

ELSA LANCOM™ Wireless L-2

Manuel de l'utilisateur

© 1999 ELSA AG, Aachen (Germany)

Toutes les informations dans ce manuel ont été rédigées après une vérification soigneuse, mais ne peuvent néanmoins garantir les caractéristiques du produit. ELSA engage sa responsabilité exclusivement dans les limites stipulées dans les conditions de vente et de livraison.

La transmission et la reproduction de la documentation et des logiciels faisant partie de ce produit, ainsi que l'exploitation de leur contenu et des logiciels faisant partie du produit sont interdites sans l'autorisation écrite d'ELSA. ELSA se réserve le droit d'effectuer des modifications à des fins d'améliorations techniques.

Marques

Windows®, Windows NT® et Microsoft® sont des marques déposées de Microsoft, Corp.

Tous les autres noms et toutes les désignations utilisés peuvent être des marques ou des marques déposées de leur propriétaire respectif. Le logo ELSA est une marque déposée d'ELSA AG.

ELSA se réserve le droit de modifier les données mentionnées sans préavis et n'accepte aucune responsabilité pour des inexactitudes et/ou manques techniques.

ELSA AG

Sonnenweg 11

52070 Aachen

Allemagne

www.elsa.com

Aachen, septembre 1999

Avant-propos

Merci de votre confiance !

Les réseaux radio de ELSA représentent une alternative bon marché ou un complément pour les réseaux locaux câblés (LAN). Les cartes réseau mobiles permettent aux notebooks et aux PC de communiquer entre-eux ou d'obtenir via une station de base un accès aux réseaux câblés et même au réseau RNIS.

Cette documentation s'adresse aux utilisateurs de la station de base *ELSA LANCOM Wireless L-2*. Nous vous présentons d'abord l'appareil et ses possibilités, nous vous aidons pour le branchement et l'installation du logiciel et nous vous montrons quelques exemples d'application.

Documentation

La documentation jointe comprend :

- Manuel de l'utilisateur
Installation du matériel, description des fonctions et modes de service, premiers exemples de configuration.
- Documentation électronique sur CD
Tous les manuels de la gamme de produits, informations techniques fondamentales (p.ex. les réseaux radio, la technique générale des réseaux, TCP/IP etc.), Workshop avec exemples d'application détaillés, ouvrage de référence contenant la description complète des menus.

Cette documentation a été rédigée par une équipe de collaborateurs de différents services de l'entreprise afin de vous offrir la meilleure assistance possible lors de l'exploitation de votre produit ELSA.

Si vous deviez trouver une erreur, ou si vous désirez exprimer une critique ou une suggestion concernant la documentation, envoyez-nous directement une e-mail à l'adresse suivante:

Lancom.doku@elsa.de



Si vous aviez encore des questions sur les thèmes abordés dans ce manuel ou si vous aviez besoin d'assistance, nos services en ligne (serveur Internet - www.elsa.com) sont à votre disposition 24 heures sur 24. Vous y trouverez entre autres la réponse aux questions les plus fréquentes dans la partie « support technique », ainsi qu'une foule d'informations dans la base de données de connaissances (KnowledgeBase). Les pilotes les plus récents, les microprogrammes, des utilitaires et les manuels peuvent être téléchargés.

KnowledgeBase se trouve également sur le CD. Pour cela, lancez le fichier `IMisc\Support\MISC\ELSASIDE\index.htm`

Contenu

Introduction	1
En France : uniquement avec une autorisation !	1
Principe de fonctionnement d'un réseau local sans fil	2
Avantages de <i>ELSA LANCOM Wireless L-2</i>	4
Installation	7
Contenu du coffret	7
<i>ELSA LANCOM Wireless</i> se présente	7
Comment brancher la station de base.....	9
Installation du logiciel	10
Configuration de base.....	10
Réglages de base avec <i>ELSA LANconfig</i>	10
Réglages de base avec Telnet	12
Configurations possibles	13
Radio ou câble: Chemins aboutissant à la configuration.....	13
Conditions	13
Alternative : Gestion des adresses à l'aide du serveur DHCP.....	14
Lancement de la configuration par <i>ELSA LANconfig</i>	14
Lancement de la configuration par Telnet.....	15
Instructions de configuration.....	15
Nouveau micrologiciel avec FirmSafe	16
Comment fonctionne FirmSafe ?.....	16
Comment charger le nouveau logiciel ?.....	17
Configuration par SNMP.....	18
Fonctions et modes d'exploitation	21
Paramètres de la transmission radio	21
La sécurité de votre configuration	23
Protection par mot de passe	23
Le verrouillage des accès.....	23
Contrôle des accès via TCP/IP	24
Gestion d'adresses automatique via DHCP	24
Le serveur DHCP.....	25
DHCP – 'actif', 'inactif' ou 'auto' ?	25
Attribution des adresses.....	26
Configuration du serveur DHCP	29
Appendice	33
Caractéristiques techniques	33
Canaux radio	33
Conditions générales de garantie du 01.06.1998.....	34

Déclaration de conformité	37
Index	41
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
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
TCP/IP Ports	R-41

Introduction

Les avantages des réseaux sans fil sont évidents : les PC et les notebooks peuvent être installés là où ils sont requis – les problèmes dus aux points d'accès manquants ou aux modifications des locaux appartiennent au passé grâce aux réseaux sans fil.

La connexion au réseau pendant les conférences ou les présentations, l'accès aux ressources installées dans les bâtiments voisins, l'échange de données avec les PC mobiles sont quelques exemples d'application dans un réseau sans fil.

Le rôle central dans un réseau filaire existant est tenu par la station de base. Toutes les stations du réseau sans fil ont accès au réseau local via la station de base.

Dans certains pays européens, l'utilisation des fréquences radio dans la plage comprise entre 2,4 et 2,48 GHz est limitée en raison des réglementations nationales ou possible uniquement après en avoir fait la demande. La liste des agréments nationaux est fournie dans un document séparé.

En France : uniquement avec une autorisation !



En France, l'exploitation de réseaux sans fil (ondes radio) requiert l'autorisation préalable des autorités publiques. Veillez aux particularités suivantes avant d'installer un réseau local sans fil en France.

Les formulaires et les informations sur l'attribution de la licence d'exploitation sont disponibles dans l'Internet à

<http://www.art-telecom.fr/licences/index-d.htm>

ou sur le CD-ROM *ELSA LANCOM Wireless* dans le répertoire \misc\support\www_art.

- Les utilisateurs habitant dans certaines zones ont juste besoin d'imprimer et de remplir le formulaire et de l'envoyer à l'adresse indiquée. Si les autorités publiques ne manifestent pas leur désaccord dans un délai d'un mois, la licence d'exploitation est réputée accordée (tacitement). Lisez les informations détaillées sur le site Web indiqué.
- Les utilisateurs habitant en-dehors des zones indiquées en France et souhaitant exploiter un réseau sans fil ont besoin d'une licence d'exploitation fournie par le Ministère de la défense. Les démarches d'obtention de l'autorisation sont également décrites sur le site Web.



En France, l'exploitation d'un réseau local sans fil dans la plage des 2.4 GHz est limité aux fréquences 2446,5 MHz – 2483,5 MHz, ce qui correspond aux canaux 8 – 13.

Principe de fonctionnement d'un réseau local sans fil

Ce chapitre vous montre le principe de fonctionnement d'un réseau sans fil. Il explique brièvement les termes utilisés et présente l'organisation et les possibilités d'application. Vous trouverez les informations techniques détaillées dans la documentation électronique sur le CD-ROM.

Cartes réseau sans fil WLAN

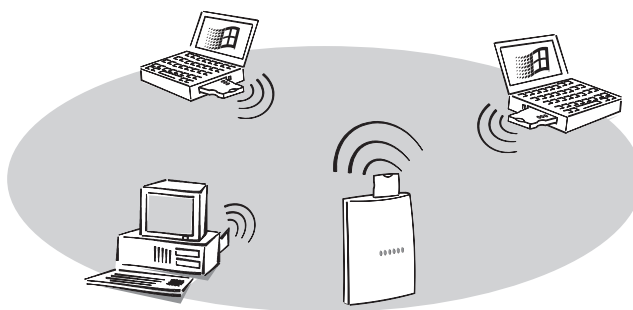
Grâce aux cartes réseau sans fil, les notebooks et les PC peuvent être reliés dans un réseau local, également appelé **Local Area Network (LAN)**. Comme dans ce réseau les câbles utilisés dans un réseau classique sont remplacés par une communication par ondes radio, il est aussi appelé **Wireless Local Area Network (WLAN)** ou réseau sans fil.

Station de base

La station de base forme le pont entre le réseau filaire (LAN) et le réseau sans fil (WLAN). Équipée d'une part d'un emplacement pour une carte réseau sans fil (*ELSA AirLancer MC-2*), d'autre part d'un connecteur Ethernet normal, la station de base échange toutes les données entre les deux réseaux. La station de base représente en quelque sorte le prolongement d'un câble jusqu'aux terminaux mobiles.

Cellule radio

La zone maximale dans laquelle les cartes réseau sans fil installées dans les terminaux mobiles peuvent communiquer avec les stations de base et réciproquement est appelée la cellule radio.

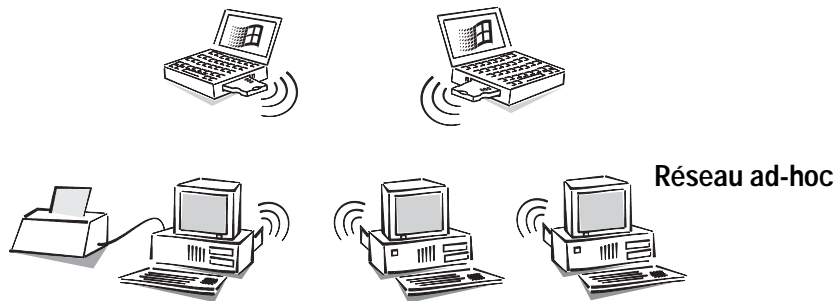


Le réseau local sans fil autorise toutes les fonctions d'un réseau filaire classique : l'accès aux fichiers, aux serveurs, aux imprimantes, etc., est tout aussi possible que l'intégration des terminaux mobiles dans un système de messagerie interne.

Les possibilités d'application offertes par les cartes réseau sans fil et les stations de base de ELSA sont les suivantes :

Connexion directe entre ordinateurs

Reliez deux ou plusieurs ordinateurs entre eux au moyen des cartes réseau sans fil. Tous les ordinateurs dans un réseau local sans fil peuvent communiquer entre eux sans qu'un autre périphérique soit nécessaire.

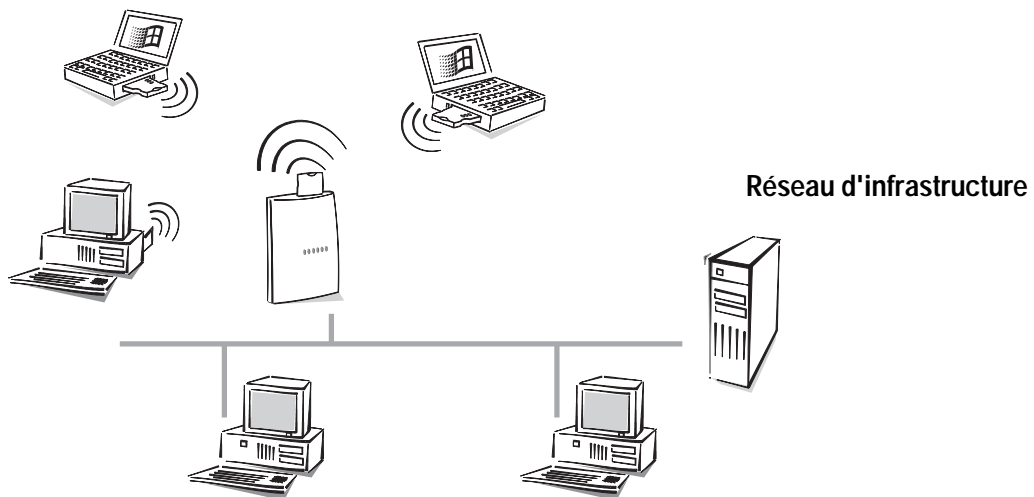


Peer-to-peer

Cette possibilité d'application est aussi appelée réseau peer-to-peer, dans une interconnexion par ondes radio on parlera du réseau ad-hoc.

Liaison avec le réseau filaire

Tous les ordinateurs équipés d'une carte réseau sans fil ont accès à un réseau local filaire via une station de base. La station de base sert d'une part de joncteur entre le réseau sans fil et le réseau filaire, d'autre part elle constitue la centrale de commande pour les échanges de données à l'intérieur du réseau sans fil.



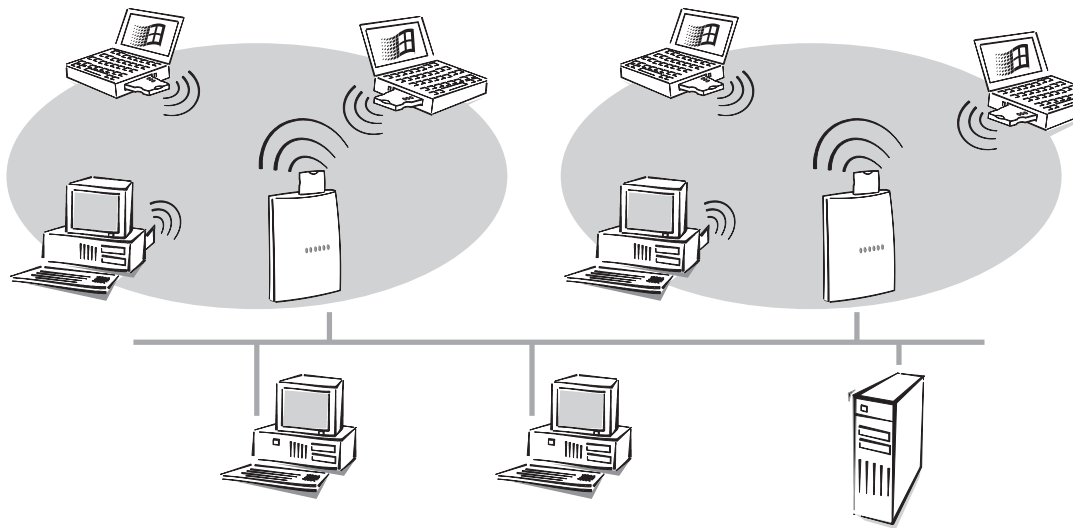
Peer-to-LAN

Un réseau local intégrant une station de base est appelé réseau peer-to-LAN, dans le jargon du réseau radio on parlera de réseau d'infrastructure.

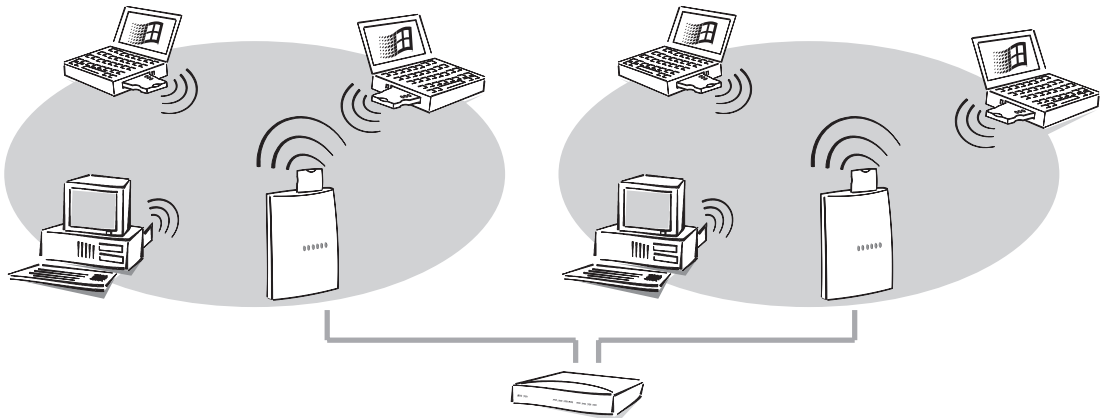
Ce type de réseau est idéal pour compléter les réseaux locaux classiques en place. Le réseau d'infrastructure est l'alternative idéale pour étendre un réseau filaire à des zones où le câblage est impossible à réaliser ou si sa réalisation n'est pas économique.

Evolutivité

Si le rayon d'action d'une cellule radio ne suffit plus pour interconnecter toutes les stations mobiles dans un réseau sans fil, il est possible de rajouter plusieurs stations de base. On utilise alors le câble du réseau filaire pour palier au rayon d'action insuffisant.



Ce principe fonctionne même dans le cas où on n'a pas de réseau filaire et si on veut réaliser un nouveau réseau entièrement radio. Si les stations mobiles ne se trouvent pas toutes dans la zone couverte par une station de base, on rajoute une deuxième station de base. Les deux stations de base peuvent par exemple être reliées au moyen d'un câble réseau simple et d'un hub.



Pour réaliser une grande zone de couverture, les cellules radio peuvent se chevaucher. Pour qu'il n'y ait pas de perturbations dans le réseau local radio, il est possible de choisir des canaux différents (jusqu'à 14 canaux différents) pour chaque cellule.

Avantages de *ELSA LANCOM Wireless L-2*

Pour vous donner un petit aperçu des fonctionnalités du réseau sans fil, voici les propriétés essentielles.

Simplicité d'installation

- Connecter *ELSA LANCOM* à une source de tension
- Réaliser la connexion avec le réseau local
- Mettre sous tension
- A vous de jouer !

Connexion à un réseau local

Les stations de base pour les réseaux sans fil de ELSA fonctionnent dans un réseau Ethernet. Un connecteur 10Base-T et un hub ou un switch permettent de relier le *ELSA LANCOM Wireless* au réseau local 10-Mbits.

Connexion au réseau local sans fil

Les cartes réseau sans fil dans les stations de base de ELSA fonctionnent selon la norme IEEE 802.11. Cette norme représente une extension des normes IEEE existantes s'appliquant aux réseaux locaux, dont IEEE 802.3 pour Ethernet est l'une des plus connues.

Pour la transmission de données sans fil, on peut en général recourir à trois principes physiques différents :

- Transmission par rayons infrarouges
- Transmission par ondes radio avec saut de fréquence
- Transmission par radio avec la méthode DSSS (**D**irect **S**equene **S**pread **S**pectrum)
Pour cette méthode, également utilisée dans le domaine militaire pour augmenter la sécurité contre les écoutes, les données sont segmentées avant la transmission et réparties sur un vaste spectre de fréquences (spread spectrum). Cette méthode garantit une transmission fiable et très sécurisée.

Les cartes réseau sans fil de ELSA recourent à la méthode DSSS. En plus des avantages de la protection contre le parasitage par les autres émetteurs qui utilisent éventuellement la même bande de fréquence, les cartes présentent aussi l'avantage d'être compatibles avec les cartes des autres constructeurs.

La norme IEEE 802.11 autorise le fonctionnement de réseaux radio sur des terrains privés et publics dans la bande de fréquence ISM (**I**ndustriel, **S**cientifique, **M**édical : 2.4 à 2.483 GHz).

La largeur de bande maximale pour la transmission de données dans le réseau radio est de 2 Mbits/s. Le rayon d'action en plein air atteint 300 mètres, et généralement env. 30 mètres à l'intérieur de bâtiments.

Bridging transparent

Les paquets de données provenant du réseau local filaire transitent dans le réseau sans fil et inversement. En outre, il est possible de limiter les échanges de données à certains protocoles et stations.

Affichage de l'état

Des témoins lumineux sur la face avant du boîtier de la station de base permettent de contrôler les accès Ethernet, ainsi que l'état de la liaison actuelle, et facilitent le diagnostic en cas d'anomalie.

Configuration avec *ELSA LANconfig*

Le réglage et l'adaptation des périphériques sur leur tâche spécifique s'effectue rapidement et confortablement à l'aide de l'outil de configuration pour Windows joint *ELSA LANconfig*. Les utilisateurs des autres systèmes d'exploitation utilisent Telnet.

L'accès au périphérique peut se faire depuis le réseau étendu WLAN ou le réseau local LAN. A côté de TFTP, SNMP est aussi pris en charge.

Les assistants d'installation intégrés vous aident à mettre les périphériques en service avec un minimum d'efforts.

Mise à jour des micrologiciels

Afin de rester à jour question logiciels, ces périphériques sont équipés d'une mémoire flash ROM. On télécharge tout simplement le nouveau micrologiciel dans le périphérique sans avoir besoin d'ouvrir le boîtier.

La version la plus récente du micrologiciel est toujours disponible sur nos services en ligne, et peut être téléchargée via le réseau local LAN ou via le réseau étendu WLAN.

FirmSafe

Vous ne courez aucun risque quand vous téléchargez le nouveau micrologiciel : la fonction FirmSafe permet de gérer deux fichiers de micrologiciel dans un périphérique. L'utilité de cette fonction est évidente : si le nouveau micrologiciel ne fonctionne pas comme vous le souhaitez après le téléchargement, vous pourrez très facilement réutiliser la version précédente.

En cas d'erreur au cours du téléchargement (par exemple suite à une erreur de transmission), le périphérique réutilise automatiquement la version précédente en état de fonctionner.

DHCP

Les stations de base de ELSA disposent également des fonctions d'un serveur DHCP. Ces fonctions vous permettent de définir une certaine plage d'adresses IP que le serveur DHCP attribue ensuite automatiquement aux diverses unités dans le réseau local.

En mode automatique, le routeur peut aussi déterminer toutes les adresses dans le réseau lui-même et les attribuer aux unités.

Installation

Ce chapitre vous aidera à établir rapidement un nouveau réseau radio. Tout d'abord vous voyez le contenu de la livraison et vous faites connaissance avec votre appareil. Ensuite nous vous montrons comment vous pouvez brancher et mettre l'appareil en service.

Contenu du coffret

Vérifiez le contenu du coffret avant de commencer l'installation. Le carton devrait contenir les composants suivants:

- Station de base *ELSA LANCOM Wireless L-2*
- Bloc transfo.
- Carte réseau-radio *ELSA AirLancer MC-2*
- Câble de raccordement au réseau local
- Documentation
- CD avec *ELSA LANconfig* et d'autres logiciels ainsi que la documentation électronique

Adressez-vous directement à votre revendeur si votre coffret n'est pas complet.

ELSA LANCOM Wireless se présente

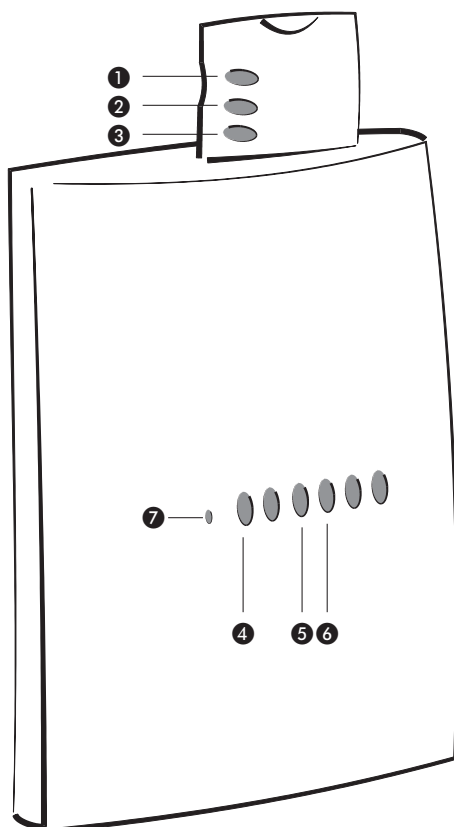
Dans ce chapitre nous vous présentons le matériel de l'appareil. Vous serez informés sur la signification des éléments d'affichage et des possibilités de raccordement.

Station de base La station de base est la liaison entre le réseau radio et le réseau câblé (LAN). Pour cela on dispose en plus du port 10-Base-T pour l'ethernet 10-Mbit également d'un socle pour la carte réseau radio *ELSA AirLancer MC-2*.

Carte PC La carte réseau-radio *ELSA AirLancer MC-2* est une carte PC qu'on enfiche simplement sur un emplacement libre de la station de base. L'antenne de la carte dépasse du boîtier de la station de base.

DEL

Sur la face avant vous trouvez quelques témoins lumineux comme éléments d'affichage.

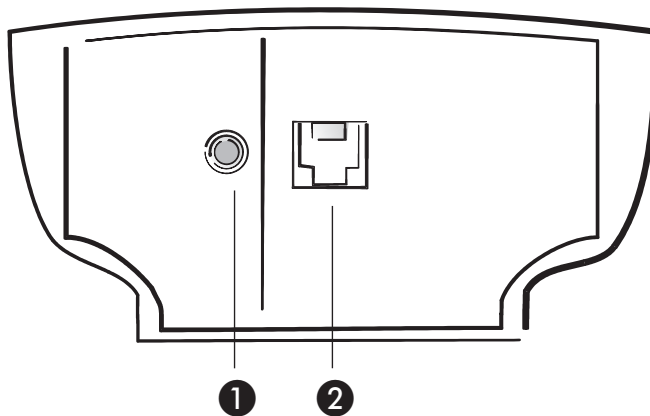


- ❶ La DEL rouge de la carte réseau-radio indique que la connexion est établie entre la carte et la station de base.
- ❷ La DEL jaune de la carte réseau-radio indique le nombre de stations mobiles connectées sur cette station de base. Sur trois stations connectées la DEL clignotera p.ex. brièvement trois fois de suite, le clignotement sera suivi d'une pause.
- ❸ La DEL verte de la carte réseau-radio indique l'activité dans le réseau radio, donc l'émission et la réception de paquets de données. Si cette DEL est éteinte ou allumée en permanence, la carte réseau-radio est perturbée.
- ❹ La DEL 'Power/Msg' sur la station de base s'allume brièvement lors de la mise sous tension. En cas d'erreur après l'auto-diagnostic, un code clignotant sera affiché, sinon, le périphérique sera en service et le témoin lumineux sera allumé constamment.

inactif		Périphérique hors circuit mais toujours sous tension
vert	1 x brièvement	Le lancement (test et chargement) a commencé
vert	clignotant	Affichage d'une erreur de lancement (codé sous forme de clignotement)
vert		Périphérique prêt au service

- ⑤ La DEL 'LAN-Status' sur la station de base indique une activité dans le réseau radio et dans le réseau local (LAN).
- ⑥ La DEL 'LAN-Collision' sur la station de base indique une collision d'émission dans le réseau local (LAN).
- ⑦ La touche Reset est dissimulée dans le boîtier et ne peut être actionnée qu'avec un objet pointu (p.ex. un trombone). Pour remettre l'appareil dans l'état à la livraison, appuyez la touche Reset jusqu'à ce que toutes les DEL soient allumées.

Et maintenant retournez le tout et regardez le dessous de l'appareil. Vous y trouvez:



- ⑧ Raccord au bloc transfo.
- ⑨ Raccordement réseau 10Base-T

Comment brancher la station de base

- ① Connectez la station de base *ELSA LANCOM Wireless L-2* au réseau local LAN. Pour cela, enfichez un côté du câble réseau joint dans le connecteur de réseau 10Base-T de la station de base, et l'autre dans une prise réseau libre de votre réseau local (ou bien une prise libre d'un HUB de votre LAN).
- ② Engagez la carte réseau-radio *ELSA AirLancer MC-2* dans la station de base. Les DEL de la carte PC doivent être orientées vers l'avant de la station de base.
- ③ Alimentez la station de base avec la tension nécessaire à l'aide du bloc d'alimentation. Après un autotest bref de l'appareil la DEL 'Power/Msg' de la station de base est allumée en permanence. La DEL rouge de la carte réseau-radio indique que la connexion est établie entre la carte et la station de base. Le scintillement de la DEL verte sur la carte réseau-radio indique que celle-ci essaye d'accéder à d'autres stations dans le WLAN. La DEL 'LAN-Status' indique une connexion correcte entre la station de base et le LAN.

Installation du logiciel

Le logiciel de configuration *ELSA LANconfig* pour systèmes d'exploitation sous Windows vous permet de régler votre station de base d'une manière simple et confortable en fonction de vos applications désirées.



A la livraison, les paramètres du réseau radio sont déjà réglés de manière à pouvoir démarrer immédiatement dans la plupart des cas. Une adaptation de la configuration ne sera nécessaire que pour des applications spéciales.

Pour l'utilisation du logiciel de configuration il vous faut un PC dans le réseau câblé ou dans le réseau radio.

- ① Installez d'abord le protocole de réseau TCP/IP sur l'ordinateur à partir duquel vous voulez régler votre station de base.
- ② Installez ensuite le logiciel de configuration *ELSA LANconfig*. Si le logiciel d'installation ne démarre pas automatiquement après avoir engagé le CD-ROM, cliquez simplement dans l'explorateur Windows sur 'autorun.exe' du *ELSA LANCOM Wireless* et suivez les instructions du programme d'installation.

Configuration de base

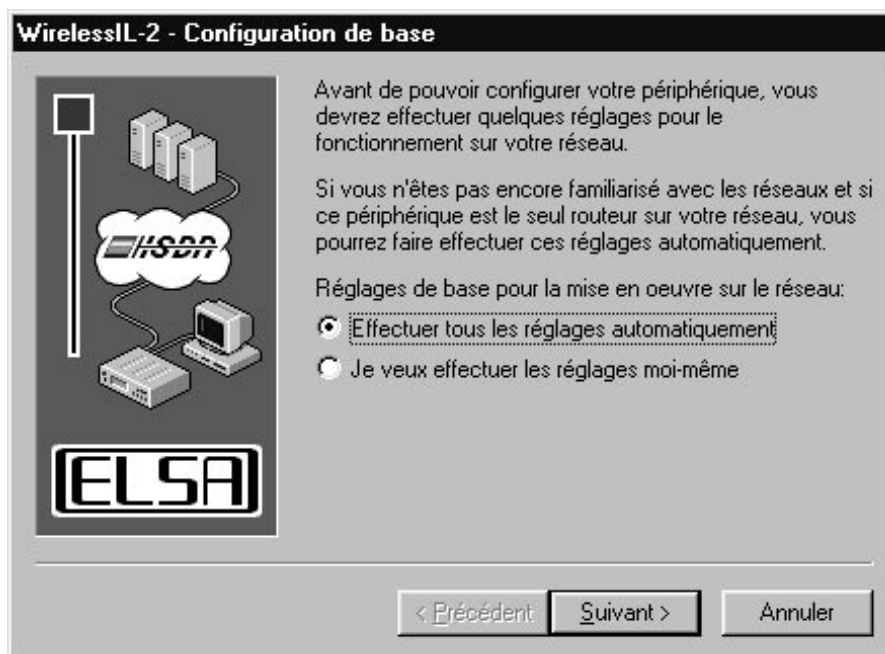
Dans la configuration de base on détermine l'adresse IP de la station de base. En outre on décidera de l'utilisation du serveur DHCP intégré. Vous pouvez procéder à la configuration de base avec *ELSA LANconfig* ou Telnet.

Réglages de base avec *ELSA LANconfig*

Lors du premier lancement de *ELSA LANconfig*, la nouvelle station de base sera reconnue dans le réseau TCP/IP et pourra être configurée immédiatement. Un assistant sera lancé automatiquement pour vous aider à procéder au réglage de base de l'appareil, ou pour vous en décharger entièrement.

Pour mettre un *ELSA LANCOM Wireless* en service, l'adresse IP XXX.XXX.XXX.254 ne doit pas être occupée dans votre réseau. Si vous avez déjà un appareil avec cette adresse, mettez-le hors-circuit pour la durée de la mise en service du *ELSA LANCOM Wireless*.

- ① Lancez le nouveau logiciel avec **Démarrer ► Programmes ► ELSAlan ► ELSA LANconfig.**



- ② Choisissez l'option 'Effectuer tous les réglages automatiquement' si vous **n'êtes pas** familiarisé avec les réseaux et les adresses IP et si l'une des suppositions suivantes est juste:

- Jusque là, vous n'avez pas encore utilisé d'adresses IP dans votre réseau, mais vous aimeriez bien le faire dès maintenant. Les adresses IP utilisées n'ont pas d'importance pour vous. En tant que serveur DHCP, la station de base déterminera et affectera alors automatiquement les adresses IP pour tous les appareils dans le réseau (LAN und WLAN).

ou

- Vous ne voulez pas utiliser d'adresses IP parce que vous utilisez p.ex. uniquement un réseau Windows.



*Si vous ne savez pas si des adresses IP ont été utilisées dans votre réseau, cliquez d'abord sur **Démarrer ► Exécuter**, entrez l'instruction `winipcfg` dans la fenêtre qui s'ouvre et cliquez sur **OK**. Sélectionnez votre carte réseau dans la fenêtre suivante. Si vous trouvez la valeur '0.0.0.0' dans la zone 'Adresse IP', votre carte réseau n'a pas encore d'adresse IP.*

- ③ Choisissez l'option 'Je désire effectuer les réglages moi-même' si vous êtes familiarisé avec les réseaux et les adresses IP et si l'une des suppositions suivantes est juste:

- Jusque là, vous n'avez pas encore utilisé d'adresses IP dans votre réseau, mais vous aimeriez bien le faire dès maintenant. Vous voulez déterminer vous-même l'adresse IP de votre station de base et lui attribuer une adresse quelconque se

trouvant dans une zone d'adresses personnelles, p.ex. '10.0.0.1' avec le masque '255.255.255.0'. De cette manière, vous déterminez aussi la zone d'adresses qu'utilisera ensuite le serveur DHCP pour les appareils dans le réseau (si le serveur DHCP n'est pas hors service).

- Vous avez déjà utilisé des adresses IP avec les ordinateurs dans le réseau local. Attribuez à la station de base une adresse libre se trouvant dans la zone d'adresses utilisée jusque là et déterminez si la station de base doit servir de serveur DHCP ou non.



Vous trouvez des informations supplémentaires sur la structure générale de réseaux et les adresses IP dans la documentation électronique sur le CD ELSA LANCOM Wireless. Le fonctionnement du serveur DHCP est décrit plus loin dans ce manuel.

- ④ Avec ces quelques clics avec la souris, la station de base est complètement réglée et prête à exécuter sa tâche fondamentale: permettre aux stations mobiles d'accéder à un réseau local câblé.

Réglages de base avec Telnet

Si vous ne voulez ou ne pouvez pas utiliser *ELSA LANconfig* (p.ex. si vous avez installé un autre système d'exploitation), les réglages de base peuvent être effectués via une connexion Telnet.

Lancez une connexion Telnet vers l'adresse '10.0.0.254' si vous n'avez pas encore utilisé d'adresses IP dans votre réseau, ou bien vers l'adresse 'x.x.x.254', 'x.x.x' représentant le groupe d'adresses utilisé jusque là dans le réseau.

Entrez les instructions suivantes:

- ① Lancez la connexion Telnet p.ex avec l'instruction **Démarrer ► Exécuter** et entrez l'instruction `telnet 10.0.0.254` dans la fenêtre qui s'ouvre.

- ② Modifiez le langage de la configuration avec l'instruction:

```
set /Setup/config-module/language français
```

- ③ Adresse Intranet et masque réseau:

```
set /Setup/TCP-IP-modul/Adresse Intranet 10.0.0.1
```

```
set /Setup/TCP-IP-modul/Masque Intranet 255.255.255.0
```



Après la modification de l'adresse Intranet il faudra relancer le routeur le cas échéant.

- ④ Désactiver éventuellement la fonction DHCP:

```
set /Setup/Module DHCP/operating off
```

Configurations possibles

Les stations de base de ELSA sont toujours livrées avec un logiciel actuel dans lequel quelques réglages sont déjà effectués pour vous.

Il sera tout de même nécessaire de compléter les indications et d'adapter le routeur à votre tâche spécifique. Ces réglages seront effectués durant la configuration.

Dans ce chapitre, nous vous montrons avec quels logiciels et par quels chemins vous pouvez accéder au périphérique pour effectuer les réglages.

Dès que l'équipe de développement aura élaboré pour vous un nouveau logiciel de firme avec de nouvelles possibilités, vous trouverez ici des indications pour le téléchargement du micrologiciel.

Radio ou câble: Chemins aboutissant à la configuration

Avec la configuration via le réseau vous pouvez accéder à la station de base à partir de n'importe quel ordinateur du LAN ou WAN. L'accès pourra toutefois être restreint ou bloqué entièrement par la liste d'accès IP. Pour cette configuration, utilisez Telnet (fait partie de la livraison de la plupart des systèmes d'exploitation) ou le programme de configuration *ELSA LANconfig* pour Windows. *ELSA LANconfig* est compris dans la livraison de votre appareil. Les versions actuelles sont toujours à votre disposition dans nos médias en ligne.

Conditions

La configuration avec Telnet ou ***ELSA LANconfig*** se déroule par TCP/IP ou TFTP. Pour cela TCP/IP doit être installé sur l'ordinateur utilisé, et votre station de base requiert une adresse IP, afin que vous puissiez la contacter.

Un périphérique non configuré a l'adresse IP XXX.XXX.XXX.254. Les X représentent l'adresse réseau dans votre LAN. Si les ordinateurs dans votre réseau ont des adresses telles que 192.110.130.1, vous pourrez alors contacter votre périphérique avec l'adresse 192.110.130.254.



Si dans votre réseau vous disposez déjà d'un ordinateur avec l'adresse XXX.XXX.XXX.254, mettez d'abord l'ordinateur avec cette adresse hors circuit. Dès que vous êtes connecté avec la station de base par ELSA LANconfig ou Telnet, donnez lui sa propre adresse IP.

Alternative : Gestion des adresses à l'aide du serveur DHCP

S'il n'est pas absolument nécessaire de configurer les adresses correctes IP « à la main », le serveur DHCP se chargera volontiers de cette tâche tout seul. Si vous utilisez le serveur DHCP, vous pouvez faire régler automatiquement les adresses IP pour tous les ordinateurs du réseau (cf. chapitre 'Affectation automatique des adresses avec DHCP').

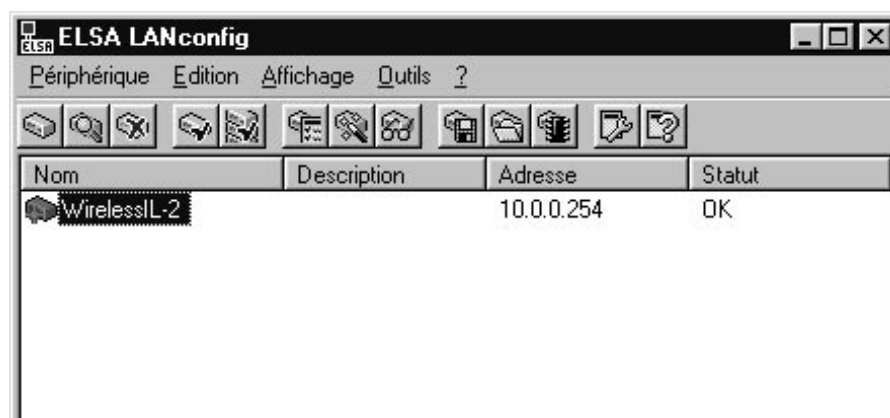
Lancement de la configuration par *ELSA LANconfig*

Appelez l'outil de configuration *ELSA LANconfig* p.ex. à partir de la barre de Windows avec **Démarrer ► Programmes ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* cherchera automatiquement des périphériques dans le réseau local.



Pour lancer une recherche de périphérique manuelle, il suffit de cliquer sur le bouton **Rechercher** ou d'appeler l'instruction par **Périphérique ► Rechercher**. *ELSA LANconfig* demandera alors, où chercher. Avec la solution inband, il suffit de sélectionner ici le réseau local, et c'est parti.

Dès que *ELSA LANconfig* a terminé sa recherche, il affichera une liste de tous les périphériques trouvés avec leur nom, éventuellement une description, leur adresse IP et leur état.



Pour la configuration des appareils avec *ELSA LANconfig* vous avez le choix entre deux possibilités de représentation différentes:

- La 'représentation simplifiée' n'affiche que les réglages nécessaires aux applications usuelles.
- La 'représentation complète' affiche tous les réglages disponible. Certains de ces réglages ne devraient être modifiés que par des utilisateurs expérimentés.

Choisissez le mode de représentation dans le menu **Affichage ► Options**.



Un double-clic sur l'inscription du périphérique marqué, un clic sur le bouton **Configurer** ou le menu **Edition ► Modifier le fichier de configuration** lit les réglages actuels du périphérique et affiche la sélection de configuration 'Généralités'.

La suite de la conduite du programme est auto-descriptive, ou alors sélectionnez l'aide en ligne. Vous pouvez à tout moment appeler l'aide contextuelle en cliquant sur le point

d'interrogation en haut à droite de chaque fenêtre, ou alors avec un clic de la touche droite de la souris sur un terme qui ne vous paraît pas clair.

Lancement de la configuration par Telnet

Avec Telnet vous lancez la configuration p. ex. à partir d'une zone DOS à l'aide de l'instruction:

```
telnet 10.1.80.125
```

Telnet établit alors une connexion vers le périphérique avec l'adresse IP entrée.

Après l'introduction du mot de passe (si vous avez convenu un mot de passe pour protéger la configuration) vous disposez de toutes les instructions figurant au paragraphe 'Instructions pour la configuration'.


Instructions de configuration

Si vous utilisez Telnet ou un émulateur de terminal pour la configuration du routeur, entrez les instructions et les chemins tels que vous les connaissez sous DOS ou UNIX.

Séparez les termes d'un chemin à l'aide d'une barre de fraction ou d'une barre de fraction inversée. Il n'est pas nécessaire d'entrer entièrement les instructions et les inscriptions au tableau, une abréviation significative suffit.

Lors de la configuration les enregistrements dans les groupes MENU, VALUE, TABLE, TABINFO, ACTION et INFO seront affichées et éventuellement modifiées. Pour cela, vous pouvez utiliser les instructions suivantes :

Cette instruction signifie p. ex. :
? ou help	appelle les textes d'aide.	–
dir, list, ll, ls <MENU>, <VALUE> ou <TABLE>	affiche le contenu de MENU, VALUE ou TABLE.	statistique dir/status/wan affiche la statistique actuelle WAN.
cd <MENU> ou <TABLE>	passer au MENU indiqué ou au TABLE.	module cd setup/tcp-ip (en bref cd se/tc) passe au module TCP/IP.
set <VALUE>	nouvelle définition du VALUE.	set ip-adresse 192.110.120.140 définit une nouvelle adresse IP.
	séparez toutes les entrées dans les lignes des tableaux par des espaces. Un * ne modifie pas l'inscription.	set /setup/name BORDEAUX nomme l'appareil 'BORDEAUX'
set <VALUE> ?	vous affiche les valeurs que vous pouvez entrer ici.	
del <VALUE>	efface une ligne dans un tableau.	del /se/wan/nam/BORDEAUX efface l'inscription vers le correspondant BORDEAUX

Cette instruction signifie p. ex. :
do <ACTION> (paramètre)	exécute l' ACTION, éventuellement avec les paramètres indiqués.	do /firmware/firmware-upload lance le chargement d'un nouveau micrologiciel.
passwd	permet l'introduction d'un nouveau mot de passe. Pour cela, il faut d'abord entrer l'ancien mot de passe, s'il en existe un. Ensuite, il faut entrer le nouveau mot de passe deux fois de suite et confirmer chaque fois avec  .	
repeat <sec> <ACTION>	répète l' ACTION avec un délai égal aux secondes indiquées. N'importe quelle touche achève la répétition.	repeat 3 dir/status/wan-statistics affiche la statistique actuelle WAN toutes les 3 secondes.
time	règle la date et l'heure-système.	time 24.12.1998 18:00:00
language <Sprache>	définit la langue de la séance actuelle de configuration.	langues prises en charge actuellement. Englisch (language english) Deutsch (language deutsch)
exit, quit, x	fin de la configuration.	

Les textes contenant des espaces ne seront acceptés qu'entre guillemets, p. ex. `set /se/snmp/admin "Un administrateur"`.

Les entrées de textes (valeurs uniques et tableaux) sont effacés comme suit:

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

Nouveau micrologiciel avec FirmSafe

Le logiciel des périphériques de ELSA est soumis à un développement constant. Afin que vous puissiez aussi profiter de nouvelles propriétés et fonctions, nous avons équipé les appareils d'une mémoire Flash-ROM, faisant de toute modification ultérieure du logiciel d'exploitation un jeu d'enfant. Pas d'EPROM à remplacer, pas de boîtier à ouvrir : Charger simplement la nouvelle version, c'est tout !

Comment fonctionne FirmSafe ?

FirmSafe rend le chargement du nouveau logiciel sûr : Le micrologiciel utilisé jusqu'à là ne sera pas écrasé, mais un deuxième micrologiciel sera chargé dans l'appareil.

Seule une des deux versions de micrologiciels dans un périphérique peut être active. Le chargement d'un nouveau micrologiciel efface le micrologiciel non actif. Vous pouvez décider vous-même quel micrologiciel devra être activé après un téléchargement :

- 'Immédiatement' : La première possibilité consiste à charger et à activer le micrologiciel immédiatement. Les situations suivantes peuvent s'en suivre :
 - Le nouveau micrologiciel est chargé avec succès et fonctionne ensuite comme voulu. Donc tout est correct.
 - Le périphérique n'est plus accessible après le chargement du nouveau micrologiciel. S'il survient une erreur déjà lors d'un téléchargement, le périphérique activera automatiquement l'ancien micrologiciel et relancera le périphérique.
- 'Login' : Afin de remédier aux problèmes d'un téléchargement incorrect, vous avez la deuxième possibilité suivant laquelle le micrologiciel sera chargé et également lancé immédiatement.
 - La différence avec l'autre variante réside dans le fait que le périphérique attendra ensuite durant cinq minutes un login correct auprès du périphérique. Le nouveau micrologiciel ne sera activé en permanence qu'après exécution correcte du login.
 - Si le périphérique n'est plus accessible, donc un login impossible, il activera automatiquement l'ancien micrologiciel et relancera le périphérique.
- 'Manuel' : La troisième possibilité vous permet de déterminer auparavant vous-même une période de temps, durant laquelle vous voulez tester le nouveau micrologiciel. Le périphérique démarre avec le nouveau micrologiciel et attend durant la période de temps réglée que le micrologiciel soit activé manuellement pour être actif en permanence.

Comment charger le nouveau logiciel ?

Plusieurs chemins mènent au but pour le téléchargement du micrologiciel (c'est comme ça qu'on appelle le chargement du logiciel) :

- Outil de configuration *ELSA LANconfig* (conseillé)
- TFTP



Certains réglages sont conservés lors du téléchargement du micrologiciel ! Par souci de sécurité, vous devriez quand-même sauvegarder votre configuration (pour **ELSA LANconfig** p. ex. avec **Edition ► Sauvegarder la configuration dans un fichier**).

Si la nouvelle version contient des paramètres n'existant pas dans le micrologiciel actuel, le périphérique complètera les valeurs manquantes par des valeurs par défaut.

ELSA LANconfig



Dans l'outil de configuration *ELSA LANconfig* marquez l'appareil souhaité dans la liste de sélection et cliquez sur **Edition ► Gestion de micrologiciel ► Charger nouveau micrologiciel** ou directement sur le bouton **Télécharger micrologiciel**. Sélectionnez

ensuite le répertoire dans lequel se trouve la nouvelle version et marquez le fichier correspondant.

ELSA LANconfig vous indiquera dans la description le numéro de la version et la date du micrologiciel et vous proposera un téléchargement. Avec **Ouvrir** vous remplacez le micrologiciel actuel par la version choisie.

Sélectionnez également si le micrologiciel doit être activé en permanence après le chargement, ou alors fixez une période de test dans laquelle vous activerez le micrologiciel vous-même. Pour activer ensuite le micrologiciel durant la période de test, cliquez sur **Edition ► Gestion du micrologiciel ► Activation du micrologiciel durant le test**.

TFTP

Avec TFTP, un nouveau micrologiciel peut être chargé à l'aide de l'instruction **writelflash**. Pour transmettre un nouveau micrologiciel, se trouvant p. ex. dans le fichier 'LC_1000U.130' dans un périphérique avec l'adresse IP 194.162.200.17, entrez p. ex. sous Windows NT l'instruction suivante :

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



*Cette instruction envoie le fichier correspondant avec **writelflash** à l'adresse IP indiquée. Pour cela, TFTP doit être commuté sur transmission de données binaires. Le format ASCII est toutefois prééglé sur beaucoup de systèmes. Dans cet exemple pour Windows NT, vous y arrivez à l'aide du paramètre '-i'.*

Après un téléchargement correct du micrologiciel, le périphérique procède à une relance en activant directement le nouveau micrologiciel. Si une erreur survient lors du chargement, (erreur d'écriture dans le Flash-ROM, erreur de transmission TFTP etc.), l'appareil procédera également à une relance et FirmSafe activera le micrologiciel précédent. La configuration sera conservée.

TFTP permet également l'exécution d'autres instructions de configuration. Voyez la syntaxe dans les exemples suivants :

- `tftp 10.0.0.1 get readconfig file1` : lit la configuration du périphérique avec l'adresse 10.0.0.1 et l'enregistre sous file1 dans le répertoire actuel
- `tftp 10.0.0.1 put file1 writeconfig` : écrit la configuration contenue dans le fichier file1 dans le périphérique avec l'adresse 10.0.0.1
- `tftp 10.0.0.1 get dir/status/verb file2` : enregistre les informations de communication actuelles dans file2.

Configuration par SNMP

Le simple protocole de management de réseau (Simple Network Management Protocol SNMP V.1 nach RFC 1157) permet la surveillance et la configuration d'appareils dans un

réseau à partir d'une instance centrale à l'aide d'un protocole de management standardisé.

Vous trouvez des informations détaillées sur la configuration d'appareils ELSA avec SNMP dans la documentation électronique sur le CD.

Fonctions et modes d'exploitation

Ce chapitre se propose de vous présenter les diverses fonctions et modes d'exploitation de votre périphérique. Vous trouverez entre autres des informations sur les points suivants :

- Réseaux sans fil (ondes radio)
- Sécurité de la configuration
- Gestion d'adresses automatique via DHCP

Parallèlement à la description de ces divers thèmes, nous vous donnerons aussi quelques astuces qui vous aideront pour la configuration.

La description détaillée de tous les paramètres et menus se trouve dans la documentation électronique.

Paramètres de la transmission radio

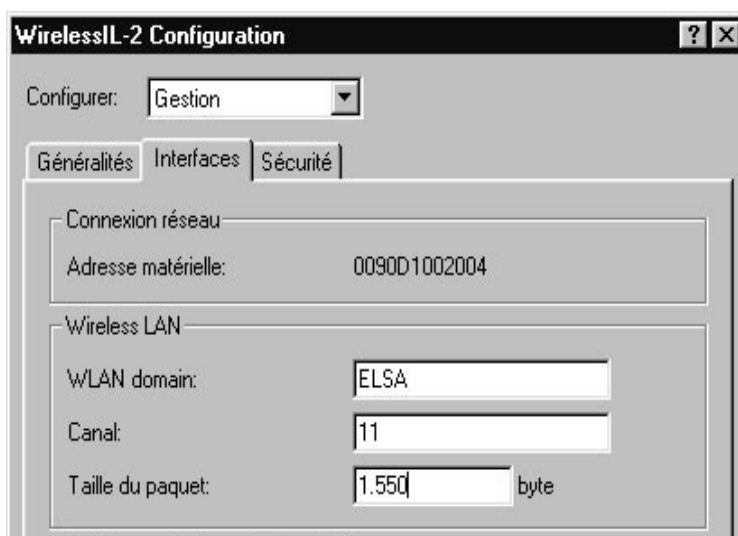
Pour que les cartes réseau sans fil installées dans les terminaux mobiles et dans les stations de base puissent s'identifier mutuellement et échanger des données entre elles, elles doivent posséder les mêmes valeurs dans divers paramètres.

Toutes les cartes réseau sans fil (dans les stations de base ou mobiles) qui fonctionnent avec les mêmes paramètres tissent un réseau. En choisissant judicieusement les paramètres, on peut créer plusieurs réseaux distincts où les transmissions de données ne s'influencent pas mutuellement.

Les paramètres des cartes dans les stations de base sont configurés avec *ELSA LANconfig* ou via Telnet.

- ① Lancez *ELSA LANconfig* avec **Démarrer ► Programmes ► ELSA lan ► ELSA LANconfig**. *ELSA LANconfig* recherche automatiquement toutes les stations de base dans le réseau local filaire (LAN) et dans le réseau sans fil (WLAN).

- ② Dans la liste des périphériques trouvés, cliquez sur la station de base que vous souhaitez configurer. Dans la zone de configuration 'Gestion', passez à l'onglet 'Interfaces'.



- ③ Entrez une nouvelle valeur pour le domaine WLAN. Le domaine WLAN doit être identique pour tous les participants d'un réseau sans fil.



Modifiez la valeur par défaut 'ELSA' le plus tôt possible, car le domaine WLAN vous sert à protéger votre réseau sans fil contre les accès non autorisés, comme s'il s'agissait d'un mot de passe !

- ④ Choisissez le même canal radio pour tous les participants du réseau sans fil. Ce canal radio sert à sélectionner la bande de fréquence que les cartes réseau sans fil utilisent pour échanger les données.

En choisissant un canal différent, vous avez la possibilité d'exploiter plusieurs réseaux sans fil distincts parallèlement. Théoriquement, 14 canaux sont disponibles, mais en raison du chevauchement des fréquences avec la méthode DSSS, seuls trois réseaux distincts sans chevauchement sont réalisables dans la bande de fréquences ISM. Si vous souhaitez exploiter simultanément plusieurs cellules radio très proches les unes des autres, nous recommandons de choisir des canaux éloignés, par exemple les canaux 1, 7 et 14 ou 3 et 13.



Veillez à consulter le tableau des canaux radio autorisés dans les divers pays. Ce tableau se trouve dans l'annexe.

- ⑤ La taille des paquets sert à définir la longueur d'un paquet acheminé via le réseau sans fil. La valeur est comprise entre 600 et 1600 octets. Les grands paquets doivent être découpés en morceaux avant la transmission (fragmentés) et être réassemblés chez le destinataire.

Les petits paquets peuvent contribuer à une meilleure transmission dans les environnements perturbés, mais la part des données utiles par rapport aux informations de gestion contenues dans le paquet se détériore.

- ⑥ Sélectionnez le dossier de configuration 'Pont WLAN' si vous
- souhaitez interdire l'échange de données avec le réseau filaire pour certaines stations mobiles ou
 - si vous souhaitez interdire l'échange au moyen de certains protocoles.



*Si le dossier de configuration 'Pont WLAN' n'est pas visible, sélectionnez le mode d'affichage intégral de la configuration en sélectionnant - dans la fenêtre principale de ELSA LANconfig - la commande **Affichage** ► **Options**.*

La sécurité de votre configuration

En configurant le périphérique, vous fixez une série de paramètres essentiels pour l'échange de données : la sécurité de votre propre réseau, le contrôle des coûts de communication et les droits d'accès des utilisateurs font par exemple partie de ces paramètres.

Les paramètres que vous avez saisis et fixés une fois pour toutes ne devraient évidemment pas être modifiés par des personnes non autorisées. C'est pourquoi *ELSA LANCOM Wireless* offre la possibilité de protéger la configuration par différents moyens.

Protection par mot de passe

La manière la plus simple de protéger la configuration est d'activer un mot de passe. Tant que vous n'avez pas activé de mot de passe, toute personne peut modifier la configuration du périphérique.

Le champ de saisie du mot de passe se trouve dans l'onglet 'Sécurité' du dossier de configuration 'Gestion' de *ELSA LANconfig*. Pour une session Telnet ou de terminal, vous activez la protection par mot de passe dans le menu `/Setup/Module Config/Entrée du mot de passe`. Dans ce cas, le mot de passe en soi est activé au moyen de la commande `passwd`.

Le verrouillage des accès

La configuration du *ELSA LANCOM Wireless* est protégée contre les attaques en force brute par un verrouillage d'accès. Dans le cas d'une attaque en force brute, un utilisateur non autorisé cherche à trouver un mot de passe et de trouver un accès à un réseau, à un ordinateur ou à un autre périphérique. Par exemple, l'intrus (un ordinateur) essaie automatiquement toutes les combinaisons de chiffres et de lettres possibles jusqu'à ce qu'il ait trouvé le mot de passe correct.

Pour se protéger contre ces intrusions, il est possible de définir le nombre maximal de tentatives d'accès infructueuses. Dès que cette limite est atteinte, l'accès est verrouillé pendant une certaine période.

Ces paramètres sont valables globalement pour toutes les possibilités de configuration (Telnet, TFTP/*ELSA LANconfig* et SNMP). Le blocage d'un accès bloque automatiquement tous les autres accès.

Pour configurer le verrouillage d'accès, vous disposez des champs suivants dans l'onglet 'Sécurité' du dossier de configuration 'Gestion' de *ELSA LANconfig* ou dans le menu / Setup/Module Config :

- 'Blocage actif après' (accès infructueux)
- 'Durée du blocage' (durée du verrouillage en minutes)

Contrôle des accès via TCP/IP

Une liste spéciale des filtres permet de restreindre l'accès aux fonctions internes des périphériques via TCP/IP. Ces fonctions internes désignent ici les sessions de configuration via Telnet ou TFTP (*ELSA LANconfig*).

Au départ, ce tableau ne contient pas d'entrées afin de permettre à tout utilisateur d'accéder au routeur via TCP/IP avec Telnet ou via TFTP depuis un ordinateur ayant une adresse IP. Le filtre est actif dès que la première adresse IP et le masque de réseau correspondant sont enregistrés. A partir de ce moment là , seules les adresses IP indiquées dans l'entrée sont autorisées à utiliser les fonctions internes. Pour élargir le cercle des personnes autorisées, il suffit de créer des entrées supplémentaires. Les entrées de filtrage peuvent désigner aussi bien un ordinateur qu'un réseau entier.

Vous trouverez le tableau des accès en sélectionnant l'onglet 'Général' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou dans le menu / Setup/Module TCP-IP/Liste d'accès.

Gestion d'adresses automatique via DHCP

Pour une exploitation sans accrocs dans un réseau TCP/IP, tous les périphériques d'un réseau local requièrent des adresses IP bien définies. De plus, ils ont besoin des adresses des serveurs DNS et NBNS ainsi que d'une passerelle par défaut, qui permet de router les paquets de données des adresses inaccessibles localement.

Dans le cas d'un petit réseau, il est tout à fait concevable de saisir ces adresses « manuellement » pour tous les ordinateurs présents dans le réseau. Dans le cas d'un réseau important comportant plusieurs ordinateurs aux postes de travail, ceci devient rapidement un travail fastidieux.

Dans un tel cas de figure, DHCP (Dynamic Host Configuration Protocol) est la réponse la mieux adaptée. A l'aide de ce protocole, un serveur DHCP peut attribuer de manière dynamique les adresses nécessaires aux différentes stations dans un réseau local basé sur TCP/IP.

Le serveur DHCP

ELSA LANCOM Wireless, en tant que serveur DHCP, peut gérer les adresses IP dans son réseau TCP/IP. Pour ce, il communique aux postes de travail les paramètres suivants :

- Adresse IP
- Masque de réseau
- Adresse de diffusion
- Serveur DNS
- Serveur NBNS
- Passerelle par défaut
- Durée de validité des paramètres attribués

Le serveur DHCP extrait les adresses IP soit d'un pool d'adresses librement défini ou calcule les adresses tout seul à partir de l'adresse IP (ou de l'adresse Intranet).

En mode DHCP automatique (DHCP-Automode), un périphérique non configuré est capable de fixer automatiquement les adresses IP pour soi-même et pour les ordinateurs du réseau.

Dans le cas de figure le plus simple, vous n'avez qu'à connecter le nouveau périphérique en état de la livraison à un réseau sans autres serveurs DHCP et à l'activer. Le routeur règle alors en combinaison avec le *ELSA LANconfig* via l'assistant toutes les allocations d'adresses supplémentaires dans le réseau local par lui-même.

DHCP – 'actif', 'inactif' ou 'auto' ?

Le serveur DHCP peut prendre trois états différents :

- 'Actif' : Le serveur DHCP est normalement actif. Lors de l'entrée de cette valeur, la configuration du serveur (validité du pool d'adresses) est vérifiée.
 - Si la configuration est correcte, le périphérique est indiqué en tant que serveur DHCP dans le réseau.
 - Si la configuration est erronée (par ex. limites pool invalides), le serveur DHCP sera désactivé et passe à l'état 'Inactif'.
- 'Inactif' : Le serveur DHCP est normalement inactif.
- 'Auto' : Le serveur se trouve en mode automatique. Dans ce mode, le périphérique recherche d'autres serveurs DHCP dans le réseau local après la mise sous tension.
 - Si au moins un autre serveur DHCP est détecté, le périphérique déconnecte son propre serveur DHCP. Ceci a pour effet d'éviter entre autres qu'un périphérique non configuré une fois activé attribue des adresses dans le réseau qui ne se trouvent pas dans le réseau local.
 - Si aucun autre serveur DHCP n'est détecté, le périphérique active son propre serveur DHCP.

Les statistiques DHCP permettent d'établir si le serveur DHCP est finalement connecté ou déconnecté.

La configuration par défaut de l'état est 'Auto'.

Attribution des adresses

Attribution d'adresses IP

Pour que le serveur DHCP puisse attribuer les adresses IP aux ordinateurs du réseau, il doit préalablement connaître les adresses qu'il peut utiliser pour cette attribution. Pour sélectionner les adresses possibles, il existe trois options différentes :

- L'adresse IP peut être extraite à partir du pool d'adresses (pool d'adresses de départ - pool d'adresses d'arrivée). Ici, des adresses quelconques valables dans le réseau local peuvent être entrées.
- Si '0.0.0.0' est entré à la place, le serveur DHCP déduit par lui-même les adresses respectives (départ ou arrivée) à partir des configurations de l'adresse IP dans le 'module TCP/IP'.
- Si le modem n'a pas d'adresse IP spécifique, le périphérique se trouve dans un état de service particulier. Il utilise alors lui-même l'adresse IP '10.0.0.254' et le pool d'adresses '10.x.x.x' pour l'affectation des adresses IP dans le réseau. Dans cet état, le serveur DHCP attribue aux autres ordinateurs dans le réseau uniquement l'adresse IP et sa validité, mais pas les autres informations.

Si un ordinateur est à présent démarré dans le réseau réclamant une adresse IP à l'aide de ses paramètres réseau via DHCP, un périphérique avec module DHCP activé lui proposera l'affectation d'une adresse. Comme adresse IP, une adresse valable issue du pool est choisie. Si une adresse IP a déjà été affectée par le passé à cet ordinateur, il réclame également cette adresse et le serveur DHCP tente de lui attribuer cette adresse à nouveau, si elle n'a pas été déjà affectée à un autre ordinateur.

Le serveur DHCP vérifie également, si l'adresse recherchée est encore libre dans le réseau local. Dès que la justesse d'une adresse a été prouvée, l'adresse trouvée sera attribuée à l'ordinateur requérant.

Allocation du masque de réseau

L'allocation du masque de réseau se fait de manière analogue à l'attribution d'adresses. Si un masque de réseau est saisi dans le module DHCP, c'est lui qui sera utilisé pour l'allocation. Sinon, le masque de réseau issu du module TCP/IP sera utilisé.

Attribution de l'adresse de diffusion

En règle générale, une adresse est utilisée dans le réseau local pour les paquets diffusés, qui résulte des adresses IP valables et du masque de réseau. Uniquement dans des cas particuliers (par ex. lors de l'utilisation de sous-réseaux pour une partie des ordinateurs aux postes de travail), il peut s'avérer nécessaire d'utiliser une autre adresse de diffusion. Dans ce cas, l'adresse de diffusion à utiliser sera saisie dans le module DHCP.



Il est recommandé que seuls des spécialistes de réseau expérimentés procèdent à la modification de la préconfiguration de l'adresse de diffusion.

Affectation du serveur DNS et du serveur NBNS

A cet effet, les entrées correspondantes sont extraites à partir du 'module TCP'.



Si les serveurs DNS ou NBNS se trouvant dans le réseau local filaire doivent également être disponibles dans le réseau sans fil, les adresses correspondantes doivent obligatoirement être déclarées. Si ce n'est pas le cas, la station de base communique sa propre adresse IP en tant que serveur DNS ou NBNS aux ordinateurs dans le réseau sans fil, mais ne peut pas répondre aux requêtes.

Affectation de la passerelle par défaut

Le périphérique affecte par défaut sa propre adresse IP comme adresse de passerelle à l'ordinateur requérant.



Si une passerelle présente dans le réseau local filaire doit également être disponible dans le réseau sans fil, l'adresse IP de la passerelle dans le module DHCP doit être déclarée en tant qu'adresse de la passerelle. Si ce n'est pas le cas, la station de base communique sa propre adresse IP en tant que passerelle aux ordinateurs dans le réseau sans fil, mais ne peut pas répondre aux requêtes.

En cas de besoin, cette affectation peut être recouverte par les paramètres sur l'ordinateur au poste de travail.

Durée de validité d'une affectation

Les adresses attribuées à l'ordinateur ne sont valides que pour une certaine durée. Une fois cette période écoulée, l'ordinateur ne doit plus les utiliser. De manière à ne pas perdre les adresses (en particulier ses adresses IP), l'ordinateur demande, suffisamment à temps, une prolongation qui lui est normalement accordée. C'est seulement lorsque la période de validité prend fin alors que l'ordinateur est éteint que l'adresse est perdue.

A chaque requête, un hôte peut demander une certaine période de validité. Toutefois, il peut arriver qu'un serveur DHCP attribue à l'hôte une durée différente. Le module DHCP propose deux paramètres permettant d'influencer la période de validité :

- Période de validité maximale en minutes

On peut indiquer ici la période de validité maximale que le serveur DHCP attribue à

un hôte.

Lorsqu'un hôte demande une période de validité dépassant la durée maximale de 6000 minutes, cette valeur lui est attribuée !

La valeur par défaut de 6000 minutes correspond à env. 4 jours.

■ Période de validité par défaut en minutes

On peut indiquer ici la période de validité à attribuer lorsque l'hôte ne fait aucune demande à ce sujet. La valeur par défaut de 500 minutes correspond à env. 8 heures.

Priorité pour le serveur DHCP – Requête d'allocation

De manière standard, la presque totalité des paramètres dans le voisinage réseau de Windows sont définis de manière que les paramètres nécessaires soient demandés par le DHCP. Vérifiez les paramètres en cliquant sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau**. Sélectionnez l'entrée pour 'TCP/IP' au niveau de votre adaptateur de réseau et ouvrez les **Propriétés**.

Sur les différents onglets, vous pouvez maintenant voir s'il y a des entrées spéciales, par ex. pour les adresses IP ou la passerelle standard. Si vous voulez que toutes les valeurs soient attribuées par le serveur DHCP, effacez uniquement les entrées correspondantes.

Priorité pour l'ordinateur au poste de travail – Ecraser l'allocation

Au cas où un ordinateur au poste de travail utiliserait d'autres paramètres que ceux qui lui ont été attribués (par ex. une autre passerelle standard), ceci doit être défini directement au niveau de l'ordinateur au poste de travail. Celui-ci ne tient alors pas compte des paramètres correspondants provenant de l'allocation par le serveur DHCP.

Sous Windows, cela se fait par ex. par les propriétés du voisinage réseau.

Cliquez sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau**. Sélectionnez l'entrée pour 'TCP/IP' au niveau de votre adaptateur de réseau et ouvrez les **Propriétés**.

Sur les différents onglets, vous pouvez maintenant indiquer les valeurs désirées.

Dans le module DHCP on peut vérifier (ou consulter) l'allocation des adresses IP aux ordinateurs aux postes de travail respectives à l'aide de la commande 'Setup/Module DHCP/Table-DCHP'. Ce tableau indique l'adresse IP attribuée, l'adresse MAC, la période de validité, le nom de l'ordinateur au poste de travail (s'il y en a un), ainsi que le type d'allocation d'adresse.

Dans la zone 'Type', on peut voir de quelle manière l'adresse a été attribuée. Cette zone peut prendre les valeurs suivantes :

- new
L'ordinateur au poste de travail a fait une première demande. Le serveur DHCP vérifie si l'adresse qui doit être attribuée à l'ordinateur est sans ambiguïté.
- unkn.
Lors de ce contrôle, il s'est avéré que l'adresse avait déjà été attribuée à un autre ordinateur. Le serveur DHCP n'a malheureusement pas la possibilité d'obtenir des informations supplémentaires concernant cet ordinateur.
- stat.
Un ordinateur a communiqué au serveur DHCP qu'il possédait une adresse IP définie. Cette adresse ne peut plus être utilisée.
- dyn.
Le serveur DHCP a attribué une adresse à l'ordinateur.

Configuration du serveur DHCP

Pour la configuration en tant que serveur DHCP, il y a fondamentalement deux situations de départ :

- Jusqu'à maintenant, vous n'aviez pas installé de réseau ou bien votre réseau local n'utilise pas TCP/IP. Grâce au serveur DHCP dans votre nouveau périphérique ELSA, vous pouvez d'un coup attribuer des adresses IP à tous les ordinateurs du réseau et au périphérique lui-même.
- Vous avez déjà utilisé un réseau avec TCP/IP, mais sans serveur DHCP, et passez maintenant au DHCP.

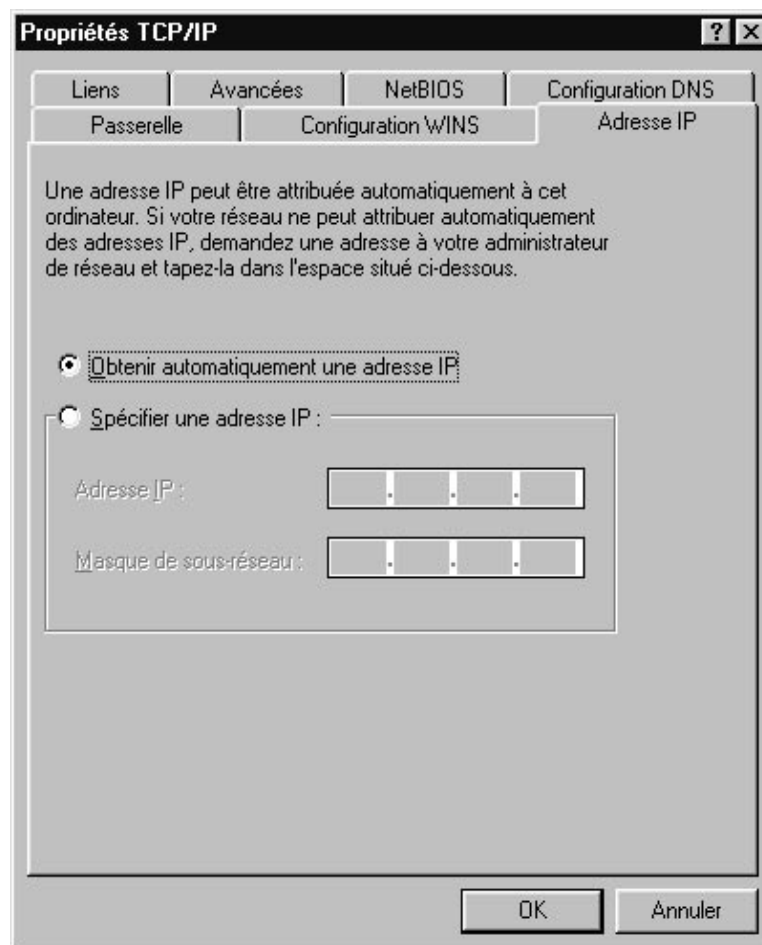
Configuration avec *ELSA LANconfig* et les assistants

Dans ces deux cas, l'*ELSA LANconfig* vous aide par un assistant à définir les paramètres nécessaires :

- ① Connectez le routeur non configuré avec votre réseau local par le câble de réseau. Lorsque vous connectez le périphérique sur un hub, le commutateur node/hub doit se trouver sur 'Node'. En revanche, si vous connectez directement le routeur sur la carte réseau d'un ordinateur du réseau, le commutateur node/hub doit se trouver en position 'Hub'.
- ② Mettez le routeur sous tension. Le routeur ne trouve pour commencer aucun autre serveur DHCP sur le réseau et active ses propres fonctions DHCP.
- ③ Si rien ne se produit, installez le protocole 'TCP/IP' sur tous les ordinateurs du réseau local.

- Lors de l'installation du protocole, les ordinateurs sont généralement réglés de manière standard de façon à aller chercher automatiquement l'adresse IP sur un serveur DHCP. Suite à un redémarrage dans le cadre de cette installation, les ordinateurs font automatiquement une demande d'adresse IP auprès du serveur DHCP.
- Si vous avez déjà installé le protocole, activez la fonction DHCP sur tous les ordinateurs sur le réseau local. Sous Windows 95 par ex., ouvrez pour cela la fenêtre de configuration des propriétés du réseau en cliquant sur **Démarrer** ► **Paramètres** ► **Panneau de configuration** ► **Réseau**. Double-cliquez sur l'entrée pour protocole 'TCP/IP'.

Activez l'option 'Obtenir automatiquement une adresse IP'. Passez à l'onglet 'Configuration DNS' et effacez toutes les adresses DNS existantes. Effacez ensuite sur l'onglet 'Passerelle' toutes les entrées éventuelles, puis fermez toutes les fenêtres avec **OK**. Après un redémarrage dans le cadre de ce paramétrage, les ordinateurs font automatiquement une demande d'adresse IP auprès du pool d'adresses du serveur DHCP.



- ④ Installez *ELSA LANconfig* sur l'un des ordinateurs du réseau.

- ⑤ Démarrez le programme dans le groupe de programmes 'ELSAIan'. Au démarrage, *ELSA LANconfig* remarque qu'il y a un routeur non configuré sur le réseau et démarre l'assistant de paramétrage par défaut.
- Si vous n'avez encore utilisé aucune adresse IP sur votre réseau, sélectionnez dans cet assistant l'option 'Effectuer tous les réglages automatiquement' puis confirmez dans la fenêtre suivante avec le bouton **Exécuter**.
L'assistant attribue alors au routeur l'adresse IP '10.0.0.1' avec le masque de réseau '255.255.255.0' et met le serveur DHCP en marche. A partir de l'adresse IP, le périphérique détermine le pool d'adresses pour l'allocation du DHCP.
 - Si, avant de passer sur le DHCP, vous aviez déjà utilisé des adresses IP sur votre réseau, sélectionnez dans cet assistant l'option 'Je veux effectuer les réglages moi-même'. Indiquez dans la fenêtre suivante une adresse IP libre provenant de la tranche d'adresses utilisée auparavant et mettez le serveur DHCP en marche. L'assistant attribue au périphérique l'adresse IP définie avec le masque de réseau correspondant. A partir de l'adresse IP, le périphérique détermine le pool d'adresses pour l'allocation du DHCP.
 - Au bout de quelques secondes, tous les ordinateurs sur réseau font l'objet d'un contrôle et se voient attribuer une nouvelle adresse IP du serveur DHCP le cas échéant. De plus, les ordinateurs reçoivent les autres paramètres tels qu'une adresse de forme de messages diffusés, un serveur DNS, une passerelle par défaut etc.

Configuration manuelle

Si la configuration au moyen de l'assistant de *ELSA LANconfig* est hors de question pour vous, vous pourrez configurer les paramètres pour le serveur DHCP manuellement dans l'onglet 'DHCP' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou dans le menu /Setup/Module DHCP).

Appendice

Caractéristiques techniques

Bande de fréquences	2400–2483,5 MHz (ISM)
Taux de transmission de données	2 Mbit/s (avec possibilité de commutation sur 1 Mbit/s, Automatic Rate Selection)
Portée	jusqu'à 300 mètres en espace libre, env. 30 mètres en bâtiment clos (portées typiques)
Taux d'erreurs de bits	Meilleur que 10 ⁻⁵
Norme	IEEE 802.11, DSSS (Direct Sequence Spread Spectrum)
Systèmes d'exploitation	Windows 95, Windows 98, Windows NT 4.0, Windows 2000, Windows CE (en préparation.)
Protocoles de réseau	Transmission de protocoles de réseau quelconques entre WLAN et LAN par Bridge
Connexions:	10Base-T, Power
Contenu du coffret :	Documentation détaillée en allemand, anglais, français et italien Câble de réseau, logiciel de configuration
Service	Garantie : 6 ans
Support :	Par Hotline et Internet

Canaux radio

En utilisant DSSS, la largeur de chacun des 14 canaux radio pouvant être réglés pour un réseau radio est de 22 MHz. Ceci permet d'obtenir au maximum trois canaux indépendants dans la bande de fréquence ISM. Le tableau donne la valeur de la fréquence moyenne et indique quels canaux sont autorisés dans quels pays.

	Canal N°	Fréquence moyenne [MHz]	UE (ETSI)	Espagne	France
1ère bande radio canal 3	1	2412	X		
	2	2417	X		
	3	2422	X		
	4	2427	X		
	5	2432	X		
2ème bande radio canal 8	6	2437	X		
	7	2442	X		
	8	2447	X		
	9	2452	X		
	10	2457	X	X	X
3ème bande radio canal 13	11	2462	X	X	X
	12	2467	X		X
	13	2472	X		X
	14	2484			

Conditions générales de garantie du 01.06.1998

Nous accordons ces conditions générales de garantie d'ELSA AG du 01.06.1998 aux acheteurs de produits ELSA. Elle complète le droit à la garantie défini par la loi, sous réserve des conditions suivantes :

1 Objet de la garantie

- a) La garantie s'applique au produit livré et à ses composants. Les composants présentant des vices de fabrication ou de matière seront, au choix, remplacés ou réparés gratuitement à condition qu'ils aient été manipulés correctement et que le mode d'emploi ait été respecté. En guise d'alternative, nous nous réservons le droit de remplacer l'appareil défectueux par son successeur ou de rembourser à l'acheteur le prix d'achat original contre la restitution du produit défectueux. Les manuels et logiciels éventuellement fournis avec le matériel sont exclus de la garantie.
- b) Les coûts des pièces et de main d'oeuvre sont à la charge d'ELSA AG ; les frais de l'envoi du matériel défectueux à l'atelier de maintenance et/ou à ELSA sont à la charge de l'acquéreur.
- c) La propriété des pièces remplacées est transférée à ELSA AG.
- d) Au-delà de la réparation et du remplacement des pièces défectueuses, ELSA AG est autorisée à effectuer des modifications techniques (par exemple une mise à jour des micrologiciels) pour mettre l'appareil au niveau technologique actuel. Ceci n'entraîne pas de frais supplémentaires pour l'acquéreur. La mise à niveau ne constitue pas pour autant un droit légitime de l'acquéreur.

2 Durée de la garantie

La durée de la garantie accordée sur les produits ELSA est de six ans, à l'exception des moniteurs couleur ELSA et des systèmes de visioconférence ELSA qui sont garantis pendant trois ans. La garantie prend effet le jour de la livraison du produit par le revendeur agréé ELSA. Les prestations fournies dans le cadre de la garantie ne conduisent aucunement à un prolongement de la durée de la garantie, et n'engendrent pas non plus une nouvelle garantie. La durée de garantie des pièces de rechange utilisée expire en même temps que la garantie du produit entier.

3 Modalités

- a) Si des défauts surviennent pendant la période de garantie, l'acquéreur doit faire valoir son droit de garantie immédiatement, au plus tard 7 jours après l'apparition du défaut.
- b) Toute avarie de transport reconnaissable de l'extérieur (par exemple boîtier endommagé) survenu lors du transport doit être signalé immédiatement à l'entreprise de transport et à ELSA AG. Tout endommagement non décelable de l'extérieur doit être signalé immédiatement après constatation, au plus tard 7 jours après la livraison et par écrit à l'entreprise de transport et à ELSA AG.
- c) Le transport du produit défectueux vers et depuis le service traitant les droits de garantie et/ou échangeant l'appareil après réparation s'effectue aux frais et aux risques de l'acquéreur.
- d) Les revendications dans le cadre de la garantie ne sont acceptées que si la facture d'origine accompagne l'appareil.

4 Application de la garantie

La garantie est exclue dans les cas suivants :

- a) en cas d'endommagement ou de destruction dans le cas de force majeure ou d'une autre influence hors du contrôle d'ELSA AG (par ex. humidité, foudre, poussière ou autres influences extérieures) ;
- b) en cas de stockage ou d'utilisation du produit non conforme aux conditions indiquées dans les spécifications techniques ;

- c) si les défauts sont dus à une mauvaise utilisation, en particulier si la description du système et le mode d'emploi n'ont pas été respectés ;
- d) si l'appareil a été ouvert, réparé ou modifié par une personne non autorisée ;
- e) si le produit présente des endommagements mécaniques, de quelque nature qu'ils soient ;
- f) si des défauts constatés sur le tube cathodique d'un écran ELSA ont été causés en particulier par des contraintes mécaniques (déplacement du masque du tube cathodique suite à un choc, ou dégradation du corps en verre), des champs magnétiques puissants dans l'environnement immédiat (taches de couleur sur l'écran), image unique et fixe (brûlure des luminophores) ;
- g) si et dans la mesure où la luminance du rétro-éclairage des écrans TFT diminue progressivement au cours du temps ;
- h) si l'acquéreur ne fait pas valoir son droit de garantie dans les délais prévus par les articles 3a) ou 3b).

5 Erreurs de manipulation

S'il s'avère que le défaut du produit a été provoqué par du matériel défectueux d'un autre constructeur, par une erreur de logiciel, par une mauvaise installation ou manipulation, nous nous réservons le droit de facturer les frais de vérification à l'acquéreur.

6 Conditions complémentaires

- a) En dehors des conditions mentionnées, l'acquéreur n'aura aucun recours envers ELSA AG.
- b) Cette garantie n'établit aucun droit supplémentaire, en particulier le droit à réhabilitation ou la prétention à diminution. Toute réclamation de dommages-intérêts, quelle qu'en soit la raison, est exclue. Cette garantie ne limite pas les droits de l'acquéreur conformément aux lois sur la responsabilité produit, par exemple dans les cas de dommages corporels ou d'endommagement des objets personnels ou dans les cas de préméditation ou de négligence grossière, dans lesquels ELSA AG engage impérativement sa responsabilité.
- c) En particulier, le remboursement d'un manque à gagner ou de dommages directs ou indirects sont exclus.
- d) Nous n'engageons aucune responsabilité pour la perte de données ou la récupération de ces données en cas de faute légère ou moyenne.
- e) Dans les cas où nous provoquons la destruction de données avec préméditation ou par négligence grossière, nous engageons notre responsabilité pour le rétablissement typique tel qu'il serait à réaliser en cas de création régulière de copies de sauvegarde selon les mesures de sécurité adéquates.
- f) La garantie s'applique uniquement au premier acheteur et ne peut être transférée à un tiers.
- g) Pour toute contestation le tribunal d'Aix-la-Chapelle (Aachen) est seul compétent, si l'acquéreur a la qualité de commerçant et en a tous les droits et obligations. Si l'acquéreur n'a pas d'attribution de juridiction en R.F.A. ou si son domicile ou son lieu de résidence habituel est transféré en dehors du champ d'application territorial de la R.F.A. après la conclusion du contrat, le tribunal de notre siège social est seul compétent. Ceci est valable également si le domicile ou le lieu de résidence habituel de l'acheteur n'est pas connu au moment de l'introduction d'une action.
- h) La loi applicable est la loi de la République Fédérale d'Allemagne. Le droit de l'ONU en matière d'achat n'est pas applicable.

Déclaration de conformité



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: 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

Index

■ Numerics

10BASE-T	R-29
802.11	5

■ A

Access-list	R-31
address pool	R-34
Adresse d'arrivée	26
Adresse de départ	26
Adresse IP	10, 13
Adresses IP	6
Affectation des adresses	14
Affichage de l'état	6
Antenne	7
Apple Talk	R-6
ARP cache	R-32
ARP-aging-minute(s)	R-32
Assemblage	22
auto mode	R-34
Automode	25

■ B

Bande de fréquence	22
Blocage	24
Boot system	R-40
Bridging	5
Broadcast address	R-8
Broadcast transfer	R-11
Buffers	R-29, R-38

■ C

Câble de raccordement au réseau local	7
Cable network	R-7
cache	R-32
Canal radio	22
Caractéristiques techniques	33
Carte PC	7
Carte réseau sans fil	2, 5
Carte réseau-radio	7
Cells	R-4
Cellule radio	2

charger le logiciel	16
Config-aging-minute(s)	R-36
Configuration	6
Instructions	15
SNMP	18
configuration options	R-36
Connect	R-29
Connecteur Ethernet	2
Connexion à un réseau local	5
Contenu du coffret	7
Contrôle des accès	24

■ D

Data packet	R-4
DHCP	6, 24, R-34
DHCP server	R-34
DHCP-Automode	25
DHCP-Server	10
Direct Sequence Spread Spectrum	5
DNS	R-31
DNS forwarding	R-32
DNS-backup-IP-address	R-32
Domaine WLAN	22
DSSS	5, 22
Durée de validité	25, 27
Dynamic Host Configuration Protocol	24

■ E

ELSA protocol	R-28
End-address-pool	R-34
Etat à la livraison	9
Ethernet	5
10Base-T	5
Ethernet 10-Mbit	7
Evolutivité	4

■ F

FirmSafe	6, 16
firmsafe	R-39
Firmware	R-38
Firmware-upload	R-38

Force brute 23
 Fragmentation 22

G

Gestion d'adresses 24

H

Heap-Reserve R-29
 hierarchical IP addresses R-9
 Host R-4

I

IANA R-8
 Identification R-28
 Inband
 avec Telnet 15
 Voraussetzungen 13
 Installation 4
 Interface R-4
 Internet R-6
 Internetwork R-6
 Intranet R-30
 IP address R-30
 IP addresses R-7
 IP network R-6
 IPX R-6
 ISDN network R-7
 ISDN time R-19
 ISM 5

L

LAN 2, R-6, R-11
 LANconfig 6, 10, 13, 14, 17, 21
 LAN-configuration R-36
 Language R-37
 Largeur de bande 5
 LED
 LAN-Collision 9
 LAN-Status 9
 Power/Msg 8
 liste d'accès IP 13
 Local Area Network 2, R-6
 local network R-6
 location R-29
 Lock-minutes R-37

Login 17
 log-in block R-37
 Login-errors R-37

M

MAC R-11
 MAC address R-29, R-38
 MAC addresses R-12
 MAC protocol R-12
 Médias en ligne 13
 Medium R-4
 Medium Access Control R-11
 Mémoire Flash-ROM 6
 Mémoire-ROM-Speicher 16
 Méthode DSSS 5
 Mise à jour des micrologiciels 6
 Modes d'exploitation 21
 Mot de passe 22
 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
 Netzteil 7
 Node-ID R-29
 Norme IEEE 802.11 5

O

Operating R-30
 Other R-40

P

Packet R-4
 Parasitage 5

Passerelle 24, 27
 password R-31
 Password-required R-36
 physical medium R-4
 Point-to-multipoint connection R-5
 point-to-point connection R-4
 Pool d'adresses 26, 31
 Port 10-Base-T 7
 Private address spaces R-8
 Protection 23
 Protection contre les parasites 5
 Protection par mot de passe 23
 Protocol R-6

R

Rayon d'action 4, 5
 registered IP address R-8
 Réseau ad-hoc 3
 Réseau d'infrastructure 3
 Réseau Peer-to-LAN 3
 Réseau Peer-to-Peer 3
 Réseau sans fil 2, 21
 Reset system R-40
 Router R-4
 Routing R-9
 Routing table R-9

S

Sécurité 23
 Serveur DHCP 14, 25
 Configuration 29
 Serveur DNS 24, 27
 Serveur NBNS 24, 27
 Setup
 DHCP-module R-34
 LAN-module R-29
 TCP-IP-module R-30
 Shared Medium R-11
 Shared medium R-6
 SNMP 18, R-33
 Start-address-pool R-34
 Station de base 2, 7
 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
 Subnet R-9
 System-administrator R-33
 System-location R-33

T

Table-ARP R-32
 Taille des paquets 22
 TCP max. connections R-32
 TCP/IP 10, 13, R-6
 TCP/IP stack R-6
 TCP-aging-minute(s) R-32
 Téléchargement 6, 16
 Téléchargement de micrologiciel
 avec LANconfig 17
 Téléchargement du micrologiciel 17
 avec TFTP 18
 Telnet 6, 12
 Telnet server R-31
 Témoins lumineux 6, 8
 Tentatives d'accès 23
 TFTP 13
 TFTP server R-31
 Time R-19
 Timeout R-35
 Touche Reset 9
 Trap-IP R-33
 Traps-active R-33

U

Upload-system R-40

V

Verrouillage d'accès 23
 Version-table R-38

W

WAN-configuration R-36
 winipcfg 11

wire	R-4	Wireless links	R-4
Wireless LAN	2	WLAN	2, 21

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.

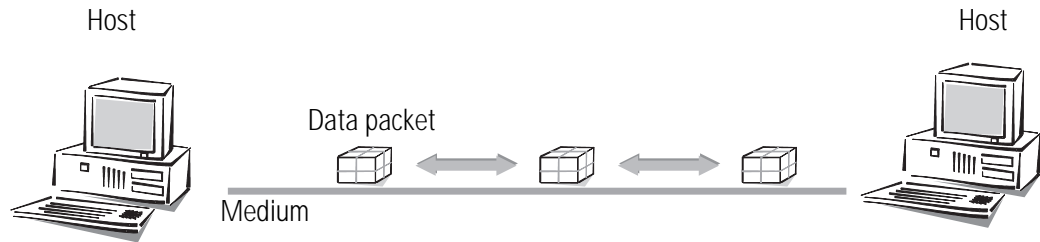
Router

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.

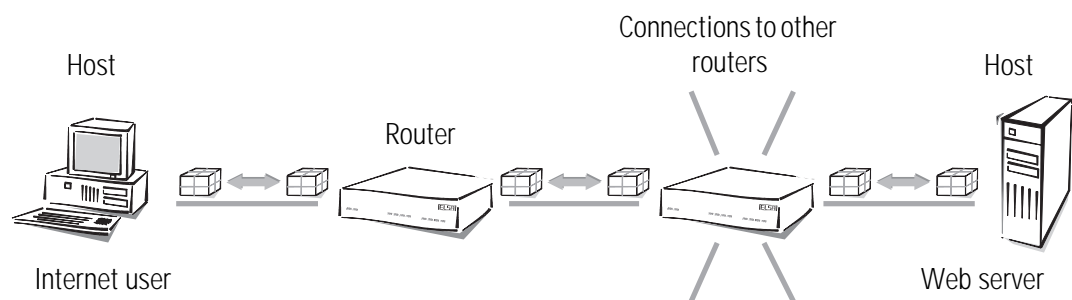
Connection modes

*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).



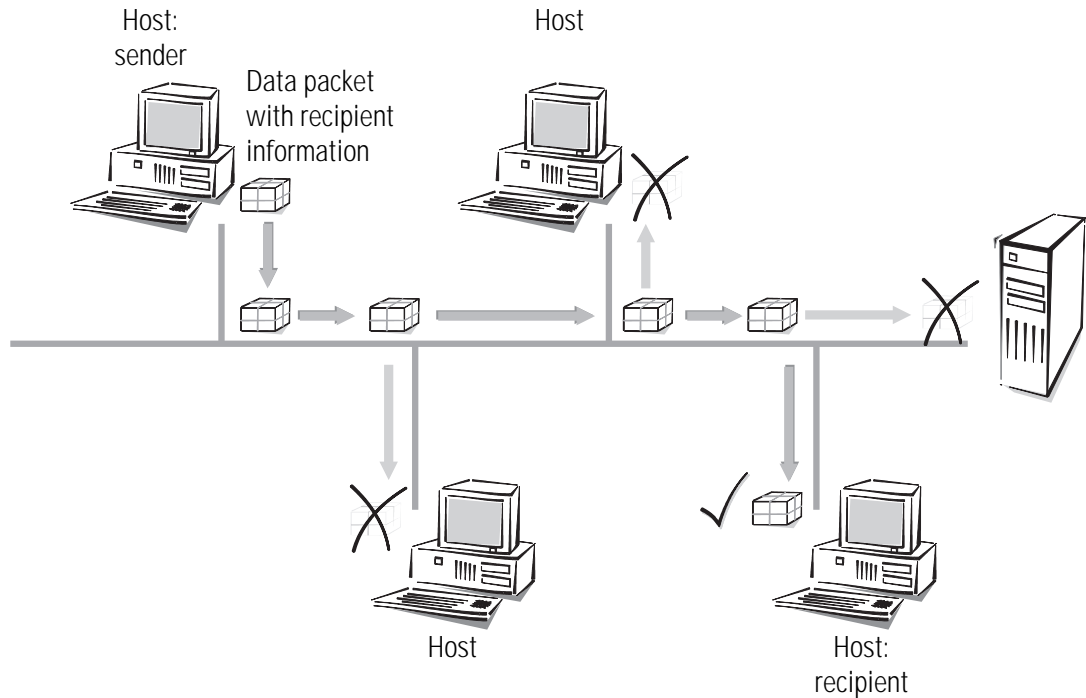
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers 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

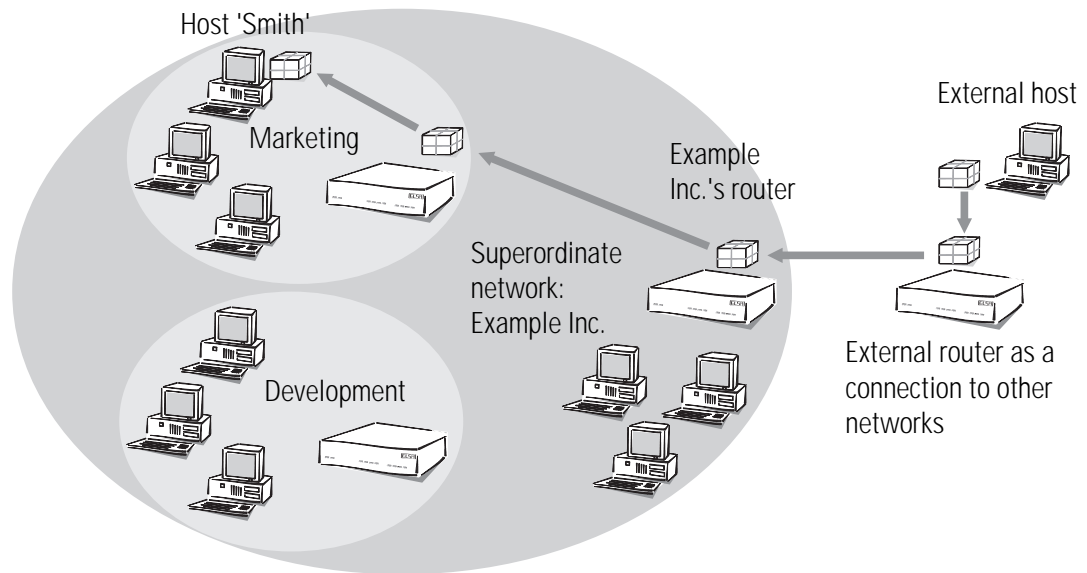
Routing method Every IP packet contains the IP addresses of the source and of the recipient. A router receives IP packets at its interface, interprets the destination address and passes the packets on to those interfaces that are nearest to the recipient. Finding the appropriate path is called routing.

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.

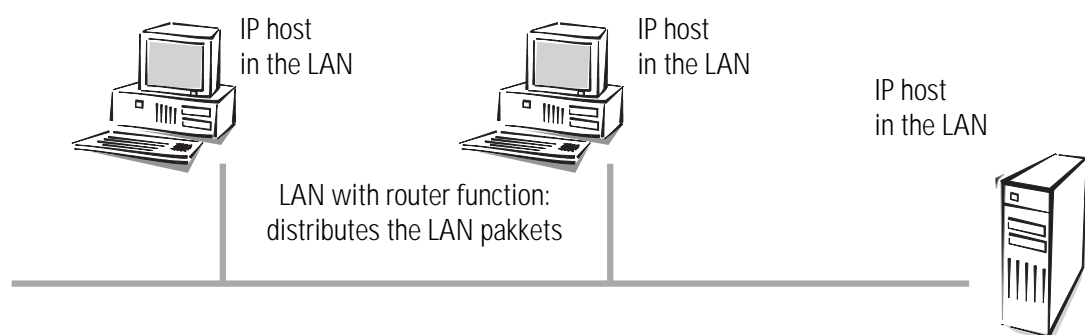
MAC-address Specific LAN addresses hardwired into the interfaces by their manufacturers are used to manage the transfer in the LAN. Since the LAN addresses are used for communication via the MAC protocol, they are called MAC addresses. They can be thought of as the fingerprint of the interface hardware. 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).

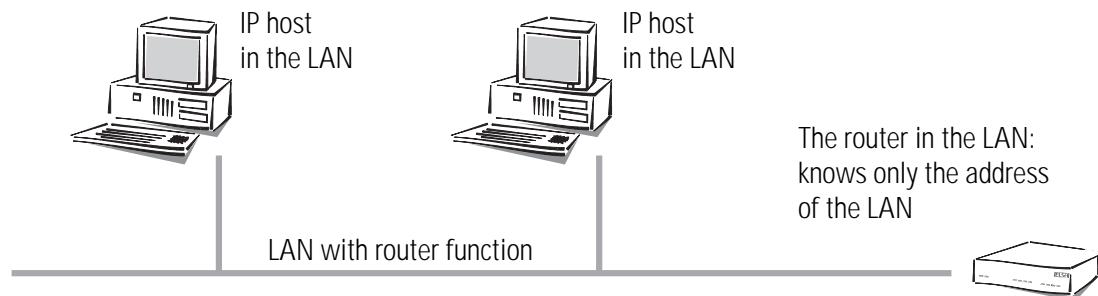
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts gives the packets to the LAN which handles the further distribution of the data packet. This is why only IP addresses from the numerical space of the specific network should be used for the internal communication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

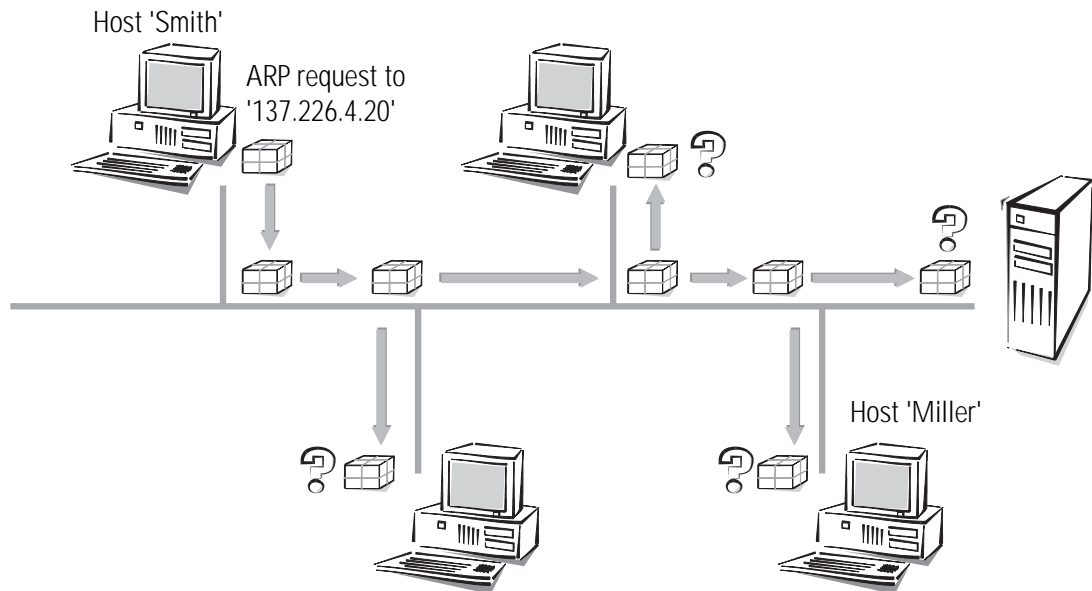
Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). Using the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located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

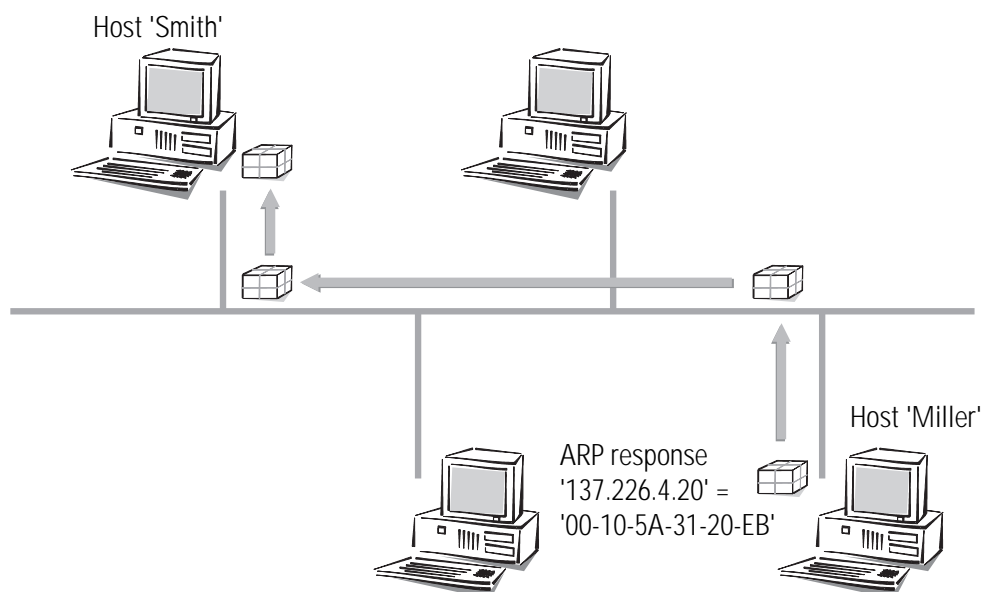
ARP

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
DHCP-statistics		Statistics from the DHCP 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
DHCP-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.

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

TCP-IP-module		TCP/IP module settings
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).

If both an IP address and an Intranet address have been entered, the network defined by an IP address and IP network mask must contain only workstations (i.e. no routers).

Access-list

The access to “internal functions” of the router may be controlled by an access list in TCP/IP applications.

The configuration data of the device are protected by a password, however this is always transferred in plain text, making it possible in principle to detect it and for any computer to read the configuration or to delete it. In order to prevent this from happening, the access list can be used to determine which computers or which networks can access the configuration.

For reasons of consistency, the access control is based on all “internal functions” of the router. The term “internal functions” refers to the following:

- Telnet server: the configuration interface based on the Telnet protocol
- TFTP server: the configuration interface based on the TFTP protocol
- SNMP: the configuration interface based on the SNMP

Each of the maximum of 16 entries in the access list has the following structure:

IP-address	IP netmask
IP address of the authorized user (or user circle)	IP network mask of the user circle

Once an IP workstation with its IP address and the network mask 255.255.255.255 is entered into the list, the internal functions of the router can only be accessed from this computer. Any requests from devices with different IP addresses are ignored.

If a complete network has access enabled to an *ELSA LANCOM*, this can be done as follows for a class C network:

IP-address	IP netmask
192.234.222.0	255.255.255.0

With this entry all IP addresses in the class C network 192.234.222.0 are authorized to use internal functions of the router.

DNS-default

The entry **DNS** (Domain Name Server) is required to announce the name server responsible for their own network for computers that have direct access via PPP to the router.

If the router is configured for access to the Internet via an Internet Service Provider, the DNS server is usually given by the provider. There are then two possible settings in the router:

- '0.0.0.0' is entered as the address of the DNS server. All computers in the local network can then use the provider's DNS server.
- The router's own IP address is entered as the DNS server. Then he uses the DNS information from the provider not only for its own local network but also forwards this information (DNS forwarding). Remote stations such as computers that dial in via remote access can then also access the provider's DNS server. This procedure is also referred to as DNS forwarding.

DNS-backup With the entry **DNS-Backup** a second name server can be named, which is used if the DNS fails.

NBNS-default The entry **NBNS-default** (NetBIOS Name Server) is required to announce the NBNS responsible for their own network for computers that have direct access via PPP to the router.

NBNS With the entry **NBNS-Backup** a second name server can be named, which is used if the NBNS fails.

Table-ARP This option allows you to display the ARP table (ARP cache), which is managed automatically for the purpose of mapping IP addresses onto physical terminal addresses. Individual entries can be removed from this table but no new entries can be entered manually.

The entries in the ARP table might, for example, have the following appearance if different devices with different IP addresses (192.168.139.20, 192.168.130.30) communicated with the router:

IP-address	Node-ID	Last-access	Connect
192.168.130.20	0000c0717860	6780443 tics	local
192.168.130.30	0800091eebf4	6214514 tics	local








ARP-aging-min. This option allows you to enter a time (from 1 to 99 minutes) at the end of which the ARP table is automatically updated, i.e. all IP addresses that have not been accessed since the last automatic update are removed. The default setting is 15 minutes.

TCP-aging-min. If data transfer stops during a TCP connection to the router, e.g. if the user does not enter any more data during the remote configuration, it will automatically release the TCP connection on expiry of the time entered here. Possible settings are from 1 to 99 minutes; The default setting is 15 minutes.

TCP-max.-conn. The maximum number of allowable connections possible at the same time can be set here. DEFAULT setting is '0', meaning the same as "any number".

Setup/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	<input type="checkbox"/>	Switch for configuring from the LAN side
WAN-config	<input type="checkbox"/>	Switch for configuring from the WAN side
Password-required	<input type="checkbox"/>	Password required on/off if there is no password
Farconfig-(EAS-MSN)	<input type="checkbox"/>	Subscriber number for remote configuration via PPP
Config-aging-minute(s)	<input type="checkbox"/>	Time limit for remote configuration connections
Login-errors	<input type="checkbox"/>	Number for failed log-in attempts before the log-in block is activated
Lock-minutes	<input type="checkbox"/>	Duration of block and period until old log-in errors are forgotten.
Language	<input type="checkbox"/>	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.

Protocol-list		<p>This list permits data packets to be blocked or permitted (depending on the positive/negative setting of the switch) on the basis of their protocol.</p> <p>Every Ethernet frame contains a 16-bit identifier stating the Layer-3 protocol of its data. These can be entered in the list as hexadecimal numbers.</p> <p>Common protocols include:</p> <p>0800 = IP 0806 = IP/ARP 8137 = IPX F0F0, E0E0 = IPX</p> <p><i>In this case as well, traffic is blocked between WLAN stations and the LAN or WAN, but not between the WLAN stations themselves. See protocol table in the Appendix</i></p>
Protocol mode		Positive/negative switch for the protocol list
Node ID		MAC layer address of the device
Spare-heap		Buffers that receive data packets from the local network

Firmware

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

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

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

Ifc	Module	Version	Serial number
Ifc	LANCOM Wireless 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 Protocols

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
nbdagaram	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
rvd-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

