

# ***ELSA LANCOM™ Wireless IL-2***

**Manuel**

© 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 décline toute responsabilité pour des inexactitudes et/ou manques techniques.

ELSA AG

Sonnenweg 11

52070 Aix-la-Chapelle

Allemagne

[www.elsa.com](http://www.elsa.com)

Aachen, octobre 1999

N° de réf. 20943/1099

# Avant-propos

## Merci de votre confiance !

Les réseaux sans fil d'ELSA sont des alternatives et compléments avantageux pour les réseaux locaux câblés (LAN). Avec des cartes de réseau mobiles, les bloc-notes et les PC peuvent communiquer entre eux ou bien avoir accès via des stations de base à des réseaux câblés et même au réseau RNIS.

Cette documentation s'adresse aux utilisateurs de la station de base *ELSA LANCOM Wireless IL-2*. Nous vous présenterons d'abord l'appareil et ses possibilités, puis vous aiderons pour son branchement et l'installation du logiciel et enfin nous vous montrerons 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, les bases techniques (p.ex. pour les réseaux sans fil, la technique de réseau, TCP/IP etc.), la partie pratique avec des exemples détaillés d'application, la partie référence à consulter avec une description détaillée 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'utilisation de votre produit ELSA.



*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](http://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-ROM. Pour cela, démarrez le fichier `Misc\Support\MISC\ELSA\SIDE\index.htm`*



# Contenu

<b>Introduction .....</b>	<b>1</b>
Principe de fonctionnement d'un réseau local sans fil .....	1
Avantages d' <i>ELSA LANCOM Wireless IL-2</i> .....	5
<b>Installation .....</b>	<b>11</b>
Contenu de l'emballage .....	11
<i>ELSA LANCOM Wireless</i> se présente .....	11
Comment brancher la station de base .....	13
Installation du logiciel .....	14
Configuration de base .....	14
Procéder à la configuration de base avec <i>ELSA LANconfig</i> .....	14
Réglages de base avec Telnet .....	16
<b>Configurations possibles .....</b>	<b>19</b>
Radio ou câble : chemins aboutissant à la configuration .....	19
Conditions .....	19
Alternative : gestion des adresses à l'aide du serveur DHCP .....	20
Lancement de la configuration par <i>ELSA LANconfig</i> .....	20
Lancement de la configuration par Telnet .....	21
Instructions de configuration .....	21
Nouveau microprogramme avec firmsafe .....	22
Comment fonctionne firmsafe ? .....	22
Comment charger le nouveau logiciel ? .....	23
Configuration par SNMP .....	24
<b>Fonctions et modes d'exploitation .....</b>	<b>27</b>
Paramètres de la transmission radio .....	27
La sécurité de votre configuration .....	29
Protection par mot de passe .....	29
Le verrouillage des accès .....	29
Contrôle des accès via TCP/IP .....	30
La sécurité de votre LAN .....	30
Le contrôle .....	30
Le rappel .....	32
La cachette – Masquerading IP (NAT, PAT) .....	32
Gestion des taxes téléphoniques .....	33
Limitation des communications en fonction du temps .....	33
Configuration dans le gestionnaire des coûts de communication .....	33

Connexions via RNIS.....	34
Liste des noms .....	34
Configuration des interfaces.....	35
Configuration de l'interface du routeur .....	35
Configuration de l'interface <i>LANCAPi</i> .....	36
Liste des couches.....	37
Liste RoundRobin .....	37
Liste PPP.....	38
Script.....	38
Prise d'appel.....	39
Liste des numéros .....	39
Protocole PPP .....	40
Le protocole.....	40
La liste PPP.....	41
Tout est bon? Vérification de la ligne avec LCP .....	42
Routage IPX.....	43
Le tableau de routage IP .....	43
Filtrage des paquets TCP/IP .....	44
Proxy-ARP.....	45
Routage local .....	45
Routage dynamique avec IP-RIP .....	46
IP masquerading (NAT, PAT).....	48
Routage par DNS .....	49
Policy Based Routing : routage stratégique.....	50
Gestion d'adresses automatique via DHCP .....	50
Le serveur DHCP.....	50
DHCP – 'actif', 'inactif' ou 'auto' ? .....	51
Attribution des adresses.....	51
Configuration du serveur DHCP .....	54
DNS.....	57
Que fait un serveur DNS? .....	57
Configurer le serveur DNS .....	58
Proxy NetBIOS.....	60
En quelques mots : définition de NetBIOS .....	61
Traitement des paquets NetBIOS .....	61
Quelles sont les conditions requises ? .....	62
Interconnecter deux réseaux Windows via le RNIS .....	65
Accès par les ordinateurs distants .....	66
Qui cherche trouve : l'environnement réseau.....	67
Bureautique et <i>ELSA LANCAPI</i> .....	68
<i>ELSA LANCAPI</i> .....	68
Le rerouteur téléphonique (least-cost router).....	72

<b>Appendice .....</b>	<b>79</b>
Caractéristiques techniques .....	79
Spécifications matérielles .....	79
Spécifications logicielles .....	79
Canaux radio .....	80
Conditions générales de garantie du 01.06.1998.....	82
Déclaration de conformité .....	84
<b>Index .....</b>	<b>87</b>
<b>Technical basics (on CD only).....</b>	<b>R1</b>
Wireless network according to the IEEE-802.11 standard.....	R1
Ad hoc mode .....	R1
Infrastructure mode.....	R2
Interchangeability with other devices .....	R3
Network technology.....	R4
The network and its components.....	R4
Connection modes.....	R4
Kinds of networks .....	R6
IP addressing.....	R6
IP routing and hierarchical IP addressing .....	R9
Expansion through local networks.....	R11
<b>Description of the menu options (on CD only) .....</b>	<b>R17</b>
Status .....	R19
Status/Connection-state .....	R20
Status/Current-time .....	R20
Status/Operating-time .....	R20
Status/SO-bus .....	R20
Status/WLAN-statistics.....	R21
Status/WAN-statistics.....	R22
Status/LAN-statistics.....	R25
Status/PPP-statistics.....	R26
Status/TCP-IP-statistics .....	R32
Status/IP-router-statistics.....	R38
Status/Config-statistics .....	R40
Status/Queue-statistics .....	R41
Status/Connection-statistics .....	R42
Status/Info-connection .....	R43
Status/Layer-connection.....	R43
Status/Call-info-table .....	R44
Status/Remote-statistics .....	R44
Status/Channel-statistics .....	R45
Status/Time-statistics.....	R46

Status/LCR-statistics .....	R47
Status/PCMCIA-status .....	R47
Status/Delete-values .....	R47
Setup .....	R48
Setup/WAN-module .....	R49
Setup/LAN-module .....	R58
Setup/TCP-IP-module .....	R59
Setup/IP-router-module .....	R62
Setup/SNMP-module .....	R70
Setup/DHCP-server-module .....	R71
Setup/NetBIOS .....	R73
Setup/Config-module .....	R76
Setup/LANCAP-module .....	R77
Setup/WLAN-module .....	R78
Setup/LCR-module .....	R79
Setup/DNS module .....	R80
Setup/Time-module .....	R82
Firmware .....	R82
Other .....	R84



<b>Ports and protocols(on CD only) .....</b>	<b>R85</b>
Ports .....	R85
Protocols .....	R87



# Introduction

Les avantages des réseaux locaux sans fil sont évidents : notebooks et PC peuvent être mis en service là où c'est pratique. Grâce cette élaboration de réseau sans fil, l'époque des problèmes causés par un manque de possibilités de raccord ou des modifications de construction est désormais révolue.

La liaison au réseau lors de conférences ou de présentations, l'accès aux ressources dans les bâtiments voisins et l'échange de données avec des terminaux mobiles ne sont que quelques-unes des possibilités d'utilisation du réseau local sans fil.

Dans un réseau câble existant, la station de base joue le rôle central. Grâce à cette station de base, toutes les stations dans le réseau sans fil ont accès au réseau local.

Le routeur IP intégré et l'interface RNIS permettent de relier votre réseau local entier au monde extérieur. L'accès à Internet pour le réseau local entier ou les fonctions de bureautique telles que l'envoi/réception de télécopies et le répondeur téléphonique à tous les postes de travail ne représentent que quelques uns des avantages offerts par le routeur RNIS.



*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.*

## 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 de  
réseau sans fil  
WLAN*

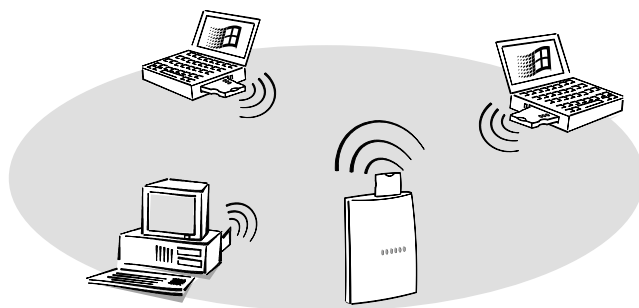
Grâce aux cartes de réseau sans fil, les notebooks et les PC peuvent être reliés dans un réseau local, également appelé **Local Area Network** (LAN). Comme dans ce réseau les câbles utilisés dans un réseau classique sont remplacés par une communication par ondes radio, il est aussi appelé **Wireless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

*Station de base*

La station de base forme le pont entre le réseau câble (LAN) et le réseau sans fil (WLAN). Equipée d'une part d'un emplacement pour une carte de 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 de réseau sans fil installée dans les terminaux mobiles peuvent communiquer avec les stations de base et réciproquement est appelée la cellule radio.

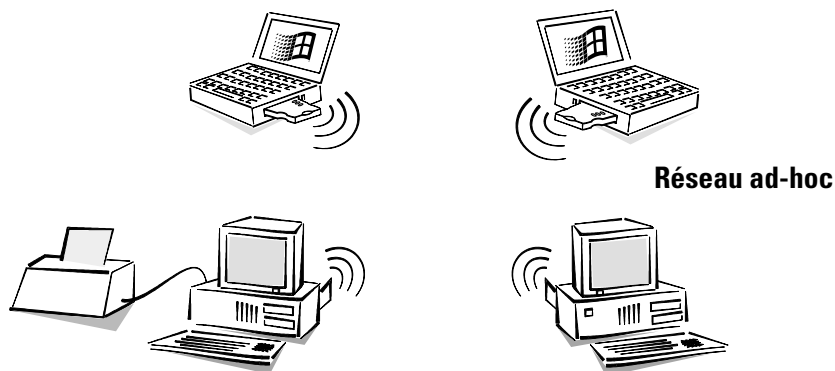


Le réseau local sans fil permet toutes les fonctions d'un réseau câblé classique : l'accès aux fichiers, au serveur, à l'imprimante etc. sont possibles tout comme la liaison des stations mobiles dans un système de courrier électronique interne de l'entreprise.

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

*Liaison directe à l'ordinateur*

Reliez avec les cartes de réseau sans fil deux ou plusieurs ordinateurs directement entre eux. Tous les ordinateurs dans un réseau local sans fil peuvent communiquer sans autre périphérique.

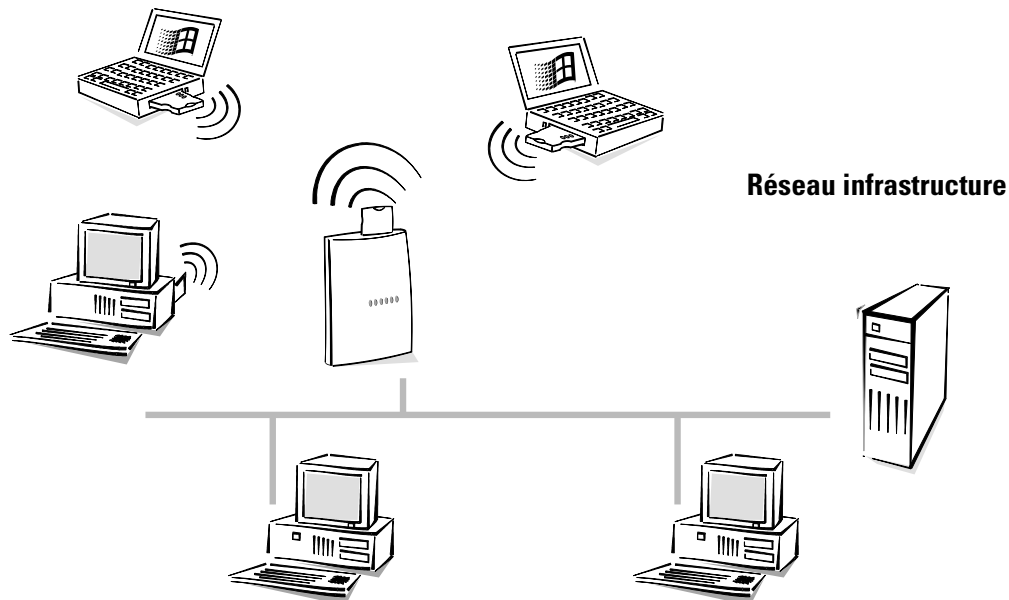
*Poste à poste*

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

*Liaison au réseau local câblé*

Par l'intermédiaire d'une station de base tous les ordinateurs avec cartes de réseau sans fil ont accès au réseau câblé. La station de base sert de liaison entre le réseau local et

le réseau sans fil ; par ailleurs elle sert de centrale de commutation pour l'échange de données à l'intérieur du réseau sans fil



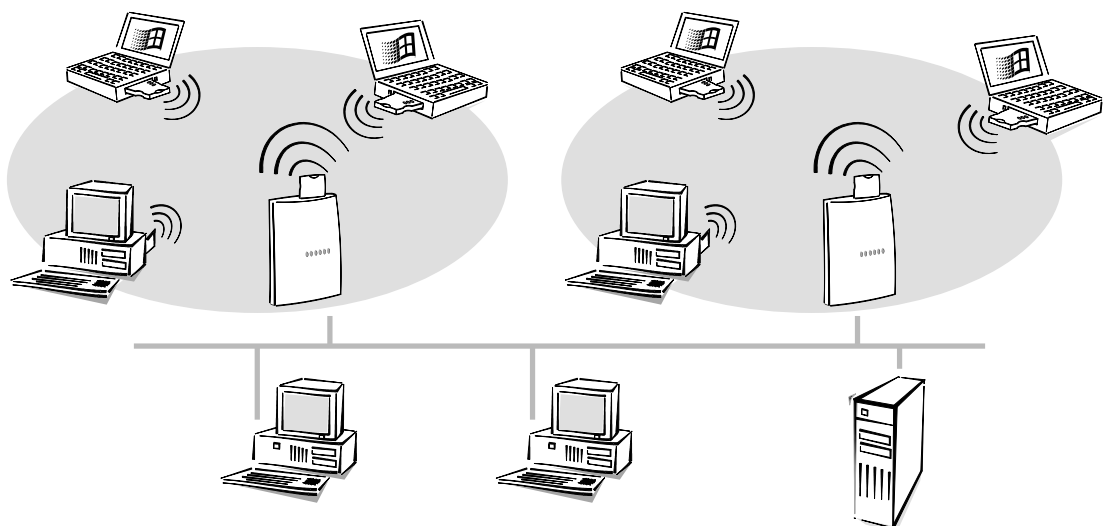
*Poste à réseau local*

Un réseau local intégrant une station de base est appelé réseau Peer-to-LAN (poste à réseau), dans le jargon du réseau sans fil on parlera de réseau d'infrastructure.

Ce type de réseau est idéal comme complément de réseaux locaux existants. Lors de l'agrandissement d'un réseau local dans des endroits où un câblage n'est pas possible ou pas rentable, le réseau infrastructure est une alternative idéale.

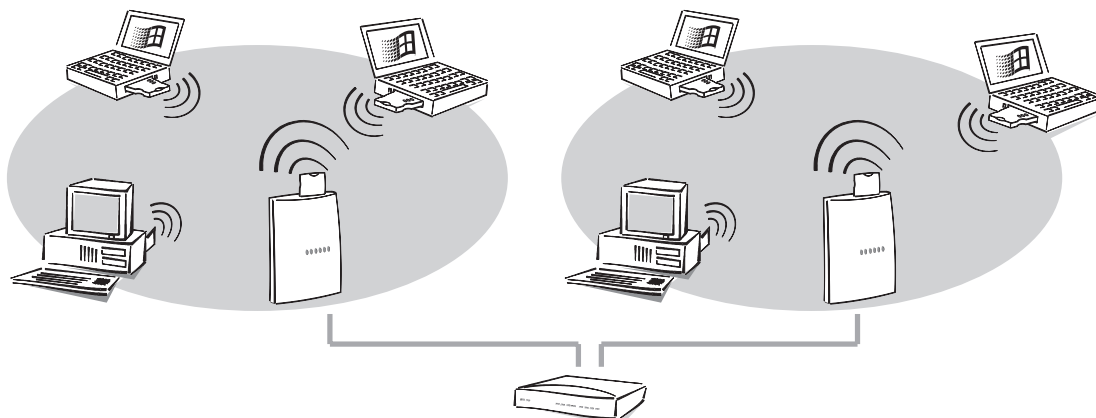
*Evolutivité*

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 câble pour palier à l'insuffisance du rayon d'action.



Ce principe fonctionne même dans le cas où l'on n'a pas de réseau câble et si l'on veut réaliser un nouveau réseau entièrement sans fil. 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 p.ex. être reliées au moyen d'un câble réseau simple et d'un concentrateur.



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 sans fil, il est possible de choisir des canaux différents (jusqu'à 14 canaux différents) pour chaque cellule.

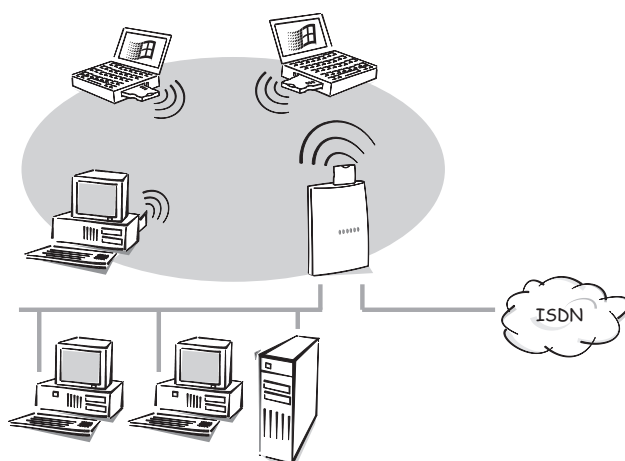
#### *Roaming*

Le roaming est le passage automatique d'un champs d'émission radio à un autre. L'utilisateur peut se déplacer d'une cellule à une autre sans perdre la connexion au réseau. Les points d'accès diffusent, constamment, de l'information aux stations validées sur le réseau sans fil.

Pour assurer un bon fonctionnement du roaming, les points d'accès doivent être connectés à un même réseau Ethernet. Entre deux points d'accès on peut utiliser des ponts, des commutateurs et des répéteurs à l'exception des routeurs.

#### *Configuration de la connexion*

La station de base *ELSA LANCOM Wireless IL-2* dispose d'une autre fonction particulière. Via l'interface RNIS, la station de base ne relie pas seulement le réseau sans fil avec le réseau câble, mais en même temps avec le réseau RNIS.



Avec les fonctionnalités d'un routeur IP, il est donc possible de réaliser d'autres applications telles que l'accès à Internet pour tous les ordinateurs dans le réseau local LAN ou dans le réseau WLAN.

## Avantages d'*ELSA LANCOM Wireless IL-2*

Pour vous donner un petit aperçu des fonctionnalités du réseau sans fil, en voici les caractéristiques essentielles :

### Simplicité d'installation

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

### Connexion à un réseau local

Les stations de base pour les réseaux sans fil d'ELSA fonctionnent dans un réseau Ethernet. Un connecteur 10Base-T et un concentrateur ou un switch permettent de relier le *ELSA LANCOM Wireless* au réseau local 10-Mbits.

### Connexion au réseau local sans fil

Les cartes de 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 de réseau sans fil de ELSA recourent à la méthode DSSS. En plus des avantages de protection contre le parasitage par les autres émetteurs utilisant éventuellement la même bande de fréquences, 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 sans fil 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 sans fil est de 2 Mbps. Le rayon d'action en plein air atteint 300 mètres, et généralement env. 30 mètres à l'intérieur de bâtiments.

### **Connexion à un réseau étendu WAN**

Le *ELSA LANCOM Wireless* est relié à l'(aux) interface(s)  $S_0$  d'un accès RNIS en configuration point-à-multipoint ou en Configuration point-à-point. Le routeur détecte automatiquement le type de votre accès et le protocole de canal D utilisé. Les liaisons commutées avec DSS1 ou 1TR6 peuvent être établies aussi bien que les liaisons spécialisées (permanentes). Les liaisons spécialisées sont une fonctionnalité supplémentaire que vous pouvez commander chez ELSA.

### **Regroupement des canaux et compression**

Sur la ligne RNIS, l'appareil prend en charge les regroupements statique et dynamique des canaux par MLPPP et BACP. La compression de données Stac (hi/fn) permet d'augmenter jusqu'à 400% le taux de transmission.

### **Bridging transparent**

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

### **Affichage de l'état**

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

### ***ELSA LANmonitor***

Sous les systèmes d'exploitation Windows, cet outil vous permet d'avoir toujours les informations sur le statut du routeur sur votre écran. Les informations les plus importantes sont toujours affichées sur chaque périphérique dans le réseau local, p.ex. :

- Etat de la liaison sur chaque canal B
- Nom du correspondant en ligne
- Module actif du périphérique (routeur, *LANCAPI*)
- Durée de communication et taux de transfert
- Extraits des statistiques du routeur (p.ex. les informations de la négociation PPP)

En outre, le logiciel permet la journalisation et l'enregistrement des messages pour l'exploitation ultérieure sur le PC.

## Contrôle des coûts de communication

Lorsque les impulsions de facturation sont communiquées pendant la transmission dans RNIS (selon AOCD), il est possible de définir une limite pour les unités de communication pendant une période donnée. Vous pouvez donc garder le contrôle de votre facture de téléphone.

Si les informations de taxation ne sont pas transmises sur votre accès RNIS, vous avez la possibilité de restreindre la durée de la communication active pour un laps de temps. Après écoulement de cette durée, le routeur ne permettra plus aucun établissement de communication propre.

## Least-cost routing

Même si le nombre d'opérateurs offrant les services de télécommunication est important, le least-cost router permet d'effectuer un appel via l'opérateur le moins cher. Vous définissez pour commencer les opérateurs ayant les tarifs les plus avantageux pour vos besoins, et le routeur fait passer chaque appel par l'opérateur le moins cher.

## Interrogation automatique de l'heure

Pour pouvoir générer des statistiques significatives et pour pouvoir sélectionner les lignes téléphoniques correctes via le least-cost router, le périphérique doit toujours savoir l'heure exacte. Il peut interroger l'heure automatiquement dans le réseau RNIS. Il compare l'heure interne avec l'heure du RNIS soit chaque fois qu'il établit une connexion soit chaque fois qu'on le met sous tension. Naturellement, il est possible de régler l'heure manuellement.

## Configuration avec *ELSA LANconfig*

Le réglage et l'adaptation des périphériques sur leur tâche spécifique s'effectuent de manière rapide et conviviale 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 WAN (via RNIS), le WLAN ou le LAN. Dans les deux premiers cas, la configuration peut se faire avec TFTP et SNMP.

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

## Protection de l'accès

En ce qui concerne la protection du réseau local contre les accès illicites, le routeur dispose naturellement de la fonction de protection par mot de passe et de l'identification du numéro de l'appelant (CLIP), et en plus de la fonction de rappel automatique en retour où c'est le routeur qui établit la liaison avec des correspondants définis au préalable. Les filtres coupe-feu et IP masquerading parachèvent le concept de sécurité. Par ailleurs, un verrou supplémentaire permet de bloquer les « attaques en force brute » : l'accès au

routeur est verrouillé après un nombre définissable de tentatives d'accès avec un mot de passe incorrect.

### **Compatibilité par PPP**

Pour communiquer avec les appareils des autres constructeurs, le routeur prend en charge entre autres PPP, un protocole très répandu utilisé pour l'échange de données dans un réseau via des liaisons point-à-point.

### **Configuration à distance via PPP**

Une particularité de la configuration des routeurs d'ELSA placés là où personne ne peut ou ne doit les paramétrer, est la configuration à distance via l'Accès réseau à distance. Pour ce, il suffit simplement de mettre sous tension le routeur, de le raccorder à l'accès RNIS et déjà vous pouvez le configurer depuis un emplacement distant en l'appelant via une connexion PPP. Lors de la première configuration, l'accès est protégé par un mot de passe contre les appels des personnes non autorisées.

### **Mise à jour des microprogrammes**

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

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

### **Firmsafe**

Vous ne courez aucun risque quand vous téléchargez le nouveau microprogramme : la fonction firmsafe permet de gérer deux fichiers de microprogramme dans un périphérique. L'utilité de cette fonction est évidente : si le nouveau microprogramme 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 (p.ex. suite à une erreur de transmission), le périphérique réutilise automatiquement la version précédente en état de fonctionner.

### ***ELSA LANCAPi et ELSA CAPI Faxmodem***

La mise en œuvre de l'interface *LANCAPi* apporte des avantages surtout économiques. *LANCAPi* est une variante spéciale de l'interface CAPI-2.0 via laquelle divers logiciels de communication (p.ex. *ELSA-RVS-COM* ou *ELSA-ZOC*) peuvent accéder au routeur par le réseau.

Toutes les stations de travail reliées au réseau local ont, via *LANCAPi*, libre accès aux fonctions de bureautique telles que le télécopieur et le transfert de fichiers. Toutes les



fonctions sont mises à disposition via le réseau sans que la station de travail ait besoin d'être dotée de matériel supplémentaire. Donc aucun achat d'adaptateurs de terminal RNIS ou de modems coûteux ne grève le budget informatique. Tout ce qu'il faut, ce sont les logiciels de communication et de bureautique à installer sur les stations de travail.

Pour l'envoi de télécopies, un télécopieur RNIS est simulé sur la station de travail. Avec l'interface *LANCAPI*, le PC envoie la télécopie au routeur via le réseau, et c'est ensuite le routeur qui établit la liaison avec le destinataire via RNIS.

En plus, avec *ELSA CAPI Faxmodem*, vous disposez sous Windows d'un pilote de télécopie (fax class 1) qui, en tant qu'interface entre *ELSA LANCAPI* et l'application, permet d'utiliser des programmes de télécopie standards en liaison avec un routeur *ELSA LANCOM Wireless*.

## 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.

## NetBIOS-Proxy

Pour l'installation de réseau Microsoft Peer-to-Peer, les routeurs ELSA présentent une caractéristique spéciale : le routage intégré de paquets IP-NetBIOS rend enfantin le couplage de deux réseaux Windows. Les correspondants avec lesquels des informations NetBIOS doivent être échangées sont inscrits dans une liste afin d'éviter que chaque paquet NetBIOS ne produise l'établissement d'une communication.

En tant que NetBIOS-Proxy, le routeur répondra localement aux demandes concernant des ordinateurs connus et évitera donc l'établissement de connexions inutiles.

## Serveur DNS

Les fonctions de serveur DNS du routeur permettent de créer des liens entre les adresses IP et les noms d'ordinateurs ou des réseaux. Lorsqu'une requête est formulée pour un nom d'ordinateur connu, la route correcte peut être attribuée directement.

Le serveur DNS pourra reprendre les noms et les IP du serveur DHCP et du module NetBIOS.

Le serveur pourra également servir aux utilisateurs de filtre efficace dans le propre réseau LAN. L'accès à certains domaines pourra être bloqué pour certains ordinateurs ou pour le réseau entier.



# Installation

Ce chapitre vous aidera à établir rapidement un nouveau réseau sans fil. Voyez tout d'abord le contenu de l'emballage et faites connaissance avec votre appareil. Ensuite nous vous montrons comment vous pouvez brancher et mettre l'appareil en service.

## Contenu de l'emballage

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

- Station de base *ELSA LANCOM Wireless IL-2*
- Bloc d'alimentation
- Carte de réseau sans fil *ELSA AirLancer MC-2*
- Câble de raccordement au réseau local
- Câble de raccordement RNIS
- Documentation
- CD-ROM avec *ELSA LANconfig* et d'autres logiciels ainsi que la documentation électronique

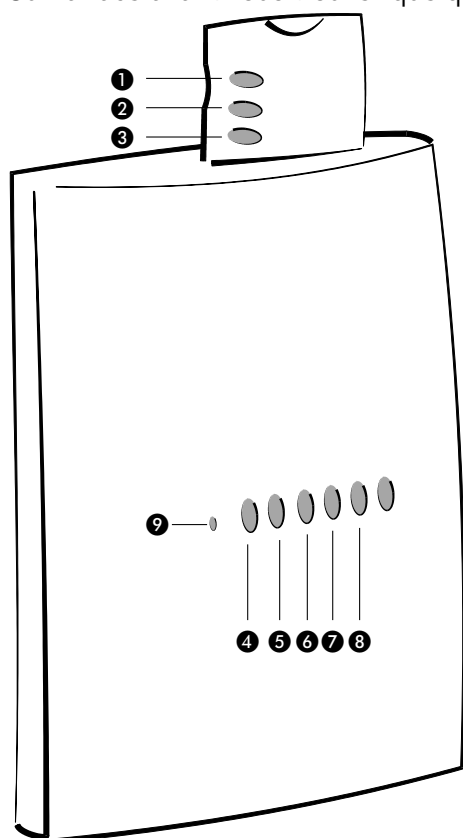
Adressez-vous directement à votre revendeur s'il manque quelque chose.

## ***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.

DEL

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

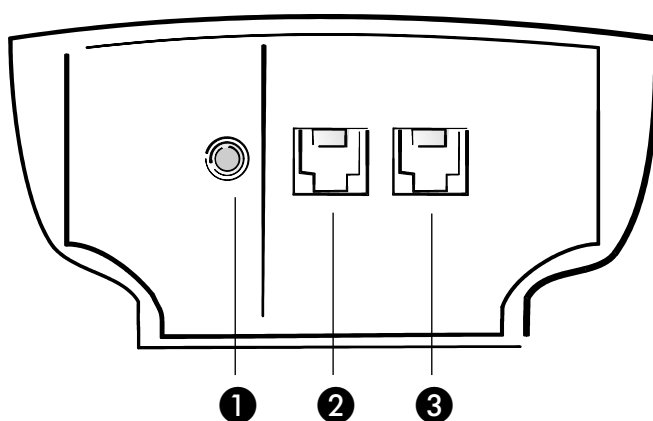


- ❶ La DEL rouge de la carte de réseau sans fil indique que la connexion est établie entre la carte et la station de base.
- ❷ La DEL jaune de la carte de réseau sans fil indique le nombre de stations mobiles connectées sur cette station de base. Sur trois stations connectées la DEL clignotera p.ex. brièvement trois fois de suite, le clignotement sera suivi d'une pause.
- ❸ La DEL verte de la carte de réseau sans fil indique l'activité dans le réseau sans fil, donc l'émission et la réception de paquets de données. Si cette DEL est éteinte ou allumée en permanence, la carte de réseau sans fil 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 Le témoin lumineux 'S<sub>0</sub>-Status' de la station de base indique l'activité du canal D.
- ⑥ Le témoin lumineux 'WAN-Channel-1' de la station de base indique l'activité du premier canal B à l'interface RNIS.
- ⑦ Le témoin lumineux 'WAN-Channel-2' de la station de base indique l'activité du deuxième canal B à l'interface RNIS.
- ⑧ 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, enfoncez 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 :



- ① Raccord bloc d'alimentation
- ② Raccordement réseau 10Base-T
- ③ Raccordement RNIS S<sub>0</sub>

## Comment brancher la station de base

- ① Connectez la station de base *ELSA LANCOM Wireless IL-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 concentrateur de votre LAN).
- ② Raccordez le routeur à un accès de base RNIS S<sub>0</sub> (en configuration point-à-point ou point-à-multipoint). Pour pouvoir utiliser la fonction de surveillance et de statistique des coûts de communication, demandez le complément de service « présentation des coûts de communication **pendant** la communication » (d'après AOCD) auprès de votre opérateur.
- ③ Engagez la carte de réseau sans fil *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.



- ④ 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 de réseau sans fil indique que la connexion est établie entre la carte et la station de base. Le scintillement de la DEL verte sur la carte de réseau sans fil 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 conviviale en fonction de vos applications désirées.

*A la livraison, les paramètres du réseau sans fil 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 câble ou dans le réseau sans fil.

- 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.

### Procéder à la configuration 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.

- 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 hypothèses 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 et 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 `winiipcfg` dans la fenêtre s'ouvrant et cliquez sur **OK**. Sélectionnez votre carte de réseau dans la fenêtre suivante. Si vous trouvez la valeur '0.0.0.0' dans la zone 'Adresse IP', votre carte de réseau n'a pas encore d'adresse IP.*

*Sous Windows NT, vous pouvez vérifier les adresses IP au moyen de la commande `ipconfig`.*

- 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 hypothèses 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 trouverez 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 de 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 s'ouvrant.
- ② Modifiez la langue 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 le cas échéant relancer le routeur.*

- 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 microprogramme avec de nouvelles possibilités, vous trouverez ici des indications pour le téléchargement du logiciel.

## Radio ou câble : chemins aboutissant à la configuration

Avec la configuration Inband (configuration via le réseau) vous pouvez accéder à la station de base à partir de n'importe quel ordinateur du WLAN, LAN ou WAN (RNIS). 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

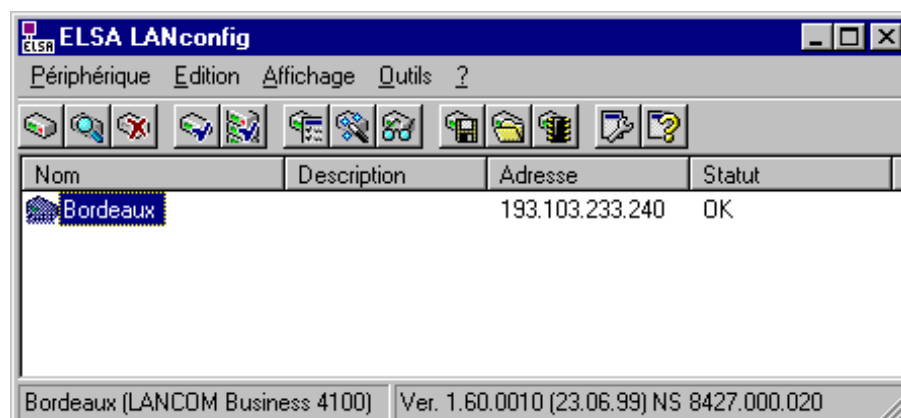
S'il n'est pas absolument nécessaire de configurer les adresses correctes IP « à la main », le serveur DHCP se chargera volontiers de cette tâche tout seul. Si vous utilisez le serveur DHCP, vous pouvez faire régler automatiquement les adresses IP pour tous les ordinateurs du réseau (cf. chapitre 'Affectation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

Le logiciel des périphériques de ELSA est sujet 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 microprogramme utilisé jusque là ne sera pas écrasé, mais un deuxième microprogramme sera chargé dans l'appareil.

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

- 'Immédiatement' : La première possibilité consiste à charger et à activer le microprogramme immédiatement. Les situations suivantes peuvent s'en suivre :
  - Le nouveau microprogramme est chargé avec succès et fonctionne ensuite comme voulu. Donc tout est correct.
  - Le périphérique n'est plus accessible après le chargement du nouveau microprogramme. S'il survient une erreur déjà lors d'un téléchargement, le périphérique activera automatiquement l'ancien microprogramme et relancera le périphérique.
- 'Login' : Afin de remédier aux problèmes d'un téléchargement incorrect, vous avez la deuxième possibilité suivant laquelle le microprogramme 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 microprogramme 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 microprogramme et relancera le périphérique.
- 'Manuel' : La troisième possibilité vous permet de déterminer auparavant vous-même un laps de temps durant lequel vous voulez tester le nouveau microprogramme. Le périphérique démarre avec le nouveau microprogramme et attend durant le laps de temps réglé que le microprogramme soit activé manuellement pour être actif en permanence.

## Comment charger le nouveau logiciel ?

Plusieurs chemins mènent au but pour le téléchargement du microprogramme (c'est ainsi que s'appelle le chargement du logiciel) :

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



Certains réglages sont conservés lors du téléchargement du microprogramme ! 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 microprogramme actuel, le périphérique complétera 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 microprogramme ► Charger nouveau microprogramme** ou directement sur le bouton **Télécharger**

**microprogramme.** 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 microprogramme et vous proposera un téléchargement. Avec **Ouvrir** vous remplacez le microprogramme actuel par la version choisie.

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

## TFTP

Avec TFTP, un nouveau microprogramme peut être chargé à l'aide de l'instruction **writeflash**. Pour transmettre un nouveau microprogramme, 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 writeflash
```



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

Après un téléchargement correct du microprogramme, le périphérique procède à une relance en activant directement le nouveau microprogramme. 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 microprogramme 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 (SNMP V.1 après RFC 1157) permet la surveillance et la configuration des périphériques dans un réseau à partir d'une instance centrale.

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 :

- Connexions ADSL
- Sécurité de la configuration
- Sécurité pour le réseau local
- Gestion des coûts de communication
- Connexions via RNIS
- Prise en charge de PPP
- Routage IP
- Gestion d'adresses automatique via DHCP
- Serveur DNS
- Proxy NetBIOS
- *ELSA LANCAPI*
- Gestion des temps
- Rerouteur téléphonique (Least Cost Router)

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

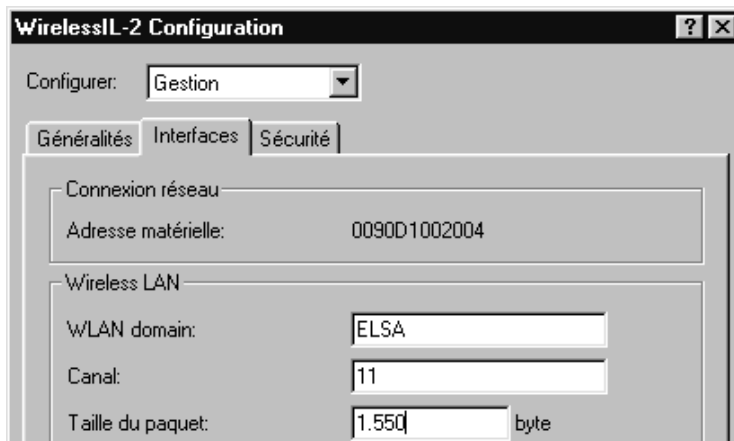
Pour que les cartes de réseau sans fil installées dans les terminaux mobiles et dans les stations de base puissent s'identifier mutuellement et échanger des données entre elles, elles doivent posséder les mêmes valeurs dans divers paramètres.

Toutes les cartes de réseau sans fil (dans les stations de base ou mobiles) fonctionnant 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 ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* recherche automatiquement toutes les stations de base dans le réseau local câblé (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 de 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, p.ex. 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 Activez la fonction du 'roaming', lorsque vous voulez utiliser simultanément plusieurs cellules radio formant une chaîne ethernet commune, ceci dans le but

d'assurer un transfert transparent d'une cellule à une autre. Les points d'accès impliqués dans le roaming doivent être configurés de façon identique (réseau sans fil, canaux radios...).

- ⑦ Sélectionnez le dossier de configuration 'Pont WLAN' si vous
- souhaitez interdire l'échange de données avec le réseau câble 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 p.ex. 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 pour avoir un accès à un réseau, à un ordinateur ou à un autre périphérique. p.ex., 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.

## La sécurité de votre LAN

Vous n'apprécierez certainement pas qu'une personne externe puisse en toute liberté consulter ou modifier les données sur votre serveur d'entreprise. Un *ELSA LANCOM Wireless* offre différentes possibilités pour limiter un accès de l'extérieur :

- Filtrage des paquets de données
- Masquering IP (NAT, PAT)

## Le contrôle

L'« identificateur » utilisé pour identifier l'appelant est sélectionné sur l'onglet 'Prise d'appel' du dossier de configuration 'Communication' ou dans le menu /Setup/Module WAN/Protection. Les choix proposés sont les suivants :

- Aucun : Les appels de tous les correspondants sont acceptés.

- Nom : Seuls les appels des correspondants dont le nom figure dans la liste des noms sont acceptés.

L'identification de l'appelant n'est évidemment possible que si son numéro est transmis (complément de service « identification d'appel »).

### Vérification du nom

La réaction des routeurs est claire : si la protection de l'accès au moyen du nom a été activée, seuls les appelants dont les noms sont connus seront acceptés, les autres seront refusés.

Dans le cas du protocole PPP, le système vérifie si le nom du correspondant est enregistré en tant que nom d'utilisateur dans la liste PPP. Lorsque ce nom d'utilisateur n'existe pas, le nom du périphérique est employé comme nom du correspondant et soumis à vérification. Vous trouverez la liste PPP en sélectionnant l'onglet 'Protocoles' du dossier de configuration 'Communication' de *ELSA LANconfig*, ou dans le menu /Setup/Module WAN/Liste PPP.

Pas de mot de passe ? Oui, cette particularité est proposée par PPP : Ici on peut demander en plus une protection spécialement valable pour ce protocole selon PAP (Password Authentication Protocol) ou CHAP (Challenge Handshake Authentication Protocol). Il s'agit là de la protection que le propre périphérique demandera au correspondant.



*Il est évident que vous n'utiliserez pas les procédures de sécurité PAP ou CHAP si vous voulez accéder vous-même p.ex. à un fournisseur d'accès Internet avec le ELSA LANCOM. Vous n'arriverez probablement pas à convaincre le FAI à répondre à une requête du mot de passe ...*

D'où viennent le nom et le mot de passe de l'appelant ?

- Avec PPP, on entre le nom et le mot de passe lors de l'établissement de la communication avec le correspondant, p.ex. dans la fenêtre correspondante d'une connexion dans l'Accès réseau à distance. Si le routeur établit une communication lui-même, le nom du périphérique, le mot de passe et le nom de l'utilisateur seront pris dans la liste PPP.

### Vérification du numéro

Lors d'un appel sur une ligne RNIS, le numéro de l'appelant est, dans la plupart des cas, déjà transmis par le canal D avant qu'une connexion ne soit établie (CLI – Calling Line Identifier).

Si le numéro d'appel figure dans la liste des numéros, l'accès au propre réseau pourra être permis, ou alors l'appelant sera rappelé si l'option de rappel est activée. Si une protection de l'accès par numéro d'appel a été convenue dans le *ELSA LANCOM*, tous les appels de correspondants dont les numéros sont inconnus seront refusés.

La protection de l'accès par numéro d'appel peut être utilisée avec tous les protocoles de canal B (couche).

## Le rappel

Une variante particulière de la protection d'accès est obtenue par la fonction de rappel : Pour cela on active dans la liste des noms l'option 'Rappel' pour l'appelant désiré et on indique, le cas échéant, le numéro de rappel.

Avec les réglages effectués dans la liste des noms et des numéros ainsi que le choix du protocole , vous pouvez contrôler le comportement au rappel de vos routeurs :

- Le routeur peut refuser le rappel.
- Il peut rappeler un numéro prédéfini.
- Le numéro d'appel pour le rappel peut être entré librement par l'appelant.

Et de plus, avec les réglages, vous contrôlez en passant la répartition des coûts de la connexion. Si dans la liste des noms un rappel a été convenu 'd'après le nom', le routeur rappelant se charge de toutes les taxes à une exception, celle qui est nécessaire pour la transmission du nom. Une unité est nécessaire pour le routeur, si l'appelant n'a pas pu être identifié par CLI. Si par contre une identification par le numéro d'appel de l'appelant est possible et permise, aucune taxe téléphonique ne sera facturée à l'appelant.

Si le routeur doit rappeler lui-même, on peut aussi utiliser le procédé fast callback (brevet déposé) pour un grand nombre de correspondants. Ceci accélère considérablement la procédure de rappel.

## La cachette – Masquerading IP (NAT, PAT)

Mais il y a là des objections venant des fournisseurs d'accès qui se soucient de la sécurité des données dans le réseau interne de l'entreprise : chaque ordinateur dans le WWW ? Tout le monde pourra donc aussi y accéder de l'extérieur ! – Non, il ne peut pas !

La cachette pour tous les ordinateurs dans Internet s'appelle masquerading IP. Seul le module routeur dans le périphérique ainsi que son adresse IP (fixe ou attribué par le fournisseur d'accès) sont signalés à Internet. Les ordinateurs dans le LAN se servent alors du routeur comme d'une passerelle et peuvent eux ne pas être reconnus. Le routeur sépare Internet et Intranet comme par un mur. On désigne donc masquerading IP comme une « technique de coupe-feu » (firewall).

Les détails supplémentaires sont décrits dans le chapitre 'Routage IP : IP masquerading'.

## Gestion des taxes téléphoniques

La caractéristique du routeur (établir de façon autonome la connexion avec tous les correspondants souhaités, puis la terminer une fois la transmission finie) permet à l'utilisateur d'accéder de façon très conviviale à Internet ou à des ordinateurs et réseaux à distance. Cependant, lors de la transmission de données via les lignes commutées RNIS, une mauvaise configuration du routeur (par ex. celle relative aux filtres) ou l'usage excessif de services (par ex. en navigant sans cesse sur Internet) peuvent occasionner des frais de téléphone élevés.

### Limitation des communications en fonction du temps

Pour pouvoir néanmoins limiter les frais de téléphone, la durée de connexion maximale peut être fixée en fonction du temps. Pour cela, par analogie avec le budget en fonction d'un certain nombre d'unités, un budget peut être fixé en fonction d'une durée déterminée. La configuration par défaut permet par ex. de n'établir de connexions actives que pour une durée maximale de 210 minutes par semaine.



*Une fois l'un des deux plafonds atteint, toutes les connexions ouvertes via routeur, établies par le routeur lui-même, sont terminées automatiquement. A l'expiration de la période actuelle, sur laquelle s'étendent les limites relatives aux unités ou à la durée de connexion, les budgets sont débloqués et les connexions actives sont à nouveau possibles. L'administrateur peut bien entendu débloquer les budgets également avant terme!*

Avec un budget de 0 unité ou de 0 minute, la surveillance des fonctions du routeur – en fonction des unités disponibles ou de la durée de connexion maximale – peut être désactivée.

### Configuration dans le gestionnaire des coûts de communication

Vous configurez ces paramètres en sélectionnant l'onglet 'Coûts de communication' du dossier de configuration 'Gestion' de *ELSA LANconfig*, ou lors d'une session Telnet ou de terminal sous /Setup/Module des coûts de communication.



*Les informations relatives aux unités et aux temps de connexion sont sauvegardées lors d'une procédure de lancement (par ex. lors de l'installation d'un nouveau microprogramme) et ne disparaissent qu'une fois le périphérique est éteint. Toutes les indications de temps reportées ici sont exprimées en minutes.*

## Connexions via RNIS

Les données entre deux terminaux RNIS sont échangées via le réseau RNIS. Les connexions RNIS peuvent fondamentalement être des liaisons commutées ou permanentes.

Les routeurs déterminent d'abord vers quel correspondant un paquet de données doit être transmis. Pour que la connexion correspondante puisse être sélectionnée et le cas échéant établie, les divers paramètres pour toutes les connexions RNIS nécessaires doivent être déclarés. Ces paramètres sont définis dans plusieurs listes permettant d'établir les connexions requises.

Les pages suivantes vous présentent brièvement ces listes et les paramètres qu'elles contiennent, montrent les liens avec les autres listes et paramètres, et leur configuration avec le logiciel.

### Liste des noms

Vous trouverez la liste des noms en sélectionnant l'onglet 'Correspondants' du dossier de configuration 'Communication' de *ELSA LANconfig*, pour les sessions Telnet ou de terminal sous `/Setup/Module WAN/Liste des noms`.

Pour définir les correspondants disponibles, ajoutez-les à la liste des noms en leur attribuant un nom significatif et les paramètres complémentaires :

- Nom

Ce nom permet aux modules de routage d'identifier le correspondant.

- Numéro d'appel

Ce numéro d'appel doit être composé si le routeur doit lui-même établir activement une connexion avec le correspondant.

Lorsque le correspondant peut être joint sous plusieurs numéros d'appel, saisissez ces numéros supplémentaires dans la liste Round-Robin.

Si ce correspondant est appelé via une liaison permanente, vous pouvez indiquer aussi une ligne de débordement-secours établie au moyen d'une liaison commutée.

- Time-out

Ces délais indiquent la période pendant laquelle les canaux B restent actifs après

- une inactivité (pas de transmission de données) de durée B1 pour les canaux établis de façon statique,
- un repli du débit de transfert sous un seuil défini, de durée B2, pour les canaux établis de manière dynamique.



■ Nom de la couche

La couche (Layer) désigne une série de protocoles devant être utilisés pour la connexion considérée. La couche doit être identique des deux côtés de la ligne.

■ Rappel

Vous pouvez indiquer ici qu'un appel du correspondant considéré ne sera pas accepté. A la place, votre routeur rappelle le correspondant avec les options suivantes :

- rappel normal
- rappel selon la procédure rapide ELSA
- rappel après vérification du nom
- attendre soi-même le rappel du correspondant selon la procédure rapide ELSA

## Configuration des interfaces

Vous configurez ces paramètres en sélectionnant l'onglet 'Interfaces' du dossier de configuration 'Gestion' de *ELSA LANconfig*, ou lors d'une session Telnet ou de terminal sous `/Setup/Module WAN/Liste des interfaces`.

Dans cette partie de configuration des interfaces, vous sélectionnez les paramètres généraux pour chaque interface (donc chaque accès  $S_0$ ). Ces paramètres sont valables pour tous les modes d'exploitation des périphériques. En particulier, il s'agit des paramètres suivants :

■ Protocole de canal D utilisé pour l'accès  $S_0$  considéré

Détection automatique, DSS1 (Euro-ISDN), DSS1 point-à-point, 1TR6, Liaison permanente du groupe 0

■ Option de liaison permanente

Canal B à utiliser éventuellement pour la liaison permanente

■ Préfixe de numérotation

Préfixe du numéro d'appel des appels sortants, p.ex. le numéro du standard dans les entreprises.

## Configuration de l'interface du routeur

Vous configurez les paramètres de l'interface du routeur en sélectionnant l'onglet 'Général' du dossier de configuration 'Communication' de *ELSA LANconfig*, ou lors des sessions Telnet ou de terminal sous `/Setup/Module WAN/Liste des interfaces de routeur`.

Ces éléments de configuration servent à définir, pour chacune des interfaces (donc pour chaque accès  $S_0$ ), les paramètres devant être utilisés dans le mode d'exploitation en tant que routeur. Ces paramètres ne s'appliquent pas aux autres modes d'exploitation des périphériques. En particulier, il s'agit des paramètres suivants :



■ Numéros d'appel (MSN/EAZ)

Le routeur réagit à ces numéros d'appel quand il reçoit un appel. Plusieurs numéros d'appel sont séparés par des points-virgules. Si vous n'entrez pas le numéro d'appel, le routeur prend tous les appels entrants.

Le premier des numéros saisis est communiqué au correspondant s'il établit la communication lui-même. Si le numéro d'appel n'est pas spécifié, c'est le numéro d'appel principal de l'accès qui est transmis.

■ Option pour les connexions en Y

Activez cette option si les deux canaux B de l'accès doivent pouvoir établir des connexions simultanées avec des correspondants différents.

■ Masquage du propre numéro d'appel

Activez cette option si vous ne voulez pas que votre propre numéro d'appel ne soit pas signalé au correspondant quand le routeur établit une connexion lui-même.

*Cette fonction doit être souscrite auprès de l'opérateur du réseau téléphonique.*

## Configuration de l'interface **LANCAPI**

Vous trouverez les éléments de configuration de l'interface **LANCAPI** en sélectionnant l'onglet 'Général' du dossier de configuration 'LANCAPI' de **ELSA LANconfig**, ou lors d'une session Telnet ou de terminal sous `/Setup/Module LANCAPI/Liste des interfaces`.

Ces éléments de configuration servent à définir, pour chacune des interfaces (donc pour chaque accès  $S_0$ ), les paramètres utilisés pour **LANCAPI**. Ces paramètres ne s'appliquent pas aux autres modes d'exploitation des périphériques. En particulier, il s'agit des paramètres suivants :

■ Numéros d'appel (MSN/EAZ)

**LANCAPI** réagit à ces numéros d'appel quand il reçoit un appel. Plusieurs numéros d'appel sont séparés par des points-virgules. Si vous n'entrez pas le numéro d'appel, le routeur prend tous les appels entrants.

■ Accès à **LANCAPI**

Vous pouvez désactiver ici les fonctions de **LANCAPI**, les limiter aux appels sortants, ou les activer pour les appels sortants et les appels entrants.

■ Transmission du propre numéro d'appel

Normalement, le numéro de téléphone signalé au correspondant, lorsque la communication est établie via **LANCAPI**, est le numéro indiqué dans l'application CAPI. Si ce numéro manque ou s'il est incorrect, **LANCAPI** ne transmet aucun numéro d'appel. Cette option permet de transmettre le premier numéro d'appel indiqué dans le champ 'Numéro d'appel' si le numéro d'appel n'a pas été saisi dans l'application CAPI.

## Liste des couches

Vous trouverez la liste des couches de communication en sélectionnant l'onglet 'Général' du dossier de configuration 'Communication' de *ELSA LANconfig*, ou lors des sessions Telnet ou de terminal sous `/Setup/Module WAN/Liste des couches`.

Dans une couche, vous combinez les paramètres du protocole de transmission à utiliser. En particulier, il s'agit des paramètres suivants :

- Nom de la couche  
Les paramètres du protocole sont enregistrés sous le nom indiqué. Dans cette liste des noms, vous sélectionnez la configuration ayant le nom de couche pour la connexion correspondante.
- Encapsulation  
Indiquez ici si un en-tête Ethernet doit être ajouté aux paquets de données. Il suffit normalement de sélectionner 'Transparent', ce paramètre peut être nécessaire uniquement pour les connexions HDLC avec les périphériques distants.
- Couche 3 (Layer-3)  
Protocole de la couche 3 pour la connexion. Est en partie détecté automatiquement dans le cas des appels entrants.  
  
Dans le cas de l'utilisation de PPP, une entrée supplémentaire dans la liste PPP est nécessaire.  
  
Dans le cas de l'utilisation de scripts, une entrée supplémentaire dans la liste des scripts est nécessaire.
- Couche 2 (Layer-2)  
Protocole de la couche 2 pour la connexion.
- Options  
Active la compression des données et le regroupement des canaux. Ces options ne peuvent être actives que si elles sont prises en charge par les protocoles de la couche 2 et de la couche 3.
- Couche 1 (Layer-1)  
Protocole de la couche 1 pour la connexion. Est en partie détecté automatiquement dans le cas des appels entrants.

## Liste RoundRobin

Vous trouverez la liste Round-Robin en sélectionnant l'onglet 'Correspondants' du dossier de configuration 'Communication' de *ELSA LANconfig*, ou lors des sessions Telnet ou de terminal sous `/Setup/Module WAN/Liste RoundRobin`.

Lorsqu'un correspondant peut être joint sous plusieurs numéros d'appel, entrez le premier numéro dans la liste des noms et tous les autres numéros dans la liste Round-Robin.

- ID distant  
Nom du correspondant tel qu'il a été défini dans la liste des noms.
- Round-Robin  
Numéros d'appel supplémentaires du correspondant considéré. Plusieurs numéros d'appel sont séparés par des traits d'union.
- Commencer par :  
Indiquez si une nouvelle tentative de connexion doit être faite en utilisant le dernier numéro d'appel ayant abouti, ou en utilisant le premier numéro dans la liste.

## Liste PPP

Vous trouverez la liste PPP en sélectionnant l'onglet 'Protocoles' du dossier de configuration 'Communication' de *ELSA LANconfig*, ou lors des sessions Telnet ou de terminal sous `/Setup/Module WAN/Liste PPP`.

La liste PPP vous sert à définir des paramètres supplémentaires pour les connexions utilisant PPP dans la couche de communication 3.(Layer 3).

- ID distant  
Nom du correspondant tel qu'il a été indiqué dans la liste des noms.
- Nom d'utilisateur  
Nom d'utilisateur utilisé pour s'annoncer chez le correspondant.
- Mot de passe  
Mot de passe utilisé pour s'annoncer chez le correspondant.
- Vérification  
Procédure d'authentification que le routeur doit demander du correspondant.
- Durée, Rép., Conf., Fail., Term.  
Paramètres modifiant le comportement de la connexion.

## Script

Vous trouverez la liste des scripts en sélectionnant l'onglet 'Protocoles' du dossier de configuration 'Communication' de *ELSA LANconfig*, ou lors des sessions Telnet ou de terminal sous `/Setup/Module WAN/Liste des scripts`.

Lorsque l'accès au correspondant nécessite l'exécution d'un script, indiquez ce script ici et attribuez-le au correspondant.

Le protocole de couche 3 sélectionné dans la liste des couches pour la connexion considérée doit prendre en charge l'exécution des scripts.

- ID distant  
Nom du correspondant tel qu'il a été indiqué dans la liste des noms.
- Script  
Entrez ici le script, comme décrit dans le manuel de référence de la documentation.

## Prise d'appel

Vous trouverez les paramètres de la prise d'appel en sélectionnant l'onglet 'Prise d'appel' du dossier de configuration 'Communication' de *ELSA LANconfig*, ou lors de sessions Telnet ou de terminal sous le menu /Setup/Module WAN/Protection.

Ces paramètres de la prise d'appel vous permettent d'indiquer sous quelles conditions le périphérique accepte les appels entrants. Ces paramètres ne s'appliquent qu'aux fonctions de routeur du périphérique.

- Tous  
Tous les appels sont acceptés.
- Nom  
Le routeur commence par accepter tous les appels. Il recherche le nom lors de la négociation du protocole et vérifie s'il existe dans la liste des noms. Dans ce cas, la connexion est maintenue. Si le nom est introuvable, la connexion est coupée.
- Numéro  
L'appel est accepté uniquement si le correspondant figure dans la liste des noms et si le numéro d'appel du correspondant est transmis (par identification d'appel).
- Nom ou numéro  
L'appel est accepté si l'une des deux vérifications aboutit.

## Liste des numéros

Vous trouverez la liste des numéros en sélectionnant l'onglet 'Prise d'appel' du dossier de configuration 'Communication' de *ELSA LANconfig*, pour les sessions Telnet ou de terminal sous /Setup/Module WAN/Liste des numéros.

La liste des numéros est utilisée pour l'établissement passif des connexions pour augmenter la sécurité lors de la prise d'appel et pour effectuer un rappel automatique.

- Numéro d'appel  
Numéro d'appel transmis par le correspondant qui appelle (éventuellement avec l'indicatif du pays et de la localité).

- ID distant

Nom du correspondant tel qu'il est défini dans la liste des noms. Lorsque le rappel automatique est défini dans la liste des noms, ce correspondant est rappelé.

## Protocole PPP

Les routeurs ELSA prennent aussi en charge le protocole point-à-point PPP (Point-to-Point Protocol). PPP est un terme générique s'appliquant à toute une série de protocoles de réseau étendu qui facilitent la communication entre les routeurs de différents constructeurs, car ce protocole est utilisé par presque tous les constructeurs.

C'est justement parce que PPP ne peut pas être mis en relation avec un mode de fonctionnement précis des routeurs, et naturellement à cause du rôle de plus en plus important de cette famille de protocoles que nous voulons vous présenter les fonctions des périphériques en rapport avec PPP dans un chapitre distinct.

### Le protocole

#### Présentation de PPP

Le protocole PPP a été développé spécialement pour les connexions réseau via des canaux sériels et s'est imposé comme standard pour les connexions entre routeurs. Il réalise les fonctions suivantes :

- Protection par mot de passe suivant PAP ou CHAP
- Négociation des protocoles réseau à utiliser pour les connexions (p.ex. IP ou IPX). En font partie les paramètres requis pour ces protocoles, p.ex. les adresses IP/IPX. Cette négociation emploie le protocole IPCP (IP Control Protocol).
- Vérification de la connexion avec LCP (Link Control Protocol)

En ce qui concerne les connexions des routeurs, PPP est le standard qui s'est imposé pour la communication entre des périphériques de constructeurs différents ou des logiciels de communication dans le réseau étendu. Pour assurer un transfert de données sans erreur, la négociation des paramètres de connexion et la fixation d'un dénominateur commun recourt à des protocoles de commande standardisés (LCP, IPCP, IPXCP, CCP) inclus dans PPP.

#### Dans quel but PPP est-il utilisé ?

La mise en œuvre de PPP est pertinente pour les applications suivantes :

- p.ex. pour la communication avec les routeurs externes pour des questions de compatibilité
- Accès Internet (avec la transmission des adresses)

## Les phases d'une négociation PPP

Une connexion avec PPP commence toujours par la négociation des paramètres à employer pour et pendant la communication. Cette négociation comprend quatre phases. Il importe de connaître ces phases pour la configuration et le diagnostic des erreurs.

- Establish phase (établissement de la connexion)

Une fois que les ETCD ont fermé le circuit, ils négocient les paramètres de la connexion via LCP.

Chacun d'entre eux vérifie si le correspondant est également prêt à utiliser PPP, et ils s'accordent sur la taille des paquets ainsi que sur le protocole d'authentification (PAP, CHAP ou aucun). LCP passe ensuite en état Opened.

- Authenticate phase (phase d'authentification)

Au besoin, les mots de passe sont échangés. Pour l'authentification selon PAP, le mot de passe n'est transmis qu'une seule fois. Dans le cas de CHAP, un mot de passe crypté est envoyé périodiquement à des intervalles configurables.

- Network phase (phase de réseau)

Lorsque la négociation des paramètres s'est terminée correctement pour au moins l'une des couches réseau, les modules routeur peuvent transmettre des paquets IP et/ou IPX par la ligne (logique) établie.

- Terminate phase (phase de la terminaison)

Dans la dernière phase, le circuit est ouvert dès que les liaisons logiques pour tous les protocoles sont inactives.

## La négociation PPP dans le *ELSA LANCOM*

Le déroulement d'un échange de protocoles PPP est journalisé dans les statistiques PPP des périphériques. En cas d'erreur, la description détaillée des paquets de protocole permet d'effectuer un contrôle.

Les traces PPP offrent une autre possibilité d'analyse. La commande

```
trace + ppp
```

permet de lancer la sortie des trames protocolaires PPP échangées au cours d'une session terminal. Lorsque cette session terminal est journalisée dans un fichier, une analyse détaillée pourra en être faite après la fin de la connexion.

## La liste PPP

A l'aide de cette liste, vous pouvez créer une définition individuelle de la négociation PPP pour chaque correspondant prenant contact avec votre réseau. Vous trouverez la liste PPP en sélectionnant l'onglet 'Protocoles' du dossier de configuration 'Communication' de *ELSA LANconfig*, ou dans le menu /Setup/Module WAN/Liste PPP.

La liste PPP peut comprendre 64 entrées ayant les valeurs suivantes :

Dans cette colonne de la liste PPP ...	... vous saisissez les valeurs suivantes :
Nom de périphérique	Nom que le correspondant utilise pour s'annoncer sur votre routeur
Sécurisation	Procédure utilisée pour sécuriser la connexion PPP (PAP, CHAP ou aucun). Votre propre routeur exige que votre correspondant respecte cette procédure ! (et pas le contraire). C'est pourquoi la sécurisation selon PAP ou CHAP ne s'applique pas aux connexions avec les fournisseurs d'accès Internet qui ne voudront peut-être pas communiquer leur mot de passe. Sélectionnez 'aucune' pour de telles connexions.
Mot de passe	Mot de passe transmis au correspondant par votre routeur (si nécessaire). Les signes * dans la liste indiquent qu'un mot de passe existe.
Durée	Délai entre deux vérifications de la connexion avec LCP. Vous exprimez ce temps par un multiplicateur de 10 secondes (p.ex. : 2 pour indiquer 20 secondes). Egalement le délai entre deux vérifications de la connexion selon CHAP. Indiquez ce délai en minutes. Ce temps doit être '0' pour les correspondants sous Windows 95, Windows 98 ou Windows NT !
Rép.	Nombre de tentatives de vérification. En choisissant plusieurs tentatives, vous contournez l'effet des perturbations sporadiques de la ligne. C'est uniquement lorsque toutes les tentatives échouent que la connexion est coupée. Le délai entre deux tentatives s'élève à 1/10e du délai séparant deux vérifications. En même temps le nombre maximal de requêtes de configuration (configure requests) que le routeur émet avant qu'il ne suppose une perturbation de la ligne et raccroche lui-même.
Conf, Fail, Term	Ces paramètres permettent d'influencer le mode de fonctionnement de PPP. Ils sont définis dans la recommandation RFC 1661 et ne seront pas décrits ici. Si vous ne pouvez pas établir de connexion PPP, vous trouverez dans cette recommandation et dans les statistiques PPP du routeur des informations sur le dépannage. En général, les paramètres par défaut suffisent. Ces paramètres ne peuvent être modifiés que par l'intermédiaire de SNMP ou de TFTP (avec le logiciel de configuration <i>ELSA LANconfig</i> !)
Nom d'utilisateur	Nom que votre routeur utilise pour s'annoncer chez le correspondant. Si ce champ reste vide, c'est le nom de périphérique de votre routeur qui est utilisé.
Droits	

## Tout est bon? Vérification de la ligne avec LCP

Pendant l'établissement de la connexion avec PPP, les périphériques en présence négocient une procédure commune pour la transmission des données. Ils décident p.ex. si une connexion est réalisable étant donné les paramètres pour la procédure de sécurisation, le nom et les mots de passe.



Une fois la connexion établie, la qualité de la ligne peut être contrôlée en permanence au moyen du protocole LCP. A cet effet, ce protocole recourt à une requête d'écho LCP (LCP echo request) et à la réponse sur écho LCP correspondante (LCP echo reply). La requête d'écho LCP est envoyée sous forme de paquet transmis au correspondant à côté des données utiles. Lorsqu'une réponse valable est renvoyée (LCP echo reply), cela signifie que la liaison est stable et fiable. Cette requête est répétée à intervalles réguliers.

Que se passe-t-il s'il n'y a pas de réponse ? Pour commencer, la requête est répétée plusieurs fois pour exclure une perturbation sporadique de la ligne. S'il n'y a toujours pas de réponse, la ligne est coupée et le périphérique cherche une voie de rechange.

Le comportement des requêtes LCP est paramétré au cas par cas pour chaque connexion dans la liste PPP. Les champs 'Temps' et 'Rép.' vous servent à fixer l'intervalle entre les requêtes LCP ainsi que le nombre de tentatives quand il n'y a pas de réponse; dès que ces valeurs sont atteintes, la ligne peut être considérée comme en dérangement. Pour désactiver totalement les requêtes LCP, le temps et les répétitions sont mis tous les deux à 0.

## Routage IPX

Un routeur IP s'intercale entre les réseaux utilisant le protocole TCP/IP. Il transmet uniquement les données dont les adresses de destination sont enregistrées dans le tableau de routage. Ce chapitre vous montre comment le tableau de routage IP est organisé dans un routeur ELSA ainsi que les fonctions de routage IP supplémentaires.

### Le tableau de routage IP

Dans le tableau de routage IP, vous déclarez au routeur les correspondants (donc les autres routeurs ou ordinateurs) auxquels doivent être envoyés les données destinées aux adresses ou aux plages d'adresses IP. L'entrée dans ce tableau est donc appelée la « route », puisqu'elle décrit le chemin des paquets. Comme vous créez ces entrées vous-même et qu'elles restent inchangées jusqu'à ce que vous les modifiez manuellement ou les supprimiez, cette politique est aussi appelée « routage statique ». A l'opposé, il existe aussi un « routage dynamique ». Dans ce cas les routeurs échangent leurs informations sur les routes et mettent ces informations à jour en permanence. Le tableau de routage statique peut contenir jusqu'à 64 entrées, le tableau dynamique 128. Lorsque IP-RIP est actif, le routeur IP tient compte des deux tableaux.

Vous trouverez le tableau de routage en sélectionnant l'onglet 'Routeur' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou dans le menu /Setup/Routeur IP/Tableau de routage IP. Voici à quoi ressemble un tableau de routage IP :

Que signifient les diverses entrées de la liste ?

#### ■ Adresse IP et masques de réseau IP

Il s'agit de l'adresse du réseau de destination avec le masque de réseau correspondant. Le routeur vérifie, au moyen du masque de réseau et de l'adresse IP de destination, si le paquet doit être « livré » dans le réseau de destination.

Adresse IP 255.255.255.255 avec le masque de réseau 0.0.0.0 : il s'agit de la route par défaut. Tous les paquets ne pouvant pas être acheminés sur la base des autres entrées de routage sont transmis au correspondant indiqué ici.

#### ■ Nom du routeur

Le nom du routeur indique comment les paquets de données correspondants à l'adresse IP et au masque de réseau.

Les routes ayant le nom de routeur '0.0.0.0' désignent des routes d'exclusion. Les paquets destinés à ces « routes zéro » sont rejetés et ne sont donc pas transmis. Ceci permet d'exclure p.ex. les routes interdites dans Internet (Private Address Spaces, p.ex. 10.0.0.0).

Lorsqu'on indique une adresse IP comme nom de routeur, il s'agit d'un routeur accessible localement chargé de la transmission des paquets de données correspondants.

#### ■ Distance

Nombre de routeurs se trouvant entre le propre routeur et la destination.

Exemples et explications

Adresse IP	Masque de réseau IP	Nom du routeur	Dist.	Voici ce qui se passe :
192.168.130.0	255.255.255.0	192.168.140.123	0	Tous les paquets destinés aux adresses IP 192.168.130.x sont transmis au routeur ayant l'adresse IP 192.168.140.123.
192.168.0.0	255.255.0.0	0.0.0.0	0	Exclut la transmission des paquets dans les réseaux commençant par 10.
172.16.0.0	255.255.0.0	0.0.0.0	0	
10.0.0.0	255.0.0.0	0.0.0.0	0	
224.0.0.0	224.0.0.0	0.0.0.0	0	

## Filtrage des paquets TCP/IP

Les entrées dans le tableau de routage vous permettent déjà de déterminer assez exactement quels paquets doivent être transmis. En plus, l'adresse 0.0.0.0 dans le champ 'Router-name' vous permet de rejeter des groupes entiers d'adresses IP.

Or, vous aurez parfois besoin de restreindre davantage l'adressage. Vous utilisez à cet effet la propriété de TCP/IP de joindre à un paquet les numéros de port de la cible et de la source, en plus des adresses IP de l'expéditeur et du destinataire. Le port cible dans

un paquet représente le service adressé dans le réseau TCP/IP. Alors que les ports cibles pour divers services dans le réseau TCP/IP sont définis de façon fixe (voir aussi 'Ports TCP/IP' dans le Manuel de référence), les ports source peuvent être sélectionnés librement dans certaines zones.

Le routeur peut consulter les ports source et cible des paquets utilisant le protocole TCP ou UDP. Il peut déduire de ces ports à quoi servent les données. Il détectera donc p.ex. des accès FTP ou des sessions Telnet.

## Proxy-ARP

Une particularité du routeur IP est l'utilisation de Proxy-ARP. « Proxy » est un terme anglais signifiant mandataire. Ce mandataire est mis à pied d'œuvre quand les données à destination des adresses IP sont transmises dans le même réseau logique que celui où se trouve l'expéditeur, mais que l'adresse de destination peut néanmoins être jointe via RNIS. Ce cas se présente p.ex. lorsque des ordinateurs aux postes de travail isolés (télétravailleurs) sont connectés au réseau local via TCP/IP. Le télétravailleur a alors une adresse IP se trouvant dans le même réseau local que tous les autres ordinateurs du réseau local. Normalement, un paquet transmis du réseau local au télétravailleur ne chercherait preneur que localement, mais n'en trouverait pas.



*Pour utiliser cette fonction, l'option 'Proxy-ARP' doit être active (dans LANconfig, dans zone de configuration 'TCP/IP', onglet 'Routeur', ou dans le menu setup/Module routeur IP pour les autres possibilités de configuration).*

Le routeur devient le Proxy du télétravailleur avec l'entrée suivante dans le tableau de routage :

Adresse IP	Masque de réseau IP	Nom du routeur	Distance	IP masquerading
192.168.110.123	255.255.255.255	Télétravailleur01	0	inactif

Comme le routeur répond à une requête ARP pour le Proxy en renvoyant sa propre adresse MAC, les hôtes Proxy ne sont pas propagés dans un paquet RIP. Pour le souligner, la distance est mise à '0'.

Le routeur renvoie en tout cas sa propre adresse MAC pour répondre à l'interrogation de l'adresse MAC correspondant à l'adresse IP 192.168.110.123. Cela fait que tous les paquets destinés au télétravailleur dans le réseau local sont envoyés automatiquement au routeur, et celui-ci transmet les données à l'ordinateur à l'autre bout de la ligne.

## Routage local

Vous connaissez déjà le comportement des ordinateurs aux postes de travail dans un réseau local : lorsque l'ordinateur veut envoyer un paquet à une adresse IP qui ne se trouve pas dans son propre réseau, il recherche un routeur capable de lui venir en aide. Ce routeur est normalement déclaré au système d'exploitation en tant que routeur par défaut ou passerelle. Lorsque plusieurs routeurs coexistent dans un réseau, on n'aura souvent qu'un seul routeur par défaut qui doit pouvoir joindre toutes les adresses IP inconnues pour l'ordinateur au poste de travail. Or, ce routeur par défaut est lui-même parfois incapable d'atteindre le réseau de destination, mais il connaît un autre routeur qui trouvera le chemin.

La question est maintenant de savoir comment venir à l'aide d'ordinateur au poste de travail.

En standard, le routeur envoie à l'ordinateur une réponse comportant l'adresse du routeur connaissant la route vers le réseau de destination (cette réponse est appelée redirection ICMP). Sur ce, l'ordinateur au poste de travail reprend cette adresse et envoie immédiatement le paquet à l'autre routeur.

Certains ordinateurs sont malheureusement incapables de gérer les redirections ICMP. Pour que les paquets de données puissent malgré tout être acheminés, utilisez le routage local (sur l'onglet 'Routeur' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou dans le menu /Setup/Module routeur IP/Routage local Actif). Vous donnez ainsi au routeur dans votre appareil l'instruction d'envoyer le paquet automatiquement à l'autre routeur correspondant. En outre, le routeur n'émet plus de redirection ICMP.

Le routage local est certes une procédure intéressante, mais elle ne devrait néanmoins être appliquée que dans les cas d'urgence, car cette fonction entraîne le doublement du transit des données : les données sont envoyées d'abord au routeur par défaut, et celui-ci les envoie ensuite au routeur compétent.

## Routage dynamique avec IP-RIP

Parallèlement au tableau de routage statique, les routeurs ELSA disposent également d'un tableau de routage dynamique comprenant jusqu'à 128 entrées. A l'inverse des tableaux statiques, l'utilisateur ne remplit pas lui-même ce tableau, mais le routeur se charge de cette tâche. Il utilise à cet effet le protocole RIP (Routing Information Protocol). Tous les routeurs d'un réseau local maîtrisant ce protocole échangent les données sur les routes disponibles selon RIP.

### Quelles sont les informations propagées avec IP-RIP ?

En envoyant des informations IP-RIP, un routeur communique aux autres routeurs du réseau les routes définies dans son tableau statique. Les entrées suivantes ne sont toutefois pas prises en compte :

- Routes rejetées dans le cas de la configuration avec '0.0.0.0'.
- Routes qui renvoient à d'autres routeurs dans le réseau local.

### Quelles informations le routeur tire-t-il des paquets IP-RIP reçus ?

Lorsque le routeur reçoit de tels paquets IP-RIP, il les intègre dans son tableau de routage IP dynamique qui ressemble alors à cela :

Adresse IP	Masque de réseau IP	Durée	Distance	Routeurs
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

### Signification de ces entrées

L'adresse IP et le masque de réseau identifient le réseau de destination, la distance indique le nombre de routeurs se trouvant entre l'émetteur et le récepteur, la dernière colonne indique quel routeur a communiqué cette route. La colonne 'Durée' indique l'âge de la route. La valeur figurant dans cette colonne vaut comme multiplicateur de l'intervalle d'arrivée des paquets RIP, c'est-à-dire que '1' signifie env. 30 secondes, '5' environ 2,5 minutes etc. Quand une information arrive par une route donnée, cette route est considérée comme accessible directement et est affectée du temps '1'. Au bout du temps correspondant, la valeur dans cette colonne est mise à jour automatiquement. Au bout de 3,5 minutes, la distance passe à '16' (route inaccessible), et au bout de 5,5 minutes la route est supprimée.

Lorsque le routeur reçoit un paquet IP-RIP, il doit décider s'il doit inclure les routes communiquées dans son tableau de routage dynamique ou non. Pour prendre cette décision, il procède de la façon suivante :

- La route n'existe pas dans le tableau, et dans ce cas elle est ajoutée (s'il y a de la place).
- La route figure dans le tableau avec un temps '5' ou '6'. La nouvelle route est insérée dans le tableau si la valeur de la distance est inférieure ou égale à l'ancienne.
- La route figure dans le tableau avec un temps de '7' à '10', donc avec la distance '16'. La nouvelle route est insérée dans le tableau dans tous les cas.

- La route figure dans le tableau. Une nouvelle route vient du même routeur qui avait déjà communiqué la première route, mais celle-ci a une distance plus avantageuse que la nouvelle route.

### Interdépendance : tableaux statiques et tableaux dynamiques

En analysant le tableau statique et le tableau dynamique, le routeur compose le tableau de routage IP en soi qu'il utilise pour déterminer le chemin à prendre par les paquets. Il ajoute aux routes de son propre tableau statique les routes du tableau dynamique qu'il ne connaît pas ou qui ont une distance moins élevée que la route statique.

### IP masquerading (NAT, PAT)

Un problème de plus en plus crucial d'Internet est la limitation des adresses IP disponibles et valables partout. Par ailleurs, l'attribution d'adresses IP fixes pour Internet par le Network Information Center (NIC) est une affaire coûteuse. Dès lors, pouvait-on trouver mieux que partager une adresse avec plusieurs autres ordinateurs ?

La solution s'appelle masquerading IP (masquage IP). Il s'agit d'une procédure où un seul routeur du réseau local se présente sur la scène d'Internet en n'utilisant qu'une seule adresse IP pour le réseau entier. Cette adresse est attribuée au routeur p.ex. définitivement par le NIC ou temporairement par un fournisseur d'accès. Tous les autres ordinateurs du réseau se « cachent » alors derrière cette adresse IP unique. Outre les répercussions sur le budget, la technique du masquerading IP offre aussi une protection efficace contre les accès au réseau local depuis Internet.

### Deux adresses pour le routeur

- 'off' : pas de masquage.

### Comment fonctionne le masquerading IP ?

Le masquerading ou masquage utilise la propriété de TCP/IP d'utiliser le numéro de port de la source et de la cible en plus de l'adresse de l'expéditeur et du destinataire. Lorsque le routeur reçoit un paquet à transmettre, il mémorise l'adresse IP et le port de l'expéditeur dans un tableau interne. Il mémorise également ce nouveau port dans le tableau interne et transmet le paquet avec ces nouveaux identificateurs.

Le routeur peut ensuite associer cette réponse à l'expéditeur initial sur la base de l'entrée dans le tableau interne et la lui envoyer.



*Vous pouvez consulter ce tableau dans les statistiques du routeur (voir aussi 'Statut' dans le Manuel de référence).*

### Masquage simple et masquage inverse

A l'inverse, lorsqu'un ordinateur envoie un paquet p.ex. à un serveur FTP relié à Intranet, il croit que le serveur FTP est le routeur. Le routeur connaît l'adresse Intranet du serveur

sur la base de l'entrée dans le tableau de service (dans l'onglet 'Masq.' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou dans le menu Setup/Module routeur IP/Masquerading/Tableau de service). Le paquet est retransmis à ce serveur. Ensuite, toutes les réponses émises par le serveur FTP sont masquées derrière l'adresse IP du routeur.

La petite différence :

- Pour les accès d'Intranet à Internet en revanche, le routeur définit lui-même l'adresse IP et le port dans le tableau des services.

Ce tableau peut comprendre 2048 entrées au maximum, c'est-à-dire qu'il permet 2048 transmissions **simultanées** entre le réseau masqué et le réseau non masqué.

Au bout d'un délai configurable, le routeur suppose que l'entrée ne sera plus réutilisée et la supprime dans le tableau.

### Quels protocoles peuvent être utilisés avec le masquerading IP ?

Evidemment uniquement ceux qui communiquent via les ports. Les protocoles ne recourant pas aux numéros de port ou qui utilisent les ports à un niveau supérieur à IP dans le modèle de référence OSI ne peuvent pas être masqués sans appliquer de procédure particulière.

Dans sa version actuelle, le routeur effectue le masquage pour les protocoles suivants :

- TCP (et tous les protocoles basés sur TCP tels que FTP, HTTP etc.)
- UDP
- ICMP

### Routage par DNS

Quand un utilisateur navigue dans Internet, il n'utilise pas une adresse IP pour accéder à un serveur, mais des noms. Et qui est le premier à savoir quelle adresse correspond à 'www.domain.com' ? Le serveur DNS !

DNS signifie Domain Name Service et désigne l'affectation des noms de domaine (tels que domaine.com) aux adresses IP correspondantes. Ces informations doivent naturellement être gérées en permanence et être disponibles dans le monde entier. C'est là qu'interviennent les serveurs DNS qui proposent des tableaux volumineux contenant les adresses IP et les noms de domaine.

Lorsqu'un ordinateur implanté dans Intranet veut accéder à une page d'accueil, il émet d'abord une requête DNS : « Quelle adresse IP appartient à www.domain.com ? »

- Le routeur recherche d'abord dans sa propre configuration si un serveur DNS a été défini (dans l'onglet 'Adresses' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou dans le menu /Setup/Module TCP-IP). S'il trouve cette

indication, il établit une connexion avec ce serveur et récupère l'information souhaitée.

- Lorsqu'aucun serveur DNS n'est déclaré dans le *ELSA LANCOM Wireless*, le routeur essaie d'accéder à un serveur DNS via une connexion PPP éventuellement en cours (p.ex. avec le fournisseur d'accès), et tire la combinaison adresse IP/nom de ce serveur. Naturellement, cela fonctionne uniquement si l'adresse d'un serveur DNS a été transmise au *ELSA LANCOM Wireless* pendant la négociation PPP.

Avec cette procédure, vous n'avez aucun besoin de connaître les adresses d'un serveur DNS. En outre, l'adresse du serveur DNS est aussi mise à jour automatiquement. p.ex., au cas où le fournisseur d'accès modifie le nom de son serveur DNS, ou si vous changez de fournisseur, le routeur obtient toujours l'information à jour.

## Policy Based Routing : routage stratégique

« Policy Based Routing » désigne une procédure de traitement préférentiel de certains paquets recourant à un champ spécial du paquet IP, le champ TOS (Type-of-Service). Ce traitement préférentiel de certains paquets est destiné p.ex. à faciliter la configuration du routeur via le réseau étendu si un volume important de données doit être transmis en même temps.



*Vous trouverez des informations complémentaires sur le routage stratégique dans le chapitre 'Description des menus' du Manuel de référence.*

## Gestion d'adresses automatique via DHCP

Pour une exploitation sans accroc 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, permettant 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. À 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 attributions 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 dans le réseau des adresses ne se trouvant 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.
- 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. Une adresse valable issue du pool est choisie comme adresse IP. 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.

### Attribution du masque de réseau

L'attribution 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'attribution. Sinon, le masque de réseau issu du module TCP/IP sera utilisé.

### Attribution de l'adresse de diffusion

En règle générale, est utilisée, dans le réseau local pour les paquets diffusés, une adresse résultant 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 aucun serveur n'est indiqué dans les zones correspondantes, le routeur définit sa propre adresse IP comme adresse DNS. Celle-ci est déterminée comme décrit au Paragraphe 'Attribution des adresses IP'. Le routeur utilise alors l'acheminement DNS (voir également 'Routage par DNS'), pour résoudre les requêtes DNS ou NBNS de l'hôte.

### **Affectation de la passerelle par défaut**

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

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 valables 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, tandis 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'attribution**

De manière standard, la presque totalité des paramètres dans l'environnement réseau de Windows sont définis de manière à ce que les paramètres nécessaires soient requis 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'attribution**

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'attribution par le serveur DHCP.

Sous Windows, cela se fait par ex. par les propriétés de l'environnement 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'attribution des adresses IP aux ordinateurs aux postes de travail respectives à l'aide de la commande 'Setup/Module DHCP/Table-DHCP'. 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'attribution 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 devant 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 :

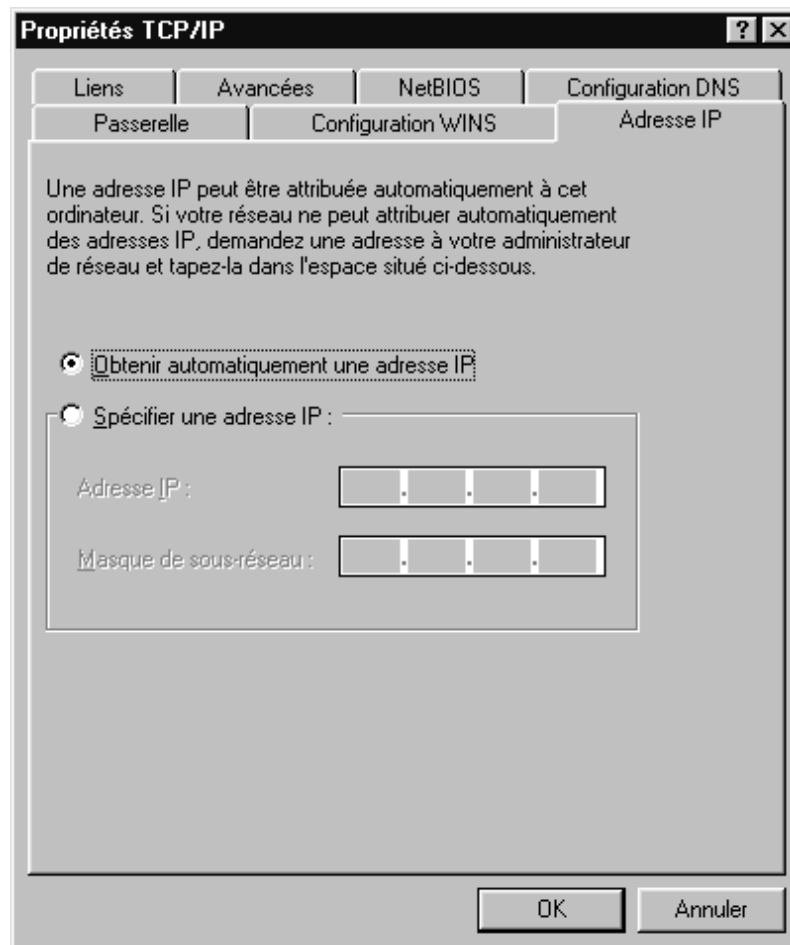
- Jusqu'à maintenant, vous n'aviez pas installé de réseau ou bien votre réseau local n'utilise pas TCP/IP. Grâce au serveur DHCP dans votre nouveau périphérique ELSA, vous pouvez d'un coup attribuer des adresses IP à tous les ordinateurs du réseau et au périphérique lui-même.
- Vous avez déjà utilisé 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.
- 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 l'outil de configuration *ELSA LANconfig* sur l'un des ordinateurs dans le réseau.
- ⑤ Démarrez le programme dans le groupe de programmes 'ELSAIlan'. 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'attribution 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'attribution 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 sous 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.

## DNS

Dans les réseaux TCP/IP, le service DNS (Domain Name Service) crée le lien entre les noms d'ordinateur ou les noms de réseau (domaines) et les adresses IP. Ce service est en tout cas nécessaire à la communication sur Internet, par ex. pour répondre par l'adresse IP appropriée à une requête adressée à 'www.elsa.de'. Toutefois, également au sein d'un réseau local, ou lors d'une connexion LAN, il est utile de pouvoir affecter les adresses IP dans le LAN aux noms des ordinateurs de manière à ce qu'il n'y ait pas d'ambiguïté.

## Que fait un serveur DNS?

Les noms demandés au serveur DNS se composent de plusieurs parties : une partie est le nom propre de l'hôte ou du service auquel on souhaite accéder; une autre partie indique le domaine. L'indication du domaine est facultative au sein d'un réseau local. Ces noms peuvent être par ex. 'www.domain.com' ou 'ftp.domain.com'.

Chaque nom inconnu au niveau local est recherché sans serveur DNS dans le réseau local via la route par DEFAULT. En revanche, l'utilisation d'un serveur DNS permet de rechercher, directement dans le bon réseau correspondant, tous les noms connus par leur adresse IP. Le serveur DNS peut en principe être un ordinateur séparé se trouvant dans le réseau. Cependant, les raisons suivantes nous amènent à envisager une implantation du serveur DNS directement dans le routeur *ELSA LANCOM Wireless* :

- Un routeur *ELSA LANCOM Wireless* faisant fonction de serveur DHCP est en mesure d'affecter de façon autonome les adresses IP aux ordinateurs au sein du réseau local. Le serveur DHCP connaît donc déjà par leur nom d'ordinateur et par leur adresse IP tous les ordinateurs de son propre réseau recevant leur adresse IP via DHCP. Lors de l'attribution dynamique de l'adresse via le serveur DHCP, un serveur

DNS externe aurait probablement des difficultés à maintenir actuelle l'association de l'adresse IP et du nom.

- Par ailleurs, lors du routage de réseaux Windows via NetBIOS, un routeur *ELSA LANCOM Wireless* connaît les noms d'ordinateur et les adresses IP au sein des autres réseaux NetBIOS connectés. En outre, les ordinateurs avec adresse IP fixe s'identifient éventuellement aussi dans le tableau NetBIOS et sont ainsi connus par leur nom et leur adresse.
- Le serveur DNS dans le routeur *ELSA LANCOM Wireless* peut être utilisé en même temps comme mécanisme filtrant très convivial. Les requêtes concernant certains domaines auxquels l'accès n'est pas permis, peuvent être verrouillées pour tout le réseau local, ou seulement pour des sous-réseaux voire des ordinateurs isolés; pour cela, il suffit d'indiquer le nom des domaines concernés.

Lors de requêtes relatives à certains noms, le serveur DNS effectue la recherche en tenant compte de toutes les informations dont il dispose :

- Le serveur DNS vérifie d'abord que l'accès à ce nom n'est pas interdit par la liste des filtres. Si tel est le cas, un message d'erreur informe l'ordinateur requérant qu'il n'a pas le droit d'accéder à ce nom.
- Puis il recherche dans son propre tableau DNS statique des entrées ayant trait au nom en question.
- Si le tableau DNS ne contient aucune entrée pour ce nom, le tableau DHCP dynamique est balayé. Au besoin, l'utilisation des informations DHCP peut être désactivée.
- Lorsque le serveur DNS ne trouve aucune information sur le nom dans les tableaux précédents, il parcourt les listes du module NetBIOS. Au besoin, l'utilisation des informations NetBIOS peut être désactivée.

Si le nom recherché ne peut être trouvé dans aucune information disponible, le serveur DNS retransmet la requête à un autre serveur DNS (par ex. chez le fournisseur d'accès Internet) via le mécanisme d'acheminement DNS normal, ou envoie un message d'erreur à l'ordinateur requérant.

## Configurer le serveur DNS

Vous trouverez les paramètres du serveur DNS dans l'onglet 'Serveur DNS' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*. Pour configurer le serveur DNS, procédez de la manière suivante :

- ① Activez le serveur DNS.  
  
`set setup/Module dns/operating on`
- ② Entrez le domaine auquel appartient le serveur DNS. C'est sur la base de ce domaine que le serveur DNS reconnaît si le nom recherché dans une requête fait partie du réseau local ou non. L'indication du domaine est facultative.

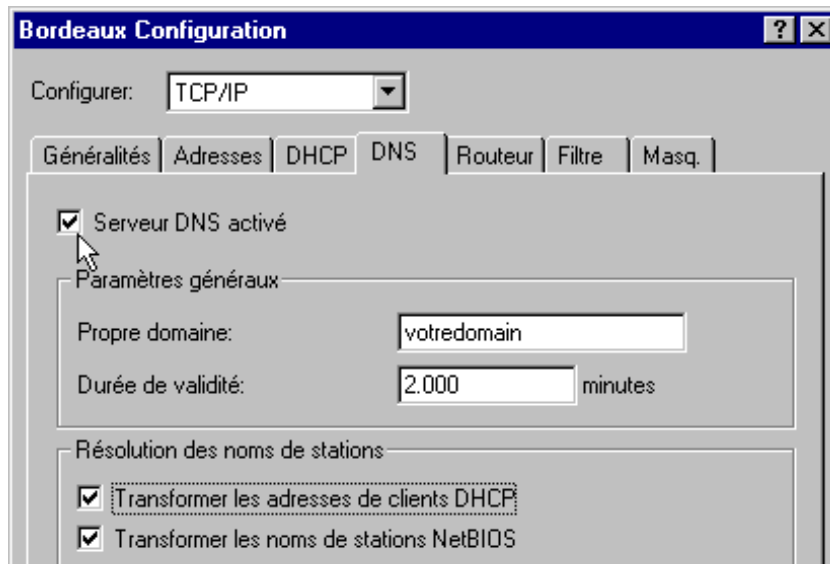


```
set setup/Module dns/domain votredomaine.com
```

- ③ Indiquez ici si les informations depuis le serveur DHCP et le module NetBIOS doivent être utilisées.

```
set setup/Module dns/utiliser dhcp oui
```

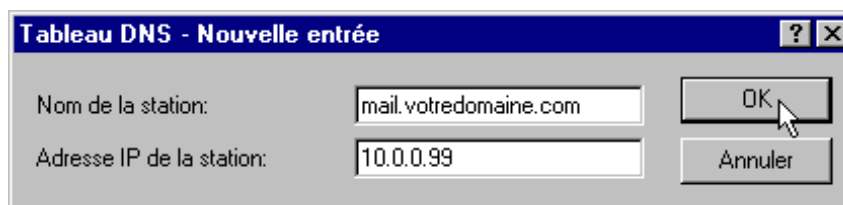
```
set setup/Module dns/utiliser NetBIOS oui
```



- ④ Le serveur DNS sert avant tout à séparer les requêtes relatives à des noms sur Internet des requêtes relatives à des noms chez d'autres correspondants. Entrez donc, dans le tableau DNS, tous les ordinateurs

- dont vous connaissez le nom et l'adresse IP,
- ne faisant pas partie de votre réseau local,
- ne se trouvant pas sur Internet, mais
- joignables via le routeur.

Si vous vous trouvez par ex. dans un bureau détaché et que vous souhaitez vous connecter sur le serveur de messagerie électronique du bureau central (nom : mail.yourdomaine.com, IP : 10.0.0.99) via le routeur, entrez :



```
cd setup/Module dns/Tableau dns
```

```
set mail.votredomaine.com 10.0.0.99
```

L'indication du domaine, bien que facultative, est recommandée.

Si vous exécutez le logiciel de messagerie électronique, il recherchera probablement automatiquement le serveur 'mail.votredomaine.com'. Le serveur

DNS renverra l'adresse IP '10.0.0.99'. Le logiciel de messagerie électronique recherche alors cette adresse IP. Sur la base d'entrées adéquates dans le tableau de routage IP et la liste des noms, etc., la connexion au réseau du bureau central est établie automatiquement, et le serveur de messagerie électronique est enfin trouvé.

- ⑤ La liste des filtres vous permet de décider qui a le droit d'accéder à quel nom ou à quel domaine.

```
cd setup/Module dns/Liste des filtres
set 001 www.offlimits-domain.com 0.0.0.0 0.0.0.0
```

A l'aide de cette entrée (avec index '001'), vous verrouillez ce domaine pour tous les ordinateurs du réseau local. L'index '001' est arbitraire et ne sert que d'exemple. Lorsque vous entrez le domaine, il est permis d'utiliser également les caractères joker '?' (remplace exactement un caractère) et '\*' (remplace un nombre non défini de caractères). Si seul un ordinateur (par ex. IP 10.0.0.123) ne doit pas pouvoir accéder aux domaines DE, entrez :

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



*Le palmarès dans la statistique DNS vous montre les 64 noms les plus demandés, et vous propose ainsi une bonne base pour la configuration de la liste des filtres.*

Un bon choix des adresses IP et des masques de réseau vous permet également de filtrer des services lors de l'utilisation de sous-réseaux au sein de votre LAN. Songez que l'adresse IP '0.0.0.0' renvoie à tous les ordinateurs d'un réseau et que le masque de réseau '0.0.0.0' à tous les réseaux.

## Proxy NetBIOS

Avec sa fonction de proxy NetBIOS, un *ELSA LANCOM Wireless* peut également router des paquets NetBIOS ou répondre localement en tant que proxy. Il est dès lors possible, entre autres, d'interconnecter économiquement des réseaux Windows via les fonctions de routeur.

Ce chapitre décrit le fonctionnement général du proxy NetBIOS ainsi que la configuration du routeur et des ordinateurs impliqués dans l'interconnexion de réseaux Windows.

## En quelques mots : définition de NetBIOS

NetBIOS sert à interconnecter simplement et sans complication plusieurs ordinateurs. Un représentant courant des réseaux NetBIOS est le réseau Windows dans lequel plusieurs ordinateurs Windows 3.11, Windows 9x et Windows NT sont interconnectés et dans lequel les ressources de chaque ordinateur (lecteurs ou imprimantes) peuvent être mises à la disposition de tous les autres.

Dans un réseau Windows, les ordinateurs sont adressés au moyen de leur nom. Plusieurs ordinateurs peuvent former un groupe, et plusieurs groupes peuvent à leur tour former un espace d'adressage (Scopes). Pour qu'un ordinateur puisse accéder aux ressources des autres, les noms utilisés doivent être connus dans tout le réseau. Afin d'éviter de devoir gérer un tableau des noms sur chaque ordinateur, les ordinateurs du réseau NetBIOS communiquent leur nom aux autres à intervalle régulier.

Les noms communiqués de cette manière doivent naturellement aussi être collectés et mis à disposition par une instance centrale du réseau Windows. Lorsque deux réseaux Windows doivent être interconnectés via un routeur, une telle instance centrale, un serveur de noms NetBIOS (NBNS) doit se trouver des deux côtés de la connexion.

- A cet effet, on peut p.ex. installer dans le réseau un serveur WINS (Windows Internet Name Service-Server) dédié.
- Mais comme de nombreux réseaux Windows doivent ou veulent être exploités sans serveur dédié, il existe une deuxième méthode : les informations sur les noms utilisés peuvent être collectés sur un « tableau d'affichage » sur lequel tous les ordinateurs inscrivent uniquement leur nom et leur adresse IP. Dans ce cas, les ordinateurs sont eux-mêmes responsables de la cohérence des noms dans le réseau.

Un *ELSA LANCOM Wireless* dispose d'un tel « tableau d'affichage ». Grâce à cette réalisation simple du NBNS, il est possible d'interconnecter des réseaux Windows sans serveur dédié. Les ordinateurs dans les réseaux communiquent leur nom également dans l'autre réseau et s'inscrivent sur le tableau d'affichage de ce réseau.

## Traitement des paquets NetBIOS

Le comportement extrêmement loquace des ordinateurs Windows peut entraîner des coûts de communication très élevés dans le cas de connexions via le RNIS, puisque chaque paquet NetBIOS contenant les informations sur le nom conduit automatiquement à l'établissement d'une connexion (p.ex. avec le FAI). En raison de ces paquets, la ligne reste constamment active et la facture gonfle sans que des données véritablement utiles soient transmises.

Afin d'éviter ces connexions inutiles, un *ELSA LANCOM Wireless* peut soit router les paquets NetBIOS ou répondre lui-même en tant que proxy :

- Pour router les paquets vraiment nécessaires, il est possible d'indiquer dans le module NetBIOS à quels correspondants les informations sur le nom doivent être transmises via NetBIOS. Quand on active le module NetBIOS, une connexion est établie avec les correspondants NetBIOS au bout d'un délai d'attente aléatoire (dans la mesure où il ne s'agit pas d'ordinateurs d'accès à distance). Si la connexion ne peut pas être établie, le délai d'attente est rallongé. C'est lors de ce premier échange des informations NetBIOS que le tableau d'affichage est rempli pour la première fois.
- Dans sa fonction en tant que proxy, le périphérique répond lui-même aux requêtes adressées aux ordinateurs connus dans le module NetBIOS (le tableau d'affichage) et se fait ainsi le délégué de l'ordinateur correspondant. Ainsi, de nouvelles connexions ne sont pas établies après le premier échange d'informations ni à l'occasion de la recherche d'un ordinateur dans le propre réseau local, ni à l'occasion de la recherche d'ordinateurs connus dans le réseau du correspondant.

Pour que la recherche des ordinateurs, ne se trouvant ni dans le réseau local ni dans les réseaux des correspondants NetBIOS, ne conduisent pas à une connexion via la route par DEFAUT dans Internet, le filtre IP préconfiguré pour les ports NetBIOS intercepte ces paquets et empêche l'établissement de la connexion.

## Quelles sont les conditions requises ?

Pour une communication parfaite entre les réseaux Windows via un routeur, certains composants requis doivent être installés sur les ordinateurs et plusieurs paramètres être configurés dans le système d'exploitation.

### Composants installés

L'installation des composants requis est illustrée ici sur la base de Windows 95 ou Windows 98, mais se déroule de façon similaire sous Windows NT 4.0. Installez les composants suivants sur tous les ordinateurs des réseaux Windows à interconnecter :

- Protocole réseau  
NetBIOS est entièrement indépendant du protocole de transfert utilisé. Ainsi, un réseau NetBIOS peut utiliser les protocoles NetBEUI (NetBIOS Extended User Interface), IPX (Internet Packet eXchange, Novell) ou IP (Internet Protocol).



*A l'inverse de IPX et de IP, NetBEUI ne peut pas être routé, ce protocole n'est donc disponible qu'au sein d'un réseau Windows. Lorsque plusieurs réseaux Windows doivent être interconnectés via routeur, NetBIOS doit se baser sur un protocole pouvant être routé, p.ex. sur IP dans ELSA LANCOM Wireless !*

Le routage des paquets NetBIOS dans *ELSA LANCOM Wireless* est basé sur TCP/IP en raison des meilleurs mécanismes de filtrage. Ce protocole doit donc être installé sur tous les ordinateurs à interconnecter.

Pour installer le protocole réseau, cliquez sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau ► Ajouter ► Protocole**. Sélectionnez 'Microsoft' comme constructeur et le protocole réseau 'TCP/IP'.

■ Client

Le client pour réseaux Windows est nécessaire pour que les ordinateurs dans le réseau Windows puissent s'annoncer avec leur nom et leur mot de passe.

Pour installer le client, cliquez sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau ► Ajouter ► Client**. Sélectionnez 'Microsoft' comme constructeur, puis 'Client pour réseaux Windows'.

■ Service

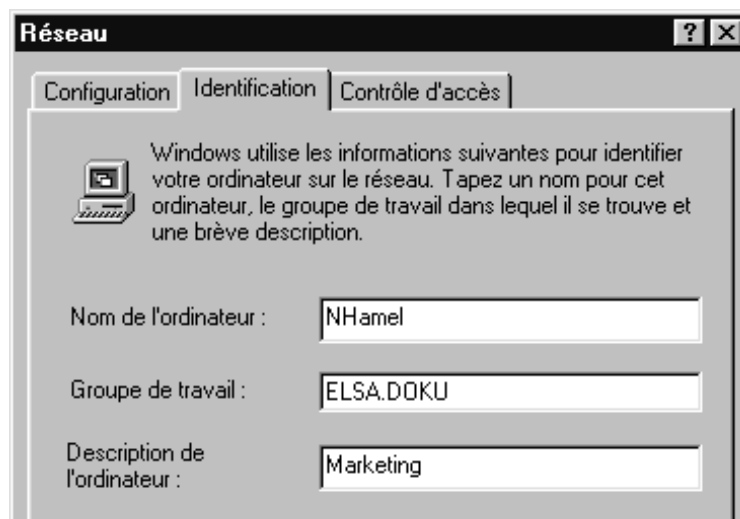
Le partage de fichiers et d'imprimantes permet à d'autres utilisateurs d'utiliser les lecteurs et les imprimantes du réseau Windows.

Pour installer le partage de fichiers et d'imprimantes, cliquez sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau ► Ajouter ► Service**. Sélectionnez 'Microsoft' comme constructeur, puis 'Partage de fichiers et d'imprimantes pour réseaux Windows'.

### Paramétrages dans le réseau Windows

■ Noms et désignation des groupes

Cliquez sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau**, et sélectionnez l'onglet '**Identification**'.

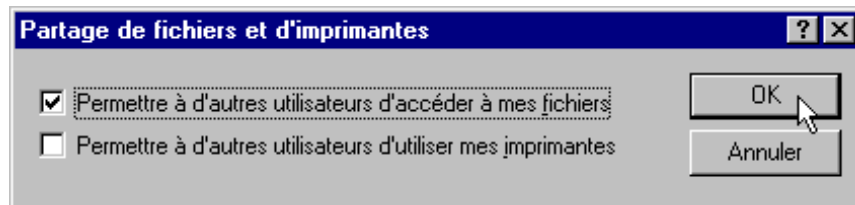


Le nom de l'ordinateur doit être unique. Ceci est valable pour tous les réseaux Windows et tous les groupes de ces réseaux devant être interconnectés via NetBIOS. Par conséquent, le même nom ne doit pas exister plusieurs fois dans des réseaux différents.

■ Partage de fichiers et d'imprimantes

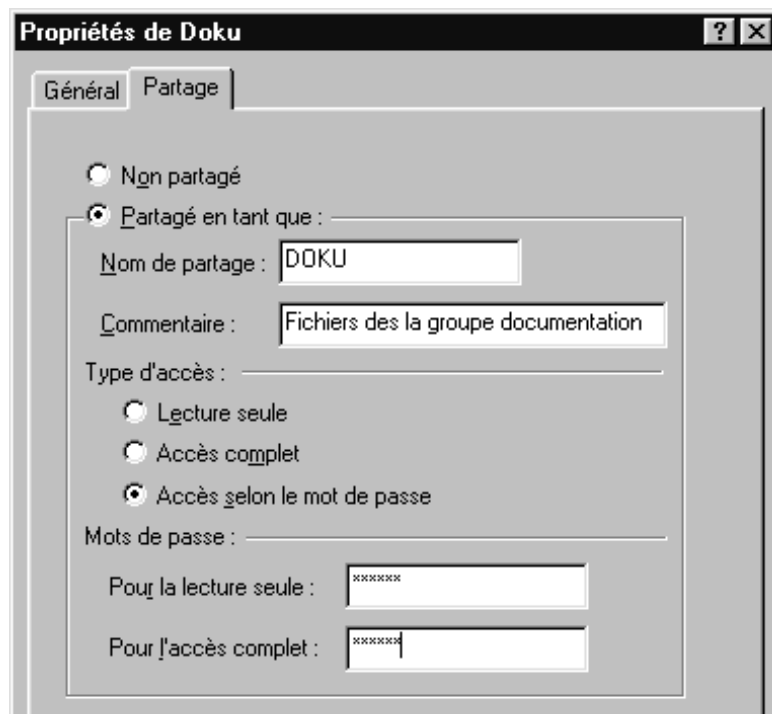
Après l'installation, vérifiez si le partage de fichiers et d'imprimantes est actif.

Cliquez à cet effet sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau ► Partage de fichiers et d'imprimantes**. Choisissez si les autres utilisateurs dans le réseau Windows doivent pouvoir accéder à l'imprimante ou aux fichiers de cet ordinateur.



Tous les utilisateurs souhaitant accéder aux ressources partagées doivent s'annoncer avec un nom d'utilisateur et un mot de passe au démarrage de Windows.

Pour partager un lecteur, un dossier ou une imprimante, cliquez sur le nom correspondant dans l'explorateur Windows avec le bouton droit de la souris, et sélectionnez la commande **Partage** du menu contextuel.



Donnez un nom au dossier partagé et, au besoin, saisissez une remarque. En sélectionnant le type d'accès et en fixant les mots de passe, vous indiquez comment l'accès aux ressources partagées est réalisé.

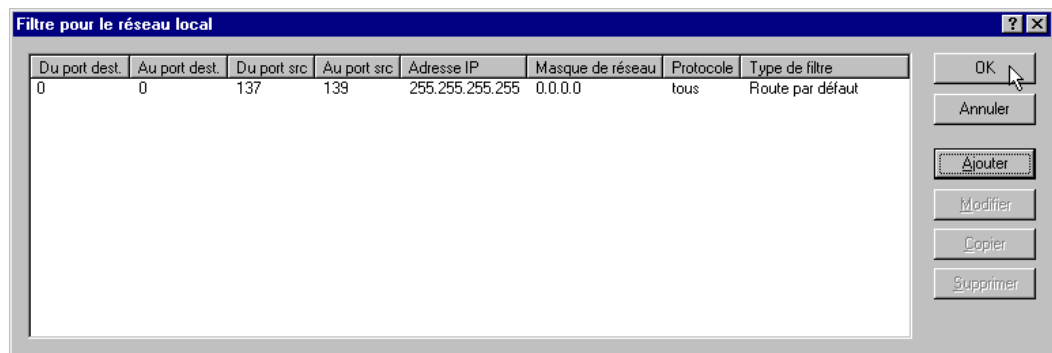


*Vous pouvez vérifier facilement si les paramètres dans le réseau Windows sont corrects : le nom de votre propre ordinateur doit être affiché dans l'environnement réseau.*

## Interconnecter deux réseaux Windows via le RNIS

Après avoir fait tous les préparatifs, vous êtes prêt à coupler deux réseaux Windows. La configuration des réseaux de groupe de travail et de domaine (Windows NT) est similaire. Les étapes suivantes doivent être réalisées des deux côtés de la connexion.

- ① Configurez les deux réseaux pour l'interconnexion entre deux réseaux locaux via TCP/IP, comme décrit dans le chapitre Workshop. A cet effet, utilisez si possible l'assistant convivial de *ELSA LANconfig*.
- ② Vérifiez la configuration du filtre IP. Ce filtre doit s'appliquer à tous les paquets NetBIOS devant être transmis via la route par DEFALT afin que les paquets NetBIOS ne conduisent pas à l'établissement d'une connexion via la route par DEFALT. Ce filtre est préconfiguré de cette façon au départ usine des périphériques.



- ③ Saisissez ensuite le correspondant pour le routage via NetBIOS. Sélectionnez le dossier de configuration 'NetBIOS' de *ELSA LANconfig*, et créez une nouvelle entrée dans le tableau 'NetBIOS via routage IP'.



Pour la configuration via Telnet, procédez de la façon suivante :

```
cd /Setup/Module NetBIOS/Onglet Correspondants
set nhamel.mobil router
```

La valeur dans le champ 'Type' indique si le correspondant doit être appelé directement après avoir activé le module NetBIOS pour échanger les informations sur les noms.



*Le paramètre 'Domaine NT' n'a en règle générale pas besoin d'être renseigné dans les réseaux Windows 95 ou Windows 98. Pour les accès aux ordinateurs Windows NT, le domaine/groupe de travail doit être saisi manuellement.*

- ④ Lorsque le couplage NetBIOS utilise une connexion PPP, vérifiez dans la liste PPP que NetBIOS soit actif.
- ⑤ Une fois tous les correspondants saisis, activez la fonction NetBIOS.

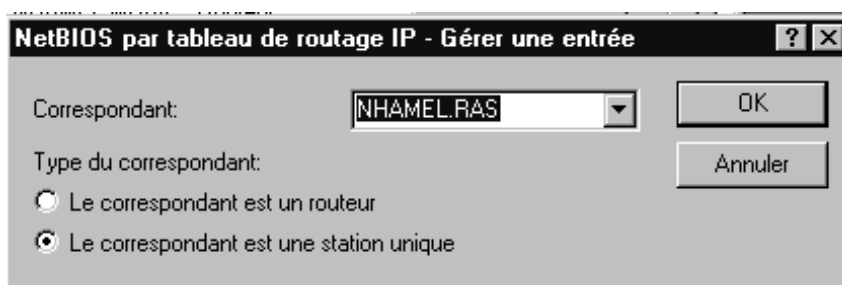
```
cd /Setup/Module NetBIOS
set état actif
```

Après la mise sous tension, une connexion est établie (après un délai d'attente aléatoire) avec tous les correspondants qui ne sont pas mis en évidence comme nœud d'accès. Les informations nécessaires sur les ordinateurs dans les réseaux sont échangées lors de cette première connexion. L'accès aux ordinateurs distants n'est possible qu'après cet échange.

## Accès par les ordinateurs distants

L'accès par un ordinateur distant à un réseau Windows via un accès à distance s'effectue aussi très rapidement.

- ① *ELSA LANCOM Wireless* et les ordinateurs distants sont préparés à l'accès réseau comme décrit dans le chapitre 'Workshop'. Ici aussi, il s'agit de vérifier les filtres IP dans *ELSA LANCOM Wireless* (voir 'Interconnecter deux réseaux Windows via le RNIS').
- ② Si les adresses IP du correspondant distant sont attribuées à partir du pool IP, une route supplémentaire doit être créée dans le tableau de routage IP pour ce correspondant.
- ③ Créez une entrée dans le tableau de routage IP NetBIOS aussi pour les correspondants distants.



```
cd /Setup/Module NetBIOS/Onglet Correspondants
set nhamel.ras workstation
```



*Mettez cette entrée en évidence en tant que 'station isolée' pour que ce correspondant ne soit pas appelé automatiquement une fois le module NetBIOS activé.*

- ④ Lorsque le couplage NetBIOS utilise une connexion PPP, vérifiez dans la liste PPP que NetBIOS est actif.



## Qui cherche trouve : l'environnement réseau

Une fois tous les participants préparés pour le routage NetBIOS, le travail dans le réseau Windows peut commencer.

### Routage NetBIOS après l'interconnexion de réseaux locaux

Une fois que les réseaux ont échangé - après la mise sous tension des modules NetBIOS - leurs informations sur les ordinateurs accessibles, une liste contenant les noms des ordinateurs est disponible dans *ELSA LANCOM Wireless*. Via Telnet, il est possible de consulter la liste des ordinateurs actuellement accessibles en sélectionnant

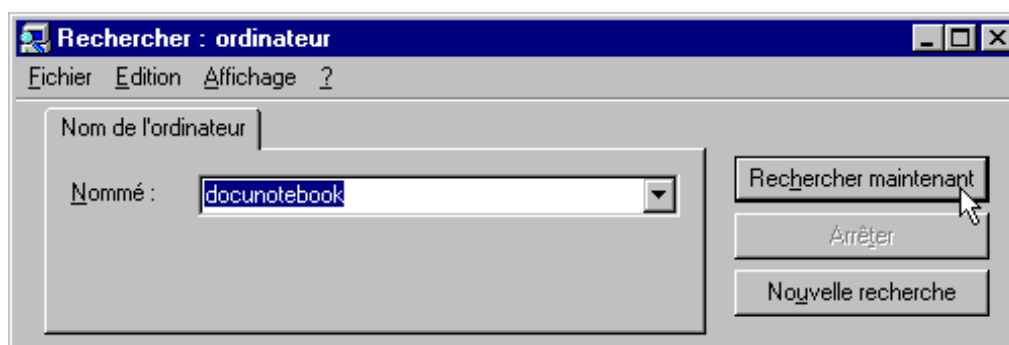
```
dir /Setup/Module NetBIOS/Liste des hôtes
```

Cette liste a p.ex. l'aspect suivant :

Nom	Type	Adresse IP	ID distant	Timeout	Flags
DOCUNOTEBOOK	00	10.10.0.53	NHAMEL.MOBIL	4939	0020
DOCUNOTEBOOK	20	10.10.0.53	NHAMEL.MOBIL	4939	0020
ELSA	1d	10.10.0.53	NHAMEL.MOBIL	4939	0020
ELSA.DOCU	1d	10.1.253.246	4935	0000	
ELSA.DOCU	1d	192.168.100.162	4997	0000	
NHAMEL.MOBIL	00	10.10.0.1	NHAMEL.MOBIL	0	0020

P.ex., ce tableau indique que l'ordinateur ayant le nom 'DOCUNOTEBOOK' est accessible avec l'adresse IP '10.10.0.53' via le correspondant 'NHAMEL.MOBIL'. Les autres paramètres sont expliqués dans la description du menu.

Pour pouvoir accéder aux ressources partagées de cet ordinateur, recherchez l'ordinateur au moyen de l'explorateur Windows en sélectionnant **Démarrer ► Chercher ► Ordinateur**.



*Pour des raisons techniques, les groupes de travail et les ordinateurs du réseau distant ne peuvent pas être trouvés par la fonction 'parcourir tout le réseau' dans l'environnement réseau Windows. On peut néanmoins rechercher des ordinateurs distants, comme décrit plus haut, ou réaliser des connexions à des lecteurs réseau.*

### Routeur NetBIOS via accès RAS

La procédure d'accès au réseau Windows via RAS est légèrement différente. Les deux différences essentielles d'interconnexion entre deux réseaux locaux sont les suivantes :

- Il n'existe pas, du côté du nœud d'accès, une liste des hôtes permettant de détecter les ordinateurs accessibles dans le réseau Windows du correspondant. L'utilisateur RAS doit donc connaître le nom des ordinateurs auxquels il souhaite accéder et auxquels il est autorisé à accéder.
- La connexion n'est pas établie automatiquement. L'utilisateur RAS doit donc d'abord établir une connexion avec *ELSA LANCOM Wireless* au moyen de l'Accès réseau à distance.

Une fois la connexion établie, il pourra rechercher et accéder aux ordinateurs du réseau distant (avec **Chercher** ► **Ordinateur**, pas via l'environnement réseau !), tout comme dans le cas de l'interconnexion de deux réseaux locaux.

## Bureautique et *ELSA LANCAPI*

*ELSA LANCAPI* est une variante spéciale de l'interface CAPI, très répandue. CAPI signifie Common ISDN Application Programming Interface et réalise le lien entre des adaptateurs RNIS et les logiciels de communication. Ces logiciels à leur tour mettent à la disposition des ordinateurs des fonctions de bureautique telles que l'envoi/réception de télécopies ou un répondeur téléphonique.

Ce chapitre vous présente *LANCAPI* ainsi que les logiciels de communication fournis et vous donne quelques informations utiles pour l'installation des divers composants.

### *ELSA LANCAPI*

#### Avantages de *LANCAPI*

La mise en œuvre de l'interface *LANCAPI* apporte des avantages surtout économiques. Tous les ordinateurs aux postes de travail reliés au réseau local ont, via *LANCAPI*, libre accès aux fonctions de bureautique telles que le fax, le répondeur téléphonique et le transfert de fichiers. Toutes les fonctions sont mises à disposition via le réseau sans que les ordinateurs aux postes de travail aient besoin d'être équipés de matériel supplémentaire. Donc aucun achat d'adaptateurs de terminal RNIS ou de modems coûteux ne grève le budget informatique. Tout ce qu'il faut, ce sont les logiciels de communication et de bureautique à installer sur les ordinateurs aux postes de travail.

p.ex., dans le cas d'envoi de télécopies, un télécopieur RNIS est simulé sur l'ordinateur au poste de travail. Avec l'interface *LANCAPI*, le PC envoie le fax au routeur via le réseau, et c'est ensuite le routeur qui établit la liaison avec le destinataire via RNIS.

La flexibilité de l'interface *LANCAPi* permet aussi un certain échelonnement des voies de communication. Lorsque plusieurs canaux B deviennent nécessaires pour assurer le trafic, on installe simplement plusieurs routeurs supplémentaires dans le réseau. Tous les périphériques du réseau local se partagent alors les tâches.



*Nota : toutes les applications que vous exploitez via LANCAPi utilisent des liaisons RNIS directes et ne passent pas par le routeur intégré dans le périphérique. Par conséquent, les fonctions de coupe-feu et de contrôle du budget sont contournées !*

Lors de l'installation de la plupart des logiciels de fax prenant en charge le fonctionnement de CAPI, *LANCAPi* est détectée et utilisée automatiquement comme matériel fax Classe II.

### Installation du client *LANCAPi*

L'interface *LANCAPi* est formée par deux composants, un serveur (dans le *ELSA LANCOM Wireless*) et un client (sur les PC). Le client *LANCAPi* est installé sur les ordinateurs du réseau local souhaitant utiliser les fonction de l'interface *LANCAPi*.

- ① Introduisez le CD-ROM *ELSA LANCOM Wireless* dans le lecteur approprié. Lorsque le logiciel d'installation n'est pas exécuté automatiquement quand vous insérez le CD-ROM, ouvrez l'explorateur Windows et cliquez sur 'autorun.exe' se trouvant sur le CD *ELSA LANCOM Wireless*.
- ② Sélectionnez 'Installation du logiciel LANCOM'.
- ③ Marquez l'option 'ELSA LANCAPi'. Cliquez sur **Suivant** et suivez les instructions du logiciel d'installation.

Après un redémarrage de l'ordinateur, l'interface *LANCAPi* est prête à remplir les tâches que lui envoient les logiciels de communication. Après installation, l'icône *ELSA LANCAPi* apparaît dans la barre des tâches. Double-cliquez sur cette icône pour ouvrir une fenêtre dans laquelle vous pouvez consulter les informations sur *ELSA LANCAPi*.

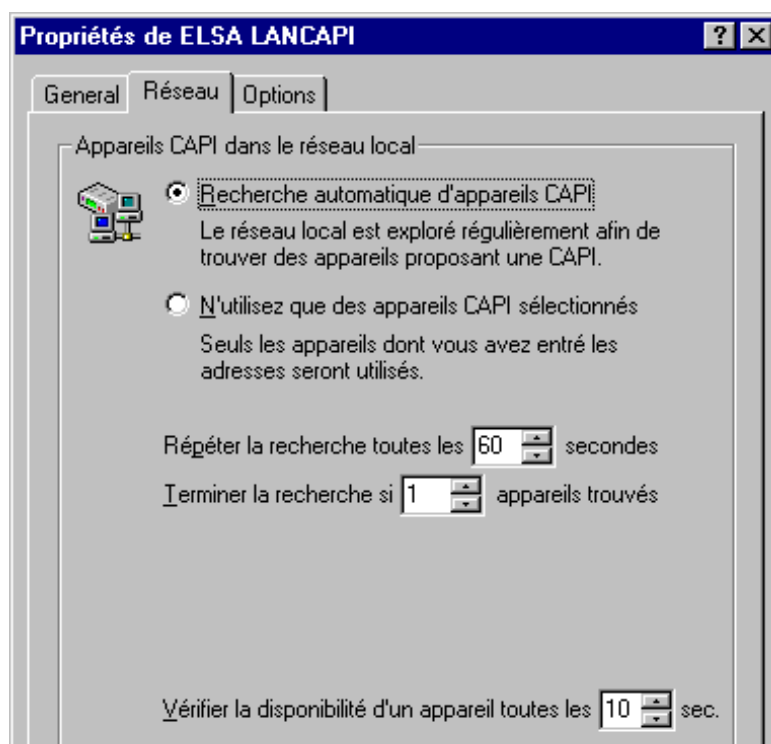
### Configuration du client *LANCAPi*

Il s'agit d'indiquer les serveurs *LANCAPi* devant être utilisés par les clients, et de sélectionner la méthode de contrôle. Si vous n'exploitez qu'un seul *ELSA LANCOM Wireless* dans votre réseau local comme serveur *LANCAPi*, vous pouvez en principe laisser tous les paramètres tels qu'ils sont (paramètres par défaut).

- ① Démarrez le client *LANCAPi* dans le dossier 'ELSAAlan'. Vous trouverez dans l'onglet 'Généralités' les informations sur le pilote du service mis à disposition.
- ② Sélectionnez l'onglet 'Serveur LANCAPi'. Indiquez si le PC doit rechercher son serveur *LANCAPi* lui-même ou s'il doit utiliser un serveur précis.
  - Dans le premier cas, indiquez aussi à quel intervalle le client doit chercher un serveur. Il recherchera jusqu'à ce qu'il ait trouvé le nombre de serveurs indiqué

dans le champ suivant. Il arrête la recherche dès qu'il a trouvé le nombre requis de serveurs.

- Lorsque le client ne doit pas rechercher automatiquement les serveurs, spécifiez dans la liste l'adresse IP des serveurs à utiliser par le client. L'indication de ces adresses est judicieuse p.ex. lorsque vous exploitez plusieurs *ELSA LANCOM Wireless* en tant que serveurs *LANCAPI* dans votre réseau local, et si un groupe de plusieurs PC doit utiliser un serveur donné.
- En ce qui concerne les deux options, vous avez encore la possibilité d'indiquer à quel intervalle le client vérifie si les serveurs trouvés ou figurant dans la liste sont encore actifs.



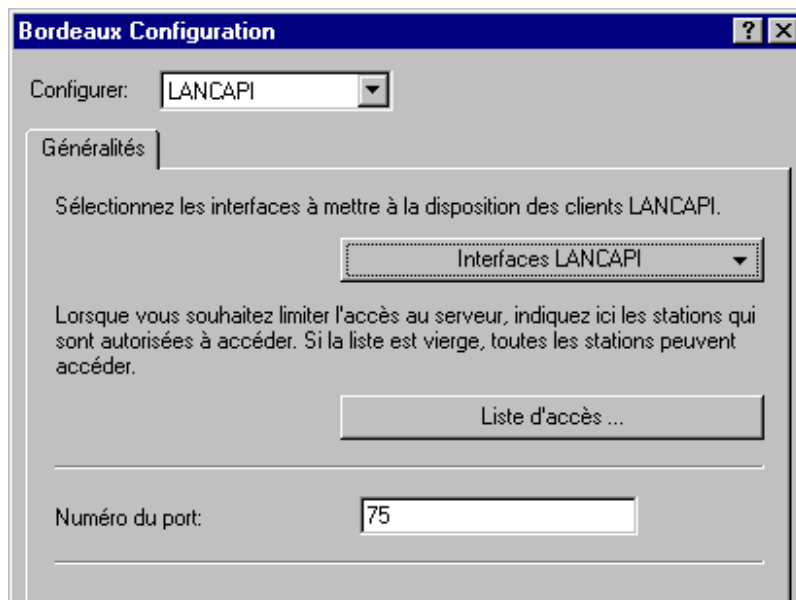
### Configuration du serveur LANCAPI

La configuration du serveur *LANCAPI* répond en principe à deux questions :

- A quels numéros d'appel l'interface *LANCAPI* doit-elle réagir ?
- Quel ordinateur du réseau local doit avoir accès au réseau RNIS via *LANCAPI* ?

Pour configurer le serveur *LANCAPI*, suivez les instructions suivantes :

- ① Démarrez *ELSA LANconfig* se trouvant dans le dossier 'ELSAIan'. Ouvrez la configuration du routeur en double-cliquant sur le nom souhaité dans la liste, et sélectionnez la zone de configuration 'LANCAPI'.



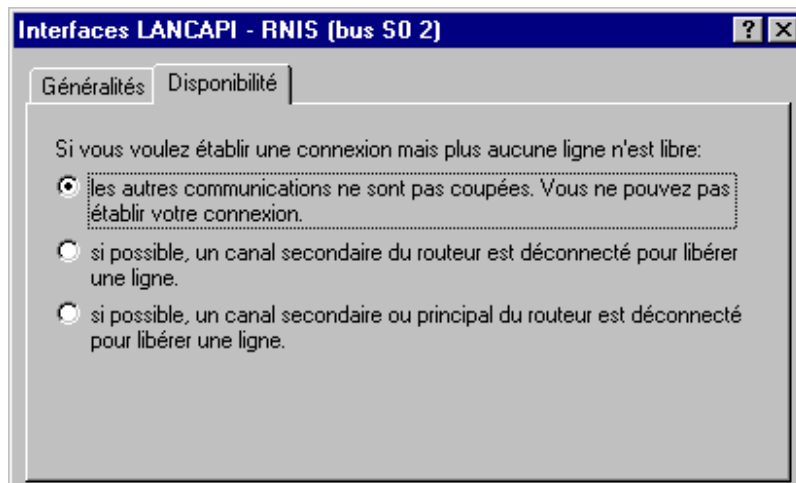
- ② Activez le serveur *LANC API*, ou autorisez uniquement les appels sortants. Dans le deuxième cas, l'interface *LANC API* ne réagit pas aux appels entrants et ne peut pas être mis en œuvre p.ex. pour la réception de télécopies. Autorisez p.ex. uniquement les appels sortants lorsque vous avez déjà attribué tous les numéros d'appel disponibles aux autres appareils de télécommunication.
- ③ Quand le serveur *LANC API* est actif, entrez dans le champ 'Numéro d'appel' les numéros de téléphone auxquels *LANC API* doit réagir. Séparez les numéros par un point-virgule. Pour que *LANC API* accepte tous les appels entrants, laissez ce champ vierge.
- ④ Par défaut, le port utilisé par *LANC API* est le port 75 (« any private telephony service »). Ne modifiez le port que si d'autres services l'utilisent déjà dans le réseau local.
- ⑤ Lorsque certains ordinateurs du réseau local ne doivent pas accéder aux fonctions de *LANC API*, spécifiez dans la liste d'accès l'adresse IP des participants autorisés.



*Si vous indiquez plusieurs numéros d'appel pour LANC API, vous pouvez mettre à la disposition des divers ordinateurs aux postes de travail p.ex. un télécopieur personnel ou un répondeur téléphonique personnel. Pour ce, indiquez des numéros d'appel différents lorsque vous installez les logiciels de communication (p.ex. ELSA-RVS-COM) sur les divers ordinateurs aux postes de travail.*

Sélectionnez l'onglet 'Disponibilité'. Indiquez comment un *ELSA LANCOM Wireless* se comporte lorsqu'une connexion doit être établie via *LANC API* (appel entrant ou sortant)

mais que les deux canaux B sont occupés (gestion des priorités). Les options disponibles sont les suivantes :



- La connexion ne peut pas être établie via *LANCAP*. Un logiciel de télécopie utilisant *LANCAP* fera vraisemblablement une deuxième tentative d'envoi ultérieurement.
- La connexion via *LANCAP* peut être établie lorsqu'un canal principal est libre. Un canal principal est le premier canal B utilisé pour une liaison établie par le routeur. Les canaux secondaires sont ceux qui s'ajoutent au canal principal pour un regroupement de canaux.
- Une connexion via *LANCAP* peut toujours être établie, une connexion du routeur sera coupée pour la durée de la communication. Ainsi, la fonction fax est toujours accessible.

### Utilisation de *LANCAP*

Vous avez deux possibilités d'utiliser *LANCAP* :

- Vous utilisez un logiciel qui accède directement à une interface CAPI (dans ce cas : *LANCAP*), p.ex. le logiciel *ELSA-RVS-COM*. Un logiciel de ce type recherche CAPI lors de l'installation et utilise ensuite cette interface automatiquement.
- D'autres logiciels tels que LapLink peuvent établir des connexions en empruntant des chemins différents, p.ex. via l'Accès réseau à distance de Windows. Lorsque vous créez une nouvelle connexion Accès réseau à distance, vous pouvez sélectionner lequel des périphériques de communication installés vous souhaitez utiliser. Pour *LANCAP*, sélectionnez 'ISDN WAN Line 1'.

## Le rerouteur téléphonique (least-cost router)

Depuis la libéralisation du marché téléphonique en Europe, les utilisateurs de services de télécommunication ont le choix entre toute une série d'opérateurs privés (Opérateur réseau) se distinguant par des tarifs pratiqués parfois très différents. Certains opérateurs proposent le reroutage à la demande (call-by-call), d'autres réclament en plus une

inscription préalable pour profiter de leurs services et vous utilisez automatiquement leur réseau, et d'autres encore ont leur propre infrastructure (Présélection). En général, pour router un appel via un opérateur alternatif, on compose d'abord le préfixe de cet opérateur pour accéder à son réseau, et on ne compose le numéro de téléphone du correspondant appelé qu'après ce préfixe.

Or, le tarif le plus avantageux n'est en règle générale jamais proposé par le même fournisseur suivant l'heure et la destination : le matin l'opérateur 1, l'après-midi l'opérateur 2 et pour les appels internationaux l'opérateur 3. Pour pouvoir toujours téléphoner, naviguer dans Internet ou transmettre des données au meilleur prix, il faudrait que vous réfléchissiez au tarif le plus avantageux systématiquement avant chaque appel. Un *ELSA LANCOM Wireless* se charge de ces réflexions pour vous. La fonction qui vous assiste ici s'appelle least-cost routing (LCR, établissement d'une communication au meilleur coût). Vous définissez pour commencer les opérateurs ayant les tarifs les plus avantageux pour vos besoins, et le routeur fait passer chaque appel (peu importe qu'il soit effectué par le routeur, l'interface *LANCAPI*, etc.) par l'opérateur le moins cher.

### Fonctionnement du reroutage téléphonique dans le *ELSA LANCOM*

Le rerouteur téléphonique (least-cost router, LCR) analyse les numéros composés p.ex. par le routeur ou l'interface *LANCAPI*.

Après chaque chiffre composé, le routeur vérifie s'il existe dans le tableau de reroutage une entrée (préfixe) correspondant aux premiers chiffres composés. Si une telle entrée existe, et si elle est valable pour l'heure et la date actuelle, le préfixe de l'opérateur privé est ajouté devant le numéro (avant l'indicatif) du correspondant. C'est uniquement lorsque le numéro du correspondant a été complété de cette façon qu'il est envoyé à l'autocommutateur public.

Le LCR a donc besoin des données suivantes :

- Les premiers chiffres d'un numéro (préfixe ou indicatif) qui détermine quels appels doivent être reroutés.
- Un ou plusieurs préfixes d'opérateur qui déterminent par quel fournisseur une communication doit être réacheminée dès qu'on compose l'indicatif du numéro d'appel.
- Les jours de semaine et les jours fériés auxquels l'entrée considérée est valable.
- L'heure ou la plage horaire pendant laquelle l'entrée est valable.

### Les premiers essais

Vous pouvez réduire votre facture considérablement rien qu'avec quelques entrées bien choisies. Nous voulons vous expliquer la programmation de la fonction de reroutage à l'aide d'un exemple simple.

Vous savez p.ex. que le reroutage permet d'économiser en particulier sur les appels longue distance et sur les appels internationaux avec Call-by-Call. Vous vous êtes renseigné chez plusieurs opérateurs privés proposant le reroutage direct et vous avez noté les tarifs les plus avantageux. Les premières entrées dans le tableau de routage ont alors p.ex. l'aspect suivant :

Préfixe du numéro (ou indicatif)	Préfixe de l'opérateur privé	Jours de semaine	Heure
03	1601	Sa + Di	0:00h à 23:59h
03	1602	Lu + Ma + Me + Je + Ve	8:00h à 18:00h
00	1601	Di	0:00h à 23:59h

Ces quatre entrées signifient que toutes les communications vers le quart nord-est de la France (numéros commençant par '03') effectuées le week-end sont reroutées sur le réseau de l'opérateur ayant le préfixe '1601'. En semaine, ces appels seraient reroutés sur le réseau de l'opérateur ayant le préfixe '1602' entre 8:00 heures et 18:00 heures. Le dimanche, les appels internationaux sont reroutés par l'opérateur ayant le préfixe '1601'.

### **Pour les initiés : optimiser le reroutage**

- Vous venez de voir dans le premier exemple que quelques entrées suffisent à réduire un peu la facture de téléphone. Pour tirer le meilleur parti du rerouteur téléphonique, vous devrez pour commencer vous renseigner sur les tarifs de tous les opérateurs actifs dans votre région. Ensuite, réfléchissez à la manière de présenter les tarifs et les zones tarifaires dans le tableau de reroutage du *ELSA LANCOM Wireless*. Vous devrez faire preuve d'une certaine méthodologie :
- Vous pouvez saisir directement les préfixes uniques ne risquant pas d'être confondus :
  - '00' pour les communications internationales
- Il serait très simple de rerouter tous les appels commençant par '0'. Mais lorsque les numéros de la propre localité et des circonscriptions de taxe environnantes appelées au tarif local commencent également par zéro, tous ces préfixes ne devraient pas figurer dans le tableau de routage. Songez aussi à tous les numéros spéciaux tels que le numéro vert commençant par '0800'.
- Une stratégie perfectionniste est de gérer tous les reroutages. On commence dans ce cas par les préfixes des zones les plus rapprochées, et on définit ensuite les zones plus éloignées. Les zones tarifaires rapprochées auront un préfixe relativement long et significatif, alors qu'il suffira de peu de chiffres pour les zones tarifaires éloignées (exemple pour la France : 01, 02, 03 et 04 si vous habitez dans la zone 05).



Le contenu du tableau pourra naturellement être amélioré au fur et à mesure. Voici quelques points auxquels vous devrez veiller :

- Dans certains pays et dans certains cas, on peut appeler un correspondant d'une autre circonscription de taxe au tarif local. Lorsque ces appels sont reroutés au moyen d'une entrée de reroutage à caractère général, le préfixe de l'opérateur normal permet d'acheminer l'appel au tarif normal (p.ex. le '8' pour le réseau de France Télécom). Une entrée vierge signifie également « pas de reroutage ».
- La plupart de vos connexions RNIS sont éventuellement destinées à un nombre limité de localités. Lorsque la plupart de vos correspondants se trouvent à Paris, vous pourrez les atteindre via le même opérateur.
- Etudiez les diverses zones tarifaires. Adressez-vous p.ex. aux opérateurs ou découvrez-les dans Internet.

Une fois les préfixes à rerouter déterminés, vous pourrez choisir l'opérateur. Vous aurez bien sûr besoin de tous leurs tarifs en vigueur. Là aussi, Internet peut vous aider à trouver ces tarifs. Il s'agit de déterminer : les tarifs par jour, heure, zone, réseau câble ou mobile. Une fois ces informations obtenues, vous pourrez entrer vos données dans le tableau de routage...

### Réglage des variables dans le least-cost router

Pour configurer le least-cost router, il s'agit notamment de répondre aux questions suivantes :

- Quels modes de fonctionnement du *ELSA LANCOM Wireless* doivent utiliser ses services de reroutage ?
- Quels appels doivent être routés, quand et via quel opérateur ?

Pour répondre à ces questions, procédez de la manière suivante :

- ① Dans *ELSA LANconfig*, sélectionnez la zone de configuration 'Least Cost Router', puis l'onglet 'Généralités'.
- ② Activez la fonction de reroutage. Elle peut être activée uniquement si l'horloge du routeur a été soit réglée manuellement, ou si l'heure a été calée sur celle du RNIS suite à une connexion (voir aussi 'Réglage de l'horloge' plus loin dans ce chapitre). Activez le LCR pour les modes de fonctionnement suivants selon vos besoins :
  - Routeurs
  - *LANCAPI*



*Si vous avez activé le least-cost routing également pour les modules de routage, des connexions seront éventuellement établies via des routeurs ne transmettant pas les informations de taxation ! Il est donc possible que vous ne puissiez plus profiter de la fonction de contrôle du budget sans que vous le remarquiez. Dans ce cas utilisez au besoin les budgets-temps.*

- ③ Sélectionnez l'onglet 'Plages horaires et jours fériés'. Ouvrez le **Tableau de Least Cost Routing**, créez une nouvelle entrée, et saisissez les données requises.
- Indiquez le préfixe ou l'indicatif à rerouter.
  - Indiquez les préfixes des opérateurs via lesquels les appels doivent être acheminés. Vous pouvez indiquer plusieurs opérateurs en les séparant par un point-virgule, et dans ce cas le LCR sélectionne automatiquement l'opérateur suivant si le précédent est occupé.
  - Indiquez les jours et la plage horaire pendant lesquels les appels considérés doivent être reroutés. Nota : la journée va de 00:00 heures à 23:59 heures ! p.ex., une plage horaire de 6 heures du soir à 6 heures du matin doit être découpée en deux périodes.
  - Cochez l'option de repli automatique au bas de la boîte de dialogue lorsque l'appel doit être acheminé via l'opérateur d'infrastructure normal (p.ex. France Télécom) lorsque tous les opérateurs alternatifs sont occupés. Si l'option de repli automatique est désactivée, le LCR reprend le premier opérateur de la série s'ils sont tous débordés.

- ④ Si vous avez créé des entrées pour des jours fériés dans le tableau de reroutage, ouvrez ensuite la liste des **Jours fériés**. Précisez la date exacte de chaque jour férié (JJ.MM.AAAA).
- ⑤ Vérifiez l'horloge interne du routeur (et la date) pour que le LCR active le reroutage à l'heure correcte (voir également 'Réglage de l'horloge' plus loin dans ce chapitre).

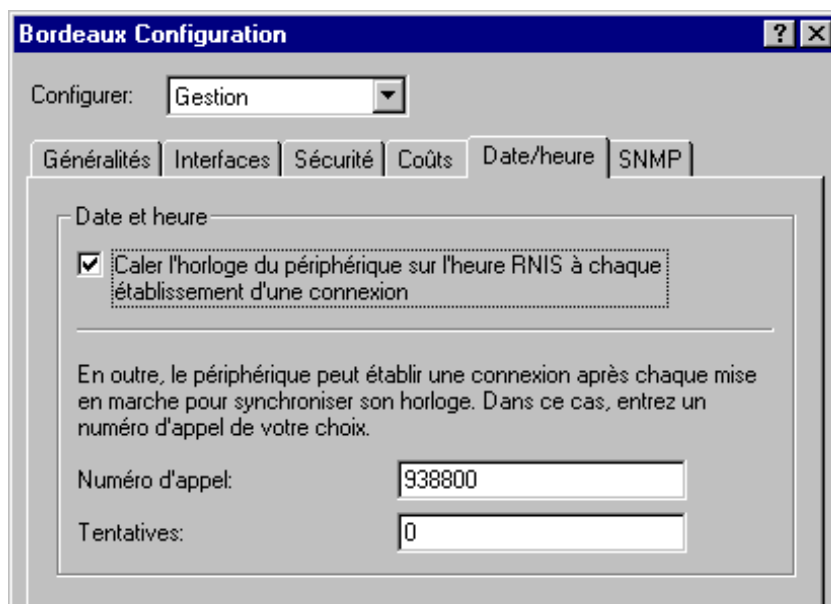


*Elargissez votre tableau de routage étape par étape, et vérifiez le résultat de chaque entrée. A cet effet, exécutez p.ex. ELSA LANmonitor et établissez - via ELSA LANAPI - les connexions avec les correspondants dans le tableau de reroutage. Vous pourrez vérifier à l'aide du numéro composé si l'entrée correspond à votre intention. En ce qui concerne les connexions via le routeur, vous pouvez consulter le numéro composé dans le fichier-journal (LANmonitor : **Affichage** ► **Options** ► **Protocole** ► **Afficher**).*

## Réglage de l'horloge

Pour que le least-cost router sélectionne l'opérateur correctement sur la base des entrées du tableau de reroutage, l'horloge interne du *ELSA LANCOM Wireless* doit naturellement toujours être exacte. Le routeur peut s'aider lui-même : il peut caler son horloge interne sur l'heure du RNIS soit chaque fois qu'il établit une connexion, soit quand on l'active.

- ① Dans *ELSA LANconfig*, sélectionnez l'onglet 'Date/heure' de la zone de configuration 'Gestion'.
- ② Au besoin, activez l'option 'Caler l'horloge du périphérique sur l'heure RNIS à chaque établissement d'une connexion'. Désactivez cette option si vous préférez régler l'horloge manuellement.
- ③ Le routeur oublie l'heure quand on le met hors tension. Entrez le numéro d'appel d'un correspondant de votre choix si le périphérique doit établir une connexion immédiatement après la mise sous tension et caler son horloge sur celle du RNIS. Indiquez également si ce correspondant est numérique (p.ex. boîte aux lettres électronique ou un FAI) ou analogique (horloge téléphonique ou service vocal).



*Contrôlez l'heure après la première connexion. Certains systèmes téléphoniques transmettent au routeur des informations incorrectes entraînant des erreurs de reroutage !*



# Appendice

## Caractéristiques techniques

### Spécifications matérielles

Bande de fréquences :	2400–2483,5 MHz (ISM)
Matériel :	Processeur : Hitachi SH3, 60 MHz, 4 Moctets de mémoire vive, 2 Moctets de mémoire flash-ROM
Débit de transmission de données	2 Mbps (avec possibilité de passage à 1 Mbps, sélection automatique de débit)
Portée :	jusqu'à 300 mètres en espace libre, env. 30 mètres en bâtiment clos (portées typiques)
Taux d'erreurs sur les bits :	Mieux que $10^{-5}$
Norme :	IEEE 802.11, DSSS (Direct Sequence Spread Spectrum)
Connexion LAN :	Ethernet IEEE 802.3, 10Base-T (RJ45)
Connexion WAN :	ISDN-S <sub>0</sub> -Bus (RJ45), conforme à I.430
Affichages/ Manipulation :	Témoins lumineux pour les statuts LAN, WAN et des périphériques
Certification :	Label CE, agréments pour tous les pays de l'UE et la Suisse
Sécurité d'exploitation :	Protection par mot de passe, cryptage (WEP, en prép.), IP masquerading (NAT), filtre coupe-feu
Connexions :	10Base-T, ISDN S <sub>0</sub> , Power
Garantie :	6 ans
Support :	via ligne d'assistance téléphonique (hotline), ELSA LocalWeb et Internet

### Spécifications logicielles

Modes de fonctionnement :	Routeur IP, Serveur DHCP, Client DHCP, Serveur DNS, Bridging transparent entre réseau local sans fil et réseau local câblé, Serveur <i>LANCAP</i> , Spoofing NetBIOS
Réseau Protocoles de réseau :	ARP, Proxy-ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, NetBIOS via IP
Filtre :	Filtre source et cible pour les réseaux, protocoles et ports ; WAN et LAN séparés
Contrôle des coûts de communication :	Taxes téléphoniques ou durée de la communication maximales pendant une période donnée ; fonctions de sécurité ou de coupe-feu configurables
Protocoles du canal D RNIS :	DSS1, 1TR6, configuration point-à-multipoint ou point-à-point, commutation automatique entre DSS1 et 1TR6 (désactivable), CLIP, MSN, EAZ, DDI

Protocoles du canal B RNIS :	Routeurs : Couche 1 : HDLC Kbps, HDLC 64 Kbps Couche 2 : X.75 LAPB, transparent Couche 3 : transparent, PPP, synchrone et asynchrone Compression de données LZS Stac, Hi/Fn Regroupement des canaux ML-PPP (statique et dynamique, incluant BACP) Traitement des scripts pour CompuServe Fonctionnement de CAPI : Couche 1 : HDLC Kbps, HDLC 64 Kbps Couche 2 : ISO 776 (X.75 SLP), transparent Couche 3 : transparent, T.90NL (avec compatibilité T.70NL)
IP masquerading NAT/PAT) :	Conversion de l'adresse IP et du port via une adresse IP ; Attribution statique et dynamique de l'adresse IP via PPP ou DHCP ; Masquage de TCP, UDP, ICMP et FTP ; DNS-Forwarding ; masquerading inverse pour services IP dans Intranet (p.ex. serveur Web)
Management :	Configuration TFTP et téléchargement du microprogramme, management SNMP via SNMP v.1 ou v.2, accès WAN et LAN activables et configurables séparément ; Accès de configuration pour le WLAN sans fil, commutable séparément, outils de diagnostic, affichage du statut <i>ELSA LANmonitor</i>
Sécurité d'exploitation :	Watchdogs matériel, autotests permanents, concept FirmSafe pour mise à jour à distance du logiciel
Sécurité :	Protection par mot de passe, PAP/CHAP, cryptage (WEP en préparation), IP masquerading (NAT/PAT), filtre de coupe-feu, protection par liste d'accès, cryptage WLAN, filtre WLAN
Statistiques :	Compteur de paquets LAN et WAN, compteurs d'erreurs, de connexions, de durée et d'unités

## Canaux radio

Chacun des 14 canaux radio qui peuvent être réglés pour un réseau sans fil a grâce à l'utilisation du DSSS une largeur de 22 MHz. Par conséquent avec la bande de fréquence ISM au maximum trois canaux indépendants les uns des autres sont possibles. Le tableau donne les fréquences moyennes et indiquent quels canaux sont autorisés dans quel pays.

	N° de canal	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		
2e bande radio canal 8	6	2437	X		
	7	2442	X		
	8	2447	X		
	9	2452	X		
	10	2457	X	X	X

	N° de canal	Fréquence moyenne [MHz]	UE (ETSI)	Espagne	France
3e 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'œuvre 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 (p.ex. une mise à jour des microprogrammes) 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 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 (p.ex. 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, p.ex. 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 ISDN / LAN Access Point  
**Type of Device:**  
**Typenbezeichnung:** LANCOM Wireless IL-2  
**Product Name:**  
**EG-Baumusterprüfbescheinigungsnummer:** D801136L  
**Registration No.:**  
**Benannte Stelle:** CETECOM ICT Services GmbH  
**Notified Body:** C E 0682 X

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:

This is to confirm that this product meets all essential protection requirements relating to the

#### Niederspannungs Richtlinie (73/23/EWG)

Low Voltage Directive (73/23/EEC)

#### EMV Richtlinie (89/336/EWG)

EMC Directive (89/336/EEC)

#### Netzzulassungsrichtlinie (98/515/EG)

Commission Decision (98/515/EC)

#### ISDN Richtlinie (97/346/EWG)

ISDN Directive (97/346/EEC)

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

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

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

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

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

**TBR 3: Nov. 1995**

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:

On behalf of the manufacturer / importer:

**ELSA AG**  
**Sonnenweg 11**  
**D-52070 Aachen**

abgegeben durch: / this declaration is submitted by:

Aachen, 9. September 1999

Aachen, 9<sup>th</sup> September 1999

i.V. Stefan Kriebel  
 Bereichsleiter Entwicklung  
 VP Engineering



# KONFORMITÄTSERKLÄRUNG

## DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

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

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:

This is to confirm that this product meets all essential protection requirements relating to the

### Niederspannungs Richtlinie (73/23/EWG)

Low Voltage Directive (73/23/EEC)

### EMV Richtlinie (89/336/EWG)

EMC Directive (89/336/EEC)

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

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

**ETS 300 328: 1996**

**ETS 300 826: 1997**

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

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

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

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:

On behalf of the manufacturer / importer:

**ELSA AG**  
**Sonnenweg 11**  
**D-52070 Aachen**

abgegeben durch: / this declaration is submitted by:

Aachen, 19. August 1999

Aachen, 19<sup>th</sup> August 1999

i.V. Stefan Kriebel  
Bereichsleiter Entwicklung  
VP Engineering



# Index

## ■ Numerics

1TR6 .....	6, R-50
802.11 .....	5

## ■ A

Accès à distance .....	62
Accès réseau à distance .....	31
Access-list .....	R-60
Address pool .....	R-72
Address ranges .....	R-8, R-64
Adressage .....	61
Adresse d'arrivée .....	52
Adresse de départ .....	52
Adresse IP .....	14, 19, 32
Adresses IP .....	9
Affectation des adresses .....	20
Affichage de l'état .....	6
AOCD .....	7
Appels internationaux .....	73
Appels longue distance .....	74
Apple Talk .....	R-6
APPP .....	R-54
ARP cache .....	R-62
ARP-aging-minute(s) .....	R-62
Assemblage .....	28
Asynchronous PPP .....	R-54
Auth. ....	R-55
Auto mode .....	R-72
Automode .....	51

## ■ B

BACP .....	6
Bande de fréquence .....	28
B-channel protocols .....	R-53
Bloc d'alimentation .....	11
Blocage .....	30
Boot system .....	R-84
Bridge .....	R-55
Bridging .....	6
Broadcast address .....	R-8
Broadcast transfer .....	R-11

Budget en fonction du temps .....	33
Buffers .....	R-58, R-79
Bureautique .....	68

## ■ C

Câble de raccordement au réseau local .....	11
Cable network .....	R-7
Câble RNIS .....	5
Cache .....	R-62
Call numbers .....	R-56
Call protection .....	R-54
Callback .....	R-51
Callback .....	R-56, R-58
Callback options .....	R-52
Call-by-Call .....	74
Call-by-call .....	R-79
Calling Line Identification Restriction .....	R-50
Canal B	
Etat de la liaison .....	6
Canal D .....	31
Canal radio .....	28
Caractères joker .....	60
Caractéristiques techniques .....	79
Carte de réseau sans fil .....	1, 5
Cells .....	R-4
Cellule radio .....	2
Challenge Handshake Authentication	
Protocol .....	31, R-55
Channel bundling .....	R-54
CHAP .....	31, R-55
Charge .....	R-52
Charger le logiciel .....	22
Charging information .....	R-51
Charging unit .....	R-51
CLI .....	31, R-56
Client LANCAPI .....	69
Client pour réseaux Windows .....	63
CLIP .....	7
CLIR .....	R-50

Common ISDN Application Programming  
 Interface ..... 68  
 Communication urbaine ..... 74  
 Compatibility ..... R-53  
 Compression ..... 6  
 Compression de données Stac ..... 6  
 Config-aging-minute(s) ..... R-76  
 Configuration ..... 7  
 Instructions ..... 21  
 SNMP ..... 24  
 Configuration à distance ..... 8  
 Configuration options ..... R-76  
 Configuration point-à-multipoint ..... 6  
 Configuration point-à-point ..... 6  
 Connect ..... R-57  
 Connecteur Ethernet ..... 1  
 Connection timeout ..... R-54  
 Connection timeouts ..... R-51  
 Connexion à un réseau étendu WAN ..... 6  
 Connexion à un réseau local ..... 5  
 Contenu de l'emballage ..... 11  
 Contrôle des accès ..... 30  
 Contrôle des coûts de communication ..... 7, 69  
 Correspondants NetBIOS ..... 62  
 Coupe-feu ..... 7, 69  
 Coûts de communication ..... 61

## D

Cata compression ..... R-54  
 Data packet ..... R-4  
 DDI numbers ..... R-53  
 Default route ..... R-65  
 DEL  
 Power/Msg ..... 12  
 Destination network ..... R-63  
 Destination port ..... R-65  
 Destination ports ..... R-65  
 Device names ..... R-51  
 Device-name ..... R-51  
 DHCP ..... 9, 50, R-71  
 DHCP server ..... R-71  
 DHCP-Automode ..... 51  
 DHCP-Server ..... 14

Dial prefix ..... R-52  
 Dialup-remote ..... R-51  
 Direct Sequence Spread Spectrum ..... 5  
 Disconnect ..... R-58  
 Disponibilité ..... 71  
 Distance d'une route ..... 44  
 DNS ..... 49, 57, R-61  
 DNS forwarding ..... R-61  
 DNS queries ..... R-66  
 DNS-backup-IP-address ..... R-61  
 Domain Name Service ..... 49, 57  
 Domaine WLAN ..... 28  
 Domaines ..... 57  
 DSS1 ..... 6, R-50  
 DSSS ..... 5, 28  
 Dst-address ..... R-66  
 Dst-netmask ..... R-66  
 Durée de communication ..... 6  
 Durée de validité ..... 50, 53  
 Dynamic assignment of the IP address ..... R-63  
 Dynamic bundling ..... R-51  
 Dynamic channel bundling ..... R-54  
 Dynamic Host Configuration Protocol ..... 50  
 Dynamic IP routing table ..... R-68  
 Dynamic short-hold ..... R-51

## E

Economies sur la facture de téléphone ..... 74  
 ELSA CAPI Faxmodem ..... 8  
 ELSA header ..... R-54  
 ELSA protocol ..... R-49  
 Encaps ..... R-53  
 End-address-pool ..... R-71  
 Environnement réseau ..... 67  
 Espace d'adressage ..... 61  
 Etablissement d'une connexion ..... 61  
 Etat à la livraison ..... 13  
 Ethernet ..... 5, R-53  
 10Base-T ..... 5  
 Evolutivité ..... 3

## F

Fast callback ..... 32  
 Fast Callback ..... R-52

- Fast callback procedure ..... R-52
- Fax Class 1 ..... 9
- Faxmodem ..... 8
- Filtre ..... 30
- Filtre IP ..... 62
- Firewall function ..... R-66
- FirmSafe ..... 8
- Firmsafe ..... 22
- Firmsafe ..... R-83
- Firmware ..... R-82
- Firmware-upload ..... R-82
- Fonction de coupe-feu ..... 32
- Force brute ..... 7, 29
- Fragmentation ..... 28
- Frais de téléphone élevés ..... 33
- **G**
- Gestion d'adresses ..... 50
- Gestion des communications ..... 33
- Gestion des priorités ..... 72
- Gestion des taxes téléphoniques ..... 33
- Group table ..... R-74
- Groupes ..... 61
- **H**
- HDLC packets ..... R-54
- HDLC56K ..... R-55
- HDLC64K ..... R-55
- Heap-Reserve ..... R-59
- Heure ..... 73
- Heure du réseau RNIS ..... 77
- Heure du RNIS ..... 7
- Hierarchical IP addresses ..... R-9
- Horloge ..... 76
- Horloge interne ..... 76
- Host ..... R-4
- Host table ..... R-74
- Hôte ..... 57
- **I**
- IANA ..... R-8
- ICMP ..... R-65, R-67, R-70
- Identification ..... 63, R-48
- Identification de l'appelant ..... 31
- Identification du numéro de l'appelant ..... 7
- Impulsions de facturation ..... 7
- Inband
- Avec Telnet ..... 21
- Conditions ..... 19
- Indicatif ..... 73
- Informations sur le nom ..... 61
- Installation ..... 5
- Interface ..... R-4
- Interface CAPI ..... 68
- Interface list ..... R-49
- Interface S0 ..... 6
- Internet ..... R-6
- Internetwork ..... R-6
- Interrogation de l'heure ..... 7
- Intranet ..... R-60
- Inverse masquerading ..... R-69
- IP ..... R-67
- IP address ..... R-59
- IP addresses ..... R-7
- IP broadcast ..... R-68
- IP header ..... R-67
- IP masquerading ..... 7, 48, R-63, R-69
- Protocoles pris en charge ..... 49
- IP multicast ..... R-68
- IP network ..... R-6
- IP network mask ..... R-60
- IP-routing-table ..... R-63
- IPX ..... R-6
- ISDN layers ..... R-53
- ISDN network ..... R-7
- ISDN time ..... R-20
- ISM ..... 5
- **J**
- Jours de semaine ..... 73
- Jours fériés ..... 73
- **K**
- Key ..... R-55
- **L**
- LAN ..... 1, R-6, R-11
- LANCAPI ..... 8, 68, R-77

LANconfig ..... 7, 14, 19, 20, 23, 27  
 LAN-configuration ..... R-76  
 LAN-filter-table ..... R-65  
 Language ..... R-77  
 LANmonitor ..... 6, 76  
 Largeur de bande ..... 6  
 Layer name ..... R-51  
 Layer-name ..... R-53  
 LCP-Echo-Reply ..... 43  
 LCP-Echo-Request ..... 43  
 LCR ..... 7, 73, R-79  
 Leased-line connection ..... R-53  
 Least Cost Router  
   Contrôle des coûts de communication ..... 75  
   Modes de fonctionnement ..... 75  
   Repli automatique ..... 76  
 Least-cost router ..... 72, 75  
 Least-cost routing ..... 7  
 Limitation des communications en fonction  
   du temps ..... 33  
 Limitation des taxes téléphoniques ..... 33  
 Liste d'accès IP ..... 19  
 Liste PPP ..... 31  
 Local Area Network ..... 1, R-6  
 Local network ..... R-6  
 Local-routing ..... R-67  
 Location ..... R-49  
 Lock-minutes ..... R-77  
 Login ..... 23  
 Log-in block ..... R-77  
 Login-errors ..... R-77  
 Looser ..... R-52

## M

MAC address ..... R-58, R-79  
 MAC addresses ..... R-12  
 MAC protocol ..... R-12  
 Manual connection ..... R-57  
 Masquerading ..... R-63, R-69  
 Masquerading ..... R-60  
 Masquerading IP ..... 30, 32  
 Masquerading table ..... R-69  
 Mécanisme d'acheminement DNS ..... 58

Médias en ligne ..... 19  
 Medium ..... R-4  
 Medium Access Control ..... R-11  
 Mémoire flash-ROM ..... 8, 22  
 Méthode DSSS ..... 5  
 Microprogramme ..... 8  
 Mise à jour des microprogrammes ..... 8  
 MLPPP ..... 6  
 Modem operation ..... R-54  
 Modes d'exploitation ..... 27  
 Mot de passe ..... 28, 31, 42  
 Mots de passe ..... 64  
 Multipoint cabling ..... R-11  
 Multiprotocol capability ..... R-12

## N

Name ..... R-48  
 Name server ..... R-61  
 Name verification ..... R-56  
 Name-list ..... R-51  
 NAT ..... 30, 32, 48  
 NBNS ..... 61, R-62  
 NBNS-backup ..... R-62  
 NetBIOS ..... 9, 58  
   Accès à distance ..... 66  
   Correspondant ..... 65  
   Filtre IP ..... 65  
   Interconnexion entre deux réseaux  
     locaux ..... 65  
   Protocole réseau ..... 62  
   TCP/IP ..... 62  
 NetBIOS name server ..... R-62  
 Network ..... R-4  
 Network adapter ..... R-4  
 Network address ..... R-7  
 Network cable ..... R-4  
 Network connection ..... R-58  
 Network Information Center ..... 48  
 Network mask ..... R-7  
 Network protocol ..... R-6  
 Networking dans un réseau Windows ..... 67  
 NIC ..... 48  
 Node-ID ..... R-58



Nom d'ordinateur ..... 61  
 Nom d'utilisateur ..... 31, 42  
 Nom du routeur ..... 44  
 Noms d'ordinateur ..... 57  
 Noms de réseau ..... 57  
 Noms et désignation des groupes ..... 63  
 Norme IEEE 802.11 ..... 5  
 NT domain ..... R-74  
 Number ..... R-51  
 Number list ..... R-56  
 Numéro vert ..... 74

## O

Opérateur ..... 72  
 Opérateur réseau ..... 72  
 Opérateurs ..... 75  
 Operating ..... R-63  
 Ordinateurs accessibles ..... 67  
 Other ..... R-84

## P

Packet ..... R-4  
 PAP ..... 31, R-55  
 Parasitage ..... 5  
 Partage ..... 64  
 Partage de fichiers et d'imprimantes ..... 63  
 Passerelle ..... 32, 50, 53  
 Password ..... R-60  
 Password Authentication Protocol ..... 31, R-55  
 Password-required ..... R-76  
 PAT ..... 30, 32, 48  
 Physical medium ..... R-4  
 Pilote de télécopie ..... 9  
 Plage horaire ..... 73  
 Point-to-multipoint connection ..... R-5  
 Point-to-point connection ..... R-4  
 Point-to-point protocol ..... R-54  
 Pool d'adresses ..... 52, 56  
 Port ..... 71  
 Ports NetBIOS ..... 62  
 PPP ..... 8, 31, R-54, R-55, R-56  
   Vérification de la ligne avec LCP ..... 42  
 PPP negotiation ..... R-60  
 Préfixe ..... 73

Présélection ..... 73  
 Private address spaces ..... R-8  
 Procédés de sécurisation ..... 31  
 Prohibited address ranges ..... R-64  
 Protect ..... R-56  
 Protection ..... 29, 30  
 Protection contre les parasites ..... 5  
 Protection de l'accès ..... 7  
   Nom ..... 31  
 Protection de l'accès  
   Aucun ..... 30  
 Protection par mot de passe ..... 7, 29  
 Protocol ..... R-6  
 Protocole de canal B ..... 32  
 Proxy ..... 9  
 Proxy ARP ..... R-63, R-64  
 Proxy NetBIOS ..... 60  
 Proxy-ARP ..... R-67

## R

R1-mask ..... R-68  
 Raccordement RNIS S0 ..... 13  
 Rappel ..... 32  
   Fast Call Back ..... 32  
 Rappel automatique ..... 7  
 Rayon d'action ..... 3, 6  
 Registered IP address ..... R-8  
 Registered IP address ..... R-60  
 Réglage automatique de l'heure ..... 77  
 Regroupement des canaux ..... 6  
 Regroupement des canaux ..... 6  
   Dynamique ..... 6  
   Statique ..... 6  
 Regroupement dynamique des canaux ..... 6  
 Remote Access ..... R-67  
 Remote station verifications ..... R-56  
 Remote-table ..... R-74  
 Reroutage direct ..... 73  
 Réseau ad-hoc ..... 2  
 Réseau d'infrastructure ..... 3  
 Réseau Peer-to-LAN ..... 3  
 Réseau Peer-to-Peer ..... 2  
 Réseau sans fil ..... 1, 27

Réseau Windows .....	61	Mécanisme filtrant .....	58
Réseaux NetBIOS .....	58	Serveur LANCAPI .....	70
Réseaux Peer-to-Peer .....	9	Serveur NBNS .....	50, 52
Réseaux TCP/IP .....	57	Serveur WINS .....	61
Réseaux Windows .....	9	Service .....	57
Reset system .....	R-84	Service table .....	R-69
Ressources partagées .....	64	Setup .....	
RIP .....	R-68	DHCP-module .....	R-71
RIP-type .....	R-68	IP-router-module .....	R-62
Round robin list .....	R-52	LAN-module .....	R-58
Round-Robin .....	R-53	TCP-IP-module .....	R-59
Routeage .....	62	WAN-module .....	R-49
Routeage dynamique .....	43	Shared Medium .....	R-11
Routeage IP .....		Shared medium .....	R-6
Filtrage .....	44	Short-hold .....	R-51
FTP .....	45	Single User Access .....	32
Telnet .....	45	SNMP .....	24, R-70
Routeage par DNS .....	49	Source port .....	R-65
Routeage statique .....	43	Special dialing characters .....	R-51, R-52
Routeage téléphonique à la demande .....	73	Speed .....	R-55
Router .....	R-4	Stac .....	R-54
Router des réseaux Windows .....	60	Start-address-pool .....	R-71
Routes d'exclusion .....	44	State .....	R-59
Routing .....	R-9	Static bundling .....	R-51
Routing table .....	R-9	Static channel bundling .....	R-54
<b>S</b> .....		Static IP address .....	R-63
Scope ID .....	R-74	Station de base .....	1
Scopes .....	61	Status .....	R-19
Script list .....	R-57	Call-info-table .....	R-44, R-46, R-47
Script processing .....	R-54, R-57	Config-statistics .....	R-40
Sécurisation .....	42	Connection-state .....	R-20
Sécurité .....	29, 30, 32	Connection-statistics .....	R-42
Security procedure .....	R-55	Delete values .....	R-47
Semipermanent leased-line connection ...	R-52	Info-connection .....	R-43
Server list .....	R-75	IP-router-statistics .....	R-38
Serveur de messagerie électronique .....	60	LAN-statistics .....	R-25
Serveur de noms NetBIOS .....	61	Layer-connection .....	R-43
Serveur DHCP .....	20, 50, 57	Operating time .....	R-20
Configuration .....	54	PPP-statistics .....	R-26
Serveur DNS .....	9, 50, 52, 57	Queue-statistics .....	R-41
Information disponible .....	58	SO-bus .....	R-20
Liste-filtres .....	60	TCP-IP-statistics .....	R-32
		WAN-statistics .....	R-21, R-22

Subnet ..... R-9  
 Suppresses the outgoing MSN ..... R-50  
 System-administrator ..... R-70  
 System-location ..... R-70

## ■ T

Table-ARP ..... R-62  
 Tableau de reroutage ..... 73  
 Tableau de routage IP ..... 43  
 Table-RIP ..... R-68  
 Taille des paquets ..... 28  
 Tarif local ..... 74, 75  
 Tarifs ..... 72, 74  
 Taux de transfert ..... 6  
 TCP ..... R-65, R-70  
 TCP max. connections ..... R-62  
 TCP/IP ..... 14, 19, 43, R-6  
 TCP/IP stack ..... R-6  
 TCP-aging-minute(s) ..... R-62  
 Téléchargement ..... 8, 22  
 Téléchargement de microprogramme  
   Avec LANconfig ..... 23  
 Téléchargement du microprogramme ..... 23  
   Avec TFTP ..... 24  
 Télécopies ..... 9  
 Telephone company ..... R-79  
 Teleworkers ..... R-67  
 Telnet ..... 7, 16  
 Telnet server ..... R-61  
 Témoins lumineux ..... 6, 12  
 Tentatives d'accès ..... 29  
 TFTP ..... 19  
 TFTP server ..... R-61  
 Time ..... R-20, R-56  
 Time ..... R-81  
 Timeout ..... R-73  
 TOS ..... R-67  
 Touche Reset ..... 13

Transfert EuroFile ..... 8  
 Trap-IP ..... R-70  
 Traps-active ..... R-70  
 Trunk seizure ..... R-52  
 Type d'accès ..... 64  
 Type-of-Service ..... 50  
 Type-of-service ..... R-67

## ■ U

UDP ..... R-65, R-70, R-77  
 Upload-system ..... R-84  
 Username ..... R-56

## ■ V

V.42bis ..... R-54  
 Verification attempt ..... R-56  
 Verrouillage d'accès ..... 29  
 Verrouiller domaines ..... 60  
 Version-table ..... R-82

## ■ W

WAN-configuration ..... R-76  
 WAN-filter-table ..... R-66  
 Windows Internet Name Service-Server ..... 61  
 Winipcfg ..... 15  
 Wire ..... R-4  
 Wireless LAN ..... 1  
 Wireless links ..... R-4  
 WLAN ..... 1, 27  
 WWW ..... 32

## ■ X

X.75 data protection ..... R-54  
 X.75 secured format ..... R-54

## ■ Y

Y connections ..... R-50

## ■ Z

Zone tarifaire ..... 74



# Technical basics

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

## Wireless network according to the IEEE-802.11 standard

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

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

### Ad hoc mode

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

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

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

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

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



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

## Infrastructure mode

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

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

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



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

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

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

## Interchangeability with other devices

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

## Network technology



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

### The network and its components

*network,  
transmission  
medium,  
interfaces*

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



*Packets  
Cells*

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

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



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

*Host*

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

*Router*

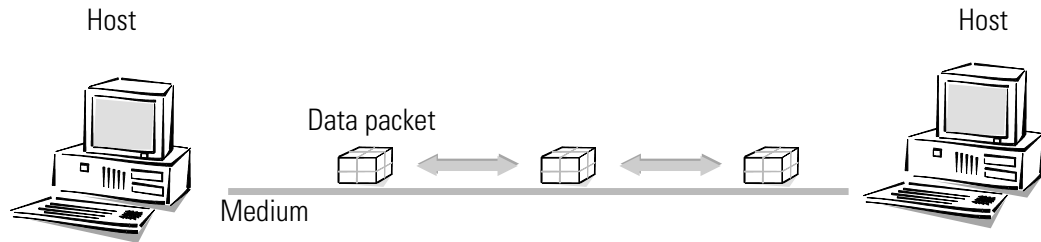
The transport of packets between two hosts occurs indirectly through exchanges that pass packets on to the target computer. These exchanges are called routers. A router has at least two interfaces so that it can receive the data from a sender and pass them on to a recipient. Apart from the exchange function,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

### Connection modes

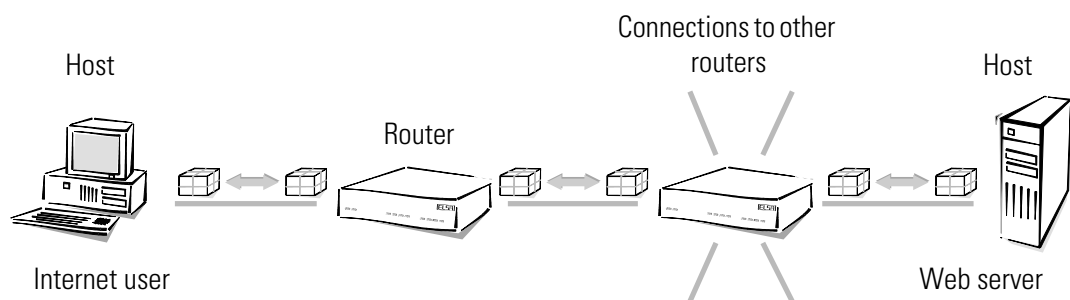
*Point-to-point  
connection*

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





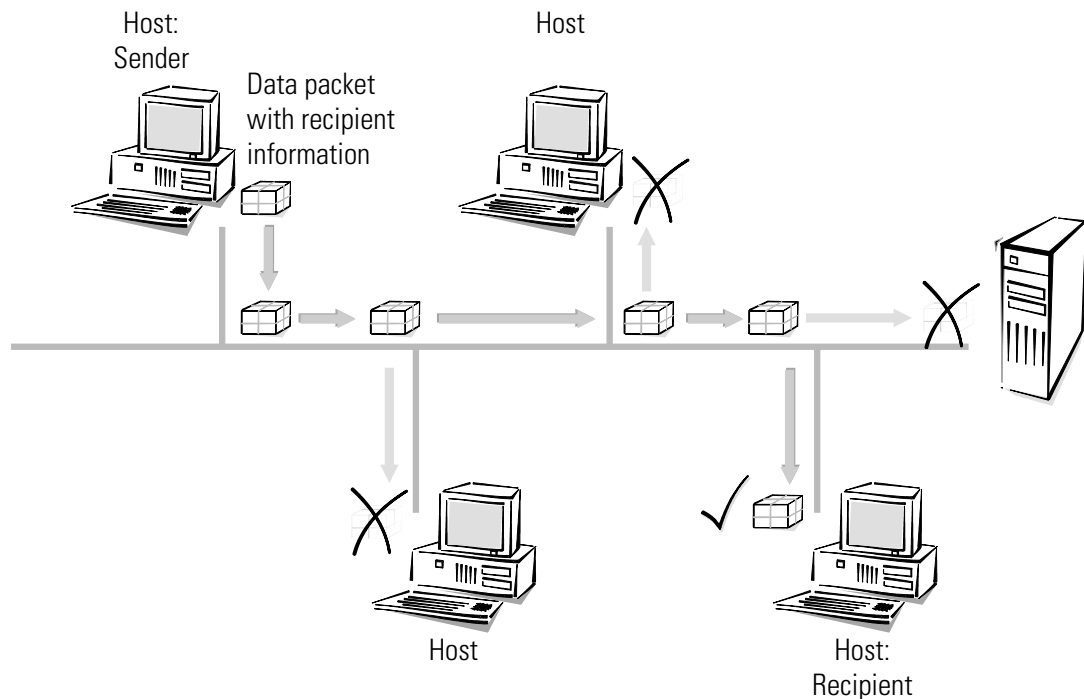
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers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



Point-to-multipoint connection

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

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



## Kinds of networks

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

## IP addressing

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

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

#### IP address

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



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

#### Network address

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

#### Netmask

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

Examples:

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

The same IP address, this time with another netmask:

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

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

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

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

#### *IP address management*

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

#### *Private address spaces*

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

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

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

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

There are two considerations when using these IP addresses:

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

## IP routing and hierarchical IP addressing

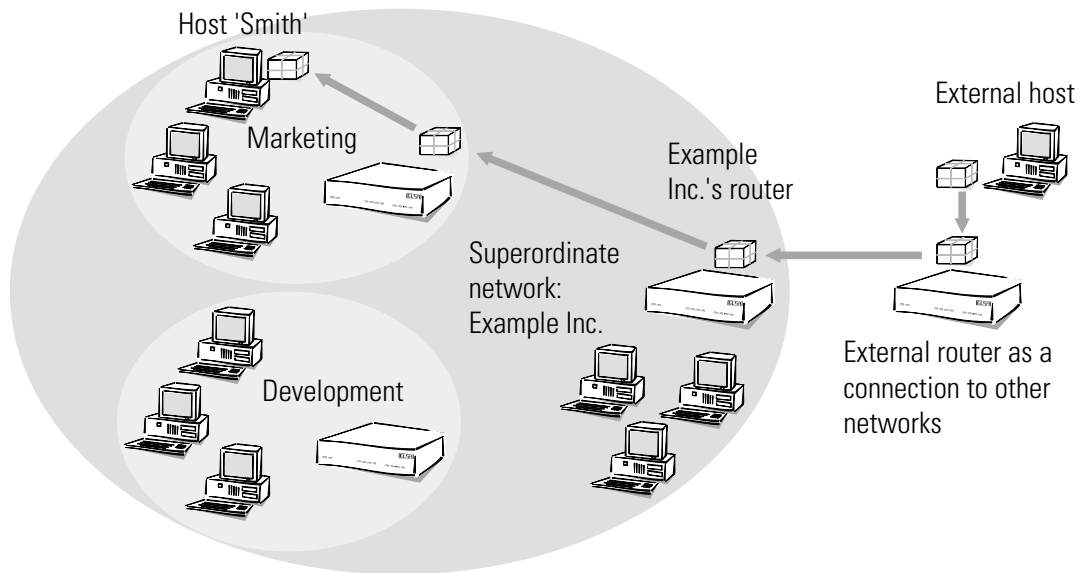
*Routing-method* Every IP packet contains the IP addresses of the source and of the recipient. A router receives IP packets at its interface, interprets the destination address and passes the packets on to those interfaces that are nearest to the recipient. Finding the appropriate path is called routing.

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

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

The consequences of this hierarchical IP addressing:

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



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

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

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

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

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

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

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

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

## Expansion through local networks

*Media access control*

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

*LAN and IP network*

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

*MAC-address*

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

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

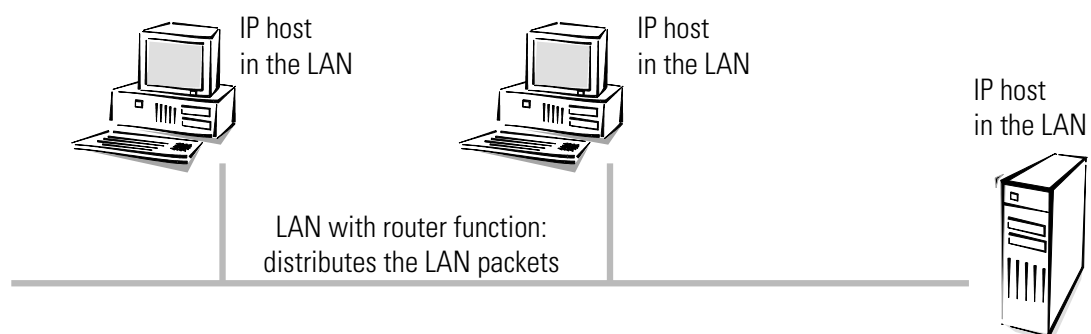
MAC addresses are independent of IP addresses. An IP host whose interface works through a LAN has an IP and a MAC address. Whereas the structure of IP addresses with its similarity to postal addresses is supposed to simplify routing in enormous IP networks, the fingerprint-like MAC addresses are designed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

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

#### *IP in the LAN*

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

To an IP host, a LAN behaves as if it were an independent network with a router. The hosts give 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.

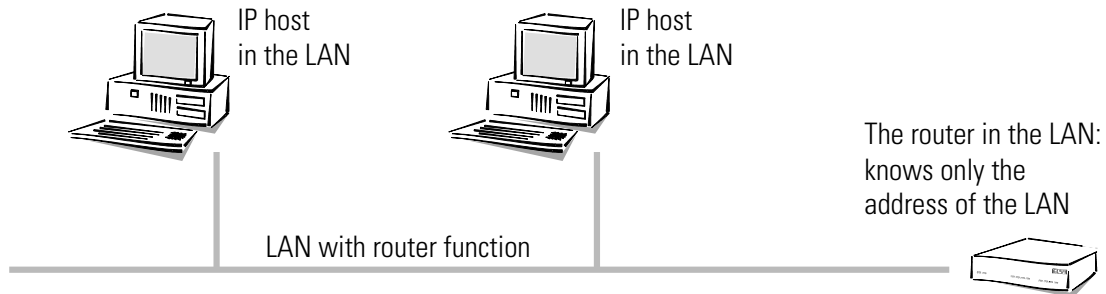


To a router in the LAN, a host in its own LAN seems to be located behind another router. So the task for the router is very simple: all it has to know for operating in the IP network are the IP addresses

- 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'.

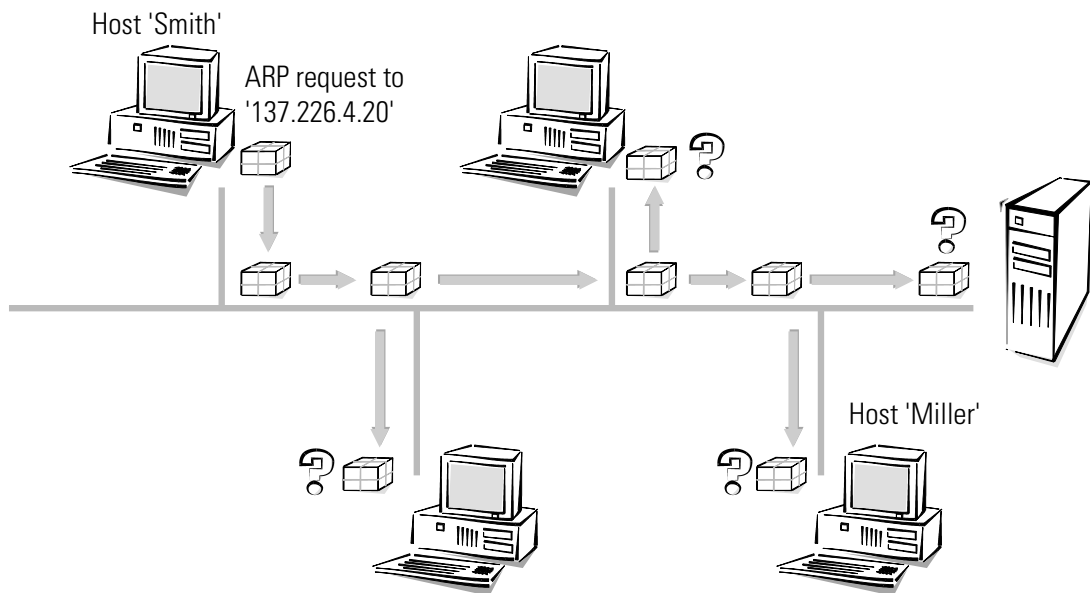
Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). Using the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located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

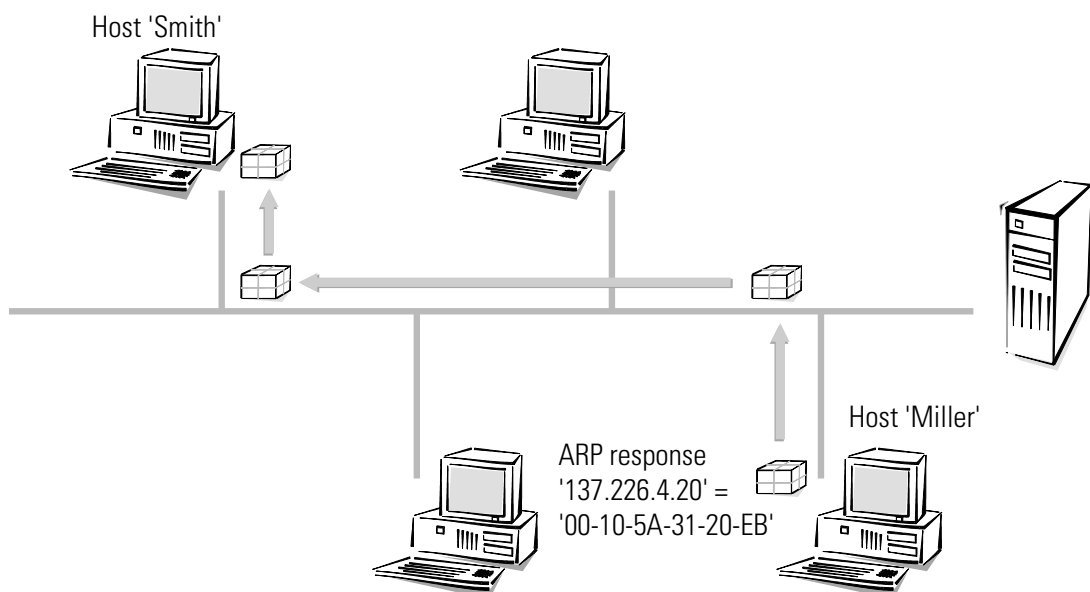
ARP

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

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



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



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

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

### Data transfer from the LAN onto the Internet

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

### LAN coupling on MAC basis

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

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

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



# Description of the menu options

The menu tree for the configuration is divided up into status information, setup parameters, firmware information and 'other'.







In order to help you familiarize yourself with the system, you will first be given an overview of the menu structure.

A complete list of all the menu options will be followed by a detailed description of all displays, menus and actions along with their associated parameters, default settings and input options.

You can access the menus when configuring via Telnet or terminal programs and via SNMP (also see 'Configuration Modes').
















When configuring with *ELSA LANconfig*, you are provided with an integrated help system that gives you brief descriptions of the individual parameters.

## Symbols







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

## Overview of the menus























### **Setup**

-  Name
-  WAN-module
-  Charges-module
-  LAN-module
-  TCP-IP-module
-  IP-router-module
-  SNMP-module
-  DHCP-module
-  DNS module
-  NetBIOS-module
-  Config-module
-  WLAN-module
-  LANCAPL-module
-  LCR-module
-  Time-module





### **Firmware**

-  Version-table
-  Table-firmsafe
-  Mode-firmsafe
-  Timeout-firmsafe
-  Firmware-upload
-  Test-firmware

### **Status**

-  Connection
-  Current-time
-  Operating-time
-  WLAN-statistics
-  WAN-statistics
-  LAN-statistics
-  PPP-statistics
-  TCP-IP-statistics
-  IP-router-statistics
-  Config-statistics
-  Queue-statistics
-  Connections-statistics
-  Info-connection
-  Layer-connection
-  Call-info-table
-  Remote-statistics
-  S<sub>0</sub>-bus
-  Channel-statistics
-  Time-statistics
-  LCR-statistics
-  PCMCIA-status
-  Delete-values

### **Other**






-  Manual-dialing
-  Reset-system
-  Boot-system
-  System-upload




## Status

The Status menu contains information on the current status and the internal sequences of operations in the LAN and WAN, which can relate to the data transmission route (e.g. dialing or connection) or to statistics (e.g. number of calls received or data blocks transmitted). The statistics displays are an important aid for verifying correct functioning and optimizing parameter settings. In addition, they provide valuable information for error analysis when malfunctions occur.

Most status displays are continually updated and can be deleted with a **value** or set to 0 in the current menu.


The menu has the following layout:

Status		Running status displays
Connection		Status of the WAN route
Current-time		Current time in device
Operating-time		Period of time the device has operated since it was last switched on
S <sub>0</sub> -bus		Status of the S <sub>0</sub> interface
WAN-statistics		Displays WAN statistics
LAN-statistics		Displays LAN statistics
WLAN-statistics		Wireless network area statistics
PPP statistics		Point-to-point-protocol statistics
Bridge-statistics		Bridge area statistics
TCP-IP-statistics		Statistics from the TCP/IP area
IP-router-statistics		Statistics from the IP router
Config-statistics		Remote configuration statistics
Queue-statistics		Statistics relating to the packets in the queues of the individual modules
Connections-statistics		Connection information for each interface
Info-connection		Information on the last connection for each interface
Layer-connection		Information on the B-channel protocol used for each interface
Call-info-table		Information on the last 10 calls received
Remote-statistics		Statistics on the last 10 connections
Channel-statistics		Information of the status of the individual channels. Also information on the a/b ports with <i>ELSA LANCOM Wireless L-2</i> .
Time-statistics		Time module information

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

## Status/Connection-state

The **Status/Connection-state** menu option displays the status messages for the individual channels.

/Connection-state		Running status displays
Connection		CH01: Ready; CH02: Ready

## Status/Current-time



This displays the current device time, used, e.g., for the least-cost-router calculations or certain statistics. The time can be read from the ISDN (ISDN time, see also Setup/time module) or set manually (with the 'time' command).

## Status/Operating-time

The operating time of the router since it was last started is displayed here in days hours, minutes and seconds.

## Status/S<sub>0</sub>-bus

This option allows you to display the current status of the S<sub>0</sub> interface. The statistics have the following layout:

/S <sub>0</sub> -bus		Running status displays
D-info		Overview of the D channel status
D2-statistics		Breakdown of the Layer-2 information of the D channel for the B channels.

### D-info

This table shows general information related to the D channel:

Channel	B channel identification.
Protocol	D channel protocol. Either the protocol fixed in the interface table or the protocol detected in the 'Auto' settings at the ISDN terminal.



Layer-2	Activation of layer 2 of the D channel ('Yes' or 'No')
TEI	TEI assigned ('Yes' or 'No')
S <sub>0</sub> -activation	Displays activation status ('Yes' or 'No')

*D2-statistics*






This table shows layer 2 information for the individual B channels:

Channel	B channel identification.
TEI	<b>T</b> erminal <b>E</b> quipment <b>I</b> dentifier assigned by the switching center.
L2-activation	Activation of layer 2 of the D channel ('Yes' or 'No').
Connections	Number of connections made over the displayed TEI.

## Status/WLAN-statistics

The current status of the WLAN interface is described here.

LAN-rx-packets	0	Number of data packets received
LAN-tx-packets	0	Number of data packets sent
LAN-rx-errors	0	Number of data packets incorrectly received
LAN-tx-errors	0	Number of data packets incorrectly sent
LAN-stack-errors	0	Number of packets without a suitable receive module (bridge/router)
LAN-queue-packets	0	Number of buffers in use
LAN-queue-errors	0	Number of packets discarded due to a lack of buffers
LAN-rx-bytes	0	Number of bytes received from the LAN
LAN-tx-bytes	0	Number of bytes sent to the LAN
LAN-rx-broadcasts	0	Number of broadcast packets received from the LAN
LAN-rx-multicasts	0	Number of multicast packets received from the LAN
LAN-rx-unicasts	0	Number of directly addressed packets received from the LAN
LAN-Tx-broadcasts	0	Number of broadcasts received from the WAN
LAN-Tx-multicasts	0	Number of multicasts received from the WAN
LAN-Tx-unicasts	0	Number of unicasts received from the WAN
LAN-tx-discarded	0	Number of packets discarded by the LAN
LAN-repeats	0	Number of packets that were repeated before being received successfully
LAN-multiple-repeats	0	Number of packets that were repeated several times before being received successfully

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



*Station table*

This table displays information on the individual mobile stations:

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

*WLAN parameters*










This table displays the current wireless-network parameters:

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

**Status/WAN-statistics**

This option allows you to display the various statistics parameters for the WAN port. A large number of values related to the data volume transferred provide you with useful information on WAN port utilization, errors that have occurred, and the internal resources of the devices that are available in the current operating state.

The WAN statistics are maintained on an interface-specific basis, i.e. separate statistics in which the transferred data and errors are recorded are available for each interface. The **Status/WAN-statistics** menu has the following layout:

/WAN-statistics		Running status displays
Byte-transport-statistics		Statistics on bytes transferred
Packet-transport-statistics		Statistics on data packets transferred
Error-statistics		Statistics on data errors that have occurred
WAN-tx-discarded		Number of packets discarded due to an error/lack of resources
WAN-heap-packets		Number of buffers in use
WAN-queue-packets		Number of buffers available
WAN-queue-errors		Number of packets discarded due to a lack of buffers
Throughput-statistics		Statistics for bytes transferred on every channel
Delete-values		Deletes WAN statistics

#### Byte-transport-statistics

The menu item **Status/WAN-statistics/Byte-transport-statistics** contains statistics of the bytes transferred over an interface for every available interface. The table maintained here has the following layout:

lfc	CRx-bytes	Rx-bytes	Tx-bytes	CTx-bytes
Ch01	0	0	0	0
Ch02	0	0	0	0

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

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

#### Packet-transport-statistics

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

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

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

Ifc	Designates the associated channel
Rx	Number of packets received
Tx-total	Number of packets sent (data and protocol packets)
Tx-normal	Number of normal data packets sent
Tx-reliable	Number of data packets transferred with secured handling
Tx-urgent	Number of data packets transferred with priority handling (urgent queue)

*Error-statistics* For each available interface, the **Status/WAN-statistics/Error-statistics** menu option provides statistics on the transmission errors that have occurred on this interface. The table maintained here has the following layout:

Ifc	Rx-l1-error	Rx-l2-error	Rx-l3-error	Stack-error	Tx-error
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

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

Ifc	Designates the associated channel.
Rx-l3-error	Number of layer-3 errors in data received (i.e., the protocol header of layer-3 is incorrect)
Rx-l2-error	Number of layer-2 errors in data received (i.e., similar to the layer-3 errors, e.g. defective PPP header)
Rx-l1-error	Number of layer-1 errors in data received (similar to layer-3 errors)
Tx-error	Number of transmission errors that occurred while sending
Stack-error	Number of stack errors for data received. Stack errors are caused when frames are received that cannot be assigned to an internal processing procedure (e.g. IP router).

*Throughput-statistics*

The menu item **Status/WAN-statistics/Throughput-statistics** contains statistics of bytes transferred over this interface for both channels. The table maintained here has the following layout:





















Ifc	Rx/s current	Tx/s current	Rx/s average	Tx/s average
Ch01	0	0	0	0
Ch02	0	0	0	0

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

Ifc	Designates the associated channel
Rx/s current	Throughput on the channel in the last second in the receiving direction
Tx/s current	Throughput on the channel in the last second in the transmission direction
Rx/s average	Average throughput on the channel in the receiving direction
Tx/s average	Average throughput on the channel in the transmission direction













## Status/LAN-statistics

Similarly to the previous menu option, this option allows you to display the statistics relating to the LAN port. The **Status/LAN-statistics** menu has the following layout:

/LAN-statistics	Running status displays	
LAN-rx-packets		Number of data packets received
LAN-tx-packets		Number of data packets sent
LAN-rx-errors		Number of data packets incorrectly received
LAN-tx-errors		Number of data packets incorrectly sent
LAN-stack-errors		Number of packets without a suitable receive module (bridge/router)
LAN-NIC-errors		Number of data packets discarded by the NIC
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
LAN-collisions		Number of collisions during a send procedure
Connection -established		Display of correct Ethernet connection (data transfer possible). Corresponds to the 'Link' LED on the device.
LAN-rx-bytes		Number of bytes received from the LAN
LAN-tx-bytes		Number of bytes sent to the LAN
LAN-rx-broadcasts		Number of broadcast packets received from the LAN
LAN-rx-multicasts		Number of multicast packets received from the LAN
LAN-rx-unicasts		Number of directly addressed packets received from the LAN
WAN-rx-broadcasts		Number of broadcasts received from the WAN
WAN-rx-multicasts		Number of multicasts received from the WAN
WAN-rx-unicasts		Number of unicasts received from the WAN
Delete-values		Deletes LAN statistics

## Status/PPP-statistics

Within the PPP statistics, the states of individual subprotocols of the PPP are managed separately for each interface. However, statistics relating to the frames transmitted for individual subprotocols are maintained only in joint statistics. Consequently, the **Status/PPP-statistics** menu has the following layout:

/PPP-statistics		Running status displays
PPP-phases		Statistics relating to the status of PPP protocol negotiation for each interface
LCP-statistics		Displays PPP/LCP statistics
PAP-statistics		Displays PPP/PAP statistics
CHAP-statistics		Displays PPP/CHAP statistics
IPCP-statistics		Displays PPP/IPCP statistics
CBCP-statistics		Displays PPP/CBCP statistics
CCP-statistics		Displays PPP/CCP statistics
ML-statistics		Displays PPP/ML statistics
BACP-statistics		Displays PPP/BACP statistics
Rx-options		Displays the LCP, IPCP and IPXCP information received
Tx-options		Displays the LCP, IPCP and IPXCP information sent
Delete-values		Deletes PPP statistics.

The PPP statistics provide detailed information on the phases of a PPP negotiation, particularly in the event of connection problems with external products. It provides important information for error diagnosis.

### PPP-phases

For each available interface, the **Status/PPP-statistics/PPP-phases** option provides a list of the current states of PPP protocol negotiation. The table maintained here has the following layout:

lfc	Phase to	LCP	IPXCP	IPCP	CCP
Ch01	DEAD	Initial	Initial	Initial	Initial
Ch02	DEAD	Initial	Initial	Initial	Initial

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

Ifc	Designates the associated channel.
Phase to	Indicates the current phase of the PPP. The possible values are <b>AUTHENTICAT</b> , <b>NETWORK</b> and <b>TERMINATE</b> .
LCP	Status of the 'Link Control Protocol' subprotocol. The possible values are: <b>Initial</b> , <b>Starting</b> , <b>Stopping</b> , <b>Stopped</b> , <b>Closing</b> , <b>Closed</b> , <b>ReqSent</b> , <b>AckRcvd</b> , <b>AckSent</b> and <b>Opened</b> .
IPCP	Similarly to 'LCP', displays the status of the 'IP Control Protocol' subprotocol.
CCP	Similarly to 'LCP', displays the status of the 'Compression Control Protocol' subprotocol.

The current PPP phases are shown under **Status/PPP-statistics/PPP-phases**. As specified above, these phases are the idle (Dead), ready (Establish), access parameter verification (Authenticate) and network phase (Network). In the substatistics, the frames exchanged are encrypted separately by type and quantity.

### Status/PPP-statistics/LCP-statistics

The **LCP** (Link Control Protocol) negotiates the basic features of the PPP connections. The LCP frames exchanged during PPP negotiation are recorded in statistics and displayed by type and quantity. If the LCP does not change to the OPEN state for a connection, these statistical values provide information on errors that occurred during the initial phase of PPP negotiation. Below is a detailed description of the meanings of the parameters for these statistics:

Rx-errors	Number of faulty PPP packets received
Rx-discarded	Number of PPP packets discarded
Rx-config-request	Number of configure request packets received for LCP
Rx-config-ack.	Number of configure acknowledge packets received for LCP
Rx-config-nak.	Number of configure negative acknowledge packets received
Rx-config-reject	Number of configure reject packets received for LCP
Rx-terminate-request	Number of terminate request packets received for LCP
Rx-terminate-ack.	Number of terminate acknowledge packets received for LCP
Rx-code-reject	Number of code reject packets received for PPP
Rx-protocol-reject	Number of protocol reject packets received for PPP
Rx-echo-request	Number of echo request packets received for LCP
Rx-echo-reply	Number of echo response packets received for LCP
Rx-discard-request	Number of discard request packets received for LCP
Tx-config-request	Number of configure request packets sent for LCP
Tx-config-ack.	Number configure acknowledge packets sent for LCP
Tx-config-nak.	Number of configure negative acknowledge packets sent

Tx-config-reject	Number of configure reject packets sent for LCP
Tx-terminate-request	Number of terminate request packets sent for LCP
Tx-terminate-ack.	Number of terminate acknowledge packets sent for LCP
Tx-code-reject	Number of code reject packets sent for PPP
Tx-protocol-reject	Number of protocol reject packets sent for PPP
Tx-echo-request	Number of echo request packets sent for LCP
Tx-echo-reply	Number of echo response packets sent for LCP
Tx-discard-request	Number of discard request packets sent for LCP
Delete-values	Deletes LCP statistics

### Status/PPP-statistics/PAP-statistics

The **PAP** (Password Authentication Protocol) is one of two common procedures for verifying remote stations in the PPP. When a connection is established, it checks the remote station password and enables the connection only after a successful exchange of passwords (refer also to Chapter 'Point-to-Point Protocol'). Below is a detailed description of the meanings of the parameters for these statistics:

Rx-discarded	Number of PAP packets discarded
Rx-request	Number of PAP request packets received
Rx-success	Number of PAP success packets received
Rx-failure	Number of PAP failure packets received
Tx-retry	Number of times PAP request packets resent
Tx-request	Number of PAP request packets sent
Tx-success	Number of PAP success packets sent
Tx-failure	Number of PAP failure packets sent
Delete-values	Deletes PAP statistics

### Status/PPP-statistics/CHAP-statistics

The **CHAP** (Challenge Authentication Protocol) is the second option for verifying the remote station under PPP. The password is checked as the connection is established and again at adjustable intervals during the connection (refer also to Chapter 'Point-to-Point Protocol'). Below is a detailed description of the meanings of the parameters for these statistics:

Rx-discarded	Number of CHAP packets discarded
Rx-challenge	Number of CHAP challenge packets received
Rx-response	Number of CHAP response packets received
Rx-success	Number of CHAP success packets received



Rx-failure	Number of CHAP failure packets received
Tx-retry	Number of times the CHAP challenge packets were resent
Tx-challenge	Number of CHAP challenge packets sent
Tx-response	Number of CHAP response packets sent
Tx-success	Number of CHAP success packets sent
Tx-failure	Number of CHAP failure packets sent
Delete-values	Deletes CHAP statistics

### Status/PPP-statistics/IPCP-statistics

When IP is used, the **IPCP** (Internet Protocol Control Protocol) indicates the status of the protocol and the packets exchanged in the negotiation.

Rx-discarded	Number of IPCP packets discarded
Rx-config-request	Number of configure request packets received for IPCP
Rx-config-ack.	Number of configure acknowledge packets received for IPCP
Rx-config-nak.	Number of configure negative acknowledge packets received
Rx-config-reject	Number of configure reject packets received for IPCP
Rx-terminate-request	Number of terminate request packets received for IPCP
Rx-terminate-ack.	Number of terminate acknowledge packets received for IPCP
Rx-code-reject	Number of code reject packets received for IPCP
Tx-config-request	Number of configure request packets sent for IPCP
Tx-config-ack.	Number of configure acknowledge packets sent for IPCP
Tx-config-nak.	Number of configure negative acknowledge packets sent
Tx-config-reject	Number of configure reject packets sent for IPCP
Tx-terminate-request	Number of terminate request packets sent for IPCP
Tx-terminate-ack.	Number of terminate acknowledge packets sent for IPCP
Tx-code-reject	Number of code reject packets sent for IPCP
Delete-values	Deletes IPCP statistics.

### Status/PPP-statistics/CBCP-statistics

The **CBCP** (Callback Control Protocol) shows the protocol status when the IP is in use and the packets exchanged during negotiation.

Rx-request	Number of CBCP request packets received
Rx-response	Number of CBCP response packets received
Rx-discarded	Number of CBCP packets discarded
Rx-acknowledge	Number of CBCP acknowledge packets received

Tx-request	Number of CBCP request packets sent
Tx-response	Number of CBCP response packets sent
TX-acknowledge	Number of CBCP acknowledge packets sent
Delete-values	Deletes IPCP statistics.

### Status/PPP-statistics/CCP-statistics

The statistics of the CCP (Compression Control Protocol) show the packets exchanged for data compression during the PPP negotiation.

Rx-discarded	Number of all CCP packets discarded
Rx-config-request	Number of CCP queries received
Rx-config-ack.	Number of CCP queries accepted
Rx-config-nak.	Number of CCP queries rejected because query parameters were not accepted.
Rx-config-reject	Number of CCP rejected for other reasons.
Rx-terminate-request	Number of CCP queries after releasing the compression.
Rx-terminate-ack.	Number of confirmed CCP queries after releasing the compression.
Rx-code-reject	Number of CCP queries rejected because the remote station will not or cannot apply compression.
Rx-reset-request	Number of CCP queries after synchronizing the compression (e.g. after transfer errors)
Rx-reset-ack.	Number of confirmed CCP queries after synchronizing the compression
Tx-config-request	Number of CCP queries sent
Tx-config-ack.	Number of CCP queries accepted by the remote station
Tx-config-nak.	Number of CCP queries rejected by the remote station because of parameters not being accepted.
Tx-config-reject	Number of CCP queries rejected by the remote station for other reasons.
Tx-terminate-request	Number of CCP queries sent after releasing the compression.
Tx-terminate-ack.	Number of CCP confirmations sent for releasing the compression.
Tx-code-reject	Number of CCP queries rejected because the <i>ELSA LANCOM</i> does not wish to use compression (by layer list settings).
Tx-reset-request	Number of CCP queries sent after synchronizing the compression (e.g. after transfer errors)
Tx-reset-ack.	Number of CCP confirmations sent for synchronizing the compression
Delete-values	Deletes CCP statistics.

### Status/PPP-statistics/ML-statistics

The MLPPP statistics mostly provide information on how the remote station handled the individual packets during a bundled PPP connection.

Bundle-connections	Number of connections that used the MLPPP.
Rx-Seq-loss	Number of packets in which an error occurred in the sequence of sequence numbers.
Rx-Seq-repeat	Number of packets in which the sequence of sequence numbers came late.
Rx-Mrru-exceeded	Number of packets in which a violation of the MRRU negotiated in the PPP negotiation was found after assembly (maximum received reassembled unit).
Rx-Header-error	Number of packets with header errors.
Rx-discarded	Number of all discarded MLPPP packets.
Rx-Frag-start	Number of packets with a start flag set (first part of a fragmented packet).
Rx-Frag-mid	Number of packets with set mid flag (middle part of a fragmented packet).
Rx-Frag-end	Number of packets with set end flag (last part of a fragmented packet).
Rx-not-fragmented	Number of packets with set start and end flag (unfragmented packets).
Delete-values	Delete ML statistics

### Status/PPP-statistics/Rx- and Tx-options

The PPP statistics options show what information was exchanged during the negotiation over LCP, IPCP or IPXCP.



#### Rx-options

This shows information on what the remote station requested (LCP) or what was assigned to the router (IPCP and IPXCP).

#### Tx-options

This shows information on what the router requested from the remote station (LCP) or what it assigned to it (IPCP and IPXCP).

The two submenus have the same layout:

/Rx- and Tx-options	Display	
LCP		Information on packet sizes, control characters, security procedures and callback
IPCP		Information on addresses in the IP network

The LCP table has separate listings for every channel:










MRU	<b>M</b> aximum <b>R</b> ecieve <b>U</b> nit designates the maximum packet size that the remote station can receive
ACCM	<b>A</b> synchronous <b>C</b> ontrol <b>C</b> haracter <b>M</b> ap designates the character in the asynchronous data flow that is interpreted as the control character
Auth.	Authentication procedure used (PAP/CHAP)
Callback	Callback negotiation type

Finally, IPCP has the negotiated IP options, again separated according to the channel:

IP-address	Again the Rx options have the addresses that were assigned by the remote station and the Tx options have those that the <i>ELSA LANCOM</i> assigned to the remote station (e.g. the IP address of the dial-up node at the Internet provider can easily be read in the Tx options).
DNS-default	
NBNS-default	

## Status/TCP-IP-statistics

The TCP/IP-related statistics are shown here, broken down according to the various TCP/IP sub-protocols. The TCP-IP statistics contain the following parameters:

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

The substatistics then provide you with further parameters for the individual menus.

## Status/TCP-IP-statistics/ARP-statistics

These statistics include the following values:

ARP-LAN-rx	Number of ARP requests and responses received from the LAN
ARP-LAN-tx	Number of ARP requests and responses sent to the LAN
ARP-LAN-errors	Number of ARP requests incorrectly received from the LAN
ARP-WAN-rx	Number of ARP requests and responses received from the WAN
ARP-WAN-tx	Number of ARP requests and responses sent to the WAN
ARP-WAN-errors	Number of ARP requests incorrectly received from the WAN
Delete-values	Deletes ARP statistics
Table-ARP	Displays ARP table

### Table-ARP

There are 128 entries with ARP information in the **ARP table**. It has the following layout:

IP-address	Node ID	Last-access	Connect
IP address that has previously been found by ARP request	Associated MAC address	Time since the last access in tics	Local or remote

## Status/TCP-IP-statistics/IP-statistics

These statistics include the following values:

IP-LAN-rx	Number of IP packets received from the LAN
IP-LAN-tx	Number of IP packets sent to the LAN
IP-LAN-checksum-errors	Number of IP packets incorrectly received from the LAN
IP-LAN fragmentation errors	Number of fragmentations incorrectly received from the LAN
IP-LAN fragmentations	Number of fragmentations received from the LAN
IP-LAN forced fragmentation	Number of fragmentations forced by the LAN
IP-LAN-service-errors	Number of IP packets received from the LAN for an incorrect service
IP-WAN-rx	Number of IP packets received from the WAN
IP-WAN-tx	Number of IP packets sent to the WAN
IP-WAN-checksum-errors	Number of IP packets incorrectly received from the WAN
IP-WAN fragmentation errors	Number of fragmentations incorrectly received from the WAN
IP-WAN fragmentations	Number of fragmentations received from the WAN
IP-WAN forced fragmentation	Number of fragmentations forced by the WAN
IP-WAN-service-errors	Number of IP packets received from the WAN for an incorrect service
IP-WAN-rx-disconnect	Number of packets from the WAN discarded by timeout
Delete-values	Deletes IP statistics

**Status/TCP-IP-statistics/ICMP-statistics**

These statistics include the following values:

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

**Status/TCP-IP-statistics/TCP-statistics**

These statistics include the following values:

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

**Status/TCP-IP-statistics/TFTP-statistics**

These statistics include the following values:

TFTP-LAN-rx	Number of TFTP packets received from the LAN
TFTP-LAN-rx-read-request	Number of TFTP read requests received from the LAN
TFTP-LAN-rx-write-request	Number of TFTP write requests received from the LAN
TFTP-LAN-rx-data	Number of TFTP data packets received from the LAN

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

### Status/TCP-IP-statistics/DHCP-statistics

These statistics include the following values:

DHCP-LAN-rx	Number of DHCP packets received from the LAN
DHCP-LAN-tx	Number of DHCP packets sent to the LAN
DHCP-WAN-rx	Number of DHCP packets received from the LAN
DHCP-discard	Number of DHCP packets discarded
DHCP-rx-discover	Number of discover messages received
DHCP-rx-request	Number of request messages received
DHCP-rx-decline	Number of decline messages received

DHCP-rx-inform	Number of inform messages received
DHCP-rx-release	Number of release messages received
DHCP-tx-offer	Number of offer messages sent
DHCP-tx-ack.	Number of DHCP packets acknowledged
DHCP-tx-nak.	Number of DHCP packets not acknowledged
DCHP-server-err.	Number of DHCP packets received that were not intended for this server
DHCP-assigned	Number of addresses currently assigned
DHCP-MAC-conflicts	Number of assignments rejected because IP addresses were in use
Table-DHCP	Table containing assignments of IP addresses to MAC addresses
Server flags	Activate/deactivate server flags
Delete-values	Deletes DHCP statistics.

*Table-DHCP*

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




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

**Status/TCP-IP-statistics/NetBIOS**

Additional information about the NetBIOS module can be found in the /Status/TCP-IP-statistics/NetBIOS-statistics menu. This menu has the following structure:

LAN-rx, WAN-rx	0	Number of NetBIOS packets received by the LAN or WAN
LAN-tx, WAN-tx	0	Number of NetBIOS packets sent to the LAN or WAN
Registers	0	Number of name registrations performed
Conflicts	0	Number of detected name conflicts. As the NetBIOS module is only a billboard to which each computer attaches its name, it also does not verify the consistency of the data. The counter is thus only incremented if a host determines a conflict and broadcasts a message to the network to this effect.
Releases	0	Number of name shares performed
Refreshes	0	Number of name renewals performed
Timeouts	0	Number of names dropped due to aging
B-Nodes	0	Number of currently active B nodes (broadcast) in the network














P-Nodes		Number of currently active P nodes (peer-to-peer) in the network
M-Nodes		Number of currently active M nodes (mixed-mode) in the network
W-Nodes		Number of currently active W nodes (hybrid) in the network

<i>B-Nodes</i>	Broadcast nodes. A B node performs name negotiations exclusively via broadcasts. Such a computer is not visible over a router connection, since broadcasts may not be routed.
<i>P-Nodes</i>	Point-to-point nodes. For name negotiations, a P node requires a NetBIOS nameserver (NBNS) as well as a NetBIOS datagram distribution server (NBDD) to transfer datagrams over a router.
<i>M-Nodes</i>	Mixed nodes. This type is a mixture of B and P nodes. It acts as a B node in the local network; if the required partner can't be found in the local network, it attempts to locate it using an NBNS query (P node behavior).
<i>W-Nodes</i>	This type of node is not permissible according to RFC, but was introduced nevertheless by Microsoft as a hybrid node.

### Status/TCP-IP-statistics/DNS-statistics

The DNS statistics provide supplementary information about the DNS module. This menu has the following structure:

LAN-rx		Number of DNS packets received by the LAN
LAN-tx		Number of DNS packets sent on the LAN
WAN-rx		Number of DNS packets received by the WAN
WAN-tx		Number of DNS packets sent on the WAN
Forwarded		Number of requests that could not be fulfilled and were thus forwarded
Errors		Number of invalid requests
DNS-access		Indicates the number of names that were looked up from the DNS table
DHCP-access		Indicates the number of names that were looked up from the DHCP table
NetBIOS-access		Indicates the number of names that were looked up from the NetBIOS tables
Filter		Number of DNS packets filtered by the filter table
Hit-list		This table contains the 16 most popular requests. These may then be prohibited via the filter list if desired.

The hit list has the following structure:

Name	Requests	Time	IP-address
www.elsa.com	1	00.00.0000 00:00:29	10.0.0.123
















The individual fields of this list have the following significance:






Name	Name of the requested computer
Requests	Total number of requests for this name since its appearance in the table
Time	Time of the last request
IP-address	Address of the computer that last requested this name

This list is sorted according to the frequency of requests. When the table is full, the names that have not been requested for the longest period will be deleted to make room for new entries.

## Status/IP-router-statistics

This menu groups together the statistics from the IP router module.

/IP-router-statistics	Statistics from the IP router area	
IPr-LAN-rx		Number of data packets to be routed from the LAN
IPr-LAN-tx		Number of data packets routed to the LAN
IPr-LAN-local-routings		Number of packets received from the LAN and routed to the LAN
IPr-LAN-network-errors		Number of LAN packets that were not routed
IPr-LAN-routing-errors		Number of LAN packets that must be sent to another router
IPr-LAN-ttl-errors		Number of LAN packets with an expired time-to-live value
IPr-LAN-filters		Number of LAN packets filtered by the filter table
IPr-LAN-discards		Number of LAN packets discarded
IPr-WAN-rx		Number of data packets to be routed from the WAN
IPr-WAN-tx		Number of data packets routed to the WAN
IPr-WAN-network-errors		Number of WAN packets that were not routed
IPr-WAN-ttl-errors		Number of WAN packets with an expired time-to-live value
IPr-WAN-filters		Number of WAN packets filtered by the filter table
IPr-WAN-discards		Number of WAN packets discarded
IPr-WAN-type-errors		Number of packets from the WAN without an IP router ID

/IP-router-statistics	Statistics from the IP router area	
IPr-ARP-errors		Number of unsuccessful accesses to the ARP cache
Delete-values		Deletes IP router statistics
Establish-table		Table of the last 20 packets that required a connection
Protocol-table		Table of routed packets arranged by protocol
RIP-statistics		Statistics from the IP/RIP area

*Establish-table* The **establish table** contains the last 20 entries, which provide information on the system time, destination and source addresses, IP protocol, destination port and source port of the data packets that should have caused a connection to be established.

An IP router establish table might have the following appearance:

Time	Dest	Source	Protocol	D-port	S-port
1T; 16:45:01	192.120.131.40	192.120.130.10	tcp	23	4711
1T; 10:45:10	192.120.131.50	192.120.130.10	udp	53	8123

The 'Time' is displayed as either the device operating time or the system time of the ISDN (if provided by the ISDN terminal). The destination and source addresses are IP addresses. The protocol might refer, for example, to tcp, udp, or the like; the destination and source ports provide a more detailed description of the relevant services (e.g. Telnet via TCP and D-port 23, name server via UDP and D-port 53).

*Protocol-table*

The protocol table also supplies valuable information on the volume of packets transferred to the LAN or WAN. These values are encrypted as per the various IP protocols, such as ICMP, TCP, UDP.

A protocol table might have the following appearance:

Protocol	LAN-tx	WAN-tx
tcp	14	30
udp	15	50
icmp	60	40

**Status/IP-router-statistics/RIP-statistics**

This option allows you to display the IP-RIP packets received by the device. These substatistics provide you with the following entries:

RIP-rx	Number of IP-RIP packets received
RIP-request	Number of IP-RIP request packets received
RIP-response	Number of IP-RIP response packets received
RIP-discards	Number of IP-RIP packets discarded
RIP-errors	Number of defective IP-RIP packets
RIP-entry-errors	Number of defective entries in IP-RIP packets
RIP-tx	Number of IP-RIP packets sent
Table-RIP	Routing table of routes learned through RIP broadcast
Delete-values	Deletes IP-RIP-statistics

*Table-RIP*








The associated RIP table contains all of the routes learned from the network. The router itself maintains this table; you cannot modify it manually.





An IP-RIP table might have the following appearance:

IP-address	IP-netmask	Time	Distance	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200

**Status/Config-statistics**



















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




/Config-statistics	Remote configuration statistics	
LAN-active-connections		Current number of active configuration connections from the LAN
LAN-total-connections		Total number of configuration connections from the LAN up until the present
WAN-active-connections		Current number of active configuration connections from the WAN
WAN-total-connections		Total number of configuration connections from the WAN up until the present
Outband-active-connections		Current number of active outband configuration connections
Outband-total-connections		Total number of previous outband configuration connections up until the present
Outband-bitrate		Bit rate of the last outband configuration session

/Config-statistics	Remote configuration statistics	
Login-errors		Total number of defective logins
Login-locks		Number of login locks
Login-rejects		Number of login attempts while the login lock was active
Delete-values		Deletes the config statistics

## Status/Queue-statistics

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

/Queue-statistics	Statistics on the queue	
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
WAN-heap-packets		Number of buffers available
WAN-queue-packets		Number of buffers in use
ARP-query-queue-packets		Number of ARP packets in the query queue
ARP-queue-packets		Number of ARP packets in the normal queue
IP-queue-packets		Number of IP packets in the normal queue
IP-urgent-queue-packets		Number of IP packets in the secured queue
ICMP-queue-packets		Number of ICMP packets
TCP-queue-packets		Number of TCP packets
TFTP-queue-packets		Number of TFTP packets
SNMP-queue-packets		Number of SNMP packets
Prot-heap-packets		Number of prot heap packets
IPr-queue-packets		Number of packets remaining to be processed by the IP router.
DHCP-server-queue-packets		Number of packets in the receive queue of the DHCP server.
IPr-RIP-queue-packets		Number of packets in the receive queue of the IP-RIP module (for RIP queries, RIP propagations...).
DNS-Tx-queue-packets		Number of packets to be forwarded to DNS or NBNS servers.
DNS-Rx-queue-packets		Number of packets that come from DNS or NBNS servers and are to be forwarded to the host.

/Queue-statistics	Statistics on the queue	
IP-Masq.- Tx-queue-packets		Number of packets to be sent masked (to the Internet).
IP-Masq.- Rx-queue-packets		Number of packets received from the Internet and have to be demasked.
WLAN management heap packets		Number of packets available in the buffer.

## Status/Connection-statistics

This menu allows you to display connection times, all charges incurred and other useful information related to ISDN port utilization.

For each available interface, the **Status/Conn.-statistics** menu option provides statistics on the connections established via this interface. The table maintained here has the following layout:

lfc	Connection	Active	Passive	Errors	Con.-Time	Charge
Ch01	0	0	0	0	No connection	0
Ch02	0	0	0	0	No connection	0

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

lfc	Designates the associated channel.
Connection	Indicates the number of connections to the particular channel.
Active	Indicates the number of connections actively established for the channel.
Passive	Indicates the number of connections established for the channel by incoming calls.
Errors	Indicates the number of connection errors.
Con.-Time	Indicates the period of time the current connection has existed. If no connection exists, "No-connection" is output.
Charge	Indicates the amount of charges for the current connection. This value is reset to zero when a new connection is established.

The total charges incurred are not displayed directly. However, the charges are totaled internally in order to permit the management of the charges budget (also see **Setup/Charges-module**).

## Status/Info-connection

The menu item **Status/Info-connection** has additional information on the current connection status (logical remote station etc.) for every available interface. The table maintained here has the following layout:

lfc	Status	Mode	Dialup-remote	Device-name	B1-HZ	B2-HZ
Ch01	Ready				0	0
Ch02	Ready				0	0

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

lfc	Designates the associated channel.
Status	Indicates the status of the particular connection. The possible values are: <b>Init</b> , <b>Setup WAN</b> , <b>Ready</b> , <b>Dial</b> , <b>Incoming call</b> , <b>Protocol</b> , <b>Connection</b> , <b>Callback</b> , <b>Bundle</b> and <b>Reserved</b> . The <b>Bundle</b> status is indicated in the display <i>ELSA LANCOM Wireless IL-2</i> by the addition of a <b>"/2"</b> in columns 15 and 16 of the associated display line. <b>Bundle</b> is displayed for the second interface either when a bundle connection has been activated via the first interface or when a leased-line connection with two B channels has been set. <b>Reserved</b> is displayed for the second interface when a connection exists to the first B channel and the Y connection has been deactivated.
Mode	Reflects the type of establishment. The following are possible: <b>Active</b> (active call establishment = dialing) <b>Passive</b> (passive call establishment = call acceptance) <b>CB</b> (call establishment via callback)
Dialup-remote	Indicates the call number of the remote station from the name list.
Device-name	Indicates the logical name of the remote station (if it can be detected). The device name is also displayed on the appropriate display line as soon as a logical connection is established.
B1-HZ	Indicates the short timeout for the connection.
B2-HZ	Indicates the short timeout for bundled channels for this connection.

## Status/Layer-connection

The menu item **Status/Layer-connection** has information on the B channel protocol used on the interface for every available interface. The entries in this table correspond to those in the layer list **Setup/WAN-module/Layer-list** in the WAN module. An additional entry exists for the interface itself. The menu has the following layout:

lfc	WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
Ch01	DEFAULT	ETHER	ELSA	X.75ELSA	compr.	HDLC64K
Ch02	PPPHDLC	TRANS	TRANS	PPP	none	HDLC64K

## Status/Call-info-table

This table displays the last ten incoming calls, regardless of whether the router answered these calls.

This allows you, for example, to determine the internal MSN used when the system is operated in connection with a PBX. The table has the following layout:

Time	Ifc	CLIP-Caller	Dial-Caller	Capab.	B chan.
OT; 00:20:57	S <sub>0</sub>	5678	1234	HDLC64K	2
OT; 00:20:46	S <sub>0</sub>	4321	1234	HDLC64K	1
OT; 00:19:47	S <sub>0</sub>	4321	1234	HDLC64K	1
OT; 00:11:33	S <sub>0</sub>	5678	1234	HDLC64K	1
OT; 00:01:13	S <sub>0</sub>	4321	1234	HDLC64K	2
OT; 00:01:02	S <sub>0</sub>	4321	1234	HDLC64K	1
OT; 00:00:06	S <sub>0</sub>	5678	1234	HDLC64K	1

The different entries have the following meaning:

Time	Time when the call came. Either the device operating time or the system time of the ISDN is displayed (if made available from the ISDN terminal).
Ifc	Designates the associated interface.
CLIP-Caller	Call number (CLIP) of the caller
Dial-Caller	The MSN/EAZ dialed by the caller
Capab.	The service requested by the caller. Possible values are HDLC64K, HDLC56K and unknown. An analog call is displayed as unknown here. <i>LANCOM Office-Router</i> can also display the values A-3 kHz (analog 3 kHz), language (for normal speech transmission) and fax G2/3 (for analog fax transmission as per group 2 or 3).
B-chan.	The B channel used. A value of 0 means that all channels have already been seized, i.e. call waiting is activated.



*A tip for those using a router in a PBX: Following a call to any ISDN device under the number of the ISDN bus, the MSN/EAZ displayed under 'Dial-Caller' is exactly the entry that must be entered in the router at /SETUP/WAN-MODULE/ROUTER-INTERFACE-LIST/MSN-EAZ in order for a call to be correctly answered from an external station.*

## Status/Remote-statistics

This table shows the last ten connections of the *ELSA LANCOMs* with information on the remote station.



The table has the following layout:

Conn.-start	Remote-ID	Mode	Ifc	Conn.-time	Charge
OT; 00:20:57	BERLIN	Active	Ch01	50	5
OT; 00:20:46	CHEMNITZ	Passive	Ch02	230	10

The different entries have the following meaning:

Conn.-start	Time at which the connection was established. Either the device operating time or the system time of the ISDN is displayed (if made available from the ISDN terminal).
Remote-ID	Logical remote station name.
Mode	Type of connection establishment: Active – the connection was actively established by the device Pas. – The device received a call RR – The device called the remote station back
Ifc	Interface, over which the connection is made (Ch01, Ch02).
Conn.-time	Duration of the connection in seconds
Charge	Charges for this connection in units.

A connection remains in the table for at least as long as it is established. Every new connection fills the table from top to bottom. If an existing connection is the lowest entry in the table, an already released connection will be deleted from the table instead if necessary.

## Status/Channel-statistics

This table shows information on the current status of the two B channels. With the *ELSA LANCOM Wireless IL-2* information on the a/b ports is also shown. The information from this table is primarily used for output via *ELSA LANmonitor*. Therefore, some values are shown simply as bits with no further explanation.

The table has the following layout:

Channel	State	App	Mode	Cause	Dialup-remote	Sub-address	Charge	Conn.-time	Extra	ISDN-display
S <sub>0</sub> -ERR	00000000 0	Router	active	0000	0241123456	00000000	3	0		
S <sub>0</sub> -B1	00000000 0	a/b	active	0000	0241123457	00000000	2	20		
S <sub>0</sub> -B2	00000000 0	LANCAP I	passive	0000	0241123458	00000000	4	180		





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

Channel	Channel (or a/b port) for the entry is valid. Only the latest status of a channel is ever displayed. A dedicated "channel" is maintained for error messages on channels.
State	The status of a channel is shown here as, e.g., 'ready'.
App	Application that occupies the channel: Router, <i>LANCAPI</i> or a/b port
Mode	Types of last connection establishment: active or passive
Cause	Last error
Dialup-remote	Remote station call number: with active establishment the number dialed, with incoming calls the number sent.
Subaddress	Addition to application that, e.g., indicates the logical channel for the router for the <i>LANCAPI</i> , e.g., the IP address of the client that is using the CAPI.
Charge	Number of charging units incurred for this connection.
Conn.-time	Duration of the last connection on this channel
Extra	Additional information on the connection, e.g. the name of the remote station for router connections.
ISDN-display	Information from the switching center, e.g. error messages, if connected to the PBX possibly also the caller's name, etc.

## Status/Time-statistics

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

The menu has the following layout:

/Time statistics	Time module statistics	
Current-time		Current device time.
Source		Time output source. The possible values are: 'ISDN' for time taken from the ISDN, 'Manual' for the manual setting of the time with the 'time' command, 'RAM' for time imported from the device RAM after booting.
Setup		Number of time imports from one of the above sources.
ISDN		Additional information on time import from the ISDN

## Status/Time-statistics/ISDN






These statistics include the following values:

Connection	Number of attempts to read time information from the ISDN
Information	Number of time updates received from the ISDN
Info-error	Number of erroneous time updates received from the ISDN

## Status/LCR-statistics




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

The menu has the following layout:

/LCR-statistics		Least-cost router statistics
Total calls		Total number of LCR calls
Successes		Number of calls in which the router found a suitable rule in its tables and successfully rerouted the connection.
Not-found-errors		Number of calls in which the router did not find a suitable rule in its tables and thus could not reroute the connection.
No-time-errors		Number of calls in which the LCR could not become active due to lack of time
Provider-statistics		A table with all providers used (or their prefixes), the number of successful and unsuccessful calls
Delete-values		Deletes LCR statistics

## Status/PCMCIA-status

General information on the inserted card can be found here:

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
















## Status/Delete-values

With the exception of the tables, this option allows you to delete all the values in the substatistics. To do so, enter the following command:

```
do delete-values
```

## Setup

This menu allows you to query and modify all the system parameters that are necessary to the functioning of the devices.

/Setup		System configuration
Name		Entering the device name
WAN-module		WAN settings
Charges-module		Charge management settings
LAN-module		LAN settings
WLAN-module		WLAN settings
TCP-IP-module		TCP/IP module settings
IP-router-module		IP router module settings
SNMP-module		Settings for configuration via SNMP
DHCP-module		DHCP server settings
Config-module		Configuration module settings
DNS module		DNS server settings
NetBIOS-module		NetBIOS module settings
LANCAPi-module		<i>ELSA LANCAPI</i> settings
LCR-module		Least-cost router settings
Time-module		Time module settings

### Name

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

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

display. In the default configuration, no name is entered.

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












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

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

In addition, the device names you assign must be unique. For example, you might match the device names to the location (e.g. Aachen, Berlin, Provider, etc.).

## Setup/WAN-module

This menu groups together all the settings necessary for starting up the WAN interface and controlling connections to logical remote stations.

/WAN-module		WAN settings
Interface-list		S <sub>0</sub> interface settings
Router-interface-list		Router module settings
Name-list		Remote station settings
RoundRobin-list		Settings for different remote station numbers
Layer-list		Settings for the layer combinations used
PPP-list		Parameter settings for PPP connections
Number-list		Settings for call numbers with access authorization
Script-list		Dial script settings
Manual-dialing		Settings for manual connection control
Protect		Protection for answering incoming calls
CB-attempts		Number of callback attempts when the remote station is busy

### Interface-list

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

lfc	Protocol	FV-B-chan.	Dial-prefix
S0	Auto	1	0

Additional, special interface settings are also available for the various modules, e.g. the call numbers to which a module should react, see also

Setup/WAN-module/Router-interface-list

setup/lancapi-module

setup/ab-module/port-list

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

Ifc	Designates the associated interface.
Protocol	D channel protocol setting. The possible values are: <b>Auto</b> : automatic detection of the D-channel protocol <b>DSS1</b> : Euro-ISDN <b>1TR6</b> : National ISDN <b>GRP0</b> : Leased-line connection group 0 <b>GRP2</b> : Leased-line connection group 2 <b>P2P-DSS1</b> : Point-to-point connection
FV-B-chan.	B channel settings for a leased-line connection. The possible values are: <b>none</b> : Leased-line connection not assigned to a specific channel. <b>1</b> or <b>2</b> : Leased-line connection operates over the assigned B channel. Please refer to the information on setting these parameters in the fixed connection description. The fixed connection function is not a standard component of the <i>ELSA LANCOM Wireless</i> .
Dial-prefix	Global dialing prefix for all modules of the devices. The digits entered here (maximum 8) are automatically prefixed to the selected call number in every call. Use this prefix when, for example, the router is connected to a PBX.

Router-  
interface-list

This table contains the interface settings that apply to the router modules of the *ELSA LANCOM*.

Ifc	MSN/EAZ	YV.	CLIP
S0	123456	Off	On

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

Ifc	Designates the associated interface.
MSN-EAZ	If your device is connected to an ISDN port with 1TR6, enter the EAZ to which the interface is to respond. If your device is connected to an ISDN port with DSS1, enter the MSN to which the interface is to respond. If you wish the interface to respond to several different MSNs, enter them here separated by semicolons. A '#' in the list enables any number of incoming MSNs. For outgoing calls, the first MSN in this list will be reported to the remote station. If no MSN is entered, the switching center sends the main MSN of the terminal.
YV.	This entry can be used to control the interface's ability to establish Y connections. Possible settings are: <b>On</b> : Y connection is supported; a number of connections can be established simultaneously (default). A channel bundling connection is broken off when a second connection to another remote station has to be established. Refer also to the settings for the availability of the <i>LANCAP</i> and the telephone system with the <i>ELSA LANCOM Wireless IL-2</i> . <b>Off</b> : Y connection not supported; only one connection can be established. The second connection is blocked. If a connection to an additional remote station is to be established, this establishment is rejected. A channel bundling connection is not affected.
CLIP	Calling Line Identification Protocol: Suppresses the outgoing MSNs. Possible values: <b>Yes</b> : Activate CLIR, do not send MSN. <b>No</b> : Deactivate CLIR, send MSN to remote station. Please note: The "selective suppression of call number transmission" may be a service feature that will have to be obtained from the telephone company.

*Name-list*

The names entered in the name list are needed by the router to determine the correct remote station and corresponding layer name. The name list is also used for the callback function.

The name list can contain 64 different device names and might, for example, have the following appearance:

Device-name	Dialup-remote	B1-HZ	B2-HZ	WAN-layer	Callback
AACHEN	875463	180	0	PPPHDLC	On
BERLIN	040785647	20	20	DEFAULT	Off

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

Device-name	In the <b>Device Name</b> column, you can enter an original remote station name, which you must then assign to the relevant remote station via the <b>Name</b> option in the <b>Setup</b> menu.
Dialup-remote	In this column, you can store the number to be called and, if applicable, supplement it with special dialing characters (see above, default: None).
B1-HZ	In this column, you can define appropriate connection timeouts (in seconds) for the first B channel. If no data is being transmitted when this time expires, the connection on this channel is released (default: 20). If charging information is transmitted over the ISDN network during the connection, the <i>ELSA LANCOM</i> will make full use of every charging unit and will only terminate the connection just before the beginning of the next unit. This function is also referred to as dynamic short-hold.
B2-HZ	In this column, you can define appropriate connection timeouts for the second B channel (same as B1-DT, default: 20). The B2 hold time controls the bundling behavior during a channel bundling. Values of 0 or 9999 identify static bundling, values between them dynamic bundling.
WAN-layer	In this column, a name is stored that must also be entered in the layer list. This establishes the transfer protocol required for this connection.
Callback	In this column, you can define whether a callback is to be made for the relevant remote station (Off/Name/Auto/Looser/ELSA; default: Off).

## ■ Callback options

Off	No callback is made.
Looser	The router stops attempting to establish a connection when there is a call from this remote station (reciprocal call establishment). This setting must be used when a callback from the remote station is expected.
Auto (not applicable to Windows 9x or Windows NT)	The connection will be rejected and a direct callback will be initiated if the remote station is specified in the number list. This means that the caller is not charged. If the remote station is not specified in the number list, a callback will be negotiated in a protocol negotiation (ELSA or PPP). A charge of one unit is incurred for this.
Name	This setting forces a protocol negotiation. This enables call number protection to be set in the number list and also a callback to be started using the protocol negotiation. A charge of one unit is incurred for this.
ELSA	This setting enables a particularly fast callback procedure. The called-back remote station must use the 'looser' setting.

- The special dialing characters in the table below can be entered along with the call number in the name list, round robin list, or logical dial prefix. They control the line access, the use of a semipermanent leased-line connection or determine the interface to be used for the connection:

#	Trunk seizure (only with some PBXs).
F	The remote station can be reached via the leased-line connection only. Syntax: F[channel:][subscriber number] The channel and subscriber number are both optional. In the case of several leased lines, the channel specifies the B channel to be used. Depending on the setting in the channel list, the subscriber number indicates whether a dynamic channel bundling or backup line is to be realized over the dial-up connection.

When **S** or **S2** is appended to the call number, the semipermanent connection (SPV) is activated for the D-channel protocol 1TR6.

*You must subscribe to an SPV through your telephone company for a fixed payment.*

*If you forget to append an **S** or **S2**, the SPV will behave like a standard dial-up line and your charges will be unnecessarily high. The telecommunications provider then charges you the fixed charges and the dial-up line charges incurred during the time the line was used.*

*RoundRobin-list* The round-robin list enables a remote station to be reached with several call numbers. It has the following layout:

Device-name	RoundRobin	Head
AACHEN	4321-5555-6666	Last



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

Device-name	In the device name column, you can enter a remote device name from the name list. If one line in the Round Robin list is insufficient for all desired call numbers, the line can be extended as shown below: The # character and a unique index are added to the device name (e.g. AACHEN#1) and it is entered on the next line.
Round-Robin	The DDI numbers of all possible remote stations are entered here under their corresponding device names. The individual DDI numbers must be separated by hyphens.
Head	In the <b>Head</b> column, the following entries are possible: <b>Last:</b> The next connection to be established will begin with the DDI that was successfully used for establishing the last connection (default). <b>First:</b> The next connection to be established will always begin with the first DDI. For a logical remote station, this field can be modified only by means of its <b>first</b> entry in the table. The field is automatically updated when other entries are made for this remote station.

#### Layer-list

In the layer list, you can freely define the different B-channel protocols by combining various ISDN layers. This enables compatibility to devices from other manufacturers that use different B-channel protocols to be set.

The following standard settings are valid for *LANCOM Office-Router*:

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

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

Layer-name	In this column, you can enter an original name designating the layer combination that you use. These names can then be used in the name list 'layer name' column depending on their spelling to set the protocol. If an entry with the name <b>DEFAULT</b> is defined in this column, the settings stored there are always used when no layer name can be assigned (e.g. a caller does not transmit his or her call number). This entry is also used when a group 0 leased-line connection is established. If the <b>DEFAULT</b> entry is not present, a B channel protocol developed by ELSA is used as the default. The user may delete or change any of the layers predefined here.	
Encaps.	Additional information regarding the data to be transmitted may be specified in the <b>Encaps</b> column. The following entries are possible:	
	ETHER	The data is provided with an Ethernet header. This setting is required for communication with older <i>ELSA LANCOM</i> devices or in bridge operation.
	TRANS	No Ethernet header is sent in this setting. Only "pure" IP data packets are transferred, for example. This setting provides the greatest possible effective data throughput.

Lay-3	In the lay-3 column, you can define additional headers for data transmission in ISDN. You can select from among the following settings:	
	TRANS	No additional header is inserted (higher data throughput). Always select this setting if the remote station sends the data transparently via ISDN layer 3 (e.g. transparent HDLC, transparent X.75LAPB).
	ELSA	The data is provided with an ELSA header. In addition, when a connection is established, a protocol negotiation is performed in which the remote stations exchange names. Incoming-call protection by name is possible only if this setting is selected. Without an ELSA setting, incoming-call protection is possible by call number only. This setting is required for communication with older <i>ELSA LANCOM</i> devices or the workstation drivers.
	PPP	A negotiation is performed according to the point-to-point protocol.
	APPP	A negotiation is performed as per the asynchronous PPP. APPP is then used when synchronous PPP is not possible because the connection does not permit a synchronous transmission (e.g. for analog modem operation).
	SCPPP	Following completion of script processing, a synchronous PPP negotiation is initiated.
	SCAPPP	Following completion of script processing, an asynchronous APPP negotiation is initiated.
	SCTrans	Following completion of script processing, a connection exists to the remote station. No further protocol negotiation is performed.
Lay-2	In this column, you can select the protocol for ISDN layer 2:	
	TRANS	The data is packed directly in HDLC packets. Always select this setting if communication is to take place via transparent HDLC.
	X.75LAPB	The data is exchanged in X.75 secured format. Always select this setting if the remote station is to work with X.75 data protection.
L2-Opt.	The L2-opt. enables the setting of an option for the data transfer setting under Lay-2 with an additional <i>ELSA LANCOM</i> .	
	none	No data compression or channel bundling is performed.
	compr.	V.42bis ( <i>ELSA LANCOM Wireless IL-2</i> ) or Stac data compression will be used. Data compression as per V.42bis is possible only in connection with X.75ELSA or X.75LAPB. Compression as per Stac (Hi/fn) must be used in connection with PPP or multilink PPP. Stac compression may also be used in connection with Windows remote stations.
	bundle	Channel bundling is performed via several B channels. Channel bundling is only possible for the Lay-2 settings of 'PPP' Static or dynamic channel bundling depends on the B2 connection timeout. A B2 hold time of '0' or '9999' will set a static channel bundling in which both channels are always used. In the event of dynamic channel bundling with other B2 hold times, the second channel is only activated when the data throughput exceeds a specified threshold.
	bnd+cmpr	Channel bundling and data compression takes place over two B channels.

Lay-1	The lay-1 column allows you to define the speed at which the data is sent in ISDN.	
	HDLC64K	The data is transmitted at 64,000 bps.
	HDLC56K	The data is transmitted at 56,000 bps. This setting is especially important for connections in the USA.

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

To link to devices from other manufacturers, please check with that manufacturer for the data format used (PPP is almost universally supported).

For Internet and remote access, PPP is generally specified.

#### PPP-list

The router needs the device names contained in the PPP list in order to determine the security procedure settings suitable for the connection and to determine the PPP parameters. It contains a maximum of 64 entries and is structured as follows:

Device-name	Auth.	Key	Time	Try	Conf	Fail	Term	Username
AACHEN	CHAP	*****	0	5	10	5	2	ELSA

Not all parameters can be reached via the telnet configuration. Use *ELSA LANconfig* so far as possible.

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

Device-name	In the Device-name column, you can enter the name with which the remote station logs onto the router. In the case of connections via the data transmission network, this is the name entered as "Username". For remote access via the data transmission network, the 'Username' field (see below) is not evaluated! Entries are not case-sensitive!	
Auth.	In this column, you can enter the security procedure to be used for verification of the remote station. Default: PAP	
	none	The router does not negotiate authentication with the remote station when establishing a connection. However, the remote station can itself require authentication from the router. This is the case when dialing up a connection to an ISP, for example.
	PAP	The remote station is checked as per the Password Authentication Protocol.
	CHAP	The remote station is checked as per the Challenge Handshake Authentication Protocol.
Key	A password may be entered in this column. Its presence is indicated by the symbol * and it is used to check the remote station. It may consist of 95 characters (7-bit ASCII, including spaces). Default: None The <code>set ?</code> command shows a list of the allowable characters.	

Time	In this column, you can enter the period of time between two remote station verifications specified in minutes. The CHAP protocol must be set here. Default: 0
Try	In this column, you can specify the number of times the verification attempt is to be repeated. If verification fails, the connection is immediately terminated. Default: 5
Conf, Fail and Term	These parameters may be used to influence the operation of the PPP. They are defined and described in RFC 1661. The default values are sufficient for most remote stations. If nothing is entered here, the values 0,0,0 appear in the display but the default values 10, 5, 2 are still used. These parameters can only be changed via SNMP or TFTP (using the <i>ELSA LANconfig</i> configuration program)!
Username	The user name (max. 64 characters) transmitted to the remote station during PPP negotiation. The router identifies itself to the remote station with it. If no user name is entered, the device name serves as the user name. Entries are case-sensitive here.

*Number-list*

Under this option, a number list is managed in which you can enter 64 different call numbers with their associated device names. This list can be used to assign the call numbers (CLI) transferred by remote stations to the remote station names.

The entries in the number list for the two calling devices AACHEN and BERLIN might appear as in the table below, thus permitting the name to be derived from the call number supplied and, if applicable, permitting a callback to be initiated via the name list:

Dialup-remote	Device-name
875463	AACHEN
040785647	BERLIN

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

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

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

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

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

*Script-list*

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

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




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

The entries in the script list have the following meaning:

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

### Setup/WAN-module/Manual-dialing

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

/Manual-dialing	Settings for manual connection control	
Connect		Establishes a connection.
Disconnect		Termination of connections
Status		Displays the current connection status.

*Connect*

Parameter: Remote station's device name (via remote configuration only).

You can use the command

Do /Setup/WAN-module/Manual-dialing/Connect to remote station

to initiate the manual establishment of a connection via remote configuration. The remote station's device name specified as a parameter must also be entered in the name list with a call number.

When the function is activated by the keyboard of the *ELSA LANCOM*, the error message 'No remote station' is displayed, because a name cannot be entered here. Therefore, this function must not be used from the keyboard of the *ELSA LANCOM*. If you attempt to establish a connection to a logical remote station for which no call number is specified in the name list, the 'No number' error message is displayed.

*Disconnect*

This command allows you to release an existing connection. If a connection is released manually, the name of a remote station may also be entered in the remote configuration. In this case, only the connection to the remote station specified is released. If a connection to the remote station specified does not exist, there is no further response. However, if a remote station name is not entered, all existing connections will be released.

**Setup/WAN-module/protection**

This option allows you to select the conditions under which incoming calls are to be answered at the transmission module.




- If 'Protect' is set to 'none', all pending calls are answered provided that the remote end supports the connection protocol.
- If this option is set to 'name', calls are accepted only from remote stations for which an entry is found in the name list. This verification provides additional protection. This verification is only available when using PPP.
- If this option is set to 'number', calls are accepted only from remote stations that are entered in the number list as authorized remote stations.
- The 'no./name' setting allows you to select combined protection using a name list and number list. First a verification that there is an entry in the number list is made. If this is not possible, the router will attempt to determine the name using the protocol negotiation.

**Setup/WAN -module/CB-attempts**

This option allows you to set the number of times (from 1 to 9) a callback is to be attempted when the remote station is busy. For international connections, you should enter a value from 3 to 5 in order to optimize the callback functions. The default setting is 3.

**Setup/LAN-module**

This menu allows you to select the settings needed for the local network. The menu has the following layout:

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

*Node-ID*

This option allows you to display the router's own Ethernet address. The value displayed here was set at the factory and cannot be changed. The Ethernet address is displayed















as a 12-digit hexadecimal value, with the first six digits '00a057' standing for an ELSA device.

#### Spare-heap

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

## Setup/TCP-IP-module

This menu allows you to enter settings for the TCP/IP module. The menu has the following layout:

/TCP-IP-module	TCP/IP module settings	
State		Activates or deactivates the TCP/IP module.
IP-address		Local IP address
IP-netmask		Local network's matching IP network mask
Intranet addr.		Local Intranet address
Intranetmask		Local network's matching Intranet network mask
Access-list		Restricts access to internal functions via TCP/IP.
DNS-default		Domain name server
DNS-backup		Backup domain name server
NBNS-default		NetBIOS name server
NBNS-backup		Backup NetBIOS name server
Table-ARP		ARP table for mapping an IP address onto a MAC address
ARP-aging-min.		Dwell time for entries in the ARP table
TCP-aging-min.		Time limit for configuration connections that are inactive
TCP-max.-conn.		Max. number of simultaneous configuration connections to the <i>ELSA LANCOM</i>

#### State

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

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

#### IP-address

The IP address for the router may be entered here. The default address on delivery is '0.0.0.0'.

If IP masquerading is used, this address takes on a special meaning in connection with the Intranet address:

If the IP address is assigned to the router by the Internet provider by PPP, all computers in the network linked by IP address and IP network mask are normally routed. These computers can then also be accessed directly from the Internet.

*IP network mask* The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network). A network mask of 255.255.255.255 means that there is only one computer in this network (the router itself). This setting (an IP address registered in the Internet with a fully assigned network mask) can be used for masquerading via a raw IP access, such as that offered by the provider of the individual network. With such an access an IP address is not assigned to the router by a PPP negotiation, but it must have a fixed IP address registered in the Internet.

*Intranet-address* A second IP address for the router may be entered here. The second IP address enables the device to be used as a router for two logical IP networks and also this address has a specific meaning with the use of IP masquerading:

In this case, all computers that are in the network linked by Intranet address and Intranet mask are hidden behind the address assigned by the provider (or the IP address).

*Intranetmask* The network mask belonging to the IP address of the local network must be entered here. The default setting is 255.255.255.0 (class C network).



*If neither an IP nor an Intranet address has been specified, the device responds to a default IP address, the first three digits of which are identical to the first three digits of the sending device XXX.XXX.XXX.YYY. The device can then be reached by dialing the IP address XXX.XXX.XXX.254.*

*In the event that such an address already exists in the network, a different address must be entered via the keyboard (ELSA LANCOM Wireless IL-2 only) or via outband configuration (terminal program).*



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

*Access-list*

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



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



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

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

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

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

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

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

IP-address	IP netmask
192.234.222.0	255.255.255.0

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

#### DNS-default

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

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

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

#### DNS-backup

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

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

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

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

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

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






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





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

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

## Setup/IP-router-module

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

/IP-router-module	IP router module settings	
State		Activates or deactivates the IP router module.
IP-routing-table		Router table for IP network and remote station assignment
LAN-filter-table		Negative/connect filter table for the TCP/UDP destination ports of LAN packets
WAN-filter-table		Negative filter table for the TCP/UDP destination ports of WAN packets
Proxy-ARP		Activates/deactivates the proxy ARP function

/IP-router-module		IP router module settings
Loc.-routing		Activates/deactivates local routing
Routing-method		Routing method for IP packets
RIP-config		Settings for IP-RIP operation
Masquerading		Settings for IP masquerading

*Operating*

This option allows you to activate or deactivate the IP router module. In the default configuration, the IP router module is activated.

*Activating the IP router module also activates the TCP/IP module.*

*IP-routing-table*

The routing table can contain a maximum of 128 entries of destination network addresses or direct IP addresses with netmasks, and the names or IP addresses of other local routers. Alternatively, you can enter a setting by means of which packets to specific destination IP addresses are discarded and are not answered by proxy ARP. This is done by entering 0.0.0.0 for the name of the responsible router.

The 'Masquerade' field indicates whether the route should be masked or not. The following options are offered here:

- **On:** IP masquerading is switched on and functions with dynamic assignment of the IP address by the remote station. In this procedure the router queries the IP address '0.0.0.0' at the remote station and is assigned a random IP address by the remote station, which is then used for further processing.
- **Off:** Masquerading is switched off.
- **Static:** IP masquerading is switched on and functions with assignment of a static IP address previously assigned by the remote station. In this procedure the router queries the IP address entered under 'Setup/TCP-IP-module' at the remote station and is assigned this address by the remote station. Use this setting when the remote station (e.g. your Internet provider) has assigned you a fixed IP address in the access data. Of course, this procedure will only function when this address has also been entered in the router as the IP address.

The IP routing table is generally sorted as shown below:

- The longest network mask is placed on top.
- For network masks of equal length, the one with the smallest IP address is placed on top.

In order to identify the correct remote station, the router searches the routing table from top to bottom using the destination IP address received. If a matching entry is found, the router name found is used for establishing the connection.

Address ranges that are prohibited in the Internet are excluded from transmission by preset entries in the IP routing table (the router name 0.0.0.0 means that packets to these addresses are not transmitted). The IP routing table below is provided by way of example and also shows the default settings:

IP-address	IP netmask	Router-name	Distance	Masquerade
192.168.0.0	255.255.0.0	0.0.0.0	0	Off
172.16.0.0	255.240.0.0	0.0.0.0	0	Off
10.0.0.0	255.0.0.0	0.0.0.0	0	Off
224.0.0.0	224.0.0.0	0.0.0.0	0	Off

However, if these addresses are required for Intranet use, for example, it is possible to delete the predefined entries at any time. If the routing table contains no entries with the router name 0.0.0.0, the router processes all IP addresses with valid routes.

#### ■ Example

- The local network address is 192.120.130.0.
- Three terminal units must be available via proxy ARP with the IP addresses 192.120.130.10, 192.120.130.11 and 192.120.130.12 via an *ELSA LANCOM* 'Dresden'.
- Two destination networks 192.120.131.0 and 192.120.132.0 can be accessed by the remote stations 'AACHEN' and 'BERLIN'.
- Data packets for the destination network 193.140.300.0 are to be sent to another local router with the IP address 192.120.130.200.
- Absolutely nothing is to be transmitted to the destination network 193.140.200.0.
- All other non-local data packets must be sent to the router 'PROVIDER' at the Internet service provider.

In this example, the router table would contain the following entries:

IP-address	IP netmask	Router-name	Distance	Masquerade
192.120.130.10	255.255.255.255	DRESDEN	0	Off
192.120.130.11	255.255.255.255	DRESDEN	0	Off
192.120.130.12	255.255.255.255	DRESDEN	0	Off
192.120.131.0	255.255.255.0	AACHEN	0	Off
192.120.132.0	255.255.255.0	BERLIN	0	Off
193.140.200.0	255.255.255.0	0.0.0.0	0	Off
193.140.300.0	255.255.255.0	192.120.130.200	0	Off
255.255.255.255	0.0.0.0	PROVIDER	0	On



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

The last line is an entry for the “default route”. The IP address 255.255.255.255 means the same as 0.0.0.0 (for technical reasons, 0.0.0.0 cannot be entered in the first column). Because it contains the IP network mask 0.0.0.0, this line is always appropriate after the rest of the table has been searched. Therefore, the router sends everything that it cannot transfer over other routes and should not discard or that comes from a WAN terminal and is not local to the router at the provider.

**LAN-filter-table** This table allows you to filter specific ranges of destination ports. In addition, you can determine how the packets are to be filtered. If packets with the entered ports are received from the LAN side, they will not be forwarded (always filter) unless a connection is currently in place (connect filter) or unless they can be routed over other than the DEFAULT route (I-Net filter).

The LAN port filters are defined in a table with the following layout::

Idx.	D-st.	D-end	S-st.	S-end	Source	Src-netmask	Prot	Type
WIN	0	0	137	139	255.255.255.255	0.0.0.0	TCP and UDP	Always-filt.

The table fields have the following meaning:

- **Idx.**  
Unique index. This entry is required to enable the filters to be distinguished. The index may be four characters long and selected as desired.
- **D-st., D-end**  
Destination port range that is to be filtered. A range of 0 to 0 means that no destination port is affected by this filter.
- **S-st., S-end**  
Source port range that is to be filtered. A range of 0 to 0 means that no source port is affected by this filter.
- **Src-address, Src-netmask**  
A subnetwork of the local network for which the filter is valid can be entered here. A source address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).
- **Prot**  
Protocol that is to be filtered. Possible entries are **TCP, UDP, ICMP** and **all**.

The setting **all** filters out every packet from the specified source network or to the destination network.

■ Type

Filter type. The possible values are Always-filt., Connect-filt. and Internet-filt.

- **Always** filter: The packet is discarded.
- **Connect** filter: The packet is discarded if there is no connection to the remote station.
- **Internet** filter: The packet is discarded if its destination can be accessed only via the default route.

The default filter is entered in the above table. It suppresses the unwanted and cost-intensive connections in Windows networks on IP. These networks regularly send items such as DNS queries to the local network, which are routed to the Internet without this filter.

WAN-filter-

This table allows you to enter specific ranges of destination ports. If packets with the entered ports are received from the WAN side, they will not be forwarded (firewall function).

The WAN port filters are defined in a table similar to the LAN filter table:

Idx.	D-st.	D-end	S-st.	S-end	Dest	Dst-netmask	Prot
WIN	53	53	137	139	0.0.0.0	0.0.0.0	TCP and UDP

The fields in the table have the same meaning as in the LAN filter table, with the following exception:

■ Dst-address, Dst-netmask

A subnetwork of the local network for which the filter is valid can be entered here. A destination address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).

The table entries are sorted in a similar fashion to the IP router table:

- Longest network mask is placed on top.
- For two network masks of equal length, the one with the smaller IP address is placed on top.

Network masks and IP addresses of 0.0.0.0 can be used as “wildcards”. Specified computers and networks may be simultaneously subjected to targeted filtering while others pass the router unfiltered.

The tables are processed from top to bottom. As soon as a matching filter is found, the packet is handled accordingly.



*Proxy-ARP* This option allows you to activate or deactivate the proxy ARP mechanism (default: 'Off'). This function permits data to be transmitted to IP addresses within the same logical network as the sender, e.g. when linking individual workstation computers (teleworkers) to the corporate network via TCP-IP

*Loc.-routing* Local routing enables the router to forward data packets via the local network. The local routing is necessary if the router, as the default gateway for the workstations receives packets for destination networks to which it cannot establish a connection itself. If the router cannot return the address of the appropriate router to the workstation via IMCP, it will forward the data to the corresponding router itself (see also 'Local Routing'). Since this setting increases network utilization in the LAN, the default setting is 'Off'.

### Setup/IP router module/Routing method

The router offers two methods for IP routing, which can be separately set for IP and ICMP packets. Both methods are based on the evaluation of the field 'Type-of-service' in the IP header.

The menu has the following layout:

/Routing-method	Routing method settings	
Routing-method		Routing method for IP packets
ICMP-routing-method		Routing method for ICMP packets

*Routing-method* This option allows you to define the routing method used for IP packets:




- If you select 'Normal', all IP packets are handled in the same way as per the routing specifications of the Internet protocol.
- If you select 'Type-of-service', IP packets are placed in the urgent queue or reliable queue, depending on the contents of the 'Type-of-service' field. All other packets are placed in the normal send queue. In this way, transmission is guaranteed, provided that it is possible.

*ICMP-routing-method* This option allows you to define the routing method used for ICMP packets:

- If you select 'Normal', the ICMP packets are handled like any other IP packets as per the routing specifications of the Internet protocol.
- If you select 'Reliable', all ICMP packets received are placed in the reliable queue.

**Setup/IP-router-module/RIP-configuration**

This option allows you to enter settings for the management of IP-RIP packets. The menu has the following layout:

/RIP-configuration	Settings for IP-RIP operation	
Type		RIP compatibility switch
R1-mask		Management of network masks
Table-RIP		Dynamic IP routing table

*RIP-type*

This option allows you to select the method to be used for handling the IP-RIP packets. The different settings have the following meaning:

- **Off:** IP-RIP is not supported (default).
- **RIP-1:** RIP-1 and RIP-2 packets are received but only RIP-1 packets are sent.
- **R1-comp:** RIP-1 and RIP-2 packets are received. RIP-2 packets are sent as an IP broadcast.
- **RIP-2:** Same as **R1-comp** except that all RIP packets are sent to the IP multicast address 224.0.0.9.

*R1-mask*

If **RIP-1** is set, this option allows you to influence the management of network masks. Therefore, these settings are required only for subnetting under **RIP-1**. The different settings have the following meaning:

- **Class** (default): The network mask used in the RIP packet is derived directly from the IP address class, i.e. the following network masks are used for the network classes:
  - Class A: 255.0.0.0
  - Class B: 255.255.0.0
  - Class C: 255.255.255.0
- **Address:** The network mask is derived from the first bit that is set in the IP address entered. This and all high-order bits within the network mask are set. Thus, for example, the address 127.128.128.64 yields the IP network mask 255.255.255.192.
- **Cl+Addr:** The network mask is formed from the IP address class and a part attached after the address procedure. Thus, the above-mentioned address and the network mask 255.255.0.0 yield the IP network mask 255.128.0.0.

*Table-RIP*

This option allows you to display the entries in the current dynamic IP routing table.

An IP-RIP routing table might, for example, have the following appearance:






IP-address	IP netmask	Time	Distance	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200



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

### Setup/IP-router-module/Masquerading

This menu allows you to enter settings for the masking function. The menu has the following layout:

/Masquerading	Settings for IP masquerading	
TCP-aging-second(s)		Time in seconds after which a TCP masking becomes invalid
UDP-aging-second(s)		Time in seconds after which a UDP masking becomes invalid
ICMP-aging-second(s)		Time in seconds after which an ICMP masking becomes invalid
Service-table		Static masquerading table
Table-masquerading		Dynamic masquerading table

#### Service-table

The use of inverse masquerading makes 'services' (e.g. a file server) selectively visible in the Internet by entering specified ports in the service table in the IP network, while all other services and computers remain invisible from the local network (see also 'IP Masquerading (NAT, PAT)'). The service table (also called the static masquerading table) can contain up to 16 entries and has the following layout:

D-port	Intranet addr.
20	10.1.1.10
21	10.1.1.10

The different columns have the following meaning:

- D-port: Destination port for the particular entry
- Intranet-addr.: Destination IP address for the computer in the local network

Through this assignment, it is possible, for example, to address the relevant service directly via telnet. Enter the IP address of the router and attach the port number, separated by a double point, to the address.

You can use the command

```
telnet 192.38.50.100:27
```

to connect directly to a news server that can be reached via a router with the IP address 192.38.50.100.

#### Table-masquerading

With IP masquerading, the IP addresses of computers in the local network are rendered invisible to external devices by means of a conversion of addresses and ports in the router. The dynamic masquerading table displays the IP addresses from the local

network that the router is currently masking. The dynamic masquerading table can contain up to 2048 entries and has the following layout:








Intranet addr.	S-port	Protocol	Time
10.1.1.10	1234	TCP	10

The different columns have the following meaning:

- Intranet-addr.: IP address of the computer in the local network
- S-port: Source port for this entry
- Protocol: Protocol used (TCP/UDP/ICMP)
- Timeout: Time in seconds until the entry is removed from the table

## Setup/SNMP-module

This menu allows you to enter settings for configuration of the device via SNMP. The menu has the following layout:

/SNMP-module	SNMP module settings	
Send-Traps		Switch for issuing SNMP traps
IP-Trap-Table		Table with 20 destination addresses for trap messages
Administrator		Device administrator
Location		Device location
Register-monitor		Command to set a destination address to which the traps are to be sent
Delete-monitor		Command to delete an address that was set with 'Register-monitor'
Monitor-table		Table with all currently active destination addresses that were set with 'Register-monitor'

*Send-Traps* This entry controls trap output (No/Yes).

*IP -Trap-Table* Enters the IP addresses to which the trap messages will be sent.

*Administrator* Administrator's name

*Location* Device location

You can also query the last two parameters via SNMP (MIB-2).

*Register-monitor* This command logs on applications with the router to retain targeted trap information. The *ELSA LANmonitor*, for example, queries the channel statistics in this way and converts them to a graphic display (under Windows).

In principle, any SNMP manager can use this command to obtain information from the router. The syntax

```
register-monitor IP-address:port mac address timeout
```

is used to direct the router to enter the given address in the monitor table and to send traps to it. If the traps are not received within the set hold time, the address will be automatically deleted from the table. A hold time of '0' permanently retains the entry in the table.

*Delete-monitor* This command removes the entries from the monitor table.










*Monitor-table* The monitor table has the following structure:

IP-address	Port	MAC-address	Timeout
10.0.0.53	1057	0080c76da46e	1

This entry indicates, for example, that an *ELSA LANmonitor* has logged on to the router.

## Setup/DHCP-server-module

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

/DHCP-server-module	DHCP server settings	
State		Switch for activating the DHCP module
Start-address-pool		Start address for the address pool
End-address-pool		End address for the address pool
Netmask		Network mask for the address pool
Broadcast-address		Broadcast address for the LAN
Gateway-address		Gateway-address for the LAN
Max.-lease-time-minute(s)		Maximum period of validity for the address assignment via DHCP
Default-lease-time-minute(s)		Default period of validity for the address assignment via DHCP
Table-DHCP		Table of current assignments via DHCP

*State* On: The device operates as a DHCP server

Off: The device does not operate as a DHCP server

Auto: The device regularly checks whether there is another DHCP server in the LAN. If not, it operates as a DHCP server and issues IP addresses to local clients.



*If there is no IP or Intranet address entered in the TCP/IP module (e.g. delivery status), the router will issue IP addresses from the address range 10.0.0.2 – 10.0.0.253 to all DHCP clients in auto mode.*

*Start-address-pool  
End-address-pool*

The IP address assigned is taken from the address pool selected ('Start-address-pool' to 'End-address-pool'). Any valid addresses in the local network can be entered here. If 0.0.0.0 is entered instead, the device will determine the appropriate addresses (start or end) from the settings under 'Setup/TCP module'. The procedure is as follows:

- If only the IP address or only the Intranet address is entered, the start or end of the pool is determined by means of the associated network mask.
- If both addresses have been specified, the Intranet address has priority for determining the pool.
- The start address of the pool is either the address given in the DHCP module or the first valid address in the local network.
- The end address of the pool is either the address given in the DHCP module or the last valid address in the local network.

A valid address is then taken from the pool for the IP address. If the computer was already assigned an IP address at some point in the past, it requests this same address and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

The DHCP server also checks whether the address that is to be assigned to the computer is unique in the local network. It does this by issuing an ARP request to the address. If the ARP request is answered, the DHCP server begins the procedure again with a new address. As soon as the uniqueness of an address has been established, the requesting computer is assigned the address found.

*Netmask*

The network mask is assigned in the same way as the address:

The system either assigns the network mask entered in the DHCP module or uses the network mask that belongs to the local network (determined during address assignment).

*Broadcast*

The broadcast mask is assigned in the same way as the address:

The system either assigns the broadcast address entered in the DHCP module or uses the broadcast address that belongs to the local network (determined during address assignment).

*Max.-lease-time-minute(s)*

Here you can enter the maximum period of validity that the DHCP server assigns a host. The DEFAULT value of 6000 minutes equals approximately 4 days.

*Default-lease-time-minute(s)*

Here you can enter the period of validity that is assigned if the host makes no request. The DEFAULT value of 500 minutes equals approximately 8 hours.

Table-DHCP








In the DHCP module, the 'Table-DHCP' option allows you to verify (or look up) the assignment of IP addresses to the relevant computers. This table has the following layout:




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

- IP-address: IP address assigned
- MAC-address: Computer's Ethernet address
- Timeout: Time remaining until the assignment becomes invalid
- Hostname: Computer's name in plain text if it was transmitted in the request
- Type: This field contains additional information on the assignment.  
The 'Type' field specifies how the address was assigned. This field can assume the following values:
  - **new**: The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.
  - **unkn.**: While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.
  - **stat.**: A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.
  - **dyn.**: The DHCP server assigned an address to the computer.

## Setup/NetBIOS

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

State		On or off
Scope-ID		NetBIOS scope in which the router is located.
NT-Domain		Workgroup/domain in which the router is located.
Remote-table		All remote stations with which NetBIOS information is to be exchanged must be entered in the remote-station table.
Group-list		All workgroups known to NetBIOS are recorded in the group list.
Host-list		All computer names known to NetBIOS are recorded in the host list.
Server-list		All servers that have logged onto the network are recorded in the server list.

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

*Scope-ID* The Scope-ID menu item can be used to specify the NetBIOS scope in which the device is located. It then sees only those NetBIOS packets originating in the same NetBIOS scope; all other packets are automatically rejected. The scope ID is only used in conjunction with Windows name servers (WINS). This entry can generally be left blank.

*NT-Domain* A workgroup/domain can be specified in the NT domain item to trigger the search procedure when starting the NetBIOS module. This is required if the network does not contain any computers running Windows 95 or Windows 98.

*Remote-table* All remote stations that are to provide or receive NetBIOS information must be entered in the remote table. When the NetBIOS module is switched on, NetBIOS packets from remote stations other than those specified will be rejected automatically. The remote-table has the following structure:

Name	Type
AACHEN	Router or workstation



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

*Type*

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

*Host table* The host table has the following structure:

Name	Type	IP-address	Remote-ID	Timeout	Flags
REMOTE	00	10.0.1.100	AACHEN	5000	xx20
WORKSTATION	00	10.0.0.10		5000	xx00

*Group table* The group table thus looks like this:

Group/Domain	Type	IP-address	Remote-ID	Timeout	Flags
WORKGROUP	1e	10.0.0.10		5000	xx00
WORKGROUP	1e	10.0.1.100	AACHEN	5000	xx20

The fields of the table have the following significance:

Name	Name of the host in the host table.
Group/Domain	Name of the group or domain in the group list. Groups and NT domains are handled in the same manner from the NetBIOS point of view.
Type	WINS type of the host. The type is not relevant for NetBIOS, but Microsoft Networks assign certain properties to the name on the basis of the type.
IP-address	IP address of the owner of the name. The same name can be assigned to multiple IP addresses in the group list.
Remote-ID	Name of the remote station for which the name became known.
Timeout	Time until the name is no longer valid. The timeout is also associated with an aging counter in the flags.
Flags	The flags contain additional information pertaining to the name.

### Flags

The flags have the following significance:

0X0003	This counter increments up each time the validity expires. The entry will be deleted if the name is not refreshed after the second expiration at the latest.
0X0004	This identifies an entry that still needs to be transferred.
0X0008	This identifies an entry that is queued for deletion, i.e. the name has not yet been refreshed after the establishment of a connection.
0X0010	Reserved
0X0020	This identifies a remote station.
0X0040	Reserved
0X0080	Reserved

The server list has the following structure:

Host	Group/ Domain	UPD	IP- address	OS- Ver	SMB- Ver	Server- type	Remote- ID	Timeout	Flags
REMOTE	WORKGROUP	00	10.0.1.100	0400	010F	0004140B	AACHEN	13	0020
WORKSTATION	WORKGROUP	07	10.0.0.10	0400	0415	00452003		31	0000

Unlike the host and group lists, this table fills gradually, as the NetBIOS module depends on messages from the servers themselves.










The individual fields have the following significance:

Host	Name of the server
Group/Domain	Workgroup or domain in which the server is located.
UPD	Update counter: indicates the number of times that the server has already propagated itself
IP-address	Address of the server

OS-Ver	Operating system version number
SMB-Ver	Version number of the SMB protocol used
Server-type	Bit mask in which the services of the server are coded
Remote-ID	Name of the remote station from which the server was announced
Timeout	Time until the entry loses its validity (for entries from the LAN) or time until the router propagates a remote entry.
Flags	Corresponds to the flags in the host or group tables.

## Setup/Config-module

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

/Config-module		Configuration module settings
LAN-config		Switch for configuring from the LAN side
WAN-config		Switch for configuring from the WAN side
Password-required		Password required on/off if there is no password
Maximum-connections		Maximum number of simultaneous connections
Farconfig-(EAZ-MSN)		Subscriber number for remote configuration via PPP
Config-aging-minute(s)		Time limit for remote configuration connections
Login-errors		Number for failed log-in attempts before the log-in block is activated
Lock-minutes		Duration of block and period until old log-in errors are forgotten.
Language		Configuration language

*LAN-config* This option allows you to define whether remote configuration from the LAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **On**.

*WAN-config* This option allows you to define whether remote configuration from the WAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **Off**.

*Password-required* This specifies whether a new password should be requested every time a remote configuration is begun (**On**), or the password request should be suppressed (**Off**). The default setting for this option is **Off**.

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

*Config-aging-minute(s)* If data transmission halts during a remote configuration session, e.g. because the user is no longer entering data, the device automatically releases the connection at the end of



the time period specified here. Possible settings are from 1 to 99 minutes; The default setting is 15 minutes.

#### Login-errors

This entry specifies the number of failed attempts allowed before the log-in block is activated. An empty password (simply pressing <ENTER> at the password prompt) is not considered an attempt and therefore does not activate the block.



*The default value is 5. A lower value may cause the log-in block to be activated with only one access on an older ELSA LANconfig! In this case obtain an updated ELSA LANconfig version over our online media.*

#### Lock-minutes

This entry has two meanings. It indicates how long the access is blocked if the log-in block has been activated. It also sets the period after which the device forgets all prior login errors.

#### Language





This option allows you to select whether you will use the German or English version of the software for performing the configuration.

## Setup/LANCAPI-module

Configuring *LANCAPI* basically involves answering two questions:

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

The *LANCAPI* module has the following layout:

/LANCAPI-module	LANCAPI settings	
Access-list		List of computers allowed to use the <i>LANCAPI</i>
LANCAPI-UDP-port		UDP port for communication between the <i>LANCAPI</i> server and clients
EAZ-MSN(s)		EAZ or MSN to which the <i>LANCAPI</i> should respond
Prio-out		Priority for the <i>LANCAPI</i> versus router connections







- **Operating:** 'on', 'off' or 'outgoing'. Under the last setting the *LANCAPI* will not accept incoming calls.
- **Access-list:** This option allows you to limit the circle of computers permitted to use the *LANCAPI*. This table can have a maximum of 16 entries. If the table is empty, all computers can access the *LANCAPI*.
- **LANCAPI-UDP-port:** In the default configuration, this option is set to '75'. Change this setting only if other devices in your network are already using this port.







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

- **EAZ/MSN(s)**: This option allows you to enter the call numbers to which the *LANCAPi* is to respond. If you wish to enter more than one number, place a semicolon between the individual numbers.
- **Prio-out**: The priority for a port controls the option for breaking outgoing connections via the *LANCAPi* router connections. Option '1' does not break router connections, the setting '2' breaks only auxiliary connections of a router connection with channel bundling, the selection '3' also breaks main channels of a router connection.

## Setup/WLAN-module

the WLAN module is configured using this menu:

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





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

## Setup/LCR-module

Enter the following information when setting the least-cost router:

- For which modules in the device should the LCR functions be active?
- Which area codes should be diverted when via which call-by-call provider?

The LCR module has the following layout:

/LCR module	Least-cost router settings	
Router-usage		Activate LCR for the router modules, <b>On</b> or <b>Off</b>
Lancapi-usage		Activate LCR for the <i>LANCAPI</i> , <b>On</b> or <b>Off</b>
Timetable		Call forwarding table
Celebration-day-table		List of holidays affecting the timetable.

### Timetable

The table has 256 entries and the following structure:

Index	Prefix	Days	Start	Stop	Number-list	Fallback
1	0171	192	0:00	23:59	01013;01070	On

The individual entries have the following meaning:

Index	Continuing index of entries in the table.
Prefix	Area code to be diverted.
Days	Validity of the entry for week days and holidays shown in an 8-bit mask: Bit 0 represents Monday, bit 7 holidays. The entry '31' therefore designates all business days, '192' Sundays and holidays.
Start	Beginning time for the validity of the entry on the defined days.

Stop	Termination time for the validity of the entry on the defined days.
Number-list	Network identification number of the call-by-call providers.
Fallback	Automatic fallback to your own telephone company if all call-by-call numbers are busy.

For example:

`set 1 02 31 1:00 11:59 01030;01090;01070` On diverts all long-distance calls to region '02' between one and twelve o'clock to the provider with the network identification number '01030'. If this number is busy, the network identification numbers '01090' and '01070' will be attempted. If they are also not available, the connection will be made via the normal telephone company.

*Celebration-day-table*

The celebration-day-table has 256 entries and the following structure:





Index	Date
1	01010000
2	01050000
3	03100000
4	25120000
5	26120000
6	02041999
7	13051999




The individual entries have the following meaning:

Index	Continuing index of entries in the table.
Date	Dates of holidays. Enter the index and the date in full without separators, e.g. 'set 8 13041999' for April 13, 1999 as the eighth entry in the list. Enter '0000' as the year for annually occurring holidays.

## Setup/DNS module

The settings for the DNS server can be modified here as required. The menu contains the following items (incl. their default settings):

State		On (default) or off
Domain		Own domain, optional, 32 characters max.
DHCP-usage		Yes (default) or no
NetBIOS-usage		Yes (default) or no

DNS-table		Static DNS table for the manual association of IP addresses to names, 64 entries
Filter-list		Filter list for the exclusion of prohibited domains, 64 entries
Leasetime		Specifies the name validity information to be given to a requesting computer. Default: 2000

*DNS-table*

The DNS table contains a simple association of local names to IP addresses. The table is sorted alphabetically by names.

The table is restricted to 64 entries, as large networks are configured more effectively using the DHCP server, which can also be used to handle name requests. The table has the following layout:

Hostname	IP-address
Host10	10.0.0.10

The name is restricted to a maximum of 32 characters. Longer names are not necessarily practical in a local network.

*Filter-list*

The filter list contains the entries for prohibited domains. In addition, it is possible to specify for whom a given domain will be prohibited. This is set using an IP address/netmask pair. An IP address of 0.0.0.0 prohibits this domain for all computers. A subnet mask of 0.0.0.0 prohibits the domain for all networks. The table has the following layout:

Name	Domain	IP-address	Netmask
F001	*xxx*	0.0.0.0	0.0.0.0

Clear IDs can be freely selected and assigned to the filters in the 'Idx.' field.

Enter the name of the domain to be prohibited in the 'Domain' field. Wildcards such as '?' and '\*' may be used. The wildcard '?' replaces exactly one character, while '\*' can stand for a random number of characters. Multiple instances of the wildcard '\*' can be used. For example, \*xxx\* filters all names containing the letters xxx in any position within the name.

The IP address and subnet mask fields can be used to specify the subnet for which the domain will be prohibited.

The filter table is sorted according to the subnet masks in descending order (the longest at the top); entries with identical subnet masks are sorted according to the IP addresses in ascending order. In the event of identical IP addresses, the entries are sorted in ascending order according to the domain to be prohibited.

The table is searched from top to bottom and an error message is returned to the requesting computer in the event of a match.





## Setup/Time-module

The least-cost router in the device requires correct time information to calculate the call number diversions via call-by-call provider. Precise time information is also desirable for some statistics.

The time may be set manually (with the 'time' command) or automatically read from the ISDN network.







For automatic time comparison when the module is switched on, a previously specified remote station is called directly and the time information is taken from the ISDN network. So long as the time module is switched on, the time will be taken from the ISDN every time the router establishes a connection.

The time module has the following layout:

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

## Firmware

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

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

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

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

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

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

Enter the following command to activate an inactive firmware version:

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





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

- 'immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
  - The new firmware is successfully loaded and then operates as desired. Everything is then in order.
  - However, if the new firmware does not operate correctly, it may not be possible to communicate with the device after the restart. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- 'login': To prevent problems caused by defective firmware, the second option will load the firmware and start it immediately.
  - In contrast to the first option, the firmsafe will wait until it has successfully logged on over outband or inband (by telnet). The new firmware will only be permanently activated when the login occurs successfully within the time set under 'Timeout firmsafe'.
  - If the device no longer responds and it is therefore impossible to log in, the firmware automatically loads the previous firmware version and reboots the device with it.
- 'manual': The third option allows you to set a period (Timeout firmsafe) beforehand for testing the new firmware. The device will start with the new firmware and wait

for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective.

## Other

The **Other** menu allows you to manage the following functions:

/Other	Various functions	
Manual-dialing		Connection testing
Boot-system		Boots the device.
Reset-system		Resets to factory settings.
System-upload		Loads new firmware.

### Other/Manual Dialing

Select this option when you wish to establish a connection manually for testing purposes.

*Boot-system*

This option allows you to reboot the device.



*Before executing the command all open connections (ISDN or TCP) will be released or closed.*

*Reset-system*

This option resets all the settings that have been entered. The device is reset to the delivery version.

For safety's sake, the system asks you to enter the configuration protection password in order to ensure that you have not mistakenly selected this command instead of the `Boot-system` command. If no password has been assigned, you must press Enter a second time.

*Upload-system*

This option starts a firmware upload (refer to chapter 'How to set up new software').

The flash ROM technology permits flexible and service-friendly handling of the system software by allowing different firmware versions to be read in. It also allows devices can be retrofitted for all future options.



# Ports and protocols

## Ports

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

Capab.	Port no.	Protocol
www	80	tcp
www	80	udp
link	87	tcp
supdup	95	tcp
hostnames	101	tcp
iso-tsap	102	tcp
dictionary	103	tcp
X400	103	tcp
x400-snd	104	tcp
csnet-ns	105	tcp
pop	109	tcp
pop2	109	tcp
pop3	110	tcp
portmap	111	tcp
portmap	111	udp
sunrpc	111	tcp
sunrpc	111	udp
auth	113	tcp
sftp	115	tcp
path	117	tcp
uucp-path	117	tcp
nnntp	119	tcp
ntp	123	udp
nbname	137	udp
nbdatagram	138	udp
nbssession	139	tcp
NeWS	144	tcp
sgmp	153	udp
tcprepo	158	tcp
snmp	161	udp
snmp-trap	162	udp
print-srv	170	tcp
vmnet	175	tcp
load	315	udp
vmnet0	400	tcp
sytek	500	udp
biff	512	udp

Capab.	Port no.	Protocol
exec	512	tcp
login	513	tcp
who	513	udp
shell	514	tcp
syslog	514	udp
printer	515	tcp
talk	517	udp
ntalk	518	udp
efs	520	tcp
route	520	udp
timed	525	udp
tempo	526	tcp
courier	530	tcp
conference	531	tcp
rxd-control	531	udp
netnews	532	tcp
netwall	533	udp
uucp	540	tcp
klogin	543	tcp
kshell	544	tcp
new-rwho	550	udp
remotefs	556	tcp
rmonitor	560	udp
monitor	561	udp
garcon	600	tcp
mairtd	601	tcp
busboy	602	tcp
acctmaster	700	udp
acctslave	701	udp
acct	702	udp
acctlogin	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctslave2	706	udp
acctdisk	707	udp
kerberos	750	tcp

Capab.	Port no.	Protocol
kerberos	750	udp
kerberos_master	751	tcp
kerberos_master	751	udp
passwd_server	752	udp
userreg_server	753	udp
krb_prop	754	tcp
erlogin	888	tcp
kpop	1109	tcp
phone	1167	udp
ingreslock	1524	tcp
maze	1666	udp
nfs	2049	udp
knetd	2053	tcp
eklogin	2105	tcp
rmt	5555	tcp
mtb	5556	tcp
man	9535	tcp
w	9536	tcp
mantst	9537	tcp
bnews	10000	tcp
rscs0	10000	udp
queue	10001	tcp
rscs1	10001	udp
poker	10002	tcp
rscs2	10002	udp
gateway	10003	tcp
rscs3	10003	udp
remp	10004	tcp
rscs4	10004	udp
rscs5	10005	udp
rscs6	10006	udp
rscs7	10007	udp
rscs8	10008	udp
rscs9	10009	udp
rscsa	10010	udp
rscsb	10011	udp
qmaster	10012	tcp

## Protocols

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

