

ELSA LANCOM™ Wireless L-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, settembre 1999

Qualche parola di presentazione

Vi ringraziamo per la fiducia accordataci

Le reti radio della ELSA sono alternative vantaggiose dal punto di vista dei costi o complementi alle reti locali a cavi (LAN). Con schede di rete mobili, i notebook e i PC possono comunicare tra loro o accedere, tramite stazioni base, alle reti a cavo e perfino alla rete ISDN.

La presente documentazione si rivolge agli utenti della stazione base *ELSA LANCOM Wireless L-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 del prodotto, le informazioni di base tecniche (ad esempio sulle reti radio, tecnica generale di rete, TCP/IP ecc.), workshop con esempi applicativi dettagliati, parte di riferimento da consultare con descrizione completa dei menù

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



Se si hanno ancora dubbi sui temi trattati in questo manuale o si ha bisogno di un aiuto supplementare, 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\\ELSASIDE\\index.htm`

Contenuti

| | |
|---|-----------|
| Introduzione | 1 |
| Come opera una rete radio? | 1 |
| Che cosa offre un <i>ELSA LANCOM Wireless L-2?</i> | 4 |
| Installazione | 7 |
| Complesso di fornitura..... | 7 |
| <i>ELSA LANCOM Wireless</i> si presenta | 7 |
| Come collegare la stazione base | 9 |
| Installazione del software | 10 |
| Configurazione di base | 10 |
| Impostazioni di base con <i>ELSA LANconfig</i> | 10 |
| Effettuare le impostazione di tramite Telnet..... | 12 |
| Possibilità di configurazione | 13 |
| Onde radio o cavo: Vie per la configurazione..... | 13 |
| Presupposti..... | 13 |
| Alternativa: Gestione indirizzi con il server DHCP | 13 |
| Avviare la configurazione tramite <i>ELSA LANconfig</i> | 14 |
| Avviare la configurazione tramite Telnet..... | 14 |
| Comandi per la configurazione | 15 |
| Nuovo firmware con FirmSafe..... | 16 |
| FirmSafe funziona così..... | 16 |
| Un nuovo software si carica così..... | 17 |
| Configurazione con SNMP | 18 |
| Funzioni e modalità | 19 |
| Parametri per i collegamenti radio | 19 |
| Sicurezza per la configurazione | 21 |
| Protezione con password | 21 |
| Il blocco del login | 21 |
| Controllo in arrivo tramite TCP/IP | 22 |
| Gestione indirizzi automatica con DHCP | 22 |
| Il server DHCP | 23 |
| DHCP – 'On', 'off' o 'auto'?..... | 23 |
| Gli indirizzi vengono assegnati in questo modo | 24 |
| Configurazione del server DHCP | 27 |
| Appendice | 31 |
| Dati tecnici..... | 31 |
| Canali radio | 31 |
| Condizioni generali di garanzia a partire dal 01.06.1998..... | 32 |
| Dichiarazione di conformità | 34 |

| | |
|--|-------------|
| Index | 37 |
| <hr/> | |
| Technical basics | R-1 |
| Wireless networks in accordance with the IEEE 802.11 standard..... | R-1 |
| Ad hoc mode | R-1 |
| Infrastructure mode..... | R-2 |
| Interchangeability with other devices | R-3 |
| Network technology..... | R-4 |
| The network and its components..... | R-4 |
| Connection modes..... | R-4 |
| Kinds of networks | R-6 |
| IP addressing..... | R-6 |
| IP routing and hierarchical IP addressing | R-9 |
| Expansion through local networks..... | R-11 |
| <hr/> | |
| Description of the menu options | R-17 |
| Status..... | R-19 |
| Status/Current-time | R-19 |
| Status/Operating-time | R-19 |
| Status/WLAN-statistics..... | R-20 |
| Status/LAN-statistics..... | R-21 |
| Status/TCP-IP-statistics | R-22 |
| Status/Config-statistics | R-26 |
| Status/Queue-statistics | R-26 |
| Status/PCMCIA-status..... | R-27 |
| Status/Delete-values | R-28 |
| Setup..... | R-28 |
| Setup/LAN-module | R-29 |
| Setup/TCP-IP-module..... | R-30 |
| Setup/SNMP-module..... | R-33 |
| Setup/DHCP-server-module..... | R-34 |
| Setup/Config-module..... | R-36 |
| Setup/WLAN-module..... | R-37 |
| Firmware | R-38 |
| Other | R-40 |
| <hr/> | |
| TCP/IP Ports | R-41 |

Introduzione

I vantaggi di LAN radio sono evidenti: Notebook e PC possono essere disposti dove è necessario – con la messa in rete senza cavi, i problemi con prese mancanti modifiche all'ambiente appartengono al passato.

Il collegamento alla rete in conferenze o in presentazioni l'accesso alle risorse in edifici vicino e lo scambio dati con periferiche mobili sono solo alcune delle possibilità di impiego della LAN radio.

Il ruolo centrale in una rete a cavo è assunto dalla stazione base. Tramite la stazione base tutte le stazioni della rete radio hanno accesso alla LAN.

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

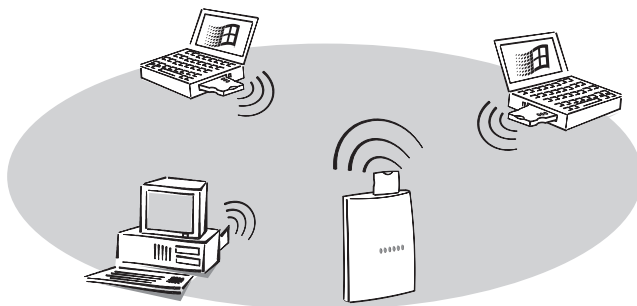
Con le schede di rete radio si collegano singoli notebook e PC in una rete locale, una **Local Area Network (LAN)**. Poiché in questa LAN il cavo comunemente usato viene sostituito da un collegamento radio, queste reti radio vengono anche chiamate **Wireless Local Area Network (WLAN)**.

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.

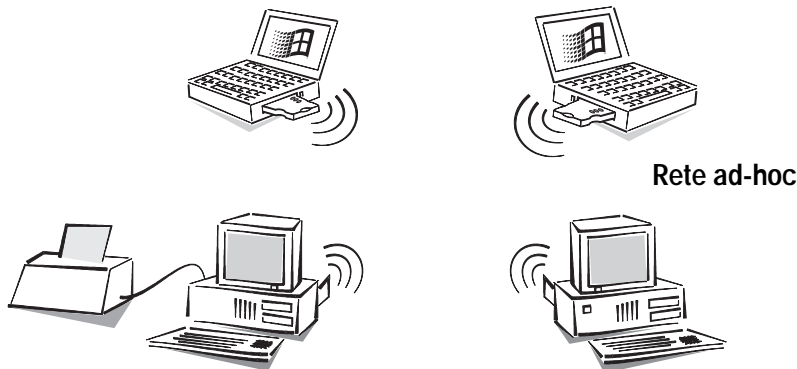


In una rete radio si hanno a disposizione tutte le funzioni di una rete a cavo: È possibile l'accesso a file, server, stampanti ecc. come pure l'implementazione delle stazioni mobili in un sistema di posta elettronica interno all'azienda.

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

Collegamento diretto di computer

Collegare con la schede di rete radio due o più computer direttamente tra loro. Tutti i computer in una WLAN possono comunicare senza ulteriore hardware tra loro.

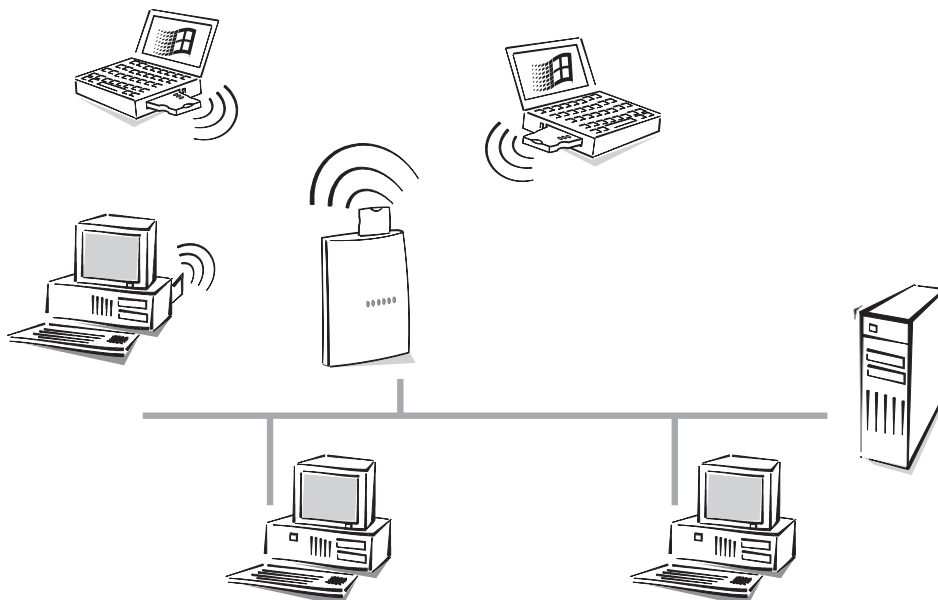


Peer-to-peer

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

Collegamento ad una LAN a cavo

Tramite una stazione base, tutti i computer hanno grazie alle schede di rete radio accesso ad una rete a cavo. La stazione base serve da un lato quale collegamento tra LAN e WLAN; dall'altro essa costituisce la centrale di commutazione per lo scambio dati all'interno della WLAN.



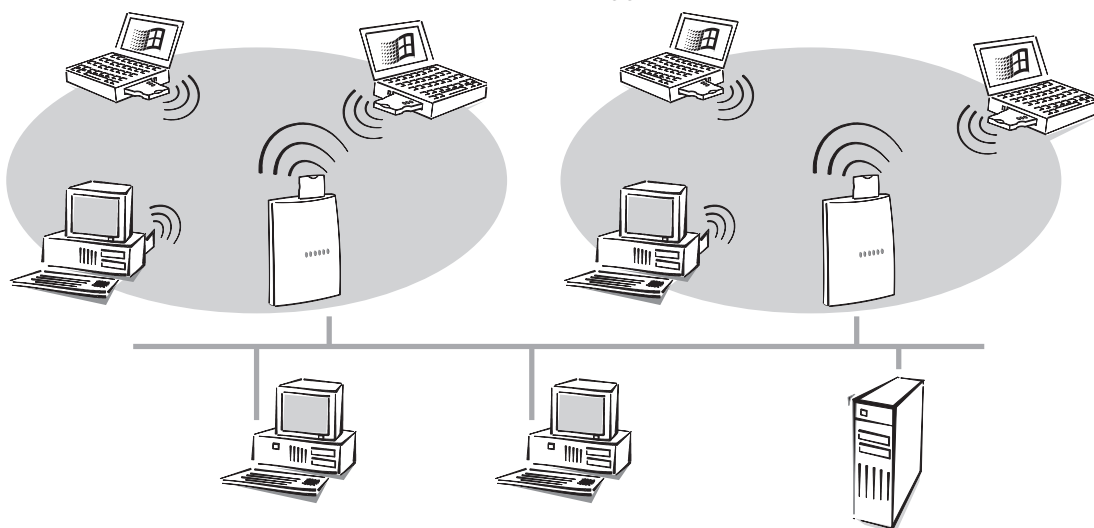
Peer-to-LAN

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.

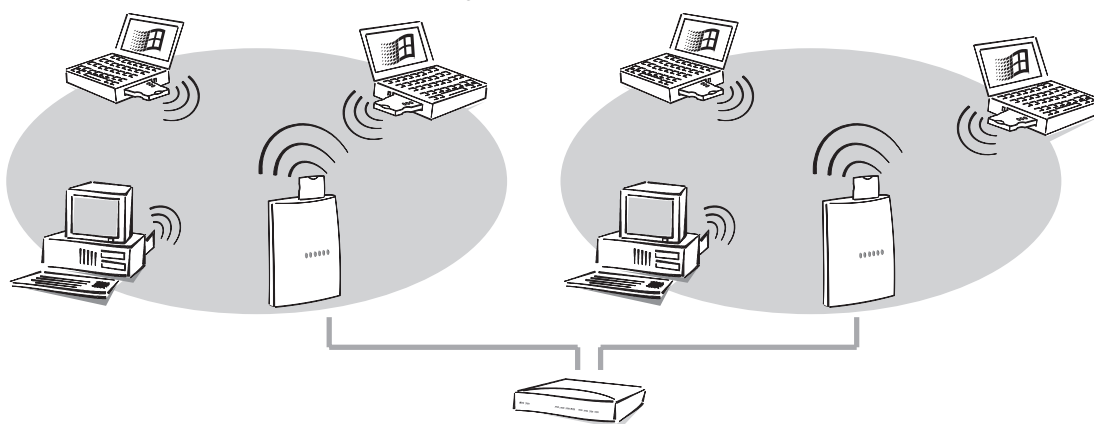
Questo tipo di rete è adatto in modo ideale quale complemento di LAN esistenti. Nel caso di ampliamento di una LAN in zone dove un cablaggio è impossibile o non economico, la rete infrastruttura rappresenta l'alternativa ideale.

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 ad esempio venire collegate tramite un semplice cavo di rete e un hub.



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

Che cosa offre un *ELSA LANCOM Wireless L-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
- Avviare
- Il sistema è pronto

Connessione LAN

Le stazioni base per rete radio di ELSA operano in Ethernet. Tramite il connettore 10Base-T ed 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 tra 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 frantumati 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 Mbps. Il raggio di azione della trasferimento è pari all'aperto a massimo 300 metri, in edifici tipicamente a ca. 30 metri.

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 Ethernet come pure dei collegamenti a cavo correnti e facilitano in tal modo la diagnosi nel caso di possibili disturbi del sistema.

Configurazione con *ELSA LANconfig*

L'impostazione e l'adattamento del apparecchio ai propri compiti specifici si realizza in modo rapido e comodo per mezzo del tool di configurazione in dotazione *ELSA LANconfig* per sistemi operativi Windows. Gli utenti di altri sistema operativi utilizzano Telnet.

L'accesso all'apparecchio è possibile da WAN o da LAN. In questo caso viene supportato oltre a TFTP anche SNMP.

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

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 o WAN.

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.

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.

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 L-2*
- Alimentatore
- Scheda di rete radio *ELSA AirLancer MC-2*
- cavo di connessione LAN
- 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

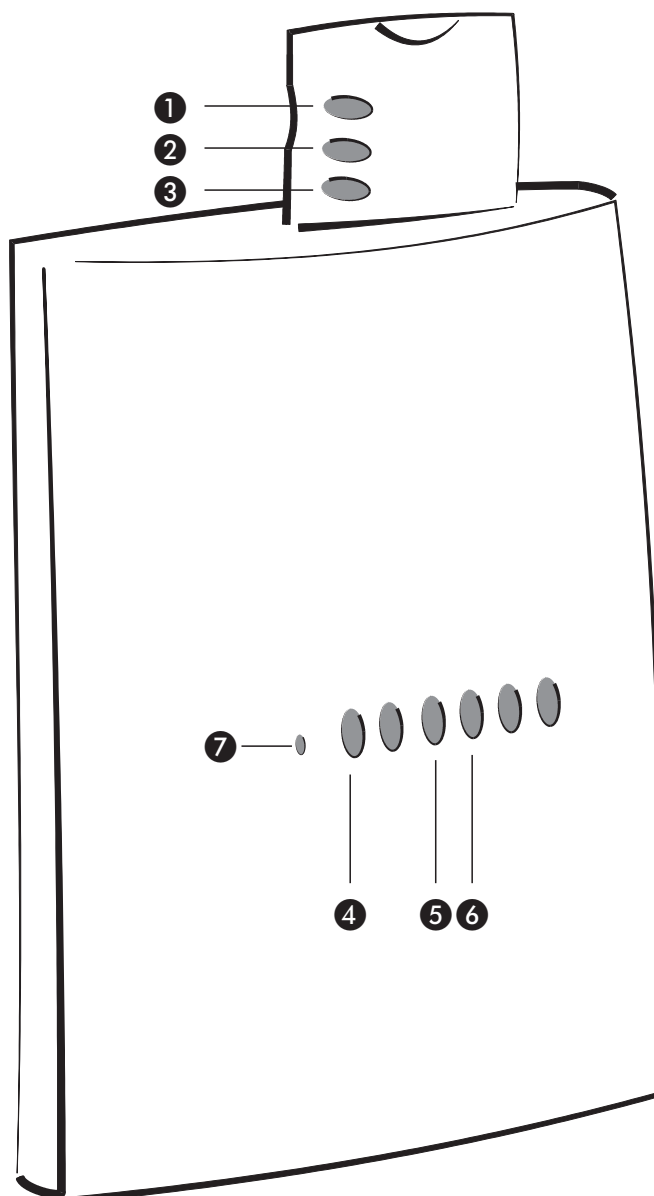
In questo capitolo viene presentato l'hardware dell'apparecchio. Si riceve qualche notizia sul significato degli elementi di visualizzazione e sulle possibilità di connessione.

Stazione base La stazione base costituisce il collegamento tra la rete radio e la rete a cavo (LAN). Essa offre a tale scopo accanto al connettore 10-Base-T per il 10 Mbit Ethernet anche uno slot per la scheda di rete radio *ELSA AirLancer MC-2*.

Scheda per PC La scheda di rete radio *ELSA AirLancer MC-2* è una scheda per PC e viene semplicemente innestata nello slot della stazione base. L'antenna della scheda sporge dal contenitore della stazione base.

LED

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



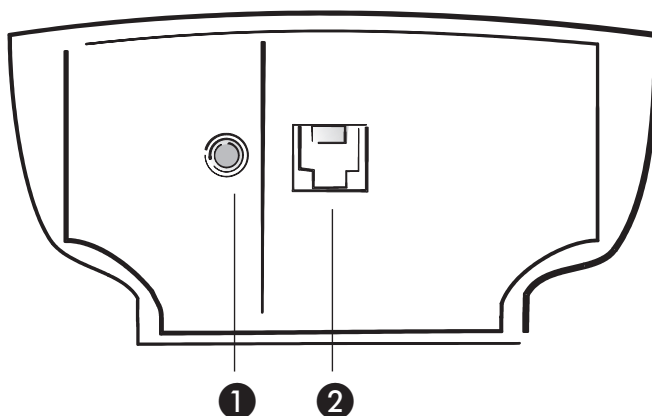
- ❶ Il LED rosso della scheda di rete radio mostra che è stabilito un collegamento tra la scheda e la stazione base.
- ❷ Il LED giallo della scheda di rete radio mostra il numero delle stazioni mobili che si sono registrate presso questa stazione base. Nel caso di tre stazioni registrate il LED lampeggia ad esempio 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 ed il LED rimane costantemente acceso.

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

- ⑤ Il LED 'LAN-Status' della stazione base indica l'attività sulla rete radio e sul LAN.
- ⑥ Il LED 'LAN-Collision' della stazione base indica una collisione di trasmissione nel LAN.
- ⑦ Il tasto di reset è nascosto nel e può essere premuto solo con un oggetto appuntito (ad esempio 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:



- ⑧ Connessione per l'alimentatore
- ⑨ Connessione di rete 10Base-T

Come collegare la stazione base

- ① Collegare la stazione base *ELSA LANCOM Wireless L-2* con il LAN. Innestare a tale scopo il cavo di rete fornito nel connettore 10Base-T della stazione base ed in una presa di rete libera della propria rete locale (o in una presa libera di un hub della propria LAN).
- ② 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.

- ③ 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 indica che il collegamento tra la scheda e la stazione base è stabilito. 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.

Impostazioni 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.

Per mettere in servizio un *ELSA LANCOM Wireless*, l'indirizzo IP XXX.XXX.XXX.254 della propria rete non deve essere occupato. Se dovesse esserci già un'apparecchiatura con questo indirizzo, per il periodo della messa in servizio del *ELSA LANCOM Wireless* spegnerla.

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



- ② Scegliere l'opzione 'Effettua tutte le Impostazioni 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 correllerà gli indirizzi IP per tutte le apparecchiature della rete (LAN e WLAN) automaticamente.
- oppure
- L'utente non desidera usare indirizzi IP poiché ad esempio si impiega una pura rete Windows.



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

- ③ Scegliere l'opzione 'Desidero effettuare le impostazioni da solo' 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, ad esempio '10.0.0.1' con la maschera di rete '255.255.255.0'. In tal modo si stabilisce anche contemporaneamente l'area di indirizzamento, che poi il server DHCP userà per le altre apparecchiature della rete (a meno che il server DHCP non venga disattivato).

- L'utente ha finora già usato per i computer della LAN indirizzi IP. Assegnare 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* (ad esempio 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 ad esempio 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/Intranet-Adr. 10.0.0.1
set /Setup/TCP-IP-module/Intranet-mask 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 tramite la rete si ha accesso da ogni computer del WLAN o LAN 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* ad esempio 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 un nuovo apparecchio, 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 il *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 file** le impostazioni attuali vengono lette dalla periferica e vengono visualizzate le informazioni generali sulla periferica.

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

Avviare la configurazione tramite Telnet

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

```
telnet 10.1.80.125
```

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


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

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/nome MILANO assegna all'apparecchio il nome 'Milano' |
| set <VALORE> ? | Mostra quali valori possono essere introdotti. | |
| del <VALORE> | Cancella una riga da una tabella. | del /se/wan/nam/MILANO Cancella la voce per la controparte MILANO |
| do <AZIONE> (parametri) | Esegue l'AZIONE, eventualmente con i parametri indicati. | do /firmware/firmware-upload avvia lo scarico di un nuovo firmware. |
| passwd | Consente di introdurre una nuova password. A questo scopo si deve introdurre prima la vecchia password, se presente. Poi si deve introdurre la nuova password due volte di seguito confermando ogni volta con  . | |

| Questo comando ... | ... ha il seguente significato ... | ... per es.: |
|-----------------------|--|---|
| 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 seduta di configurazione. | Le lingue supportate sono attualmente Inglese (language english) Tedesco (language deutsch) |
| exit, quit, x | Si esce dalla configurazione. | |

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

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

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

Nuovo firmware con FirmSafe

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

FirmSafe funziona così

FirmSafe rende sicuro il caricamento del nuovo software: Il firmware attualmente in uso non viene semplicemente sovrascritto, viene invece memorizzato nell'apparecchio 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 il firmware upload (così si definisce il caricamento del software) esistono diverse vie:

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



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

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

ELSA LANconfig



Nel 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'aggiornamento. 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 **writelflash**. 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 ha un errore (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) rende possibile la sorveglianza e la configurazione di apparecchiature in una rete da una istanza centrale tramite un protocollo di gestione standardizzato.

Informazioni dettagliate sulla configurazione di apparecchiature ELSA con 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:

- Reti radio
- Sicurezza per la configurazione
- Gestione indirizzi automatica con DHCP

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

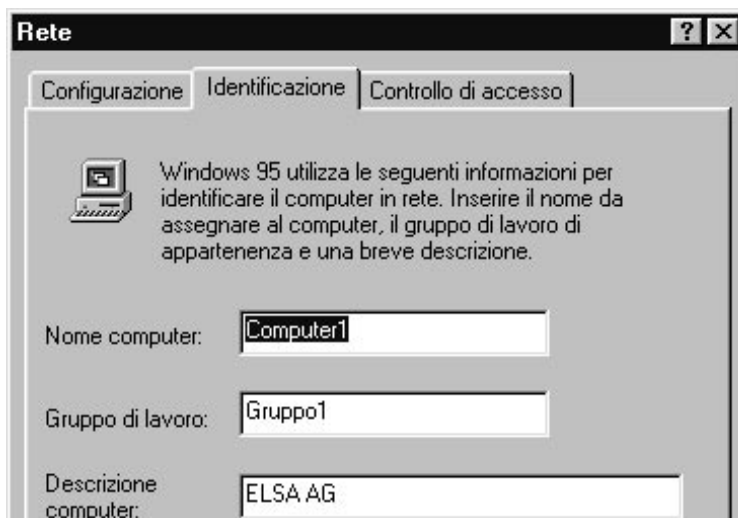
Affinché le schede di rete radio nelle stazioni mobili e nelle stazioni base si riconoscano a vicenda e possano scambiare dati, esse devono avere nei diversi parametri gli stessi valori.

Tutte le schede di rete radio (nelle 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 sì 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; ad esempio 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 gestioni di un pacchetto peggiora.

- ⑥ 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 seduta 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 ad esempio un computer prova automaticamente tutte le possibili combinazioni di lettere e numeri fino a che non ha trovato la password giusta.

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

Questi parametri valgono in modo globale per tutte le possibilità di configurazione (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 sedute di configurazione tramite Telnet o TFTP (*ELSA LANconfig*).

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

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

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

Il *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 indirizzi autonomamente dai propri indirizzi IP o Intranet.

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

Nel caso più semplice pertanto è solo necessario connettere il nuovo apparecchio nello stato di fornitura in una rete senza altri server DHCP e attivarlo. Il router 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.
- Se invece si introduce '0.0.0.0', il server DHCP determina autonomamente i rispettivi indirizzi (iniziali oppure finali) dalle impostazioni per gli indirizzi IP nel 'modulo TCP/IP'.
- Se il modem a cavo non ha alcun indirizzo IP proprio, l'apparecchiatura si trova in uno stato operativo particolare. 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 i server DNS o NBNS presenti in una LAN a cavo devono essere disponibili anche nella rete radio, è necessario allora riportare in ogni caso gli indirizzi corrispondenti. La stazione base inoltra altrimenti il proprio indirizzo IP quale server DNS o NBNS ai computer nella rete radio, ma non può rispondere alle richieste.

Assegnazione del gateway di default

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



Se un gateway presente in una LAN a cavo deve essere disponibile anche nella rete radio, è necessario allora riportare l'indirizzo IP del gateway nel modulo DHCP quale 'Indirizzo di gateway'. La stazione base inoltra altrimenti il proprio indirizzo IP quale gateway ai computer nella rete radio, ma non può rispondere alle richieste.

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 impostazione, 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

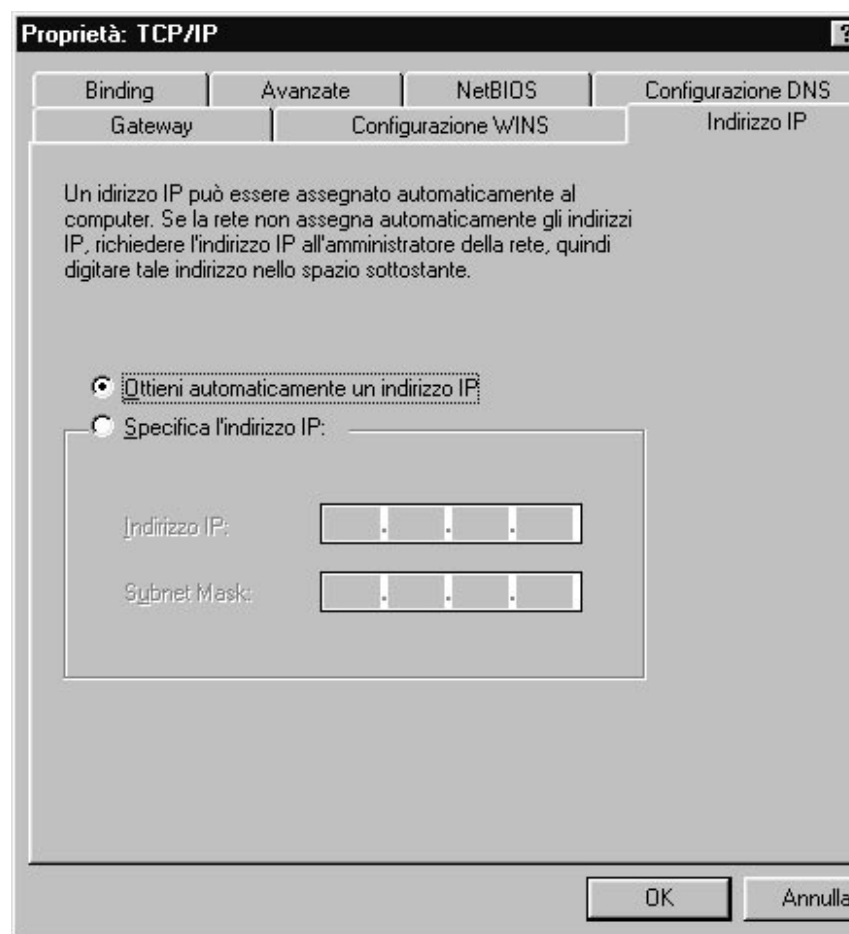
In entrambe le situazioni *ELSA LANconfig* fornisce la sua assistenza per effettuare le necessarie impostazioni:

- ① Connettere per mezzo del cavo di rete il router non configurato alla rete locale. Se si collega il apparecchio a un « hub », il commutatore node/hub si deve trovare in posizione 'Node'. Se invece si collega il router direttamente alla scheda di rete di un computer della rete, il commutatore node/hub si deve trovare in posizione 'Hub'.
- ② Accendere l'apparecchio. Il router non trova nessun altro server DHCP in rete e attiva le proprie funzioni DHCP.
- ③ Se questo non è stato già fatto, installare il protocollo 'TCP/IP' su tutti i computer della rete locale.
 - Durante l'installazione del protocollo i computer generalmente sono impostati in modo tale da richiedere automaticamente l'indirizzo IP a un server DHCP. Dopo il

riavvio, che è collegato con questa installazione, i computer richiedono automaticamente un indirizzo IP al server DHCP.

- Se il protocollo è stato già installato, attivare la funzione DHCP su tutti i computer della rete locale. A questo scopo per es. sotto Windows 95 con **Avvio ► Impostazioni ► Pannello di controllo ► Rete** aprire la finestra di configurazione delle proprietà di rete. Fare doppio clic sulla voce per il protocollo 'TCP/IP'.

Attivare l'opzione 'Ottieni un indirizzo da un server DHCP'. Passare alla scheda registro 'DNS', e cancellare tutti gli indirizzi DNS presenti. Poi cancellare sulla scheda registro 'gateway' tutte le voci eventualmente presenti e chiudere tutte le finestre con **OK**. Dopo il riavvio, che è collegato con questa impostazione, i computer richiedono automaticamente un indirizzo IP del pool di indirizzi del server DHCP.



- ④ Installare *ELSA LANconfig* su uno dei computer della rete.
- ⑤ Avviare il programma dal gruppo di programmi 'ELSAIan'. 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: in *ELSA LANconfig* nel campo di configurazione 'TCP/IP' sulla scheda di registro 'DHCP' oppure nel menu / Setup/DHCP-module).

Appendice

Dati tecnici

| | |
|-------------------------------|---|
| Banda di frequenza | 2400–2483,5 MHz (ISM) |
| Velocità di trasmissione dati | 2 mbit/s (con possibilità di passaggio a 1 Mbit/s, Automatic Rate Selection) |
| Raggio di azione | 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) |
| Sistemi operativi | Windows 95, Windows 98, Windows NT 4.0, Windows 2000, Windows CE (in preparazione) |
| Protocolli di rete | Tra WLAN e LAN vengono trasmessi protocolli di rete qualsiasi tramite bridge |
| Connessioni | 10Base-T, Power |
| Materiale fornito | Documentazione dettagliata in tedesco, inglese, francese e italiano Cavo di rete, software di configurazione |
| Servizio | Garanzia: 6 anni |
| Supporto | Tramite hotline e Internet |

Canali radio

Ognuno dei 14 canali radio impostabili per una rete radio ha grazie all'uso di DSSS una larghezza di 22 MHz. In tal modo sono possibili nella banda di frequenza ISM al massimo tra canali indipendenti. La tabella indica le frequenze centrali e mostra quali canali sono autorizzati nei vari Paesi.

| | Canale nr. | Frequenza centrale [MHz] | EU (ETSI) | Spagna | Francia |
|----------------------------|------------|--------------------------|-----------|--------|---------|
| Banda radio 1 Canale 3 | 1 | 2412 | X | | |
| | 2 | 2417 | X | | |
| | 3 | 2422 | X | | |
| | 4 | 2427 | X | | |
| | 5 | 2432 | X | | |
| Banda radio 2 Canale 8 | 6 | 2437 | X | | |
| | 7 | 2442 | X | | |
| | 8 | 2447 | X | | |
| | 9 | 2452 | X | | |
| | 10 | 2457 | X | X | X |
| Banda radio 3 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 i danni sono stati causati da un trattamento non appropriato – in particolare dalla mancata considerazione della descrizione del sistema e del manuale d'uso;
- d) se l'apparecchio è stato aperto, riparato o modificato da persone non da noi autorizzate;
- e) se l'apparecchio presenta danni meccanici di qualsiasi genere;
- f) se vengono riscontrati danni al tubo catodico di un monitor ELSA, in particolare a causa di sollecitazioni meccaniche (spostamento della maschera del tubo catodico a causa di urti o danni al vetro), forti campi magnetici in vicinanza (macchie colorate sullo schermo), visualizzazione permanente della stessa immagine (bruciatura del fosforo);
- g) se la luminanza dell'illuminazione posteriore nei pannelli TFT si riduce progressivamente nel corso del tempo;
- h) se la rivendicazione di garanzia non viene presentata secondo il punto 3a) o 3b).

5 Errori di comando

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

6 Regole supplementari

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

Dichiarazione di conformità



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

Geräteart: **Wireless LAN Access Point**

Type of Device:

Typenbezeichnung: **LANCOM Wireless L-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**

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

EN 50082-1: 1992 Teile/ parts: EN55024: 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



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

Indice

■ Numerics

| | |
|------------------------|------|
| 10Base-T | R-29 |
| 10 Mbit Ethernet | 7 |
| 802.11 | 4 |

■ A

| | |
|------------------------------------|------|
| Access-list | R-31 |
| Address pool | R-34 |
| Alimentatore | 7 |
| Antenna | 7 |
| Apple Talk | R-6 |
| ARP cache | R-32 |
| ARP-aging-minute(s) | R-32 |
| Assegnazione degli indirizzi | 13 |
| Assemblaggio | 20 |
| Auto mode | R-34 |

■ B

| | |
|------------------------------|------|
| Banda di frequenza | 20 |
| Banda di frequenza ISM | 4 |
| Blocco | 22 |
| Blocco del login | 21 |
| Boot system | R-40 |
| Bridging | 5 |
| Broadcast address | R-8 |
| Broadcast transfer | R-11 |
| Brute-Force | 21 |
| Buffers | R-29 |

■ C

| | |
|--------------------------------|------|
| Cable network | R-7 |
| Cache | R-32 |
| Canale radio | 20 |
| Caricamento del software | 16 |
| Cavo di connessione LAN | 7 |
| Cells | R-4 |
| Complesso di fornitura | 7 |
| Config-aging-minute(s) | R-36 |
| Configuration options | R-36 |
| Configurazione | 5 |
| comandi | 15 |

| | |
|----------------------------|------|
| SNMP | 18 |
| Connect | R-29 |
| Connessione LAN | 4 |
| Connettore 10 Base-T | 7 |
| Connettore Ethernet | 1 |
| Controllo in arrivo | 22 |

■ D

| | |
|---|-------------|
| Data packet | R-4 |
| Dati tecnici | 31 |
| DHCP | 5, 22, R-34 |
| DHCP server | R-34 |
| Dimensione del pacchetto | 20 |
| Direct Sequenz Spread Spectrum | 4 |
| Display di stato | 5 |
| Disturbi | 4 |
| DNS | R-31 |
| DNS forwarding | R-32 |
| DNS-backup-IP-address | R-32 |
| Dominio WLAN | 20 |
| Dynamic Host Configuration Protocol | 22 |

■ E

| | |
|------------------------|------|
| ELSA protocol | R-28 |
| End-address-pool | R-34 |
| Ethernet | 4 |
| 10Base-T | 4 |

■ F

| | |
|-----------------------|---------|
| FirmSafe | 5 |
| Firmware | 5, R-38 |
| Firmware upload | 17 |
| con LANconfig | 17 |
| con TFTP | 17 |
| Firmware-upload | R-38 |
| Frammentazione | 20 |

■ G

| | |
|--------------------------|--------|
| Gateway | 22, 25 |
| Gestione indirizzi | 22 |

■ **H**

| | |
|---------------------------------|------|
| Heap-Reserve | R-29 |
| Hierarchical IP addresses | R-9 |
| Host | R-4 |

■ **I**

| | |
|--------------------------|-----------|
| IANA | R-8 |
| Identification | R-28 |
| Inband | |
| con Telnet | 14 |
| Presupposti | 13 |
| Indirizzi IP | 5 |
| Indirizzo finale | 24 |
| Indirizzo iniziale | 24 |
| Indirizzo IP | 10, 13 |
| Installazione | 4 |
| Interface | R-4 |
| Internet | R-6 |
| Internetwork | R-6 |
| Intranet | R-30 |
| IP address | R-7, R-30 |
| IP network | R-6 |
| IPX | R-6 |
| ISDN network | R-7 |
| ISDN time | R-19 |

■ **L**

| | |
|---------------------------|-----------------------|
| LAN | 1, R-6, R-11 |
| LANconfig | 5, 10, 13, 14, 17, 19 |
| LAN-configuration | R-36 |
| Language | R-37 |
| Larghezza di banda | 4 |
| LED | 8 |
| LAN-Collision | 9 |
| LAN-Status | 9 |
| Power/Msg | 8 |
| Lista di accessi IP | 13 |
| Local Area Network | 1, R-6 |
| local network | R-6 |
| location | R-29 |
| Lock-minutes | R-37 |
| Login | 16 |
| log-in block | R-37 |
| Login-errors | R-37 |

■ **M**

| | |
|--------------------------------|------------|
| MAC | R-11 |
| MAC address | R-12, R-29 |
| MAC protocol | R-12 |
| Medium | R-4 |
| Medium Access Control | R-11 |
| Memoria flash ROM | 5, 16 |
| Metodo DSSS | 4, 20 |
| Modalità | 19 |
| Modo automatico | 23 |
| Modo automatico DHCP | 23 |
| Multipoint cabling | R-11 |
| Multiprotocol capability | R-12 |

■ **N**

| | |
|---------------------------|------|
| Name | R-28 |
| name server | R-31 |
| NBNS | R-32 |
| NBNS-backup | R-32 |
| NetBIOS name server | R-32 |
| Network | R-4 |
| Network adapter | R-4 |
| Network address | R-7 |
| Network cable | R-4 |
| network connection | R-29 |
| Network mask | R-7 |
| Network protocol | R-6 |
| Node-ID | R-29 |

■ **O**

| | |
|-----------------|------|
| Operating | R-30 |
| Other | R-40 |

■ **P**

| | |
|--------------------------------------|--------|
| Packet | R-4 |
| Password | 20 |
| password | R-31 |
| Password-required | R-36 |
| Periodo di validità | 23, 25 |
| physical medium | R-4 |
| Point-to-multipoint connection | R-5 |
| point-to-point connection | R-4 |
| Pool di indirizzi | 24, 29 |
| Private address spaces | R-8 |

Protezione con password 21
 Protocol R-6

R

Radiocellula 1
 Raggio di azione 3, 4
 registered IP address R-8
 Reset system R-40
 Rete ad-hoc 2
 Rete infrastruttura 3
 Rete Peer-to-LAN 3
 Rete peer-to-peer 2
 Rete radio 1, 19
 Router R-4
 Routing R-9
 Routing table R-9

S

Scalabilità 3
 Scheda di rete radio 1, 4, 7
 Scheda per PC 7
 Schermatura 4
 Server DHCP 5, 10, 13, 23
 Configurazione 27
 Server DNS 22, 25
 Server NBNS 22, 25
 Servizi online 13
 Setup
 DHCP-module R-34
 LAN-module R-29
 TCP-IP-module R-30
 Shared Medium R-11
 Shared medium R-6
 Sicurezza 21
 SNMP 18, R-33
 Software-Update 5
 Spie LED 5
 Standard IEEE 802.11 4
 Start-address-pool R-34
 Stato al momento della fornitura 9
 Status R-19
 Call-info-table R-27

Config-statistics R-26
 Delete values R-28
 LAN-statistics R-21
 operating time R-19
 Queue-statistics R-26
 TCP-IP-statistics R-22
 WAN-statistics R-20
 Stazione base 1, 7
 Subnet R-9
 System-administrator R-33
 System-location R-33

T

Table-ARP R-32
 Tasto di reset 9
 TCP max. connections R-32
 TCP/IP 10, 13, R-6
 TCP/IP stack R-6
 TCP-aging-minute(s) R-32
 Telnet 5, 12
 Telnet server R-31
 Tentativi di login 21
 TFTP 13
 TFTP server R-31
 Time R-19
 Timeout R-35
 Trap-IP R-33
 Traps-active R-33

U

Upload 5, 16
 Upload-system R-40

V

Version-table R-39

W

WAN-configuration R-36
 winipcfg 11
 wire R-4
 Wireless LAN 1
 Wireless links R-4
 WLAN 1, 19

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 networks in accordance with the IEEE 802.11 standard

The units of the *ELSA LANCOM Wireless* series comply with the IEEE 802.11 standard. This standard is a supplement of the existing IEEE standards for LANs, of which IEEE 802.3 for Ethernet is the best 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 32 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 a base station, also known as an access point or distribution system. The *ELSA LANCOM Wireless* units were designed to serve as base stations. The base station 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 base station, and each station entering the network must log onto the base station before being permitted to exchange data in the cell. The base station generally also fulfills the function of a 'relay station' for data. While this reduces the achievable data rate, careful positioning of the base station can increase the size of a cell. The actual role of a base station, however, is the connection of a wireless cell to a wired Ethernet. If the base station receives a data packet for a workstation that is not logged onto it, it forwards the packet to the Ethernet. In the other direction, the base station "listens" to the Ethernet for data intended for wireless stations and forwards it accordingly. As all mobile stations must log onto the base station, the base station

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.

As mentioned earlier, an Ethernet backbone can also be used to extend the range of a wireless LAN. In this case, multiple base stations 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 base station with the strongest signal. Two mobile stations logged onto different base stations can thus communicate with one another even though they are not within direct radio range. The Ethernet linking the base stations closes the gap.

If a station continues to monitor the radio situation after logging on, it can determine the relative signal strengths of the base stations and automatically switch over to the strongest base station 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 802.11 devices from other manufacturers. However, as the 802.11 standard is relatively new and many manufacturers are only just making the transition from proprietary wireless LAN solutions to 802.11, interoperability cannot be guaranteed at all times. 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.

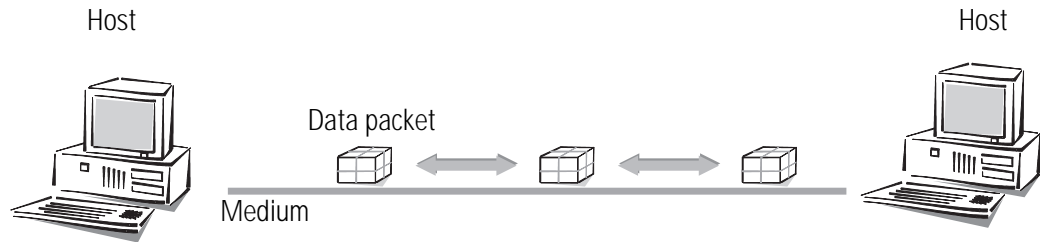
Router

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.

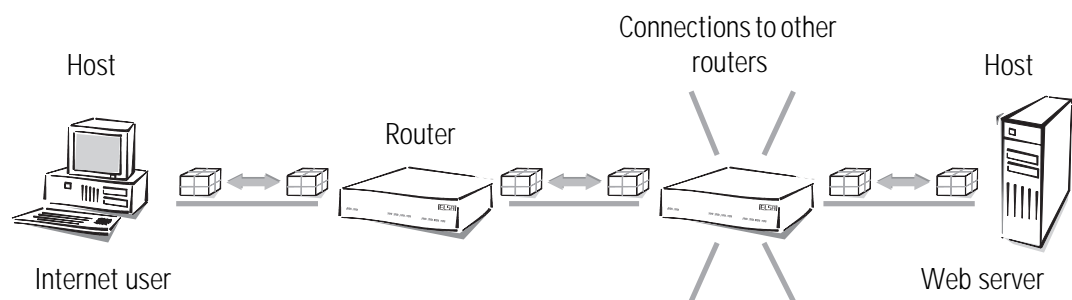
Connection modes

*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).



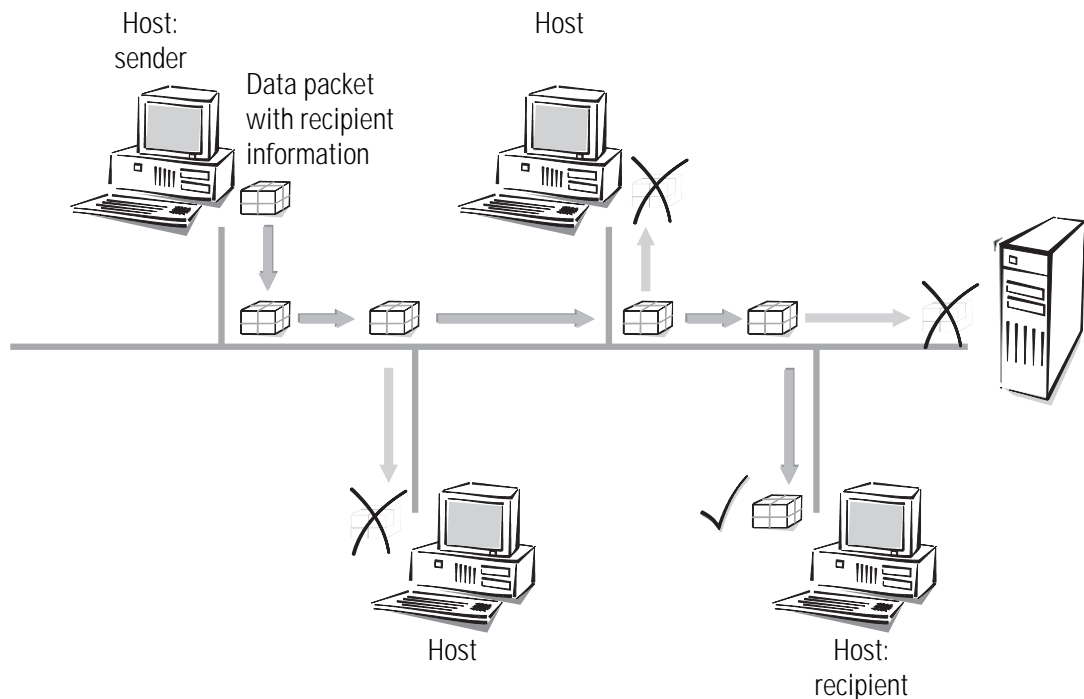
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers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



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

Point-to-multipoint connection

Generally speaking, it would be uneconomical to directly connect all computers in a network via point-to-point 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 $254 \times 254 = 64.516$ 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

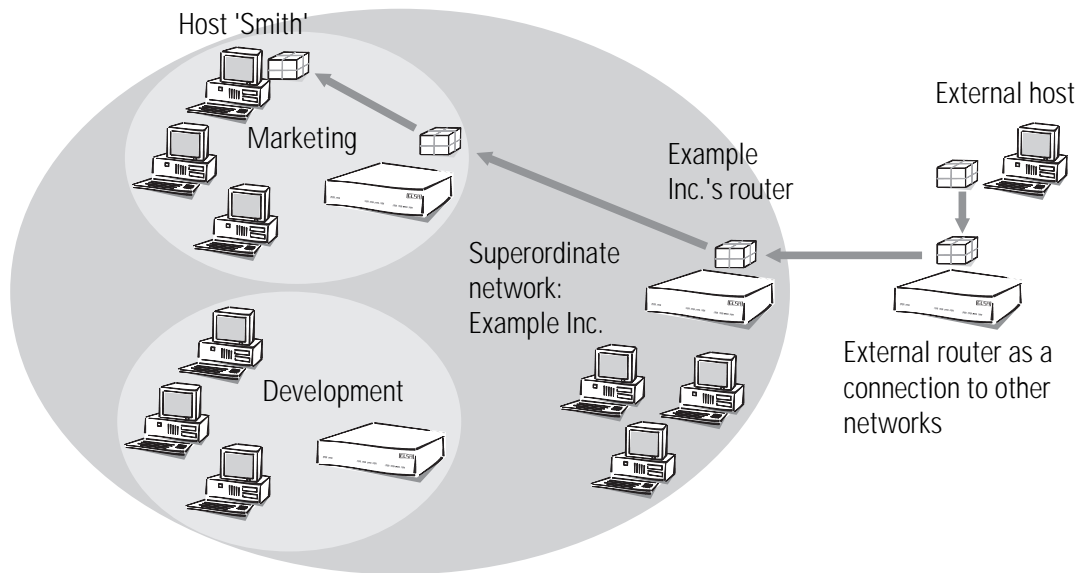
Routing-method Every IP packet contains the IP addresses of the source and of the recipient. A router receives IP packets at its interface, interprets the destination address and passes the packets on to those interfaces that are nearest to the recipient. Finding the appropriate path is called routing.

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 (**M**edia **A**ccess **C**ontrol, MAC) for the avoidance and resolution of such collisions.

LAN and IP network

The connection of all computers communicating through a shared medium using a MAC protocol is called a LAN (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. LAN refers to a limitation of the area covered by the network, not a restriction of the number of workstations connected to it.

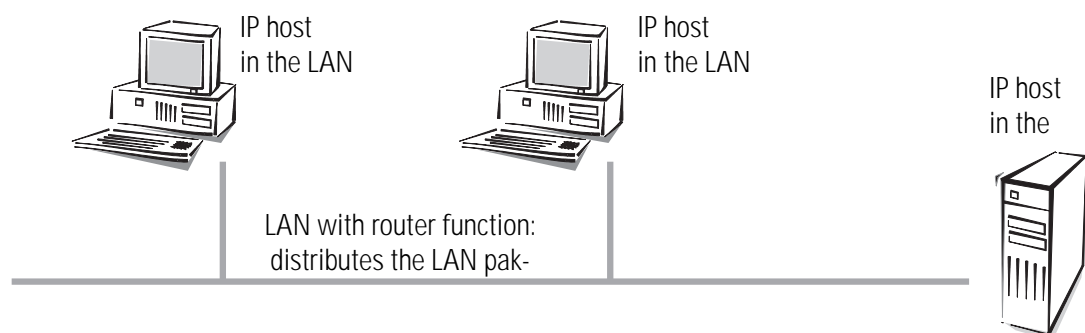
MAC-address Specific LAN addresses hardwired into the interfaces by their manufacturers are used to manage the transfer in the LAN. Since the LAN addresses are used for communication via the MAC protocol, they are called MAC addresses. They can be thought of as the fingerprint of the interface hardware. MAC addresses can look like this, for example: 00-80-C7-6D-A4-6E.

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

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

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

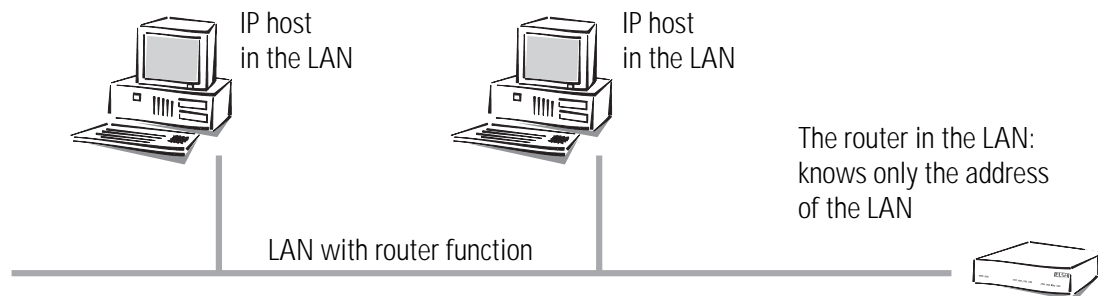
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts gives the packets to the LAN which handles the further distribution of the data packet. This is why only IP addresses from the numerical space of the specific network should be used for the internal communication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

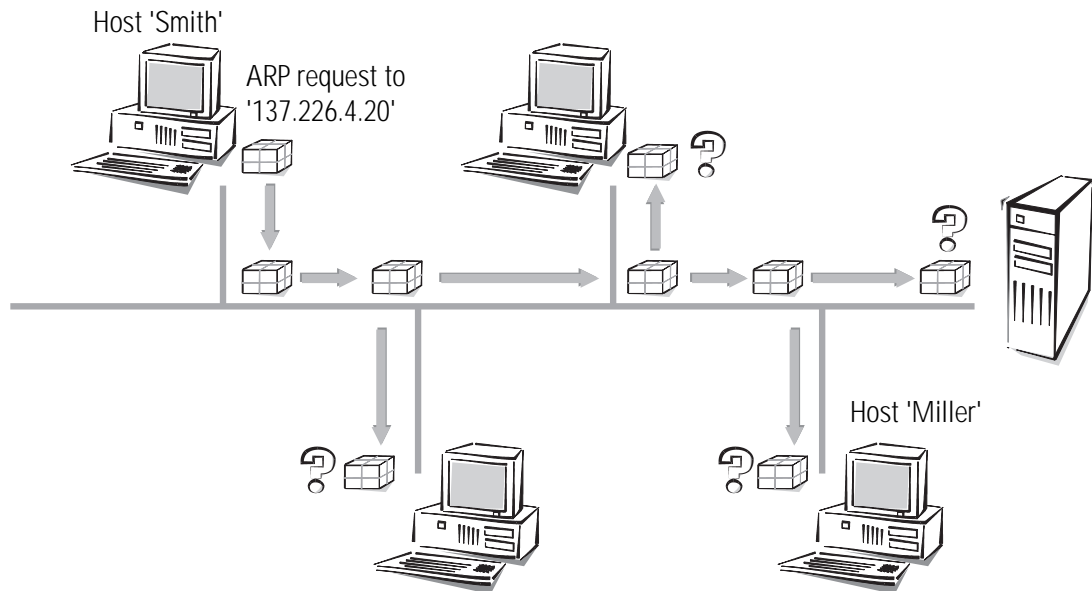
Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). Using the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located 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.

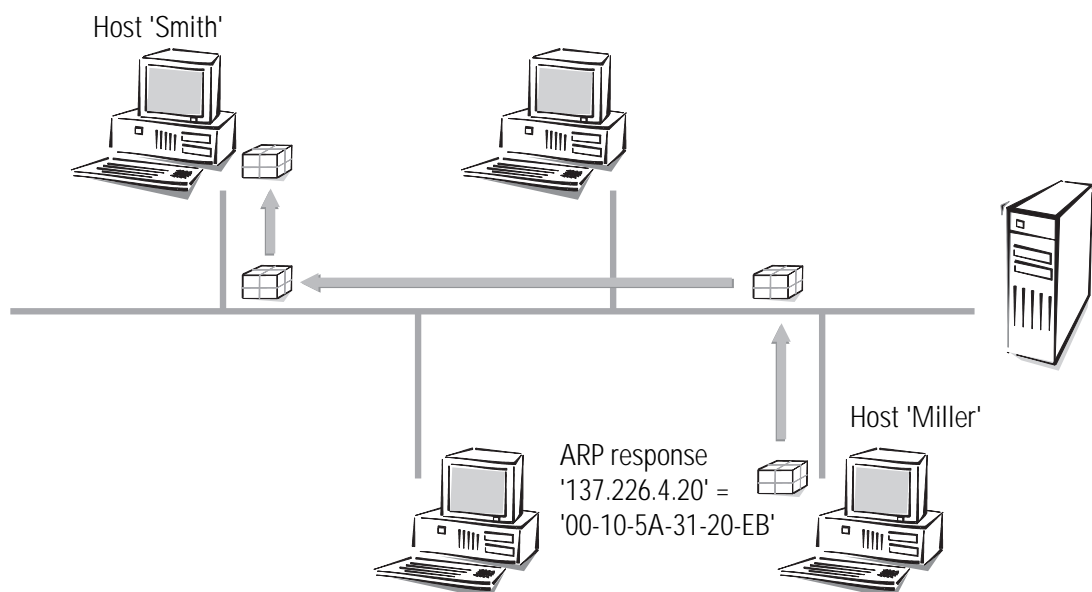
ARP

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, feels addressed and answers with an ARP response packet that it sends directly to host 'Smith'. The MAC address '00-10-5A-31-20-DF' of host 'Smith' is extracted from the sender field in the ARP request packet. Host 'Smith' recognizes this as an answer to its request, extracts the MAC address '00-10-5A-31-20-EB' from the ARP response packet and enters it into 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 hosts 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.































All channel-related statistics and menus in this documentation refer to two channels only, even if more than two channels are available to the specific devices. Interface-related information is also provided for a single interface only. The information is equally applicable to the additional channels and interfaces.



Symbols

| | | |
|---|------------|---|
|  | Menu | Indicates a further submenu. |
|  | Info | Indicates a value that cannot be modified. |
|  | Value | Indicates a value that can be modified. |
|  | Table | Indicates a table whose entries can be modified. |
|  | Info table | Indicates a table whose entries cannot be modified. |
|  | Action | Performs an action. |

Overview of the menus








| | | | |
|---|-------------------|---|-------------------|
|  | Setup |  | Status |
|  | Name |  | Current-time |
|  | LAN-module |  | Operating-time |
|  | TCP-IP-module |  | WLAN-statistics |
|  | SNMP-module |  | LAN-statistics |
|  | DHCP-module |  | TCP-IP-statistics |
|  | Config-module |  | Config-statistics |
|  | WLAN-module |  | Queue-statistics |
|  | Firmware |  | PCMCIA-status |
|  | Version-table |  | Delete-values |
|  | Table-firmsafe |  | Other |
|  | Mode-firmsafe |  | Manual-dialing |
|  | Timeout-firmesafe |  | Reset-system |
|  | Firmware-upload |  | Boot-system |
|  | Test-firmware |  | 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 |
|-------------------|---|--|
| Current-time |  | Current time in device |
| Operating-time |  | Period of time the device has operated since it was last switched on |
| LAN-statistics |  | Displays LAN statistics |
| TCP-IP-statistics |  | Statistics from the TCP/IP area |
| Config-statistics |  | Remote configuration statistics |
| Queue-statistics |  | Statistics relating to the packets in the queues of the individual modules |
| Delete-values |  | Deletes all values except tables with substatistics. |

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/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-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 base station |
| 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. |

Station table

















This table displays information on the individual mobile stations:







| | |
|------------|--|
| 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. |
| State | 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. |

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. |
| Negotiation-complete |  | The negotiation of the transfer mode between the router and the remote station is complete. This is only relevant if Setup/LAN/Connection is set to 'Auto'. |
| Connect |  | The preselected LAN connection is fixed at 10Base-T. See Setup/LAN-/connection. |
| LAN-rx-bytes |  | Number of bytes received from the LAN |
| LAN-tx-bytes |  | Number of bytes sent to the LAN |
| LAN-rx-broadcasts |  | Number of broadcast packets received from the LAN |

| /LAN-statistics | Running status displays | |
|-------------------|---|--|
| 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/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 |
| DCHP-statistics |  | Statistics from the DCHP 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-service-errors | Number of IP packets received from the LAN for an incorrect service |
| IP-WAN-rx | Number of IP packets received from the WAN |
| IP-WAN-tx | Number of IP packets sent to the WAN |
| IP-WAN-checksum-errors | Number of IP packets incorrectly received from the WAN |
| IP-WAN-service-errors | Number of IP packets received from the WAN for an incorrect service |
| IP-WAN-rx-disconnect | Number of packets from the WAN discarded by timeout |
| Delete-values | Deletes IP statistics |

Status/TCP-IP-statistics/ICMP-statistics

These statistics include the following values:

| | |
|--------------------------|--|
| ICMP-LAN-rx | Number of ICMP packets received from the LAN |
| ICMP-LAN-tx | Number of ICMP packets sent to the LAN |
| ICMP-LAN-checksum-errors | Number of ICMP packets incorrectly received from the LAN |
| ICMP-LAN-service-errors | Number of non-supported ICMP packets received from the LAN |
| ICMP-WAN-rx | Number of ICMP packets received from the WAN |
| ICMP-WAN-tx | Number of ICMP packets sent to the WAN |
| ICMP-WAN-checksum-errors | Number of ICMP packets incorrectly received from the WAN |
| ICMP-WAN-service-errors | Number of non-supported ICMP packets received from the WAN |
| Delete-values | Deletes ICMP statistics |

Status/TCP-IP-statistics/TCP-statistics

These statistics include the following values:

| | |
|-------------------------|---|
| TCP-LAN-rx | Number of TCP packets received from the LAN |
| TCP-LAN-tx | Number of TCP packets sent to the LAN |
| TCP-LAN-tx-repeats | Number of TCP packets repeatedly sent to the LAN |
| TCP-LAN-checksum-errors | Number of TCP packets incorrectly received from the LAN |
| TCP-LAN-service-errors | Number of TCP packets received from the LAN for an incorrect port |
| TCP-LAN-connections | Current number of TCP connections from the LAN |
| TCP-WAN-rx | Number of TCP packets received from the WAN |
| TCP-WAN-tx | Number of TCP packets sent to the WAN |
| TCP-WAN-tx-repeats | Number of TCP packets repeatedly sent to the WAN |
| TCP-WAN-checksum-errors | Number of TCP packets incorrectly received from the WAN |
| TCP-WAN-service-errors | Number of TCP packets received from the WAN for an incorrect port |
| TCP-WAN-connections | Current number of TCP connections from the WAN |
| Delete-values | Deletes TCP statistics |

Status/TCP-IP-statistics/TFTP-statistics

These statistics include the following values:

| | |
|---------------------------|--|
| TFTP-LAN-rx | Number of TFTP packets received from the LAN |
| TFTP-LAN-rx-read-request | Number of TFTP read requests received from the LAN |
| TFTP-LAN-rx-write-request | Number of TFTP write requests received from the LAN |
| TFTP-LAN-rx-data | Number of TFTP data packets received from the LAN |
| TFTP-LAN-rx-ack. | Number of TFTP acknowledges received from the LAN |
| TFTP-LAN-rx-option-ack. | Number of TFTP option acknowledges received from the LAN |
| TFTP-LAN-rx-errors | Number of TFTP error packets received from the LAN |
| TFTP-LAN-rx-bad-packets | Number of unknown TFTP packets received from the LAN |
| TFTP-LAN-tx | Number of TFTP packets sent to the LAN |
| TFTP-LAN-tx-data | Number of TFTP data packets sent to the LAN |
| TFTP-LAN-tx-ack. | Number of TFTP acknowledges sent to the LAN |
| TFTP-LAN-tx-option-ack. | Number of TFTP option acknowledges sent to the LAN |
| TFTP-LAN-tx-errors | Number of TFTP error packets sent to the LAN |
| TFTP-LAN-tx-repeats | Number of TFTP packets repeatedly sent to the LAN |
| TFTP-LAN-connections | Number of TFTP connections established to the LAN |
| TFTP-WAN-rx | Number of TFTP packets received from the WAN |
| TFTP-WAN-rx-read-request | Number of TFTP read requests received from the WAN |

| | |
|---------------------------|--|
| TFTP-WAN-rx-write-request | Number of TFTP write requests received from the WAN |
| TFTP-WAN-rx-data | Number of TFTP data packets received from the WAN |
| TFTP-WAN-rx-ack. | Number of TFTP acknowledges received from the WAN |
| TFTP-WAN-rx-option-ack. | Number of TFTP option acknowledges received from the WAN |
| TFTP-WAN-rx-errors | Number of TFTP error packets received from the WAN |
| TFTP-WAN-rx-bad-packets | Number of unknown TFTP packets received from the WAN |
| TFTP-WAN-tx | Number of TFTP packets sent to the WAN |
| TFTP-WAN-tx-data | Number of TFTP data packets sent to the WAN |
| TFTP-WAN-tx-ack. | Number of TFTP acknowledges sent to the WAN |
| TFTP-WAN-tx-option-ack. | Number of TFTP option acknowledges sent to the WAN |
| TFTP-WAN-tx-errors | Number of TFTP error packets sent to the WAN |
| TFTP-WAN-tx-repeats | Number of TFTP packets repeatedly sent to the WAN |
| TFTP-WAN-connections | Number of TFTP connections established to the WAN |
| Delete-values | Deletes TFTP statistics |

Status/TCP-IP-statistics/DHCP-statistics

These statistics include the following values:

| | |
|--------------------|--|
| DHCP-LAN-rx | Number of DHCP packets received from the LAN |
| DHCP-LAN-tx | Number of DHCP packets sent to the LAN |
| DHCP-WAN-rx | Number of DHCP packets received from the LAN |
| DHCP-discard | Number of DHCP packets discarded |
| DHCP-rx-discover | Number of discover messages received |
| DHCP-rx-request | Number of request messages received |
| DHCP-rx-decline | Number of decline messages received |
| DHCP-rx-inform | Number of inform messages received |
| DHCP-rx-release | Number of release messages received |
| DHCP-tx-offer | Number of offer messages sent |
| DHCP-tx-ack. | Number of DHCP packets acknowledged |
| DHCP-tx-nak. | Number of DHCP packets not acknowledged |
| DCHP-server-err. | Number of DHCP packets received that were not intended for this server |
| DHCP-assigned | Number of addresses currently assigned |
| DHCP-MAC-conflicts | Number of assignments rejected because IP addresses were in use |
| Table-DHCP | Table containing assignments of IP addresses to MAC addresses |
| Delete-values | Deletes DHCP statistics. |












Table-DHCP

There are entries with DHCP information in the **DHCP table**. It contains 16 entries (or multiples of 16). The table adapts dynamically to the given requirements and grows or shrinks accordingly. It has the following layout:

| IP-address | Node ID | Timeout | Hostname | Type |
|------------------------------|------------------------|--|---------------|-----------------|
| IP address assigned via DHCP | Associated MAC address | Duration of assignment validity in minutes | Computer name | Assignment type |




Status/Config-statistics




















This menu allows you to display the statistics from the remote configuration area. It allows you to retrieve information on the number of past and present configuration sessions at any time. Encryption is performed by LAN, WAN and outband port.

| /Config-statistics | Remote configuration statistics | |
|----------------------------|---|---|
| LAN-active-connections |  | Current number of active configuration connections from the LAN |
| LAN-total-connections |  | Total number of configuration connections from the LAN up until the present |
| WAN-active-connections |  | Current number of active configuration connections from the WAN |
| WAN-total-connections |  | Total number of configuration connections from the WAN up until the present |
| Outband-active-connections |  | Current number of active outband configuration connections |
| Outband-total-connections |  | Total number of previous outband configuration connections up until the present |
| Outband-bitrate |  | Bit rate of the last outband configuration session |
| Login-errors |  | Total number of defective logins |
| Login-locks |  | Number of login locks |
| Login-rejects |  | Number of login attempts while the login lock was active |
| Delete-values |  | Deletes the config statistics |

Status/Queue-statistics




These statistics allow you to observe the flow of the individual packets through the various modules of the *ELSA LANCOM*.

| /Queue-statistics | Statistics on the queue | |
|-------------------|---|-----------------------------|
| LAN-heap-packets |  | Number of buffers available |
| LAN-queue-packets |  | Number of buffers in use |
| WAN-heap-packets |  | Number of buffers available |

| /Queue-statistics | | Statistics on the queue |
|-------------------------------|---|--|
| WAN-queue-packets |  | Number of buffers in use |
| Bridge-internal-queue-packets |  | Number of bridge packets from the LAN |
| Bridge-external-queue-packets |  | Number of bridge packets from the WAN |
| ARP-query-queue-packets |  | Number of ARP packets in the query queue |
| ARP-queue-packets |  | Number of ARP packets in the normal queue |
| IP-queue-packets |  | Number of IP packets in the normal queue |
| 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. |
| IP-Masq.-Tx-queue-packets |  | Number of packets to be sent masked (to the Internet). |
| IP-Masq.-Rx-queue-packets |  | Number of packets received from the Internet and have to be demasked. |

Status/PCMCIA-status

General information on the inserted card can be found here:

| | | |
|---------------------|---|--|
| LAN 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 |
| LAN-module |  | LAN settings |
| TCP-IP-module |  | TCP/IP module settings |
| SNMP-module |  | Settings for configuration via SNMP |
| DHCP-module |  | DHCP server settings |
| WLAN-module |  | Wireless network settings |
| Config-module |  | Configuration module settings |

Name

Here you can enter the device name (maximum 16 characters). The set of characters available includes uppercase and lowercase letters as well as some special characters. You can display the full range of available characters during a configuration session by entering the following command:

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

In the default configuration, no name is entered.

The device name is required for identification purposes; it is a prerequisite for any connection via the IPX or IP router module, since the routers can exchange data only with known remote stations, and is also required for the unambiguous identification of a remote bridge station.




In the case of PPP connections, either the user name with the password from the PPP list or the device name is transferred to the remote station as a device ID during a verification by PAP or CHAP.

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/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 |

Connect

This option allows you to select from among the following network connections:

| Connect | Meaning |
|---------|---|
| Auto | Default setting, as the LAN connection is fixed at 10Base-T. This item does not require manual configuration. |
| 10B-T | 10BASE-T |



When making settings for the fast-Ethernet operation, please note that the selected transfer mode must also support the additional terminals.

When the system is switched off and on again, the last port to be selected remains activated.

Node-ID















This option allows you to display the router's own Ethernet address. The value displayed here was set at the factory and cannot be changed. The Ethernet address is displayed as a 12-digit hexadecimal value, with the first six digits '00a057' standing for an ELSA device.

Spare-heap

The spare heap blocks for the local network affect the number of buffers that are always available for receiving frames from the local network. The default value is 10, which ensures that, e.g., four Telnet sessions can be activated via the local network at any time.

Setup/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 <i>ELSA LANCOM</i> |

Operating

The TCP/IP module of the router may be activated or deactivated here. In the default configuration, the TCP/IP module is activated.

Configuration via TCP/IP using Telnet and the IP router is possible only if the TCP/IP module is activated.

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).



Access-list

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).

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.

DNSDNS-
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/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 |
| 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/Config-module

This menu allows you to enter settings for router configuration options. The menu has the following layout:

| /Config-module | Configuration module settings | |
|------------------------|---|--|
| LAN-config |  | Switch for configuring from the LAN side |
| WAN-config |  | Switch for configuring from the WAN side |
| Password-required |  | Password required on/off if there is no password |
| Farconfig-(EAS-MSN) |  | Subscriber number for remote configuration via PPP |
| 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-(EAS-MSN) This subscriber number permits remote configuration via PPP. If no number is specified here, remote-configuration calls will be accepted on all numbers.

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/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. The default setting is 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. |

| | | |
|-------------|---|--|
| Access-list |  | <p>This list can be used to explicitly exclude WLAN stations from data communications with the LAN/base port. Alternatively, authorized stations can be specified.</p> <p>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.</p> <p><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></p> |
|-------------|---|--|

| | | |
|-------------|---|--|
| Access-mode |  | <p>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.</p> |
|-------------|---|--|

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-firmesafe |  | Time in minutes required to test new firmware |
| Test-firmware |  | Tests the inactive firmware |
| Firmware-upload |  | Initiates a firmware upload |

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

| Ifc | Module | Version | Serial number |
|-----|----------------------|------------------------|---------------|
| Ifc | LANCOM Business 4100 | 1.60.0012 / 30.06.1999 | 8427.000.020 |

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

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

Enter the following command to activate an inactive firmware version:

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




Mode-firmsafe Only one of the firmware versions stored in the device can be active at any one time. When new firmware is loaded the inactive firmware is overwritten. You can decide which firmware will be activated after the upload:

- 'immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
 - The new firmware is successfully loaded and then operates as desired. Everything is then in order.
 - However, if the new firmware does not operate correctly, it may not be possible to communicate with the device after the restart. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- 'login': To prevent problems caused by defective firmware, the second option will load the firmware and start it immediately.
 - In contrast to the first option, the firmsafe will wait until it has successfully logged on over outband or inband (by telnet). 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 |
|---------------|---|-----------------------------|
| 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.

TCP/IP Ports

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

| Capab. | Port no. | Protocol |
|------------|----------|----------|
| www | 80 | udp |
| link | 87 | tcp |
| supdup | 95 | tcp |
| hostnames | 101 | tcp |
| iso-tsap | 102 | tcp |
| dictionary | 103 | tcp |
| X400 | 103 | tcp |
| x400-snd | 104 | tcp |
| csnet-ns | 105 | tcp |
| pop | 109 | tcp |
| pop2 | 109 | tcp |
| pop3 | 110 | tcp |
| portmap | 111 | tcp |
| portmap | 111 | udp |
| sunrpc | 111 | tcp |
| sunrpc | 111 | udp |
| auth | 113 | tcp |
| sftp | 115 | tcp |
| path | 117 | tcp |
| uucp-path | 117 | tcp |
| nntp | 119 | tcp |
| ntp | 123 | udp |
| nbname | 137 | udp |
| nbdatagram | 138 | udp |
| nbssession | 139 | tcp |
| NeWS | 144 | tcp |
| sgmp | 153 | udp |
| tcprepo | 158 | tcp |
| snmp | 161 | udp |
| snmp-trap | 162 | udp |
| print-srv | 170 | tcp |
| vmnet | 175 | tcp |
| load | 315 | udp |
| vmnet0 | 400 | tcp |

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

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

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

