- ④ Installare il tool di configurazione *ELSA LANconfig* in un PC della rete.
- ⑤ Avviare il programma dal gruppo di programmi 'ELSA lan'. 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, in questa assistenza selezionare l'opzione 'Tutto impostato automaticamente', 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.
L'assistenza assegna al apparecchio l'indirizzo IP introdotto con la rispettiva maschera di rete. Dall'indirizzo IP il apparecchio determina il pool di indirizzi valido per l'assegnazione DHCP.

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

Configurazione manuale

Se non si vuole eseguire la configurazione con l'assistenza di *ELSA LANconfig*, i parametri per il server DHCP possono anche essere impostati a mano: Nel tool di configurazione *ELSA LANconfig* nell'area di configurazione 'TCP/IP' nella scheda 'DHCP' o nel menù /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 Service è necessario per la comunicazione in Internet, per es. per poter rispondere a una richiesta secondo 'www.elsa.de' con il corrispondente indirizzo IP. Ma anche nell'ambito di una rete locale o di un accoppiamento LAN ha senso poter assegnare in modo univoco gli indirizzi IP della LAN ai nomi dei computer.

Che cosa fa un server DNS?

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

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

- Un *ELSA LANCOM Wireless* 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 Wireless* 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 nel *ELSA LANCOM Wireless* 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
```

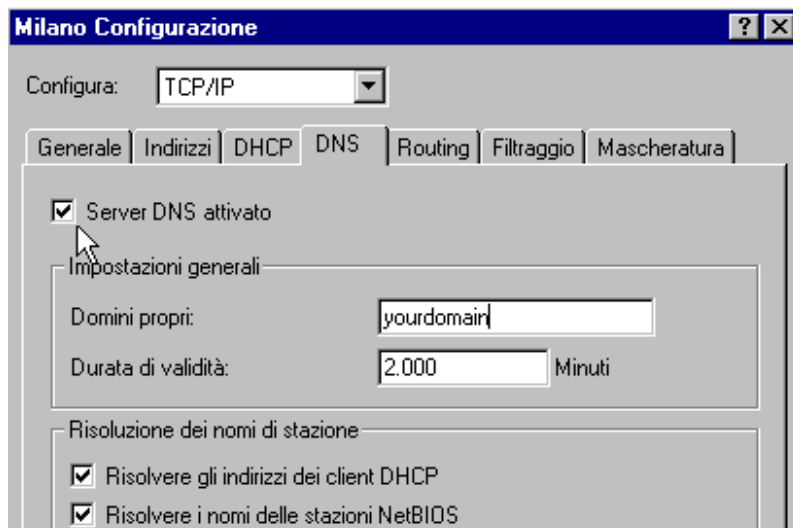
- ② Introdurre il dominio in cui si trova il server DNS. Con l'ausilio di questo dominio il server DNS riconosce su richiesta se il nome ricercato si trova o meno nella propria LAN. L'indicazione del dominio è opzionale.

```
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
```

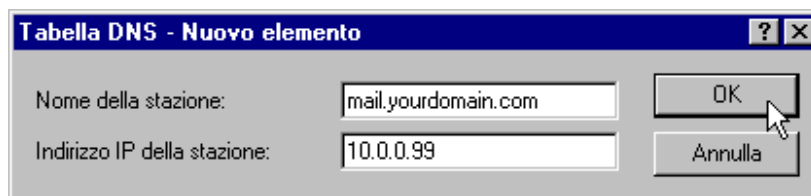
```
set setup/DNS-module/NetBIOS-usage YES
```



- 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 si sa che,
- non appartengono alla propria LAN,
- non si trovano in Internet,
- possono essere raggiunti attraverso il router.

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



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

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

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

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



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

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

Con questa voce (con indice '001') si blocca questo dominio per tutti i computer della rete locale. L'indice '001' è scelto liberamente e serve soltanto per facilitare la lettura. Per l'introduzione del dominio sono anche consentite le wildcard '?' (rappresenta un carattere qualunque) e '*' (rappresenta un numero qualunque di caratteri). Per es. se solo un determinato computer (IP 10.0.0.123) non deve accedere ai domini DE, introdurre:

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

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

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

NetBIOS-Proxy

Funzionando come NetBIOS-Proxy un *ELSA LANCOM Wireless* 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 partecipanti per la connessione tramite 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, Windows 9x e

Windows 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 Wireless* 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 « conversevole » 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 stabilito). Con siffatti pacchetti la linea rimane continuamente stabilita 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 Wireless* può instradare i pacchetti NetBIOS o rispondere direttamente ad essi come proxy:

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

successo, il tempo di attesa viene prolungato. Con il successivo scambio di informazioni NetBIOS, il tabellone viene completato per la prima volta.

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

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

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 Wireless su IP!

Il routing dei pacchetti NetBIOS nel *ELSA LANCOM Wireless*, 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

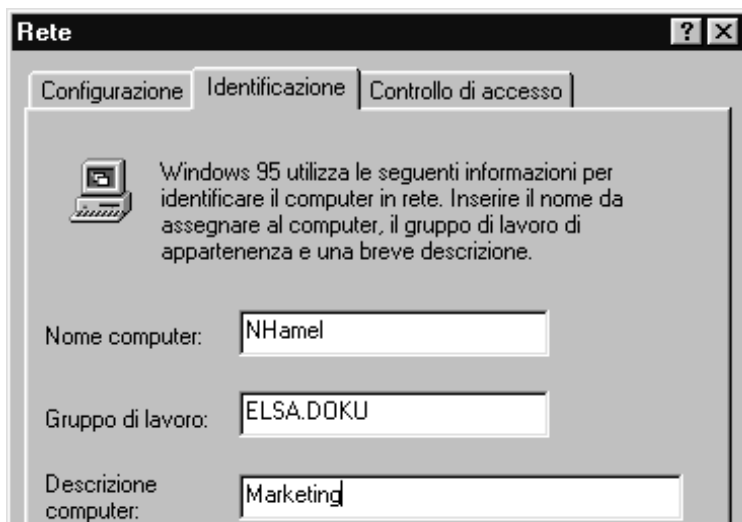
L'abilitazione di file e stampanti consente di abilitare unità disco o stampanti per altri utenti della rete Windows.

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.

■ Abilitazione di file e stampanti

Dopo l'installazione, controllare se è attivata l'abilitazione di file e stampanti. A questo scopo cliccare su **Avvio ► Impostazioni ► Pannello di controllo ► Rete ► Condivisione 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.

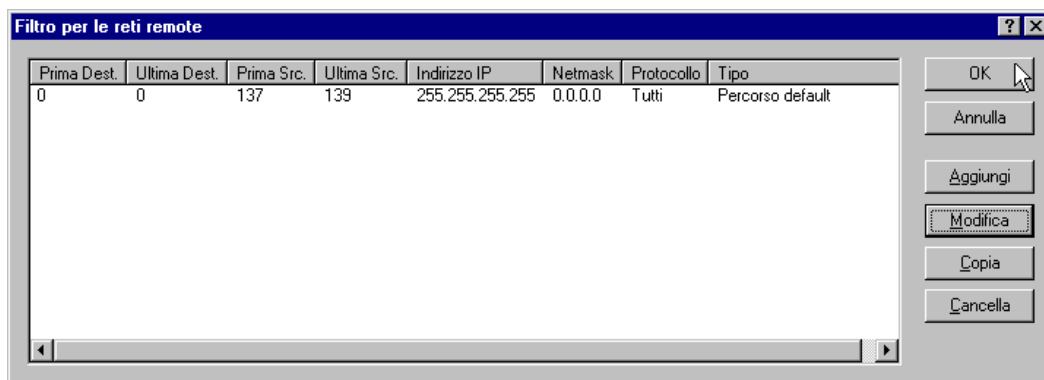


Si può controllare facilmente se le impostazioni nella rete Windows sono corrette: il proprio computer deve essere visualizzato nell'ambiente di rete con il rispettivo nome.

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.

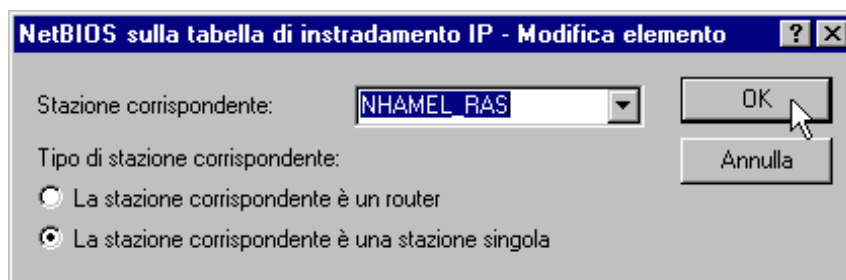
```
cd /Setup/NetBIOS-module  
set operating on
```

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 Wireless* 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 Wireless* (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, nel *ELSA LANCOM Wireless* è disponibile una lista con tali nomi di computer. Tramite Telnet con

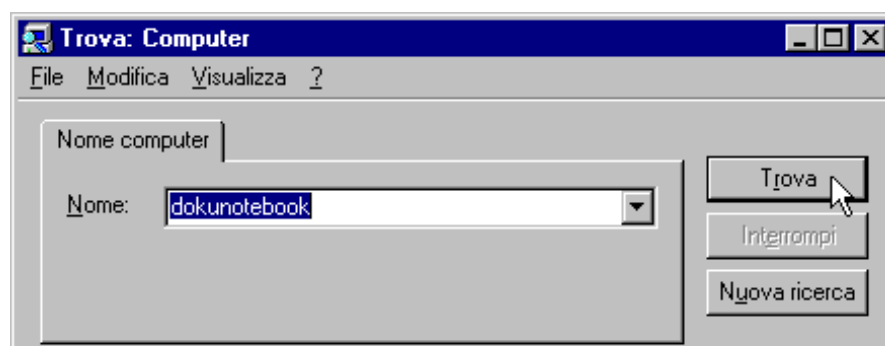
```
dir /Setup/NetBIOS-module/Host-list
```

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 'Sfoggia 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 Wireless*.

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.

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 al router, 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, nella rete vengono semplicemente installati più router. 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 del apparecchio. Pertanto la funzione Firewall e le funzioni di monitoraggio addebiti vengono disattivate!

Al momento dell'installazione dalla maggior parte dei programmi per inviare fax che supportano il servizio CAPI, la *LANCAPI* viene riconosciuta automaticamente quale fax hardware Class II e usata.

Installazione del *LANCAPI* client

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



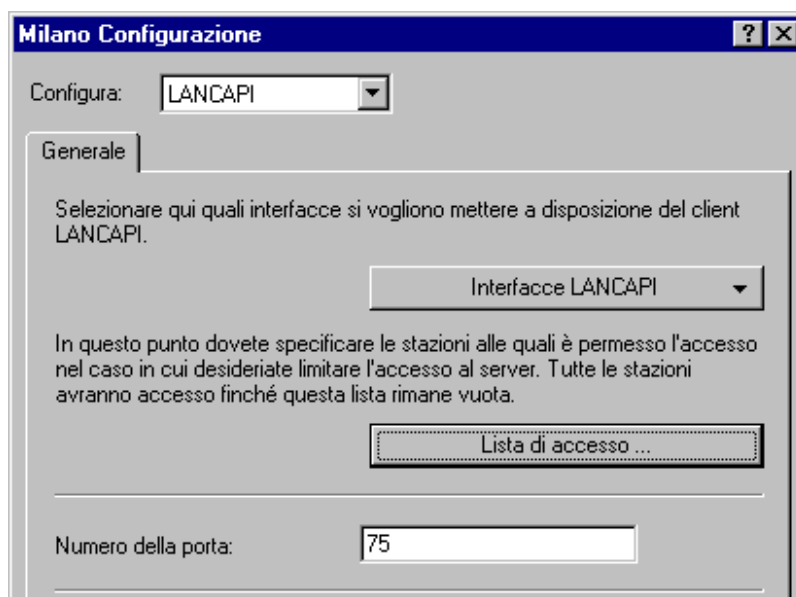
Impostazione del *LANCAPI* server

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'.



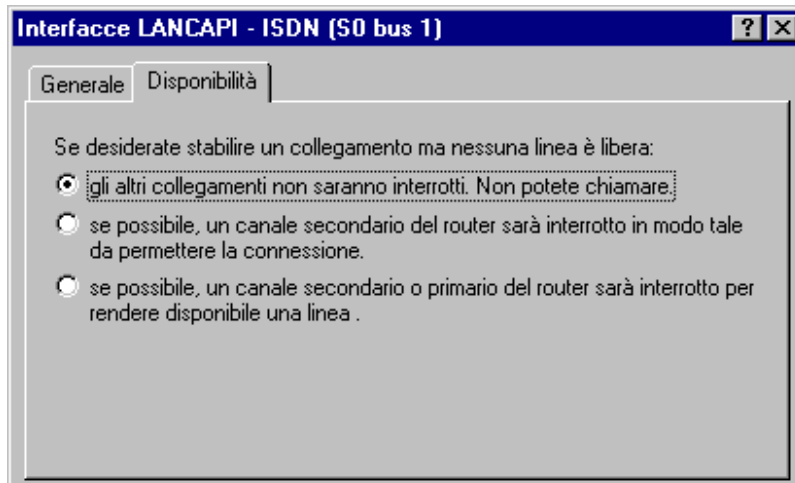
- ② Attivare il *LANCAPI* server, o consentire 'solo chiamate in uscita'. In questo caso la *LANCAPI* non reagisce alle chiamate in arrivo e non può essere impiegata per es. per ricevere messaggi fax. Per es. consentire solo le chiamate in uscita se per la *ELSA LANCAPI* non si dispone di un numero telefonico 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 sui diverse workstation indicare di volta in volta numeri telefonici diversi, ai quali il programma deve reagire.

Passare alla scheda registro 'Opzioni'. In questa si definisce come si comporta un *ELSA LANCOM Wireless* 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 *LANCAP*. Un programma fax che utilizza la *LANCAP* probabilmente tenterà di nuovo l'invio in un momento successivo.
- La connessione può essere stabilita attraverso la *LANCAP* 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 *LANCAP* 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 *LANCAP*

Per usare la *LANCAP* esistono due possibilità:

- Si impiega un software applicato direttamente a un'interfaccia CAPI (in questo caso la *LANCAP*), come per es. *ELSA-RVS-COM*. Un siffatto software cerca la CAPI durante l'installazione e successivamente la usa automaticamente.
- Altri programmi come LapLink possono stabilire connessioni su diversi percorsi, per es. tramite la rete di accesso remoto di Windows. Quando si crea una nuova connessione di accesso remoto si può scegliere quale delle periferiche di comunicazione installate si intende utilizzare. Per la *LANCAP* selezionare la voce 'ISDN WAN Line 1'.

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

Per le telefonate in determinate ore del giorno e in diverse regioni, purtroppo la tariffa più conveniente non è sempre offerta dallo stesso provider, anzi abbastanza spesso si ottiene da fornitori diversi: al mattino il provider 1, al pomeriggio il provider 2 e per le conversazioni internazionali 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 Wireless* 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 Wireless*. 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. '01033' per la 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 fornitore.
- Esaminare le diverse zone tariffarie. I prefissi per le diverse zone possono essere visualizzati per es. in www.risparmio-telefonico.it in Internet.

Una volta trovati i prefissi che da smistare, si può passare all'assegnazione del provider call-by-call. A questo scopo naturalmente ci vogliono le tariffe aggiornate di tutte le possibili società telefoniche. Anche in questo caso Internet può aiutare. 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 del *ELSA LANCOM Wireless* devono utilizzare i servizi del Least-Cost-Router?
- Quali chiamate devono essere effettuate attraverso quale provider?

Per rispondere a queste domande, procedere nel modo seguente:

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



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

- ③ Passare alla scheda di registro 'Orari e festività nazionali'. Aprire la **Tabella del costo minimo...**, inserire una nuova voce, e introdurre i dati necessari:
 - Quale prefisso deve essere smistato?

- Su quale provider deve essere smistato questo prefisso? Se si introducono più numeri identificativi di rete separati da punto e virgola, il LCR passa automaticamente al prefisso successivo, se quello precedente è occupato.
- In quali giorni e a quali ore deve essere attivo lo smistamento? Tenere presente che non sono possibili ore che superano la giornata (18:00 fino alle 6:00)!
- La chiamata deve essere effettuata attraverso la normale società telefonica, se tutte le linee call-by-call sono occupate? Se è disattivata la 'fallback automatico...', eventualmente il LCR dopo l'ultimo numero identificativo di rete ricomincia con il primo ...

Tabella del costo minimo - Nuovo elemento

Inoltra questo prefisso:

Verso numero Call-by-Call:

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

Ora d'inizio:

Ora di chiusura:

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

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



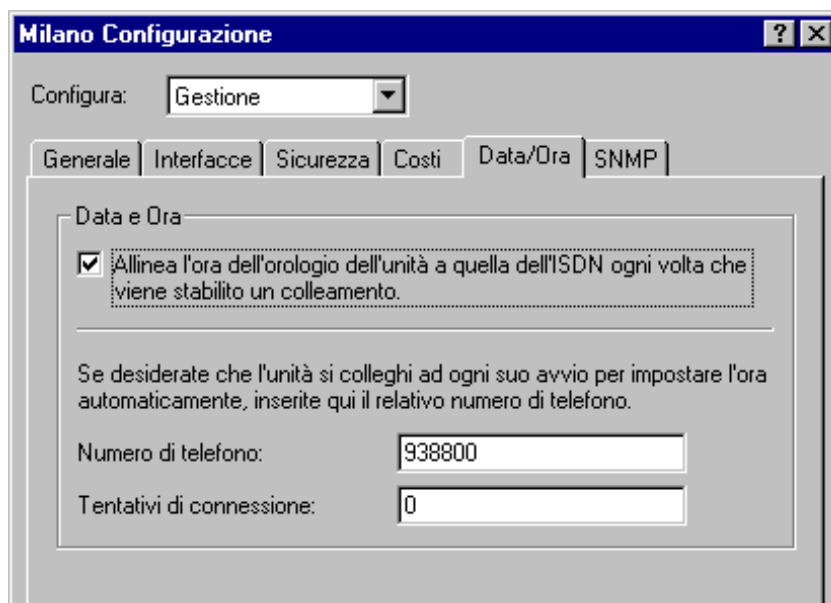
*Costruire la tabella LCR per passi, e controllare ogni volta il risultato. A questo scopo aprire per es. ELSA LANmonitor e avviare attraverso ELSA LANCAPI connessioni verso controparti che dovrebbero essere smistate in base alla tabella. In base al numero telefonico selezionato si può facilmente vedere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

Appendice

Dati tecnici

Specifiche hardware

Banda di frequenza:	2400–2483,5 MHz (ISM)
Hardware:	Processore: Hitachi SH3, 60 MHz, 4 MByte RAM, 2 MByte Flash-ROM
Velocità di trasmissione dati:	2 Mbit/s (con possibilità di commutare su 1 Mbit/s, Automatic Rate Selection)
Portata:	fino a 300 metri all'aperto, ca. 30 metri in ambienti chiusi (raggio di azione tipico)
Velocità di errore in bit:	Migliore di 10^{-5}
Norma:	IEEE 802.11, DSSS (Direct Sequence Spread Spectrum)
Connessione LAN:	Ethernet IEEE 802.3, 10Base-T (RJ45)
Connessione WAN:	ISDN-S ₀ -Bus (RJ45), corrispondentemente a I.430
Display/comando:	LED per stato LAN, WAN e apparecchiatura
Certificazione:	Contrassegno CE (EG), autorizzazioni per tutti i Paesi dell'UE e svizzera
Sicurezza:	Protezione tramite password, codificazione (WEP, in preparaz.), IP-Masquerading (NAT), filtro Firewall
Connessioni:	10Base-T, ISDN S ₀ , Power
Servizio di garanzia:	6 anni
Supporto:	tramite Hotline e Internet

Specifiche software

Modalità di funzionamento:	IP-Router, DHCP-Server, DHCP-Client, DNS-Server, Bridging trasparente tra WLAN e LAN, L ^A N ^C A ^P I-Server, NetBIOS-Spoofing
Protocolli di rete:	ARP, Proxy-ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, NetBIOS tramite IP
Filtro:	Filtro sorgente e destinazione per reti, protocolli e porte; WAN e LAN separati
Protezione addebiti:	Importo massimo costi telefonici o tempo di collegamento in un periodo indicato; funzioni di Security e Firewall impostabili
Protocolli ISDN canale D:	DSS1, 1TR6, configurazione punto-punto e punto-multipunto, commutazione automatica tra DSS1 e 1TR6 (disattivabile), CLIP, MSN, EAZ, DDI

Protocolli ISDN canale B:	Router: Layer 1: HDLC Kbit/s, HDLC 64 Kbit/s Layer 2: X.75 LAPB, trasparente Layer 3: trasparente, PPP, sincrono e asincrono Compressione dati LZS Stac, Hi/Fn Aggregazione di canale ML-PPP (statica e dinamica, incl. BACP) Elaborazione di script per CompuServe Funzionamento CAPI: Layer 1: HDLC Kbit/s, HDLC 64 Kbit/s Layer 2: ISO 776 (X.75 SLP), trasparente Layer 3: trasparente, T.90NL (con compatibilità T.70NL)
Masquerading IP NAT/PAT):	Conversione indirizzo IP e porta tramite un indirizzo IP; Correlazione statica e dinamica dell'indirizzo IP tramite PPP o DHCP; Mascheratura di TCP, UDP, ICMP e FTP; DNS-Forwarding; inverses Masquerading per servizi IP dall'Intranet (per. es. Web-Server)
Management:	Configurazione TFTP e upload del firmware, SNMP-Management via SNMP v.1 o v.2, accessi WAN e LAN attivabili e configurabili separatamente; Accesso di configurazione per WLAN, commutabile separatamente, tools di diagnosi, spia di stato <i>ELSA LANmonitor</i>
Sicurezza di esercizio:	Watchdog hardware, autotest regolari, FirmSafe per aggiornamenti remoto del software
Sicurezza:	Protezione tramite password, PAP/CHAP, codificazione (WEP in prep.), IP-Masquerading (NAT/PAT), filtro Firewall, protezione tramite liste di accesso, codificazione WLAN, filtro WLAN
Statistiche:	Contatori di pacchetti LAN e WAN, contatori di errori, connessioni, tempo e addebiti

Canali radio

Ognuno dei 14 canali radio, che possono essere impostati per la rete radio, ha un'ampiezza di 22 MHz grazie all'utilizzo del DSSS. In questo modo nella banda di frequenze ISM è possibile utilizzare un massimo di tre canali indipendenti tra di loro. Nella tabella sono indicate le medie frequenze e quali canali sono ammessi in quale Paese.

	Numero di canale	Media frequenza [MHz]	EU (ETSI)	Spagna	Francia
1. Banda radio Canale 3	1	2412	X		
	2	2417	X		
	3	2422	X		
	4	2427	X		
	5	2432	X		
2. Banda radio Canale 8	6	2437	X		
	7	2442	X		
	8	2447	X		
	9	2452	X		
	10	2457	X	X	X

	Numero di canale	Media frequenza [MHz]	EU (ETSI)	Spagna	Francia
3. Banda radio Canale 13	11	2462	X	X	X
	12	2467	X		X
	13	2472	X		X
	14	2484			

Condizioni generali di garanzia a partire 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'event. software in dotazione sono esclusi dalla garanzia.
- b) Le spese per materiali e lavoro sono a nostro carico, ma non le spese di spedizione dall'acquirente all'officina di servizio e/o a noi.
- c) Le parti sostituite diventano di nostra proprietà.
- d) Siamo autorizzati, in occasione della riparazione o della sostituzione, ad apportare le modifiche tecniche (per es. aggiornamento del firmware), per adattare l'apparecchio allo stato attuale della tecnica. Nessun costo aggiuntivo viene addebitato all'acquirente per questo. Non sussiste alcun diritto rivendicabile per questo.

2 Periodo di garanzia

Per i prodotti ELSA il periodo di garanzia è di sei anni. Fanno eccezione da ciò i monitor 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 in andata o ritorno al punto dove vengono presentate le rivendicazioni di garanzia e/o l'apparecchio riparato viene sostituito, avviene a rischio e a spese dell'acquirente.
- d) Le rivendicazioni di garanzia vengono prese in considerazione solo se insieme all'apparecchio viene presentata la fattura originale.

4 Esclusione della garanzia

In particolare, qualunque rivendicazione di garanzia è esclusa

- a) se l'apparecchio è stato danneggiato o distrutto a causa di forza maggiore o per effetto di circostanze ambientali (umidità, fulmini, polvere e altro);
- b) se l'apparecchio è stato conservato o fatto funzionare in condizioni che non rientrano nelle specifiche tecniche;
- c) se il danno sono stati causati da un trattamento non appropriato – in particolare dalla mancata considerazione della descrizione del sistema 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 brillantezza dell'illuminazione posteriore nei pannelli TFT si riduce progressivamente nel corso del tempo;
- h) se la rivendicazione di garanzia non viene presentata secondo il punto 3a) o 3b).

5 Errori di comando

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

6 Regole supplementari

- a) Le suddette disposizioni regolano in modo conclusivo il rapporto legale verso di noi.
- b) Questa garanzia non copre ulteriori rivendicazioni, e in particolare quelle per variazione o diminuzione. Sono escluse le rivendicazioni per rimborso di danni, indipendentemente dal motivo legale. Questo non si applica se per es. in caso di danni alle persone o di danni a cose di uso privato esiste una responsabilità obbligatoria in base alla legge sulla responsabilità per i prodotti o nei casi di dolo o di grave negligenza.
- c) In particolare sono escluse le rivendicazioni per rimborso di mancati guadagni, danni indiretti o conseguenti.
- d) Non ci assumiamo la responsabilità per la perdita di dati e/o il ripristino di dati in caso di lieve o media negligenza.
- e) Nei casi in cui la perdita di dati è stata da noi causata per dolo o per grave negligenza, rispondiamo per il tipico impegno di ripristino, connesso con copie di sicurezza preparate in modo regolare e commisurato al pericolo.
- f) La garanzia si riferisce solo al primo acquirente e non è trasferibile.
- g) Il foro competente è Aguisgrana, 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: Wireless ISDN / LAN Access Point
Type of Device:
Typenbezeichnung: LANCOM Wireless IL-2
Product Name:
EG-Baumusterprüfbescheinigungsnummer: D801136L
Registration No.:
Benannte Stelle: CETECOM ICT Services GmbH
Notified Body: C E 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)

EMV Richtlinie (89/336/EWG)

EMC Directive (89/336/EEC)

Netzzulassungsrichtlinie (98/515/EG)

Commission Decision (98/515/EC)

ISDN Richtlinie (97/346/EWG)

ISDN Directive (97/346/EEC)

Zur Beurteilung der Konformität wurden folgende **Normen** herangezogen:

The assessment of this product has been based on the following **standards**

EN 50081-1: 1992 Teile/ parts: EN 55022: 1998

EN 50082-1: 1992 Teile/ parts: EN 55024: 1999

EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997

TBR 3: Nov. 1995

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, 9. September 1999

Aachen, 9th September 1999

i.V. Stefan Kriebel
 Bereichsleiter Entwicklung
 VP Engineering



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

Geräteart: Wireless LAN PC card (PCMCIA)
Type of Device:
Typenbezeichnung: *AirLancer MC-2*
Product Name:

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)

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**

ETS 300 328: 1996

ETS 300 826: 1997

EN 50081-1: 1992 Teile/ parts: EN 55022: 1998

EN 50082-1: 1992 Teile/ parts: EN 55024: 1999

EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997

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, 19. August 1999

Aachen, 19th August 1999

i.V. Stefan Kriebel
Bereichsleiter Entwicklung
VP Engineering

Index

■ Numerics

- 1TR6 6, R50
- 802.11 5

■ A

- Abilitazione di file e stampanti 58
- Access-list R60
- Accesso remoto 27, 56
- Addebiti 56
- address pool R72
- address ranges R8, R64
- Alimentatore 11
- Ambiente di rete 62
- AOCD 6
- Apple Talk R6
- APPP R54
- ARP cache R62
- ARP-aging-minute(s) R62
- Assegnazione degli indirizzi 17
- Assemblaggio 24
- asynchronous PPP R54
- Auth. R55
- auto mode R72

■ B

- BACP 6
- Banda di frequenza 24
- Banda di frequenza ISM 5
- B-channel protocols R53
- Blocco 26
- Blocco dei domini 55
- Blocco del login 25
- Boot system R84
- bridge R55
- Bridging 6
- Broadcast address R8
- Broadcast transfer R11
- Brute-Force 7, 25
- Budget di tempo 29
- Buffers R58, R79

■ C

- Cable network R7
- cache R62
- call numbers R56
- call protection R54
- Callback R51
- callback R56, R58
- Callback options R52
- Call-by-Call 68
- call-by-call R80
- Calling Line Identification Restriction R50
- Canale B
 - stato di connessione 6
- Canale D 27
- Canale radio 24
- Caricamento del software 20
- cavo di connessione LAN 11
- Cavo ISDN 5
- Cells R4
- Challenge Handshake Authentication Protocol
 - 27, R55
- channel bundling R54
- CHAP 27, R55
- charge R52
- charging information R51
- charging unit R51
- Chiamata di risposta 28
 - Fast Call Back 28
- Cifra identificativa di rete 68
- CLI 27, R56
- Client per reti Windows 58
- CLIP 7
- CLIR R50
- Collegamento ISDN-S0 13
- Comando priorità 67
- Common ISDN Application Programming Inter-
 - face 63
- compatibility R53
- Complesso di fornitura 11
- Compressione 6

Compressione dati Stac 6
 Computer 52
 Computer raggiungibili 62
 Comunicazione di ufficio 63
 Condivisione 59
 Config-aging-minute(s) R76
 Configuration options R76
 Configurazione 7
 comandi 19
 SNMP 22
 Configurazione punto-a-più punti 5
 Configurazione punto-a-punto 5
 Configurazione remota 7
 Connect R57
 connection timeout R54
 connection timeouts R51
 Connessione impianto 5
 Connessione LAN 5
 Connessione multipla 5
 Connessione router di reti Windows 55
 Connessione WAN 5
 Connettore Ethernet 1
 Controllo in arrivo 26
 Controllo ora 7
 Controparti NetBIOS 56
 Conversazione urbana 69
 Conversazioni internazionali 68
 Conversazioni interurbane 68
 Costi telefonici elevati 29

D

data compression R54
 Data packet R4
 Dati tecnici 73
 DDI numbers R53
 default route R65
 Definizione di nomi e gruppi 58
 destination network R63
 Destination port R65
 destination ports R65
 device names R51
 Device-name R51
 DHCP 8, 45, R71

DHCP server R71
 dial prefix R52
 Dialup-remote R51
 Dimensione del pacchetto 24
 Direct Sequenz Spread Spectrum 5
 Disconnect R58
 Display di stato 6
 Distanza di una rotta 40
 Disturbi 5
 DNS 45, 52, R61
 DNS forwarding 44, R61
 DNS queries R66
 DNS-backup-IP-address R61
 Domain Name Service 45, 52
 Domini 52
 Dominio WLAN 24
 Driver fax 8
 DSS1 6, R50
 Dst-address R66
 Dst-netmask R66
 Durata della connessione 6
 dynamic assignment of the IP address R63
 dynamic bundling R51
 dynamic channel bundling R54
 Dynamic Host Configuration Protocol 46
 dynamic IP routing table R68
 dynamic short-hold R51

E

ELSA CAPI Faxmodem 8
 ELSA header R54
 ELSA protocol R49
 Encaps R53
 End-address-pool R71
 Ethernet 5, R53
 10Base-T 5
 EuroFileTransfer 8

F

Fast Call Back 28
 fast Callback R52
 fast callback procedure R52
 Fax 8
 Faxmodem 8

Filtri	26
Filtro IP	57
Firewall	7
firewall function	R66
FirmSafe	8
Firmsafe	20
firmsafe	R83
Firmware	8, R82
Firmware-upload	R82
Frammentazione	24
Funzione di monitoraggio addebiti	64
Funzione di richiamata	7
Funzione Firewall	28, 64

■ G

Gateway	28, 45, 48
Gestione degli addebiti	28
Gestione indirizzi	45
Gestori di rete	67
Giorni feriali	68
Giorni festivi	68
Group table	R74
Gruppi di nomi	56
Gruppo	56

■ H

HDLC packets	R54
HDLC56K	R55
HDLC64K	R55
Heap-Reserve	R59
Hierarchical IP addresses	R9
Host	R4
Host table	R74

■ I

IANA	R8
ICMP	R65, R67, R70
Identification	R48
Identificativi	59
Identificazione	58
Identificazione del chiamante	27
Inband	
con Telnet	19
Presupposti	17

Indirizzi IP	8
Indirizzo finale	47
Indirizzo iniziale	47
Indirizzo IP	14, 17, 28
Informazioni di addebito	6
Informazioni sul nome	56
Installazione	5
Interfaccia CAPI	63
Interfaccia S0	5
Interface	R4
Interface list	R49
Internet	R6
Internetwork	R6
Intranet	R60
inverse masquerading	R69
IP	R67
IP address	R59
IP addresses	R7
IP broadcast	R68
IP header	R67
IP masquerading	R63, R69
IP multicast	R68
IP network	R6
IP network mask	R60
IP-Masquerading	26
IP-Routing	
Filtro	40
IP-routing-table	R63
IPX	R6
ISDN layers	R53
ISDN network	R7
ISDN time	R20

■ K

Key	R55
-----------	-----

■ L

LAN	1, R6, R11
LANCAPI	8, 63, R77
LANCAPI Client	64
LANCAPI Server	65
LANconfig	7, 14, 17, 18, 21, 23
LAN-configuration	R76
LAN-filter-table	R65

Language R77
 LANmonitor 6, 71
 Larghezza di banda 5
 layer name R51
 Layer-name R53
 LCP echo reply 38
 LCP echo request 38
 LCR 7, 68, R79
 leased-line connection R53
 Least Cost Router
 Caduta automatica 71
 modalità 70
 Monitoraggio addebiti 70
 Least-Cost-Router 67, 70
 Least-Cost-Routing 7
 LED 12
 Power/Msg 12
 Limitazione degli addebiti 28
 Limitazione della connessione 29
 Limitazione della connessione in base al tempo
 29
 Lista di accessi IP 17
 Lista PPP 27
 Local Area Network 1, R6
 Local network R6
 Local-routing R67
 location R49
 Lock-minutes R77
 Login 21
 log-in block R77
 Login-errors R77
 Looser R52

M

MAC address R58, R79
 MAC addresses R12
 MAC protocol R12
 Mail Server 54
 manual connection R57
 Masquerading R63, R69
 masquerading R60
 Masquerading IP 7, 28, 43
 protocolli supportati 44

Masquerading table R69
 Meccanismo di forwarding DNS 53
 Medium R4
 Medium Access Control R11
 Memoria flash ROM 20
 Memoria Flash-ROM 8
 Metodo DSSS 5, 24
 MLPPP 6
 Modalità 23
 modem operation R54
 Modo automatico 46
 Modo automatico DHCP 46
 Multipoint cabling R11
 Multiprotocol capability R12

N

Name R48
 name server R61
 name verification R56
 Name-list R51
 Nameserver NetBIOS 56
 NAT 26, 28, 43
 NBNS 56, R62
 NBNS-backup R62
 NetBIOS 9, 52
 Accesso remoto 61
 Accoppiamento LAN-LAN- 60
 Controparte 60
 Filtri IP 60
 Protocollo di rete 57
 TCP/IP 57
 NetBIOS name server R62
 NetBIOS-Proxy 55
 Network R4
 Network adapter R4
 Network address R7
 Network cable R4
 network connection R58
 Network Information Center 43
 Network mask R7
 Network protocol R6
 Networking Windows 62
 NIC 43

Node-ID R58
 Nome del router 39
 Nome utente 27, 37
 Nomi 56
 Nomi dei computer 56
 Nomi di computer 52
 Nomi di rete 52
 NT domain R74
 number R51
 Number list R56
 Numeri speciali 69

O

Operating R63
 Opzioni 66
 Ora 68, 71
 Ora del giorno 68
 Ora della rete ISDN 72
 Ora ISDN 7
 orologio interno 71
 Other R84

P

Packet R4
 PAP 27, R55
 Password 24, 27, 37
 password R60
 Password Authentication Protocol 27, R55
 Password-required R76
 PAT 26, 28, 43
 Periodo di validità 46, 48
 Physical medium R4
 Point-to-multipoint connection R5
 Point-to-point connection R4
 point-to-point protocol R54
 Pool di indirizzi 47, 51
 Porta 66
 Porte NetBIOS 57
 Possibilità di risparmio nelle telefonate 69
 PPP 7, 27, R54, R55, R56
 Controllo della linea con LCP 38
 PPP negotiation R60
 Prefisso 68
 Preselezione 68

Private address spaces R8
 Procedura di sicurezza 27
 Prohibited address ranges R64
 protect R56
 Protezione addebiti 6
 Protezione con password 7, 25
 Protezione di accesso 7
 per nome 27
 tutte 26
 Protocol R6
 Protocollo di canale B 27
 Provider 67
 Proxy 9
 proxy ARP R63, R64
 Proxy-ARP R67

R

R1-mask R68
 Radiocellula 2
 Raggio di azione 3, 5
 Raggruppamento di canali 6
 dinamico 6
 statico 6
 Raggruppamento di canali dinamico 6
 Raggruppamento di canali statico 6
 Registered IP address R8
 registered IP address R60
 Regolazione automatica dell'ora 72
 Remote Access R67
 remote station verifications R56
 Remote-table R74
 Reset system R84
 Rete ad-Hoc 2
 Rete infrastruttura 3
 Rete Peer-to-LAN 3
 Rete Peer-to-Peer 2
 Rete radio 1, 23
 Rete urbana 69
 Rete Windows 55
 Reti NetBIOS 52
 Reti Peer-to-Peer 9
 Reti TCP/IP 52
 Reti Windows 9

riconoscimento del numero d'utenza 7
 RIP R68
 RIP-type R68
 Risorse abilitate 59
 Rotte di esclusione 39
 Round robin list R52
 round robin list R52
 Round-Robin R53
 Router R4
 Routing 56, R9
 Routing dinamico 39
 Routing IP
 FTP 40
 Telnet 40
 Routing statico 39
 Routing table R9

S

Scalabilità 3
 Scheda di rete radio 1, 5
 Schermatura 5
 Scope ID R74
 Scopes 56
 Script list R57
 script processing R54, R57
 security procedure R55
 semipermanent leased-line connection R52
 Server DHCP 8, 14, 17, 46, 52
 Configurazione 50
 Server DNS 9, 45, 48, 52
 Informazioni disponibili 53
 Lista di filtro 55
 Meccanismo di filtro 53
 Server list R75
 Server NBNS 45, 48
 Server WINS 56
 Service table R69
 Servizi online 17
 Servizio 52
 Setup
 DHCP-module R71
 IP-router-module R62
 LAN-module R58

TCP-IP-module R59
 WAN-module R49
 Shared Medium R11
 Shared medium R6
 Short-hold R51
 Sicurezza 25, 26, 28
 Single User Access 28
 Smistamento 68
 SNMP 22, R70
 Società telefonica 70
 Software-Update 8
 Source port R65
 special dialing characters R51, R52
 speed R55
 Spie LED 6
 Stabilimento della connessione 56
 Stac R54
 Standard 1 8
 Standard IEEE 802.11 5
 Start-address-pool R71
 State R59
 static bundling R51
 static channel bundling R54
 static IP address R63
 Stato al momento della fornitura 13
 Status R19
 Call-info-table R44, R46, R47
 Config-statistics R40
 Connection-state R20
 Connection-statistics R42
 Delete values R47
 Info-connection R43
 IP-router-statistics R38
 LAN-statistics R25
 Layer-connection R43
 operating time R20
 PPP-statistics R26
 Queue-statistics R41
 S0-bus R20
 TCP-IP-statistics R32
 WAN-statistics R21, R22
 Stazione base 1
 Struttura tariffaria 69

Subnet R9
 Suppresses the outgoing MSN R50
 System-administrator R70
 System-location R70

T

Tabella di routing IP 39
 Tabella LCR 68
 Table-ARP R62
 Table-RIP R68
 Tariffa urbana 69
 Tariffe 67
 Tasto di reset 13
 TCP R65, R70
 TCP max. connections R62
 TCP/IP 14, 17, 39, R6
 TCP/IP stack R6
 TCP-aging-minute(s) R62
 telephone company R80
 teleworkers R67
 Telnet 7, 16
 Telnet server R61
 Tentativi di login 25
 TFTP 17
 TFTP server R61
 Time R20, R56
 time R82
 Timeout R73
 Tipo di accesso 59
 TOS R67
 Trap-IP R70
 Traps-active R70
 trunk seizure R52
 Type-of-service 45, R67

U

UDP R65, R70, R77
 Upload 8, 20
 Upload del firmware 21
 con LANconfig 21
 con TFTP 22
 Upload-system R84
 Username 38, R56

V

V.42bis R54
 Velocità di trasmissione 6
 verification attempt R56
 Version-table R83

W

WAN-configuration R76
 WAN-filter-table R66
 Wildcard 55
 Windows Internet Name Service Server 56
 winipcfg 15
 wire R4
 Wireless LAN 1
 Wireless links R4
 WLAN 1, 23
 WWW 28

X

X.75 data protection R54
 X.75 secured format R54

Y

Y connections R50

Z

Zona tariffaria 69

Technical basics

This chapter is a short introduction into the technology used by your device. Network professionals will find themselves just skimming these pages, but novices will find this section to be very helpful for understanding the technical terms and processes.

Wireless network according to the IEEE-802.11 standard

The *ELSA LANCOM Wireless* series devices conform to the IEEE-802.11 standard. This standard is a supplement to the current IEEE standards for LANs, with IEEE 802.3 for Ethernet being the most well-known. In fact, wireless networks that comply with 802.11 can easily be connected to existing Ethernet networks. This is the most important function of the *ELSA LANCOM Wireless* units. With the exception of a couple of additional parameters, wireless adapters that comply with 802.11 are seen by the computer as a normal Ethernet card. This means that you can also use any protocol that you would otherwise use in a wired Ethernet (IP, IPX, NetBIOS,...) on an 802.11 wireless network; the only difference is that there's no need for wires between the computers!

The range of wireless LAN systems is limited as the IEEE standard only covers the definition of LANs; a typical line-of-sight range would be under 300 meters, with considerable reductions in range due to building walls. The group of wireless LAN stations directly within one another's range is generally referred to as a cell.

Ad hoc mode

The IEEE standard makes provision for two operating forms that differ with regard to the security and range of such wireless LANs.

A wireless LAN in ad hoc mode consists of a single cell which is 'closed' from the Ethernet vantage point, i.e. an external connection is only possible by routing superordinate protocols. An example for such an element would be a *ELSA LANCOM Wireless IL-2* that serves as an Internet access router for all other stations via its ISDN port. Ad hoc networks tend to be spontaneous, for example when a workgroup would like to network its workstations for data exchange purposes. Workstations can enter and leave the network as required; there is no expressly designated node that must be present at all times. A special authentication process is not required, or for that matter possible, because of the lack of a central station to monitor the participants.

But what happens when a workgroup in a neighboring office has the same idea and also sets up a network? While normal Ethernets would consist of two wired physical structures without connections between them, it's not quite so simple to lock up radio waves to prevent interference. This problem is avoided in that every IEEE wireless LAN

has a specific parameter – the name of a WLAN domain. From the viewpoint of the user, the WLAN domain is a freely chosen string of up to characters; at the radio level, this name is converted to an additional addressing component that permits data packets to be associated with a specific cell. To enter an existing wireless LAN, the name of the WLAN domain must be entered in the advanced settings for the network adapter driver. When initialized, the driver will then look for an existing wireless network with this identification. If it finds one, it will then establish a connection, permitting you to communicate with the computers in that wireless network. If it does not find an existing network, it will establish a new cell of its own.

Even if the cells are logically separated in this manner, they can still interfere with one another physically, as only one station can transmit at a time. In other words, none of the cells would be able to take advantage of the full bandwidth in the event of an overlap. This can be prevented by not only assigning different domain names, but also different radio channels to the individual networks. Just as two radio transmitters can transmit simultaneously on different frequencies, two wireless LANs can work simultaneously on different channels without interference. If two cells are very close to one another, there should be a difference of 4–5 channels between the channels used, as the cells also partially use the neighboring channels.



Not all of the channels included in the IEEE standard are permitted in all countries!

Infrastructure mode

The actual strength of wireless networks based on the IEEE 802.11 standard is the ease of interoperability with existing Ethernet networks. A wireless network can be used to connect mobile stations to an existing wired network. Existing networks can also be used to link multiple cells, thus increasing the range of the wireless network. This requires all participants to operate in a different mode, the infrastructure mode.

In addition to the mobile stations, infrastructure mode uses an access point, also known as an access point or distribution system. The *ELSA LANCOM Wireless* units were designed to serve as access points. The access point handles monitoring functions in the infrastructure mode. Domain names and radio channels are still required, and stations entering a network still search for an existing cell. However, unlike ad hoc mode, the cell is always established by the access point, and each station entering the network must log onto to the access point before being permitted to exchange data in the cell. The access point generally also fulfills the function of a “relay station” for data. While this reduces the achievable data rate, careful positioning of the access point can increase the size of a cell. The actual role of an access point, however, is the connection of a wireless cell to a wired Ethernet. If the access point receives a data packet for a computer that is not logged in to it, it forwards the packet to the Ethernet; in the other direction it continuously monitors the Ethernet for data directed to stations logged on to it and forwards the packets to the radio cell. As all mobile stations must log onto the access point, the access point always knows which stations are available on the wireless side,

and thus knows exactly how any given data packet is to be handled. This process is also known as bridging.



Important: Because it is not necessary to log on in ad-hoc mode, this bridging (which fully automatic from the user's point of view) is only possible in infrastructure mode. Therefore, no provision is made for operating a ELSA LANCOM Wireless in ad-hoc mode.

As mentioned earlier, an Ethernet backbone can also be used to extend the range of a wireless LAN. In this case, multiple access points can be incorporated in the same LAN and configured to the same WLAN domain. When a mobile station wants to establish a connection with the network, it seeks out and logs onto the access point with the strongest signal. Two mobile stations logged onto different access points can thus communicate with one another even though they are not within direct radio range. The Ethernet linking the access points closes the gap.

If a station continues to monitor the radio situation after logging on, it can determine the relative signal strengths of the access points and automatically switch over to the strongest access point at any given time without user intervention. This process is known as roaming.

Interchangeability with other devices

ELSA LANCOM Wireless devices based on the IEEE-802.11 standard are in principle interoperable with devices based on 802.11 from other manufacturers; but because the 802.11 standard is still quite new and many manufacturers are only now converting from proprietary wireless LAN solutions to 802.11, interoperability cannot in principle be guaranteed. At the very latest, interoperability can fail due to the modulation process used: *ELSA LANCOM Wireless* devices use the so-called direct sequenced spread spectrum (DSSS) process, while some other manufacturers use the frequency hopping spread spectrum (FHSS) process. The exchange of data between devices based on FHSS with those using DSS is not possible as a rule.

Network technology



*This paragraph will give you a brief introduction to the basics of network technology. These descriptions do **not** cover all possible techniques, processes and terms associated with network technology. They only covered to the degree necessary to provide an understanding of the product information.*

The network and its components

*network,
transmission
medium,
interfaces*

Whenever several computers communicate with one another, this connection is called a "network". For computers to be able to communicate, they need a physical medium through which the information can be transmitted. This can be a wired or radio link, for example, that is connected to the computers using special interfaces (e.g. network adapters).



*Packets
Cells*

The term network cable (or simply wire) in the following text also refers to any other physical medium that can take on the function of the cable, such as wireless links.

The individual bits of electronic information that are sent from one computer to another through a medium are called packets or cells, depending on the process.



For most of the following explanations, the difference between packets and cells is irrelevant. Therefore, we will use the term packet or data packet in a general sense and only detail the special characteristics of cells as necessary.

Host

The computer and other terminal devices (e.g. the printer) in a network that generate or process information are called hosts. Ideally, the host is not responsible for the task of forwarding information. A host normally has exactly one interface to the network.

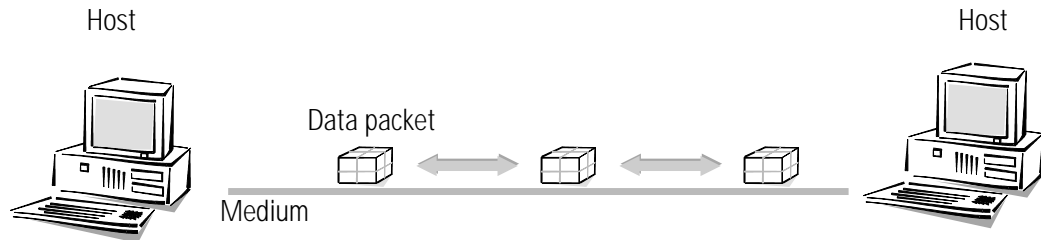
Router

The transport of packets between two hosts occurs indirectly through exchanges that pass packets on to the target computer. These exchanges are called routers. A router has at least two interfaces so that it can receive the data from a sender and pass them on to a recipient. Apart from the exchange function, the router also has the properties of a host so that it can also be the recipient of data packets, for configuration purposes for example.

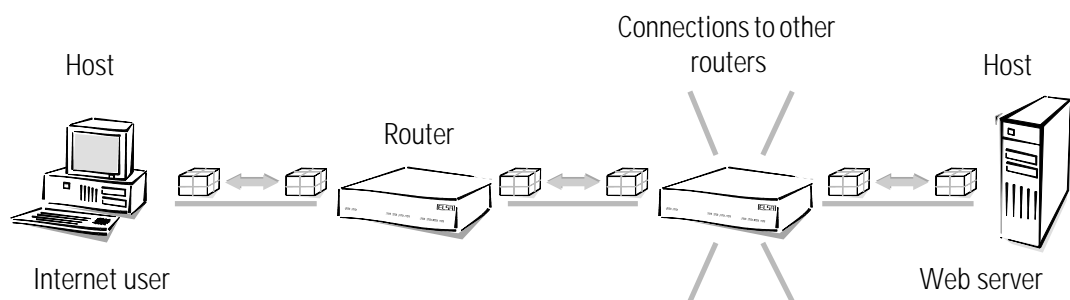
Connection modes

*Point-to-point
connection*

When exactly two hosts are connected via a medium, this is referred to as a point-to-point connection. One host transmits packets that can only be received by exactly **one** recipient (unambiguous connection).



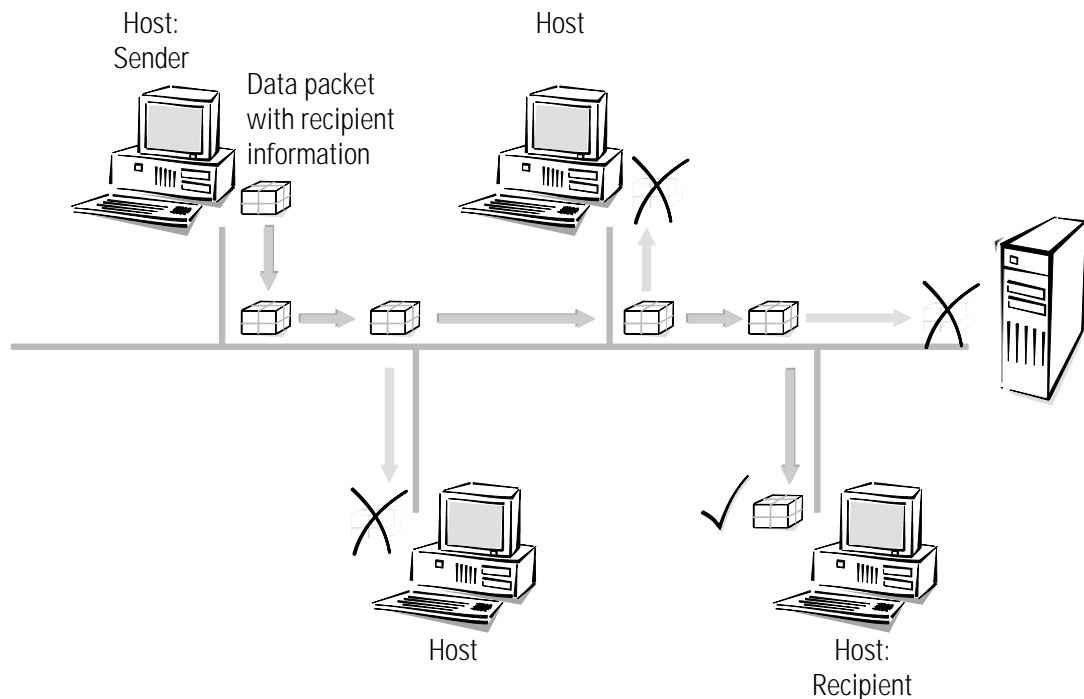
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers will only forward the data packets to one recipient. That's why we also call this connection unambiguous.



Point-to-multipoint connection

Strictly speaking, the term “point-to-point connection” is not quite correct. For our purposes though, it is sufficient to distinguish this kind of connection from the following “point-to-multipoint connections”.

Generally speaking, it would be uneconomical to directly connect all computers in a network via point-to-point wired connections, as the computers would then require multiple interfaces. Computers in a network are therefore plugged into a joint medium shared by all hosts. The sender simply sends its packet with instructions concerning the recipient to the medium to which other hosts are connected. The data packet arrives at **every** host in the network. Each host then decides whether it is the recipient of the packet or not. If the packet is addressed to the corresponding host, it will then accept it. If not, the host will ignore (reject) it. This is a point-to-multipoint connection, since we are not dealing with an unambiguous connection.



Kinds of networks

<i>Protocol</i>	An important prerequisite for communications between computers is a common language among the hosts. In the world of network technology this language is called "network protocol" or simply "protocol".
<i>TCP/IP</i>	The most broadly distributed network protocol is the TCP/IP (T ransmission C ontrol P rotocol/ I nternet P rotocol). It is used mainly in the Internet, but nowadays more and more company networks use it. Examples of other network protocols are IPX or Apple Talk. Because of its wide use, this chapter deals mainly with the TCP/IP.
<i>IP network</i>	All hosts wanting to communicate using the TCP/IP protocol have to be plugged into the same network and have to have the TCP/IP protocol (also known as TCP/IP stack) installed. Such a network is referred to as an IP network.
<i>Internetwork Internet</i>	The connection of multiple networks based on the IP protocol is referred to as an internetwork. The largest union of many small, public IP networks is the Internet.
<i>Local network (LAN)</i>	A network covering a limited area with hosts on the same hierarchical level and using the same medium (shared medium) is called a local network (L ocal A rea N etwork, LAN).

IP addressing

<i>Packet-oriented transfer</i>	In IP networks the communication between computers takes place in a packet oriented fashion. This means that data or messages are packed together in parcels of variable length and are as such sent from the source computer to the target computer. Apart from
---------------------------------	--

the actual information to be transmitted (useful data), the data packet also contains address and control information.

IP address

IP addresses are used in IP networks for communications between various devices. In this case, every host has its own unique address by which it can be identified unambiguously. What does an IP address look like? It comprises four bytes separated by points, making a total of 32 bits. Each of the four bytes can take on values from 0 to 255, e.g. 192.168.130.124.



To be precise, the IP address refers to the interface, and not the host itself. A terminal device with more than one interface (such as a router) has to have an IP address at its disposal for every single interface. This is why ISDN routers from ELSA for example, have an IP address for communication with the hosts in their own network, as well as a second IP address for communication with the "outside world" using the ISDN network. In the same way, ELSA cable modems have an IP address for their own network and another IP address for the exchange of data with the cable network.

Network address

An IP address contains the address of the network as well as that of the host. The network address is the same for all hosts on one network, whereas the address of the host is exclusive and unique to the network. A router, for example, can have more than one IP address, each one unique to the network.

Netmask

How then can you differentiate between the part that determines the network and the part that identifies the host? With the network mask. You all know what masks are: They cover up one part of something and only allow the other part to be visible. This is exactly how a network mask operates. It is a number which is identical in structure to the IP address, i.e. 32 zeros or ones. The network mask usually starts with ones at the beginning and ends with zeros. The zeros at the end thus cover the part of the IP address which does not belong to the network address.

Examples:

This address...	...in bytes...	...looks like this in bits:
IP address	192.168.120.253	11000000.10101000.01111000.11111101
Netmask	255.255.255.0	11111111.11111111.11111111.00000000
Network address	192.168.120.0	11000000.10101000.01111000.00000000

The same IP address, this time with another netmask:

This address...	...in bytes...	...looks like this in bits:
IP address	192.168.120.253	11000000.10101000.01111000.11111101
Netmask	255.255.0.0	11111111.11111111.00000000.00000000
Network address	192.168.0.0	11000000.10101000.00000000.00000000

You can see from this that an IP address alone is not enough. A host can only be identified unambiguously in combination with a netmask.

And you can also see that there are more bits available to identify the individual hosts in a connected network if there are fewer bits in a netmask that contain a one. While only 254 different addresses could be allocated in the first example with the netmask 255.255.255.0, the second example has as many as $254 \times 254 = 64516$ different addresses available! The first and the last digit of an address space are reserved for the network address and the broadcast address (addresses for packets to all hosts in an IP network). In the netmask 255.255.255.0 this is the '0' for the network address and the '255' for the broadcast address.

A new notation of the netmask simply attaches the number of bits available for the network address to the IP address: 137.226.4.101/24. The number after the slash tells us that the first 24 bits indicate the network address. This notation reduces the length of the entries in the routing tables.

IP address management

The IP addresses must be unique within a specific network in order to avoid confusion. Since the Internet is based on TCP/IP and thus uses IP addresses for its millions of connected computers, all Internet addresses must also be unique. Bodies exist that manage and distribute these publicly-accessible addresses. Since the number of IP addresses theoretically available is limited, these distributing bodies charge high rates for the addresses.

Private address spaces

A range of IP addresses are reserved for use free of charge (private address spaces) so that companies do not have to purchase individual IP addresses for every workstation. In a closed network, these addresses can be used as desired, in a private network or company, for example. The same address can be used in other closed networks (e.g. in different companies), but the addresses within one network must be unique.

However, these reserved IP addresses must **not** be made public (on the Internet). Only **those** devices in a network that are connected to a public network (e.g. the router at the interface to the Internet) must have a registered IP address.

The allocation of IP addresses by the IANA (**I**nternet **A**ssigned **N**umbers **A**uthority) permits the following address ranges to be used for private use:

IP address	Netmask	Remark
10.0.0.0	255.0.0.0	"10" networks: All IP addresses beginning with 10. and whose mask begins with 255. belong to the address range reserved for private use.
172.16.0.0	255.240.0.0	All IP addresses beginning with 172.16.–172.31. which are associated with a net mask greater than or equal to 255.240.0.0 are within the address range reserved for private networks.
192.168.0.0	255.255.0.0	All IP addresses beginning with 192.168. and whose mask begins with 255.255. belong to the address range reserved for private use.
224.0.0.0	224.0.0.0	All IP addresses beginning with a 224 which are associated with a net mask also beginning with 224 are within the reserved address range. This range is reserved for broadcasting purposes and should not be used for private networks.

There are two considerations when using these IP addresses:

- The IP addresses used in a private network should not leave this network, i.e. an Internet connection is only possible when using IP masquerading, for example.
- The packets for these IP addresses will not be routed in the Internet, i.e. backbone routers will simply reject such IP packets. Depending on the provider, consequences may result if such IP packets are released on the Internet.

IP routing and hierarchical IP addressing

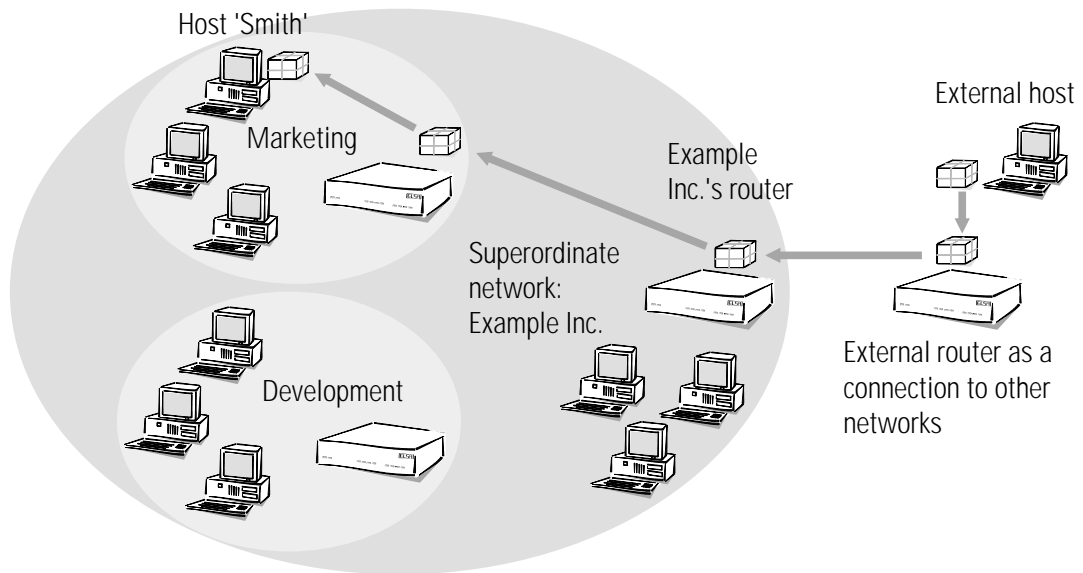
Routing-method Every IP packet contains the IP addresses of the source and of the recipient. A router receives IP packets at its interface, interprets the destination address and passes the packets on to those interfaces that are nearest to the recipient. Finding the appropriate path is called routing.

Routing-table Every router manages a table (routing table). This table indicates the quickest interface connection to the host for every host in the network. You can imagine that, as they grow, these tables may exceed the capacity of the router – the Internet, as a worldwide linking up of publicly accessible IP computers contains several millions of hosts.

Hierarchical IP addresses For this reason, hierarchical IP addresses were introduced. This means dividing the IP network into subnets in which IP addresses are appointed from a coherent numerical range. It is possible to establish several hierarchy levels, so that different subnets can be merged. The principle is similar to the hierarchical address used by paper mail, consisting of a country, a city, a street and a number.

The consequences of this hierarchical IP addressing:

- Since all hosts within one network have the same network address, the host address is sufficient for the hosts within this network to communicate with one another.
- A router has to know both the addresses of the hosts that are directly connected to it, and the addresses of all networks and subnets that are reachable via adjacent routers.
- It is **not** necessary for a router to know **all** other possible IP addresses.



As an example, think of a company with one large network, in which the different divisions are incorporated as small subnets. The address of the network for the marketing division is made up hierarchically from the address of the company and that of the department.

Whenever a host external to the company network sends a packet to a host in the Example Inc., this is what happens:

- ① The sender gives the packet the destination address "host 'Smith' – Marketing – Example Inc.".
- ② An external router that establishes the connections to other networks has to know how to reach Example Inc. As soon as it receives a packet with the address for Example Inc., it passes the packet on to the router responsible for Example Inc.
- ③ The router in Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division.
- ④ The router in the marketing division receives the packet and extracts from the address the information that it is directed at the marketing division of Example Inc. Since it is itself part of this division, it takes a closer look at the address to find the name of the host. It then passes the packet on to the host of the employee Sam 'Smith'.

Now we shall take a look at the example using proper IP addresses instead of symbolic names. The network of Example Inc. has the numerical space '192.168.100.0' to '192.168.100.255' at its disposal, with the '0' for the network address and the '255' for the sender address.

All the router has to remember is that every address beginning with '192.168.100' is located within the network of Example Inc.

Now imagine a router that is connected to the network of Example Inc. through an interface. If it receives a packet with destination address '192.168.100.4' and netmask '255.255.255.0', it will compare this with every network address it knows. In doing so it carries out a logical AND with the netmask, and compares the results with the network address: '192.168.100.4' AND '255.255.255.0' is '192.168.100.0'. This is the network address of the Example Inc. network. The router recognizes that the recipient is located within Example Inc. and passes the packet on to the appropriate interface for Example Inc. Within Example Inc. the packet is then passed on to the appropriate subnet.

The same procedure is used for the transfer of IP packets within a network:

- ① If a host in the subnet of the development department wants to send a data packet to Mr. 'Smith', the sender attaches the destination address "Host 'Smith' – Marketing – Example Inc.".
- ② The router in the development division receives the packet and extracts from the address the information that it is directed at the marketing division of Example Inc. Since it is itself part of Example Inc., but not of the marketing division, it passes the packet on to the router in the superordinate network.
- ③ The router in Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division, where the packet is passed on to the recipient.

Expansion through local networks

Media access control

Up to now we have only considered the point-to-point connections. However, many computer networks are based on multipoint cabling such as Ethernet. All computers connected to the same network can then receive the signals of all other computers (so-called broadcast transfer to a shared medium). If several computers are sending simultaneously, the superimposed signals are destroyed. A variety of access methods such as CSMA/CD or Token Ring are implemented in the MAC layer (**Media Access Control**) for the avoidance and resolution of such collisions.

LAN and IP network

The connection of all computers communicating through a shared medium using a MAC protocol is called a LAN (local area network). A LAN forms an independent network and is subordinate to the IP network, i.e. IP networks can use the physical connections of the LAN to establish connections between the hosts and the routers. A LAN – Local Area Network – is, as the name indicates, spatially limited.

MAC-address

Specific LAN addresses hardwired into the interfaces by their manufacturers are used to manage the transfer in the LAN. Since the LAN addresses are used for communication

via the MAC protocol, they are called MAC addresses. They can be thought of as the fingerprint of the interface hardware. MAC addresses can look like this, for example: 00-80-C7-6D-A4-6E.

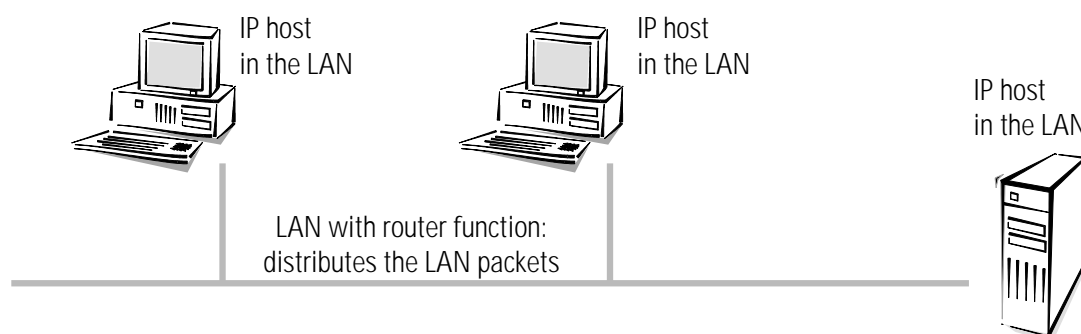
MAC addresses are independent of IP addresses. An IP host whose interface works through a LAN has an IP and a MAC address. Whereas the structure of IP addresses with its similarity to postal addresses is supposed to simplify routing in enormous IP networks, the fingerprint-like MAC addresses are designed to make the connection to a LAN as easy as possible.

Transfer in LAN is also packet-oriented. Every MAC packet contains the MAC addresses of the source and of the recipient. Although every packet is received by all computers, it is processed only by the target computer. There is an additional MAC broadcast address that is processed by all computers in the LAN.

IP in the LAN

Every LAN packet contains an entry with the type of the network protocol. An IP packet can be transferred through a LAN by packing it in a LAN packet and adding the 'IP' protocol type to it. Because of the IP entry, the LAN interface at the receiving host recognizes that the LAN packet contains an IP packet, extracts it and processes it as an ordinary IP packet. In this way, IP packets and packets of other network protocols like IPX can be transferred simultaneously through the same LAN without conflicts (this is why a LAN is called multiprotocol-capable).

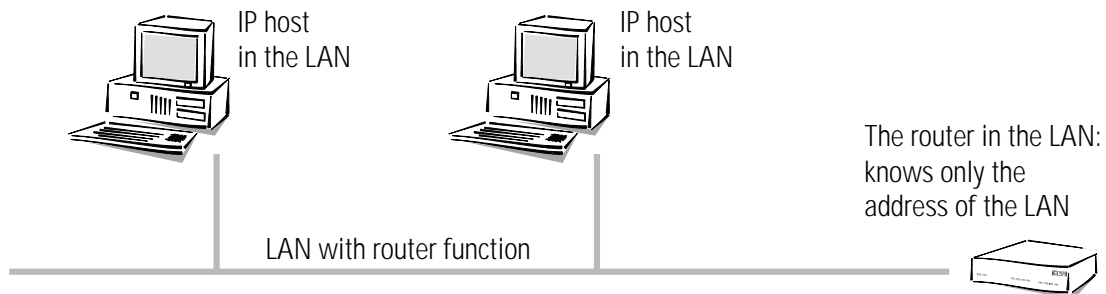
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts gives the packets to the LAN which handles the further distribution of the data packet. This is why only IP addresses from the numerical space of the specific network should be used for the internal communication of the hosts through the IP protocol.



To a router in the LAN, a host in its own LAN seems to be located behind another router. So the task for the router is very simple: all it has to know for operating in the IP network are the IP addresses

- of the directly connected hosts and
- of the available networks and subnets,

i.e. all it has to remember is the network address and the netmask of the subnet in the LAN.



In contrast, the host is confronted with a more difficult task than the router. In case of a wired point-to-point interface, the host knows that all packets that it sends through the interface automatically arrive at its router, for example. In case of the point-to-multipoint connection to the LAN, it has to distinguish two cases, however.

- A packet with an address outside the LAN is passed on to a by a sending host to a router in the LAN that takes care of the further processing of the packet.
- A packet with an address within the LAN has to be sent immediately to the target host, since the router in the network does not know the addresses of all the different hosts.

Data transfer within the LAN

Let's use an example to explain this. Imagine the hosts of the subnet in the marketing division are linked via a LAN. The hosts have IP addresses from the numerical space '137.226.4.1' to '137.226.4.254' (the addresses '137.226.4.0' and '137.226.4.255' are reserved), the network address is '137.226.4.0' and the netmask is '255.255.255.0'. A router connected to the LAN provides access to the wide world of the Internet. Its LAN interface has the IP address '137.226.4.1' and the MAC address '00-80-C7-6D-A4-6E'.

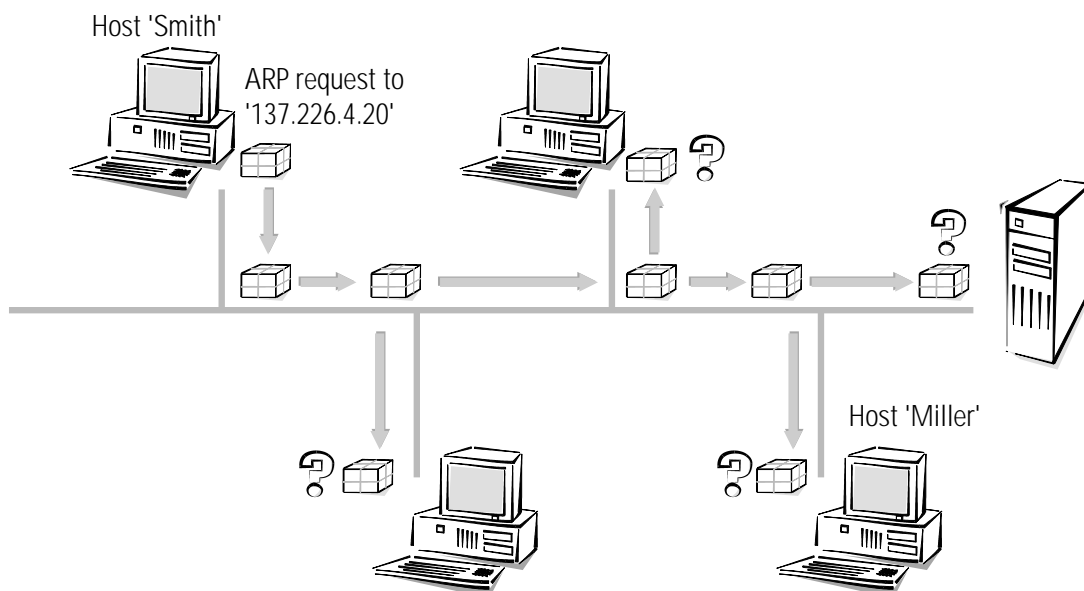
Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). Using the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located in the own network. It therefore has to send the packet through the LAN, directly to host 'Miller'. Unfortunately the LAN interface cannot say: "Send the IP packet to IP address 137.226.4.20", because the LAN interface only understands MAC addresses.

This is why every host has to manage a table that translates IP addresses to MAC addresses. But how do the entries end up in the table? They could be entered manually, but that would not satisfy the objective of making the connecting of a new computer to the LAN as easy as possible.

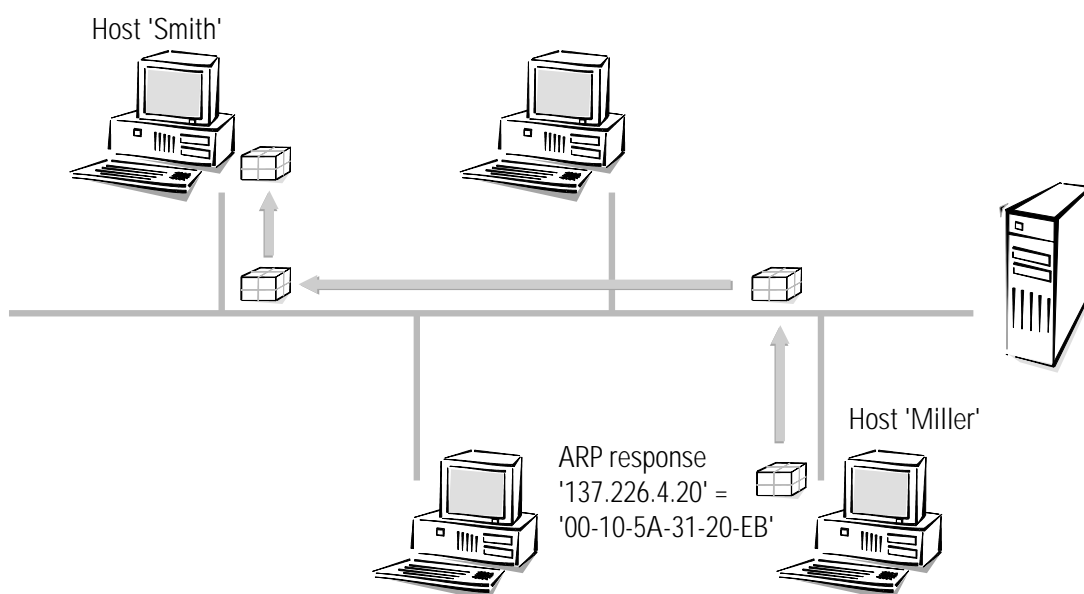
ARP

Therefore the LAN has a special mechanism that automates this process: the **Address Resolution Protocol**, ARP. The table itself is called the ARP table. Whenever a host does not find an entry in the table for a particular IP address (in our example '137.226.4.20'), it

sends an ARP request packet to all hosts in the LAN (with the LAN broadcast address as a target address).



This ARP request packet is simply a question to all hosts listening to the IP address '137.226.4.20'. Host 'Miller' receives the packet, detects that it is addressed and responds with an ARP response packet, which it sends directly to host 'Smith' host (it takes the MAC address '00-10-5A-31-20-DF' of host 'Smith' from the sender field in the ARP request packet). Host 'Smith' recognizes this as an answer to its request, extracts the MAC address '00-10-5A-31-20-EB' from the ARP response packet and enters it into his ARP table.



Then it can finally turn to its original task: sending the IP packet to host 'Miller'. It now finds the entry "IP address 137.226.4.20 corresponding to MAC address '00-10-5A-31-20-

EB'' in the ARP table and tells his LAN interface: "Send this IP packet to the computer with the MAC address '00-10-5A-31-20-EB'".

Data transfer from the LAN onto the Internet

Imagine the second task, sending an IP packet from host 'Smith' to the remote host 'External' with IP address 151.189.12.43. Host 'Smith' compares the IP address with his network address and realizes that host 'External' is located outside the LAN. So host 'External' can only be reached through the router. The MAC address of router '00-80-C7-6D-A4-6E' finds out about its IP address by going through the ARP table (if necessary another ARP request is made). So host 'Smith' tells its LAN interface: "Send this IP packet to the computer with the LAN address '00-80-C7-6D-A4-6E'". The router extracts the IP packet from the LAN packet and finds out about the IP address of host 'External'. In the routing table the router then looks for the network address of this host and thus finds the interface through which to pass on the IP packet.

LAN coupling on MAC basis

You know how LANs simplify the connection of computers to a local network. Nearly all house networks are thus LAN based. In some cases a LAN is covers such a large area that the physical characteristics of the wiring prohibit the connection of any more computers. This results in the necessity to couple up several LANs in such a way that electrically and in terms of the MAC protocol they act as independent LANs, but for the IP protocol look like one big LAN.

This coupling of LANs is carried out using bridges. A bridge works somewhat like a router, but uses only MAC addresses for routing, not IP addresses. Since MAC addresses do not give any information on the structure of the network the way IP addresses do, every bridge has to know all MAC addresses in the whole LAN.

And so we encounter the same problem that we had with the routers before the introduction of subnets: As the LAN expands, it will at some point exceed the capacity of the address tables of the bridges. So one cannot use bridges to connect as many LAN's as desired. On the other hand, the unstructured MAC addresses allow the bridges to learn automatically about the location of computers in the network, using the received packets. This is called an "intelligent bridge".

Description of the menu options

The menu tree for the 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.




























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.

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		WLAN-statistics
	TCP-IP-module		WAN-statistics
	IP-router-module		LAN-statistics
	SNMP-module		PPP-statistics
	DHCP-module		TCP-IP-statistics
	DNS module		IP-router-statistics
	NetBIOS-module		Config-statistics
	Config-module		Queue-statistics
	WLAN-module		Connections-statistics
	LANCAPi-module		Info-connection
	LCR-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
	Firmware-upload		PCMCIA-status
	Test-firmware		Delete-values
			Other
			Manual-dialing
			Reset-system
			Boot-system
			System-upload




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
S ₀ -bus		Status of the S ₀ interface
WAN-statistics		Displays WAN statistics
LAN-statistics		Displays LAN statistics
WLAN-statistics		Wireless network area statistics
PPP statistics		Point-to-point-protocol statistics
Bridge-statistics		Bridge area statistics
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 10 calls received
Remote-statistics		Statistics on the last 10 connections
Channel-statistics		Information of the status of the individual channels. Also information on the a/b ports with <i>ELSA LANCOM Wireless L-2</i> .
Time-statistics		Time module information

Status		Running status displays
LCR-statistics		Least-cost router information
PCMCIA-status		Information on PCMCIA status
Delete-values		Deletes all values except tables with substatistics. Delete statistics

Status/Connection-state

The **Status/Connection-state** 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/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/WLAN-statistics

The current status of the WLAN interface is described here.

LAN-rx-packets		Number of data packets received
LAN-tx-packets		Number of data packets sent
LAN-rx-errors		Number of data packets incorrectly received
LAN-tx-errors		Number of data packets incorrectly sent
LAN-stack-errors		Number of packets without a suitable receive module (bridge/router)
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
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 WAN
LAN-Tx-multicasts		Number of multicasts received from the WAN
LAN-Tx-unicasts		Number of unicasts received from the WAN
LAN-tx-discarded		Number of packets discarded by the LAN
LAN-repeats		Number of packets that were repeated before being received successfully
LAN-multiple-repeats		Number of packets that were repeated several times before being received successfully

BSSID		Numerical cell identifier; numerical translation of the WLAN domain name. In infrastructure mode this is always identical with the MAC address of the access point
Phy-channel		The radio channel currently being used by the base port.
LAN-Ready		Successful initialization of the wireless network adapter.
Station table		Display of the mobile stations currently logged on.
WLAN parameters		Wireless network parameters

Station table This table displays information on the individual mobile stations:

Channel	B channel identification.
Index	displays the sequence of entries in the table.
Age	Age of the station: Time since the last data packet was transferred.
Phy-signal	Average signal strength of the data packets received from this station.
Node ID	Address of the station. Depending on availability, a MAC address, IP address or a symbolic name if this station uses DHCP.
LAN-tx-bytes and LAN-rx-bytes	Data volume transmitted from or to this station.
Status	Can be either 'None', 'Auth' or 'Assoc'. When logging on, a station first authenticates itself, then it 'associates' itself, i.e. makes itself available for data communications. The base port will to transfer data without the 'Assoc' status! 'Auth' indicates whether the station replies to an authentication on the part of the base port.
Encaps.	Ethernet frames can be encapsulated in a variety of ways in a WLAN frame. In the 'IEEE' method, a new header is prepended to the complete Ethernet packet. A different method uses a more intelligent process in which the headers are converted in one another and 'LLC-SNAP' coding is applied to identify the protocol. The base port automatically recognizes both coding forms. If the choice is available, select SNAP coding, as the overhead per frame is 6 bytes lower.

WLAN parameters










This table displays the current wireless-network parameters:

Regulatory domain		The frequency band made available by the WLAN-card firmware
PHY type		Radio transmission technique used, set to DSSS.

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:

lfc	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:

lfc	Designates the associated channel.
CRx-bytes	Number of bytes received (compressed)
Rx-bytes	Number of bytes received (uncompressed)
Tx-bytes	Number of bytes sent (uncompressed)
CTx-bytes	Number of bytes sent (compressed)

Packet-transport-statistics

For each available interface, the **Status/WAN-statistics/Packet-transport-statistics** menu option provides statistics on the data packets transferred via this interface. The table maintained here has the following layout:

lfc	Rx	Tx-total	Tx-normal	Tx-reliable	Tx-urgent
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

Below is a detailed description of the meaning of each field:

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-I1-error	Rx-I2-error	Rx-I3-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-I3-error	Number of layer-3 errors in data received (i.e., the protocol header of layer-3 is incorrect)
Rx-I2-error	Number of layer-2 errors in data received (i.e., similar to the layer-3 errors, e.g. defective PPP header)
Rx-I1-error	Number of layer-1 errors in data received (similar to layer-3 errors)
Tx-error	Number of transmission errors that occurred while sending
Stack-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		Number of data packets received
LAN-tx-packets		Number of data packets sent
LAN-rx-errors		Number of data packets incorrectly received
LAN-tx-errors		Number of data packets incorrectly sent
LAN-stack-errors		Number of packets without a suitable receive module (bridge/router)
LAN-NIC-errors		Number of data packets discarded by the NIC
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
LAN-collisions		Number of collisions during a send procedure
Connection -established		Display of correct Ethernet connection (data transfer possible). Corresponds to the 'Link' LED on the device.
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
WAN-rx-broadcasts		Number of broadcasts received from the WAN
WAN-rx-multicasts		Number of multicasts received from the WAN
WAN-rx-unicasts		Number of unicasts received from the WAN
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
IPCP-statistics		Displays PPP/IPCP statistics
CBCP-statistics		Displays PPP/CBCP statistics
CCP-statistics		Displays PPP/CCP statistics
ML-statistics		Displays PPP/ML statistics
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	IPXCP	IPCP	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.
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/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-response	Number of CBCP response 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
Delete-values	Deletes IPCP statistics.

Status/PPP-statistics/CCP-statistics

The statistics of the CCP (Compression Control Protocol) 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
IPCP		Information on addresses in the IP network

The LCP table has separate listings for every channel:










MRU	M aximum R ecieve 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
Auth.	Authentication procedure used (PAP/CHAP)
Callback	Callback negotiation type

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/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
TCP-statistics		Statistics for TCP packets from TCP sessions to the router
TFTP-statistics		Statistics for TFTP operations
DHCP-statistics		Statistics from the DHCP server
NetBIOS-statistics		NetBIOS module statistics
DNS-statistics		Statistics from the DNS server
Delete-values		Deletes TCP/IP statistics

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
Delete-values	Deletes ARP statistics
Table-ARP	Displays ARP table

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 fragmentation errors	Number of fragmentations incorrectly received from the LAN
IP-LAN fragmentations	Number of fragmentations received from the LAN
IP-LAN forced fragmentation	Number of fragmentations forced by 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 fragmentation errors	Number of fragmentations incorrectly received from the WAN
IP-WAN fragmentations	Number of fragmentations received from the WAN
IP-WAN forced fragmentation	Number of fragmentations forced by 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
Server flags	Activate/deactivate server flags
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

<i>B-Nodes</i>	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.
<i>P-Nodes</i>	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.
<i>M-Nodes</i>	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).
<i>W-Nodes</i>	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 NetBIOS tables
Filter		Number of DNS packets filtered by the filter table
Hit-list		This table contains the 16 most popular requests. These may then be prohibited via the filter list if desired.

The hit list has the following structure:

Name	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:






Name	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

/IP-router-statistics	Statistics from the IP router area	
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

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	Source	Protocol	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-RIP	Routing table of routes learned through RIP broadcast
Delete-values	Deletes IP-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

/Config-statistics	Remote configuration statistics	
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
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
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
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.

/Queue-statistics	Statistics on the queue	
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.
WLAN management heap packets		Number of packets available in the buffer.

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:

lfc	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:

lfc	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-HZ	B2-HZ
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 Wireless IL-2</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-HZ	Indicates the short timeout for the connection.
B2-HZ	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	PPPHDLC	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:

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:

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. <i>LANCOM Office-Router</i> can also display the values A-3 kHz (analog 3 kHz), language (for normal speech transmission) and fax G2/3 (for analog fax transmission as per group 2 or 3).
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 ten connections of the *ELSA LANCOMs* with information on the remote station.

The table has the following layout:

Conn.-start	Remote-ID	Mode	Ifc	Conn.-time	Charge
OT; 00:20:57	BERLIN	Active	Ch01	50	5
OT; 00:20:46	CHEMNITZ	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 RR – 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/Channel-statistics

This table shows information on the current status of the two B channels. With the *ELSA LANCOM Wireless IL-2* information on the a/b ports is also shown. 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 -ERR	0000000 0	Router	active	0000	0241123456	00000000	3	0		
S ₀ -B1	0000000 0	a/b	active	0000	0241123457	00000000	2	20		
S ₀ -B2	0000000 0	LANCAP I	passive	0000	0241123458	00000000	4	180		





Below is a detailed description of the meaning of each field:

Channel	Channel (or a/b port) 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> or a/b port
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 Wireless* 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

Status/LCR-statistics




This menu has information on the current time in the device and on the path over which the *ELSA LANCOM Wireless* has obtained the time.

The menu has the following layout:

/LCR-statistics		Least-cost router statistics
Total calls		Total number of LCR calls
Successes		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.
No-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/PCMCIA-status

General information on the inserted card can be found here:

DHCP adapter present		Indicates whether card is inserted – this does not necessarily mean that the card is working, but only that something has been inserted in the PCMCIA slot!)
Card ID		The card name read out of the PCMCIA-Config-Space, i.e. the device name for which Windows requests a driver when the card is inserted for the first time.
Firmware version		Information about the firmware of the WLAN card, provided that the card initialized correctly.
















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
WLAN-module		WLAN settings
TCP-IP-module		TCP/IP module settings
IP-router-module		IP router module settings
SNMP-module		Settings for configuration via SNMP
DHCP-module		DHCP server settings
Config-module		Configuration module settings
DNS module		DNS server settings
NetBIOS-module		NetBIOS module settings
LANCAPi-module		<i>ELSA LANCAPI</i> settings
LCR-module		Least-cost router 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 ?
```

display. 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.

Since the router permits only upper case letters in the device name list, the name is transferred in uppercase letters in the case of a verification by the ELSA protocol. Special characters should not be used in device names unless the remote station can process them.

In addition, the device names you assign must be unique. For example, you might match the device names to the location (e.g. Aachen, Berlin, 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
Name-list		Remote station settings
RoundRobin-list		Settings for different remote station numbers
Layer-list		Settings for the layer combinations used
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

Interface-list

This table contains the interface settings, which apply to all operating modes (modules) of the devices.

lfc	Protocol	FV-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

setup/ab-module/port-list

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 GRP2 : Leased-line connection group 2 P2P-DSS1 : Point-to-point connection
FV-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. The fixed connection function is not a standard component of the <i>ELSA LANCOM Wireless</i> .
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	YV.	CLIP
S0	123456	Off	On

Below is a detailed description of the meaning of each field:

Ifc	Designates the associated interface.
MSN-EAZ	If your device is connected to an ISDN port with 1TR6, enter the EAZ to which the interface is to respond. 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. 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.
YV.	This entry can be used to control the interface's ability to establish Y connections. Possible settings are: 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. Refer also to the settings for the availability of the <i>LANCAP</i> and the telephone system with the <i>ELSA LANCOM Wireless IL-2</i> . 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.
CLIP	Calling Line Identification Protocol: Suppresses the outgoing MSNs. Possible values: Yes : Activate CLIR, do not send MSN. No : Deactivate CLIR, send MSN to remote station. Please note: The "selective suppression of call number transmission" may be a service feature that will have to be obtained from the telephone company.

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-HZ	B2-HZ	WAN-layer	Callback
AACHEN	875463	180	0	PPPHDLC	On
BERLIN	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-HZ	In this column, you can define appropriate connection timeouts (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-HZ	In this column, you can define appropriate connection timeouts 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
AACHEN	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. AACHEN#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 standard settings are valid for *LANCOM Office-Router*:

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	TRANS	PPP	TRANS	compr.	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	none	HDLC64K
RAWHDLC	TRANS	TRANS	TRANS	none	HDLC64K
BRIDGE	ETHER	TRANS	X.75LAPB	none	HDLC64K

Below is a detailed description of the meaning of each field:

Layer-name	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 or in bridge operation.
	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).
	ELSA	The data is provided with an ELSA header. In addition, when a connection is established, a protocol negotiation is performed in which the remote stations exchange names. Incoming-call protection by name is possible only if this setting is selected. Without an ELSA setting, incoming-call protection is possible by call number only. This setting is required for communication with older <i>ELSA LANCOM</i> devices or the workstation drivers.
	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.	V.42bis (<i>ELSA LANCOM Wireless IL-2</i>) or Stac data compression will be used. Data compression as per V.42bis is possible only in connection with X.75ELSA or X.75LAPB. 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' Static or dynamic channel bundling depends on the B2 connection timeout. A B2 hold time of '0' or '9999' will set a static channel bundling in which both channels are always used. In the event of dynamic channel bundling with other B2 hold times, the second channel is only activated when the data throughput exceeds a specified threshold.
	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.

In order for the device to function correctly as a bridge, **ETHER** must always be entered in the **Encaps** field. If the ELSA LANCOM is used as a router, any entry may be made and it should be adapted to the remote station.

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
AACHEN	CHAP	*****	0	5	10	5	2	ELSA

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.

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 AACHEN and BERLIN 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	AACHEN
040785647	BERLIN

This number list is required for passive connection establishment. The remote station call numbers must be entered without leading zeros.

The D-channel protocol that is currently activated is then used for a call number test.

If the 'Protect number' setting is selected and a call is received from a remote station, the remote station call number sent is compared to the entries in the number list. If the station number sent is identical to an entry in the list, the caller is authorized and the connection is established.

If the 'Protect no./name' setting is selected and a call is received from a remote station, the remote station call number sent is compared to the entries in the number list. If the call number sent is identical to an entry in the list, the caller is authorized to establish the connection. In addition, it is possible to derive the name of the remote station from the number list and, therefore, the layer that is to be used for this connection. The connection is then established using this layer and name verification is initiated using the layer detected (or using the default layer if no layer is detected).

If the name of the remote station (and thus the layer to be used) cannot be determined using the number list, the call will be accepted using the default layer and the name list will be checked for a suitable entry after the protocol (PPP) negotiation.

Script-list

Some Internet providers (e.g. CompuServe) conduct a script-controlled log-on procedure before a PPP negotiation. In order to be able to establish this type of connection as well, a simple script processing procedure is also implemented in the *ELSA LANCOM* (see 'Script processing').

In this table, the scripts are defined and assigned to the remote stations. The table has the following layout:




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

The entries in the script list have the following meaning:

- Device name: Name of the logical remote station
- Script: All commands to be executed – a maximum of 58 characters per line is available. If the required command sequence is longer, an additional entry for the logical remote station may be added as in the round-robin list. The syntax for this is: Device name followed by '#' and a number. The entries are processed from top to bottom.

Setup/WAN-module/Manual-dialing

This option can be used for manual connection control for testing purposes.

/Manual-dialing	Settings for manual connection control	
Connect		Establishes a connection.
Disconnect		Termination of connections
Status		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 functions. The default setting is 3.

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	
Connect		Selection of the network connection
Node ID		MAC layer address of the device
Spare-heap		Buffers that receive data packets from the local network

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/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	
State		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 ELSA LANCOM

State

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 network mask 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. The second IP address enables the device 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 IP address).

Intranetmask The network mask belonging to the IP address of the local network 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 the keyboard (ELSA LANCOM Wireless IL-2 only) or 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	
State		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

/IP-router-module	IP router module settings	
Loc.-routing		Activates/deactivates local routing
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* 'Dresden'.
- Two destination networks 192.120.131.0 and 192.120.132.0 can be accessed by the remote stations 'AACHEN' and 'BERLIN'.
- 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	DRESDEN	0	Off
192.120.130.11	255.255.255.255	DRESDEN	0	Off
192.120.130.12	255.255.255.255	DRESDEN	0	Off
192.120.131.0	255.255.255.0	AACHEN	0	Off
192.120.132.0	255.255.255.0	BERLIN	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	Source	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-

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	Dest	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'.

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	
Type		RIP compatibility switch
R1-mask		Management of network masks
Table-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-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

Here specify whether RIP packets will be sent to the LAN or the cable network.

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	Time
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 device 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-server-module

This menu allows you to enter settings for the DHCP server. The menu has the following layout:

/DHCP-server-module	DHCP server settings	
State		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
Gateway-address		Gateway-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

State 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	MAC-address	Timeout	Hostname	Type
10.1.1.10	00a0570308e1	500	ELSA	new

- IP-address: IP address assigned
- MAC-address: 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

The Setup/NetBIOS menu contains the settings for the NetBIOS module. The menu has the following layout:

State		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 be 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		Sets handling of watchdog packets.
Compensation		Compensation type of routing information.
WAN-update-min.		Compensation interval in minutes.

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
AACHEN	Router or workstation



If the connection to the selected remote station is to be realized via a PPP connection, the NetBIOS rights must be enabled for the corresponding entry in the PPP table.

Type

The 'Type' field specifies whether the remote station is a router or a workstation. In the case of a workstation, all of the known names and servers in the local network and all other connected routers are logged off and deleted from their respective tables as soon as the connection to the remote station is closed.

Host table The host table has the following structure:

Name	Type	IP-address	Remote-ID	Timeout	Flags
REMOTE	00	10.0.1.100	AACHEN	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-ID	Timeout	Flags
WORKGROUP	1e	10.0.0.10		5000	xx00
WORKGROUP	1e	10.0.1.100	AACHEN	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-ID	Name of the remote station for which the name became known.
Timeout	Time until the name is no longer valid. The timeout 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- ID	Timeout	Flags
REMOTE	WORKGROUP	00	10.0.1.100	0400	010F	0004140B	AACHEN	13	0020
WORKSTATION	WORKGROUP	07	10.0.0.10	0400	0415	00452003		31	0000

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-ID	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
Maximum-connections		Maximum number of simultaneous connections
Farconfig-(EAZ-MSN)		Subscriber number for remote configuration via PPP
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.
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 **Off**.

Farconfig-(EAZ-MSN) This subscriber number permits remote configuration via PPP. If no number is specified here, remote-configuration calls will be accepted on all numbers.

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 15 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>
LANCAPI-UDP-port		UDP port for communication between the <i>LANCAPI</i> server and clients
EAZ-MSN(s)		EAZ or MSN to which the <i>LANCAPI</i> should respond
Prio-out		Priority for the <i>LANCAPI</i> versus router connections







- **Operating:** 'on', 'off' or 'outgoing'. Under the last setting the *LANCAPI* will not accept incoming calls.
- **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*.
- **LANCAPI-UDP-port:** In the default configuration, this option is set to '75'. Change this setting only if other devices in your network are already using this port.







When you change the port, all active connections via the LANCAPI are lost!

- **EAZ/MSN(s)**: This option allows you to enter the call numbers to which the *LANCAPi* is to respond. If you wish to enter more than one number, place a semicolon between the individual numbers.
- **Prio-out**: 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/WLAN-module

the WLAN module is configured using this menu:

WLAN-Domain		The WLAN domain is entered here, i.e. the symbolic name that the mobile stations use to find the base port. An ASCII string with a maximum of 32 characters. The default setting is 'ELSA'.
Phy-channel		The radio channel to be used by the base port. The possible values are 1 to 14. However, the channels overlap due to the spread-spectrum process, so that the entire radio band offers a maximum of 3 completely independent channels. <i>Not all channels are permitted in all countries (please see the table of radio channels in the Appendix).</i>
Packet size		A value between 600 and 1600 that states the maximum size of WLAN packets in bytes. Default: 1550.
Access-list		This list can be used to explicitly exclude WLAN stations from data communications with the LAN/base port. Alternatively, authorized stations can be specified. Enter the MAC addresses of stations in this list – in other words, the 12-character hexadecimal numbers printed on the cards – but without separators, i.e. 00-60-B3-1F-02-11 would become 0060B31F0211. <i>This only denies the stations access to the LAN or WAN. Data communications between stations in the WLAN via the base port – which typically serves as a relay – is not affected.</i>
Access-mode		This positive/negative switch determines whether the list is to serve as an authorization or exclusion. By default, the mode is set to negative and the access list is empty, i.e. no stations are excluded from data communications.
Protocol-list		This list permits data packets to be blocked or permitted (depending on the positive/negative setting of the switch) on the basis of their protocol. Every Ethernet frame contains a 16-bit identifier stating the Layer-3 protocol of its data. These can be entered in the list as hexadecimal numbers. Common protocols include: 0800 = IP 0806 = IP/ARP 8137 = IPX F0F0, E0E0 = IPX 809B and 80F3 = Appletalk 6001 to 6007 = Decnet 80D5 and 0808 to 0D0D = IBM SNA <i>In this case as well, traffic is blocked between WLAN stations and the LAN or WAN, but not between the WLAN stations themselves.</i>





Protocol mode		Positive/negative switch for the protocol list
Node ID		MAC layer address of the device
Spare-heap		Buffers that receive data packets from the local network
IAPP protocol		On/Off switch for roaming. Roaming requires that all access points involved must be set with the same WLAN domain and must use the same radio channels.
IAPP announce interval		Time interval for the communication of an access point to all other access points within the wired LAN when roaming is activated.
IAPP handover timeout		Maximum wait period for the access point to communicate with the mobile station.

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.

For 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):

State		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:

Name	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	
State		Activating the module: On, Off
Current-time		Displays the current time in the device.
Time-EAZ-MSN		Call number to which a connection must be established to receive time information from the ISDN.
Dialing-attempts		Number of possible attempts to receive time information

Firmware

This menu allows you to display various firmware parameters and to initiate a firmware upload:

/Firmware	Display and keyboard settings	
Version-table		Displays hardware releases and serial numbers for the router
Table-firmsafe		Information on the two firmware versions stored in the device and on the bootloader.
Mode-firmsafe		Firmware activation mode
Timeout-firmsafe		Time in minutes required to test new firmware
Test-firmware		Tests the inactive firmware
Firmware-upload		Initiates a firmware upload

Version table The version table displays the firmware version and serial number of the device.

lfc	Module	Version	Serial number
lfc	LANCOM Business 4100	1.60.0012 / 30.06.1999	8427.000.020

Table firmsafe This table provides the following details for the two firmware versions stored in the device: the position in memory (1 or 2), status information (active or inactive), the version number, the date, the size and the index (sequential number).

Position	Status	Version	Date	Size	Index
1	Inactive	1.60	23061999	690	6
2	Active	1.60	30061999	692	7
3	<Lader>	1.60	07061999	64	0

Enter the following command to activate an inactive firmware version:

```
set <position number> active.
ein.
```





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). 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.
System-upload		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.

Ports and protocols

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

Capab.	Port no.	Protocol
www	80	tcp
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
sytek	500	udp
biff	512	udp

Capab.	Port no.	Protocol
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
mairtd	601	tcp
busboy	602	tcp
acctmaster	700	udp
acctslave	701	udp
acct	702	udp
acctlogin	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctslave2	706	udp
acctdisk	707	udp
kerberos	750	tcp

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

Protocols

Protocol	Protocol no.
apollo domain	8019
apple talk 1 & 2	809B
apple talk arp 1 & 2	80F3
banyan vines	0BAD
banyan vines echo	0BAF
decnet phase IV	6003
hp probe control	8005
ibm sna services	80D5
IP	0800
ip-arp	0806
novell (econfig e)	8137
rarp reverse arp	8035
snmp over ethernet	814c
xyplex	0888

