

LANCOM™ Office

© 2000 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 sont interdites sans l'autorisation écrite d'ELSA. ELSA se réserve le droit d'effectuer des modifications à des fins d'améliorations techniques.

ELSA est certifié DIN-EN-ISO-9001. L'Office de Contrôle Technique allemand (TÜV-CERT), accrédité à délivrer les certificats, atteste par le document du 15/6/1998 la conformité à la norme DIN EN ISO 9001, qui est reconnue dans le monde entier. Le numéro de certificat délivré à ELSA est le 09 100 5069.

Vous trouverez en annexe de cette documentation toutes les déclarations et documents concernant l'homologation des produits pour autant qu'elles étaient disponibles le jour de l'impression.

Marques

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

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

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

Aix-la-Chapelle, avril 2000

20588/0300

Avant-propos

Merci de votre confiance !

En acquérant *ELSA LANCOM Office* vous avez porté votre choix sur un routeur qui permet à des réseaux locaux ou différentes stations de travail d'accéder à Internet via une connexion RNIS.

Modèles

Cette documentation décrit différents modèles de la série *ELSA LANCOM Office* qui se différencient par leur équipement matériel et logiciel :

- *ELSA LANCOM 800 Office*
- *ELSA LANCOM 1000 Office*
- *ELSA LANCOM 1100 Office*
- *ELSA LANCOM 2000 Office*

*Restrictions
selon les modèles*

Les parties de la documentation qui ne se rapportent qu'à une partie des modèles sont repérés soit dans le texte même soit à côté du texte.

Documentation

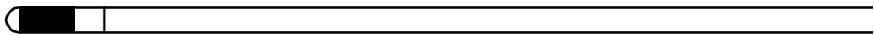
La documentation jointe comprend :

- Manuel de l'utilisateur
Installation du matériel, description des fonctions et modes de service, exemples de configuration.
- Documentation électronique sur CD
Bases techniques (p.ex. pour la technique de réseau, TCP/IP etc.), 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, notre serveur Internet - www.elsa.com est 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, lancez le fichier Misc\Support\MISC\ELASIDE\index.htm.

FR

Contenu

1 Introduction	11
1.1 Champs d'application du routeur	11
1.2 Avantages d'un routeur <i>ELSA LANCOM Office</i>	13
2 Installation	21
2.1 Contenu de l'emballage	21
2.2 Configuration système requise	21
2.3 Installer la station de travail	22
2.3.1 Windows 95 et Windows 98	22
2.3.2 Windows NT 4.0	23
2.4 <i>ELSA LANCOM Office</i> se présente	25
2.4.1 La face avant de l'appareil	25
2.4.2 La face arrière de l'appareil	28
2.5 Pour raccorder l'appareil	29
2.5.1 Installation du logiciel	30
2.6 Configuration	30
2.6.1 Réglages de base	31
2.6.2 Configurer un accès Internet	37
3 Configurations possibles	39
3.1 De nombreux chemins mènent au <i>ELSA LANCOM</i>	39
3.2 La voie directe : Outband	40
3.2.1 Conditions pour la configuration Outband	40
3.2.2 Configuration outband avec <i>ELSA LANconfig</i>	40
3.2.3 Configuration Outband avec programme de terminal	41
3.3 La voie confortable : Inband	41
3.3.1 Conditions	41
3.3.2 Alternative : gestion des adresses à l'aide du serveur DHCP	41
3.3.3 Configuration par <i>ELSA LANconfig</i>	42
3.3.4 Configuration par Telnet	43
3.4 L'accès à distance : Configuration par Accès réseau à distance	43
3.4.1 Ce dont vous avez besoin pour la configuration à distance	43
3.4.2 Préparation de la configuration à distance	44
3.4.3 La première connexion à distance par Accès réseau à distance (<i>ELSA LANconfig</i>)	44
3.4.4 La première connexion à distance avec un client PPP et Telnet	44
3.4.5 Restriction de la configuration à distance	45

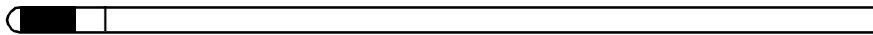
3.5 Nouveau microprogramme avec FirmSafe	47
3.5.1 Comment fonctionne FirmSafe ?	47
3.5.2 Comment charger le nouveau logiciel ?	48
3.6 Supervision de la ligne ?	50
3.6.1 <i>ELSA LANmonitor</i>	51
3.7 Éditions des tracés	53
3.8 Configuration par SNMP	56

4 Fonctions et modes d'exploitation	57
4.1 La sécurité de votre configuration	57
4.1.1 Protection par mot de passe	58
4.1.2 Le verrouillage des accès	58
4.1.3 Contrôle des accès via TCP/IP	59
4.2 La sécurité de votre LAN	59
4.2.1 Le contrôle	59
4.2.2 Le rappel	61
4.2.3 La cachette – masquering IP (NAT, PAT)	62
4.3 Gestion des unités de taxation	62
4.3.1 Limitation des communications RNIS en fonction des unités de taxation. . .	63
4.3.2 Limitation des communications RNIS en fonction de la durée	63
4.3.3 Configuration dans le gestionnaire des coûts	64
4.4 Connexions RNIS	65
4.4.1 Liste RNIS des noms	67
4.4.2 Configuration des interfaces	68
4.4.3 Configuration des Interfaces du routeur	69
4.4.4 Configuration de l'interface <i>LANCAPI</i>	69
4.4.5 Couche communication	70
4.4.6 Liste round-robin	71
4.4.7 Liste des scripts	72
4.4.8 Prise d'appel	72
4.4.9 Liste des numéros	73
4.5 Gestion d'adresses automatique via DHCP	73
4.5.1 Le serveur DHCP	74
4.5.2 DHCP – 'Actif', 'Inactif' ou 'Auto' ?	74
4.5.3 Attribution des adresses	75
4.5.4 Configuration du serveur DHCP	79
4.6 DNS	81
4.6.1 Que fait un serveur DNS ?	82
4.6.2 Configurer le serveur DNS	83
4.7 Proxy NetBIOS	86

4.7.1 En quelques mots : définition de NetBIOS	86
4.7.2 Traitement des paquets NetBIOS	87
4.7.3 Quelles conditions doivent être satisfaites ?	88
4.7.4 Interconnecter deux réseaux Windows	92
4.7.5 Accès par les ordinateurs distants	94
4.7.6 Qui cherche trouve : le Voisinage réseau	94
4.8 Le rerouteur téléphonique (least-cost router)	96
4.9 <i>ELSA CAPI Faxmodem</i>	102
4.9.1 Installation	103
4.9.2 Transmettre des télécopies via <i>ELSA CAPI Faxmodem</i>	103
4.10 Bureautique et <i>ELSA LANCAPI</i>	103
4.10.1 <i>ELSA LANCAPI</i>	103
4.11 La régie téléphonique intégrée	108
4.11.1 Raccordement des terminaux analogiques	109
4.11.2 Configuration avec <i>ELSA LANconfig</i> et les assistants d'installation	109
4.11.3 Configuration manuelle avec <i>ELSA LANconfig</i>	111
4.11.4 Utilisation de la régie téléphonique avec le téléphone	121
4.12 Comptabilisation	129
4.12.1 Configuration de la comptabilisation	130
4.12.2 Lecture des informations de comptabilisation	131
5 Annexe	133
5.1 Caractéristiques techniques	133
5.2 Déclarations de conformité	135
5.3 Conditions générales de garantie	138
● Index	141
● Technical basics (seulement sur CD)	R-1
Network technology	R-1
The network and its components	R-1
Connection modes	R-2
Kinds of networks	R-3
IP addressing	R-3
IP routing and hierarchical IP addressing	R-6
Expansion through local networks	R-8
Point-to-point protocol	R-12
The protocol	R-13
The PPP list	R-14
Everything ok? Checking the line with LCP	R-15

Assigning IP addresses via PPP	R-16
Callback functions	R-17
Fast ELSA callback	R-20
Callback as specified in RFC 1570 (PPP LCP extensions)	R-20
Channel bundling with MLPPP	R-21
IPX routing	R-22
Naming IPX addresses	R-23
Information about the LAN	R-23
IPX routing table	R-23
What happens when data is transmitted on an IPX network?	R-24
RIP and SAP tables	R-25
So many routers around here.....	R-25
Redundant routes	R-25
Exponential backoff	R-26
IPX packet filters	R-26
IP routing	R-28
The IP routing table	R-28
TCP/IP packet filters	R-31
Proxy-ARP	R-32
Local routing	R-32
Dynamic routing with IP RIP	R-33
IP masquerading (NAT, PAT)	R-35
DNS forwarding	R-37
Policy Based Routing	R-38
Bridging	R-38
● Description of the menu options (seulement sur CD)	R-41
Status	R-43
Display and keyboard	R-44
Status/Connection	R-45
Status/Current-time	R-45
Status/Operating-time	R-45
Status/WAN-statistics	R-46
Status/LAN-statistics	R-48
Status/PPP-statistics	R-49
Status/IPX-statistics	R-57
Status/TCP-IP-statistics	R-62
Status/IP-router-statistics	R-68
Status/Config-statistics	R-70
Status/Queue-statistics	R-70

Status/Connection-statistics	R-71
Status/Info-connection	R-72
Status/Layer-connection	R-73
Status/Call-info-table	R-73
Status/Remote-statistics	R-74
Status/SO-bus	R-75
Status/Channel-statistics	R-75
Status/Time-statistics	R-76
Status/LCR-statistics	R-77
Status/Delete-values	R-77
Setup	R-77
Setup/WAN-module	R-78
Setup/LAN-module	R-88
Setup/IPX-module	R-89
Setup/TCP-IP-module	R-97
Setup/IP-router-module	R-101
Setup/SNMP-module	R-109
Setup/DHCP-module	R-110
Setup/NetBIOS-module	R-112
Setup/Config-module	R-114
Setup/LANCAPI-module	R-116
Setup/LCR-module	R-117
Setup/DNS-module	R-118
Setup/Time-module	R-119
Firmware	R-120
Other	R-122



FR

1 Introduction

Quand il est question de mettre en place une infrastructure à l'échelle de l'entreprise, on rencontre de plus en plus les routeurs RNIS au premier plan des solutions choisies. Grâce à ses vitesses de transmission élevées le réseau RNIS offre la base économiquement la plus attrayante pour surmonter les distances dans un réseau étendu. Des réseaux locaux (LAN) développés à différents endroits et des ordinateurs isolés peuvent être reliés à moindre prix avec les routeurs. Les filiales et les agences peuvent être intégrées de façon transparente au réseau de l'entreprise mère via RNIS et disposent des mêmes banques de données qu'elle.

Ce chapitre présente sommairement l'appareil et ses fonctions. Vous trouverez dans les chapitres suivants une description détaillée des fonctions, du logiciel et de son utilisation ainsi qu'une introduction aux principes techniques de base.

1.1 Champs d'application du routeur

Avec un routeur, les réseaux locaux et les PC distants peuvent être reliés entre eux ; ils formeront alors un réseau étendu WAN (Wide Area Network). Chaque ordinateur dans ce réseau étendu peut alors accéder, suivant ses droits d'accès, aux ordinateurs et aux services dans tout le réseau. Le rôle du routeur est de trouver un chemin via lequel les ordinateurs peuvent échanger leurs données.

Ce chemin se présente sous forme d'une connexion RNIS.

Une forme particulièrement répandue de connexion par réseau est l'accès à l'Internet. Quand le réseau local d'une entreprise est relié au réseau d'un fournisseur d'accès Internet, tous les ordinateurs dans le réseau local pourront accéder aux pages et aux services du World Wide Web.

Via les connexions RNIS des liaisons réseau (IP, IPX) ou des services d'accès distant peuvent être fournis aux agents extérieurs.

Mais les routeurs sont encore plus performants. Grâce à une interface spéciale, *ELSA LANCAPI*, les fonctions modernes de la bureautique comme le Fax ou EuroFileTransfer (télédisquette) sont proposées dans l'ensemble du réseau local. Les logiciels de communication employés transmettent dans ce cas les données à l'interface *LANCAPI*, puis au routeur qui se charge ensuite de les envoyer. Il n'est donc pas nécessaire d'équiper chaque poste de travail avec un terminal RNIS onéreux nécessitant une maintenance intense.

Au besoin, il établit la liaison avec le correspondant via la ligne RNIS. Si l'entreprise a loué une ligne spécialisée avec liaison permanente, la durée d'établissement de connexion disparaît.

Concrètement, quand avez-vous besoin du routeur ?

En fait, chaque fois qu'il s'agit d'interconnecter des ordinateurs et lorsqu'un simple modem ne suffit plus. Ces cas se présentent par ex. pour les applications suivantes :

- Internet dans le réseau local

Dans de nombreuses entreprises, la possibilité d'accéder à l'Internet depuis chaque poste de travail du réseau est un besoin qui se fait ressentir de plus en plus fortement. La recherche en ligne, le transfert de fichiers et l'échange de courrier électronique (e-mail) sont quelques exemples d'application destinées à faciliter le travail des utilisateurs.

Un routeur relie tous les postes de travail dans votre réseau local avec l'Internet. Les fonctions de sécurité telles que le masquage IP permettent non seulement d'économiser des coûts, mais protègent votre réseau contre les accès de l'extérieur.

- Interconnexion de réseaux locaux

Quand les affaires marchent, il est éventuellement temps de créer une filiale ou une agence. La filiale a évidemment son propre réseau et aimerait toujours être au courant.

L'interconnexion de réseaux locaux, donc un couplage LAN-LAN regroupe les réseaux pour en faire un seul, éventuellement même sur un autre continent. Dans le cas de liaisons commutées, une gestion intelligente des lignes et des mécanismes de filtrage sophistiqués se chargent de réduire les coûts de communication. Naturellement, les lignes spécialisées peuvent coexister avec les liaisons commutées.

- Télétravail avec un accès à distance

Les tâches de nombreux salariés dans les entreprises modernes sont de moins en moins liées à un endroit précis – la matière brute étant l'information, et le point essentiel étant l'accès permanent aux informations communes.

Dans ce contexte, le mot magique est « accès à distance ». Le télétravail pour les salariés travaillant à domicile, dans leur home office, ou l'accès aux données de l'entreprise pour les agents en déplacement est possible via le routeur se trouvant dans le réseau local de la centrale. Même dans le cas de l'accès à distance, un routeur *ELSA LANCOM* fait naturellement

tout pour protéger les données internes de l'entreprise : la fonction de rappel automatique des utilisateurs et des numéros d'appel enregistrés sert à donner le sésame-ouvre-toi uniquement à des personnes triées sur le volet. En plus, les coûts de communication sont alors saisis centralement pour faciliter la facturation.

- Bureautique avec *LANCAPI*

Télécopier directement depuis une application, utiliser le répondeur téléphonique avec des messages d'accueil variant suivant l'heure, effectuer les transactions bancaires, le tout sans quitter le bureau : toutes ces fonctions sont possibles avec l'interface *LANCAPI*.

LANCAPI est une variante spéciale de l'interface CAPI-2.0 via laquelle divers logiciels de communication tels que *ELSA-RVS-COM* ou *ELSA-ZOC* peuvent accéder au routeur.

- Téléphonie

En plus de ses propriétés de routeur RNIS, *ELSA LANCOM 2000 Office* intègre un mini-standard avec quatre accès analogiques (ports A/N). Ces ports permettent de raccorder au routeur des appareils de télécommunication analogiques tels qu'un téléphone ou un télécopieur. Il n'est donc pas nécessaire d'acheter des nouveaux appareils RNIS quand on migre de l'ancien RTC vers RNIS/Numéris.

Pour tous ces appareils branchés sur les ports A/N, un routeur *ELSA LANCOM* offre de nombreuses fonctions confortables telles que le transfert d'appel, les appels internes, le va-et-vient, la consultation d'un collègue, le renvoi d'appel, l'affichage du coût de la communication, etc.

1.2 Avantages d'un routeur *ELSA LANCOM Office*

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 routeurs RNIS d'ELSA fonctionnent dans des réseaux Ethernet :

- Vous connectez *ELSA LANCOM 1000 Office* ou *ELSA LANCOM 2000 Office* avec le réseau 10 Mbps via les connecteurs 10Base-2 ou 10Base-T.
- Un *ELSA LANCOM 800 Office* trouve la voie d'accès au réseau locale 10 Mbps via le connecteur 10Base-T.
- Un *ELSA LANCOM 1000 Office* est raccordé à un réseau (Fast) Ethernet via le connecteur 10/100Base-T.

Connexion à un réseau étendu WAN

Le *ELSA LANCOM Office* est relié à (aux) l'interface(s) S_0 d'un accès RNIS en configuration point-à-multipoint ou en configuration point-à-point (connecteur multiple) Configuration point-à-point (connecteur mini-standard). 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).

L'option payante de liaison permanente doit être activée séparément.

Configuration

Le réglage et l'adaptation des périphériques sur leur tâche spécifique s'effectue rapidement et confortablement à l'aide de l'outil de configuration pour Windows joint *ELSA LANconfig*. Les utilisateurs d'autres systèmes d'exploitation utilisent la configuration basée sur le HTML via un navigateur Web, telnet ou un émulateur de terminal quelconque.

L'accès au périphérique peut se faire depuis le réseau étendu WAN, le réseau local LAN ou directement via l'interface de configuration. Dans les deux premiers cas, la configuration peut se faire avec TFTP et SNMP.

Les assistants intégrés d'installation de *ELSA LANconfig* et de configuration HTML vous aident à mettre les appareils en service avec quelques manipulations simples.

Mise à jour des microprogrammes

Afin de rester à jour question logiciels, ces périphériques sont équipés d'une mémoire flash. 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, via le réseau étendu ou via l'interface de configuration.

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.

Protection de l'accès

Pour la protection contre les accès illicites au réseau de l'entreprise, le routeur dispose en plus de la protection par mot de passe et de l'identification du numéro de l'appelant (CLIP) une fonction de rappel qui permet d'établir la liaison seulement avec des numéros d'appel RNIS déterminés au préalable. Mécanismes d'authentification dans le PPP, filtre coupe-feu et masquage IP 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.

Contrôle des coûts de communication

Lorsque les « informations de taxation sont communiquées pendant la transmission » dans le réseau RNIS (selon AOCD), vous pouvez déterminer les unités de communication disponibles pour l'accès RNIS pendant une période. Vous pouvez donc garder le contrôle de votre facture de téléphone.

Si les informations de taxation ne sont pas transmises à votre accès RNIS, vous avez cependant aussi la possibilité de restreindre la durée de la connexion active RNIS pour un laps de temps déterminé. Une fois cette durée écoulée, le routeur ne permet plus aucun établissement actif de communication.

Least Cost Routing = rerouteur téléphonique

Même si le nombre d'opérateurs offrant les services de télécommunication est important, le rerouteur téléphonique permet d'obtenir toujours les lignes RNIS les plus avantageuses.

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* ou les ports A/N) 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. Il est naturellement possible de régler l'heure manuellement.

Regroupement des canaux et compression

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

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 pour chaque canal de transmission
- Nom du correspondant en ligne
- Quel module de l'appareil est raccordé (routeur, *LANCAPI*, port a/b)
- 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.

Affichage de l'état

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

Statistiques

Grâce aux nombreuses fonctions de statistique, vous avez le routeur *ELSA LANCOM Office* dans votre poche. Vous trouverez ici p.ex. toutes les informations concernant les paquets de données transmis et pourrez ainsi optimiser la configuration de votre appareil.

DHCP

Les routeurs 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.

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 DNS 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.

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.

Avec *ELSA CAPI Faxmodem*, en plus 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 Office*.

Uniquement ELSA
LANCOM 2000
Office

Le mini-standard intégré

Un *ELSA LANCOM 2000 Office* a encore plus de fonctions. Quatre ports A/N intégrés permettent de raccorder à ce routeur des téléphones analogiques, des télécopieurs analogiques ou de modems.

Les ports A/N sont intéressants surtout pour ceux qui migrent du RTC classique vers le RNIS. Ils permettent de continuer d'utiliser les équipements analogiques tels que les téléphones ou les télécopieurs. On n'a donc pas besoin d'acheter les nouveaux appareils numériques. Par ailleurs le mini-standard du *ELSA LANCOM 2000 Office* des fonctions RNIS supplémentaires comme le renvoi d'appel, le double appel, le va-et-vient, la mise en attente et la conférence à trois, les appels internes, la numérotation directe, l'affichage des unités de taxation et bien d'autres encore.

Etablissement et gestion des liaisons

Dans un réseau, le routeur contrôle toutes les données et vérifie si elles doivent être envoyées dans un autre réseau ou non. Lorsque les données doivent être transmises, le routeur établit la liaison automatiquement et la termine à la fin de la transmission. Les unités de communication commencées sont exploitées jusqu'à la fin si les informations de facturation sont transmises également pendant la transmission de données.

Afin de réduire les coûts de communication, le routeur dispose de plusieurs filtres suivant le mode d'exploitation actif. Ceci permet d'exclure de la transmission les données d'un réseau entier ou de parties d'un réseau. De même, les données faisant partie de certains services (par exemple les services d'impression) peuvent être filtrées.

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.

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 s'occuper de leur paramétrage est la configuration à distance via les accès RNIS et l'accès réseau à distance de Windows. Pour cela, 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.

Comptabilisation

La plus grande partie des transmissions de données via les routeurs de ELSA se font soit par des connexions établies par commutation pour lesquelles les coûts de taxation du temps en ligne sont calculés ou par des liaisons directes pour lesquelles les coûts de taxation sont calculés d'après le volume de données. Seule une petite partie des utilisateurs utilise de véritables liaisons permanentes avec taxation forfaitaire.

Pour nombre d'utilisateurs il est donc important de savoir quelques ordinateurs dans le propre réseau local utilisent le plus les voies de connexion des routeurs et quels coûts en résultent.

Avec la fonction comptabilisation *ELSA LANCOM Office* offre la possibilité de détailler les temps en ligne et les volumes de données pour chaque

ordinateur ayant participé aux liaisons. On peut ainsi détecter rapidement les mauvaises configurations des ordinateurs ou des routeurs et les coûts peuvent être attribués à ceux qui sont à leur origine.

2 Installation

Ce chapitre a pour but de vous aider à établir le plus tôt possible une liaison avec Internet. Voyez tout d'abord le contenu de la livraison et faites connaissance avec votre appareil. Ensuite nous vous montrons comment vous pouvez brancher et mettre l'appareil en service.

Les informations suivantes s'adressent à des utilisateurs expérimentés qui ont des connaissances sur la configuration matériel et réseau.

FR

2.1 Contenu de l'emballage

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

- *ELSA LANCOM Office*
- Bloc transfo.
- Câble de raccordement au réseau local
- Câble de raccordement RNIS
- Câble pour l'interface de configuration (seulement *ELSA LANCOM 1000 Office*, *ELSA LANCOM 2000 Office* et *ELSA LANCOM 1100 Office*)
- Adaptateur pour le câble de configuration (seulement *ELSA LANCOM 1000 Office*, *ELSA LANCOM 2000 Office* et *ELSA LANCOM 1100 Office*)
- 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.

2.2 Configuration système requise

Les ordinateurs que vous voulez raccorder à Internet à l'aide du périphérique doivent remplir les conditions suivantes :

- Système d'exploitation de votre choix prenant en charge le protocole réseau TCP/IP, p.ex. Windows 95, Windows 98, Windows 2000, Windows NT 4.0, OS/2, Linux ou BeOS
- Windows 95, Windows 98, Windows 2000 ou Windows NT 4.0 et un lecteur de CD pour les ordinateurs sur lesquels vous voulez installer le logiciel de configuration *ELSA LANconfig*.

- Carte réseau Ethernet
- Protocole réseau TCP/IP installé et relié à la carte réseau

2.3 Installer la station de travail

Les routeurs ELSA font de la gestion des adresses dans un réseau local un jeu d'enfant. Quelques réglages sont éventuellement nécessaires sur les postes de travail pour permettre le travail entre les routeurs et les ordinateurs des postes de travail.

2.3.1 Windows 95 et Windows 98

A partir de l'exemple de Windows 95 et Windows 98, nous vous montrons ici brièvement, si ce n'est déjà fait, ce que vous devez configurer pour une communication sans faille des ordinateurs dans le réseau TCP/IP avec le routeur.

- Installation du protocole réseau
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'.
- Faire attribuer les adresses IP (utiliser DHCP)
Si vous exploitez le routeur en tant que serveur DHCP, les stations de travail doivent être configurées pour l'obtention automatique des adresses IP. **Démarrer ► Paramètres ► Panneau de configuration ► Réseau ► Protocole réseau ► Propriétés ► Adresse IP ► Attribuer automatiquement l'adresse IP**. Supprimez en outre d'éventuels enregistrements de serveur DNS et de passerelle (dans les onglets 'Passerelle' et 'Configuration DNS'. L'ordinateur recherche ensuite, après un redémarrage, un serveur DHCP dans le réseau et se fait attribuer une adresse IP par ce serveur.
- Réglage d'adresses IP fixes (ne pas utiliser DHCP)
Si vous ne voulez pas utiliser de serveur DHCP dans votre réseau, réglez des adresses IP fixes aux ordinateurs : **Démarrer ► Paramètres ► Panneau de configuration ► Réseau ► Protocole réseau ► Propriétés ► Adresse IP ► Fixer l'adresse IP**.

Attribuez des adresses IP univoques, p.ex. d'une tranche d'adresses réservée. Les stations de travail peuvent par exemple obtenir les

adresses 10.1.1.2 à 10.1.1.253, le routeur obtient 10.1.1.1, le masque de réseau étant toujours 255.255.255.0. Pour vérifier si l'adresse IP choisie pour le routeur est disponible, par exemple 10.1.1.1, exécutez la commande ping 10.1.1.1 dans une fenêtre DOS. Si vous n'obtenez pas de réponse, cette adresse est probablement disponible.

- Inscrire la passerelle et le serveur DNS (inutile en cas d'utilisation de DHCP)

Configurez les stations de travail avec l'adresse du routeur dans votre propre réseau local en guise de passerelle et de serveur de noms de domaines (serveur DNS) : **Démarrer ► Paramètres ► Panneau de configuration ► Réseau ► TCP/IP ► Propriétés ► Passerelle et Configuration DNS**. Pour la configuration DNS, entrez également un nom d'hôte. Pour des raisons de cohérence, utilisez à cet effet le nom du PC (dans le cas idéal, identique au nom de l'utilisateur).

- Contrôle de la configuration IP

Sous Windows 95 ou Windows 98, vous pouvez consulter la configuration IP actuelle de l'ordinateur dans **Démarrer ► Exécuter ► winipcfg**. Vous pouvez y voir, entre autres, quelle adresse le serveur DHCP a attribué à l'ordinateur et quelles adresses ont été communiquées pour le serveur DNS et la passerelle.

2.3.2 Windows NT 4.0

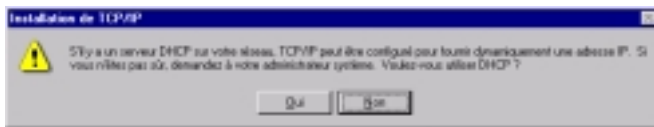
A partir de l'exemple de Windows NT 4.0, nous vous montrons ici brièvement, si ce n'est déjà fait, ce que vous devez configurer pour une communication sans faille des ordinateurs dans le réseau TCP/IP avec le routeur.

- Installation du protocole réseau

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

- Faire attribuer les adresses IP (utiliser DHCP)

Si vous exploitez le routeur en tant que serveur DHCP, les stations de travail doivent être configurées pour l'obtention automatique des adresses IP. Cliquez à cet effet sur le bouton **Oui** une fois terminée l'installation du protocole de réseau.



Windows copie ensuite les données nécessaires et puis attend un redémarrage.

- Réglage d'adresses IP fixes (ne pas utiliser DHCP)

Si vous ne voulez pas utiliser de serveur DHCP dans votre réseau, réglez des adresses IP fixes aux ordinateurs : **Démarrer ► Paramètres ► Panneau de configuration ► Réseau ► Protocoles ► Propriétés**. Sur cet onglet vous pouvez par ailleurs activer la passerelle standard.



Attribuez des adresses IP univoques, p.ex. d'une tranche d'adresses réservée. Les stations de travail peuvent par exemple obtenir les adresses 10.1.1.2 à 10.1.1.253, le routeur obtient 10.1.1.1, le masque de réseau étant toujours 255.255.255.0. Pour vérifier si l'adresse IP choisie pour le routeur est disponible, par exemple 10.1.1.1, exécutez la commande ping 10.1.1.1 dans une fenêtre DOS. Si vous n'obtenez pas de réponse, cette adresse est probablement disponible.

- Inscrire le serveur DNS (inutile en cas d'utilisation de DHCP)

Inscrivez sur l'onglet 'DNS' l'adresse du routeur du propre réseau local et comme serveur de noms de domaine (serveur DNS) aux stations de travail. Pour la configuration DNS, entrez également un nom d'hôte. Pour

des raisons de cohérence, utilisez à cet effet le nom du PC (dans le cas idéal, identique au nom de l'utilisateur).



- Contrôle de la configuration IP

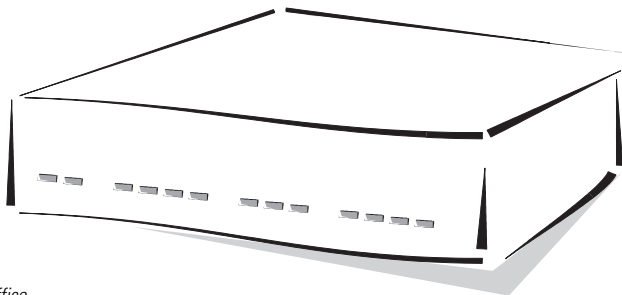
Sous Windows 95 ou Windows 98, vous pouvez consulter la configuration IP actuelle de l'ordinateur dans **Démarrer ► Exécuter ► ipconfig**. Vous pouvez voir ici quelle adresse IP le serveur DHCP a attribué à l'ordinateur et quelle adresse a été transmise pour la passerelle (pas pour le serveur DNS).

2.4 ***ELSA LANCOM Office 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.

2.4.1 **La face avant de l'appareil**

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



Exemple modèle :
ELSA LANCOM 2000 Office

Power/Msg

Ce témoin lumineux s'allume brièvement une fois lors de la mise sous tension d'alimentation. 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
rouge	1 x brièvement	Le lancement (test et chargement) a commencé
rouge	clignotant	Affichage d'une erreur de lancement (codé sous forme de clignotement)
rouge		Périphérique prêt au service
rouge	interruption	Message d'erreur ou appels sortants empêchés par un blocage des unités de taxation

Etat S_0

Ce témoin lumineux indique l'état de la connexion S_0 :

inactif		non branché ou pas de tension S_0 (sur les lignes RNIS, la tension S_0 est souvent désactivée après une durée d'inactivité)
vert	clignotant	Initialisation (prise de contact avec le poste connecteur)
vert		prêt au service (bus S_0 activé, TEI présent et protocole canal D vérifié)
vert	Alimentation arrêt	Témoin lumineux allumé bien que le témoin lumineux "Power" est éteint : appareil dans le moniteur de lancement

a/b 1 à a/b 4

Ces témoins lumineux indiquent l'état des connexions analogiques sur le *ELSA LANCOM 2000 Office* :

inactif		Port a/b en veille
vert		La connexion est établie
vert	clignotant	Appel sortant en cours (Port offhook) (clignotement normal)
vert	clignotant	- aucun canal B disponible (sur le bus ou interne) - (plus) aucun récepteur DTMF présent - ligne RNIS non disponible
rouge	clignotant	Appel entrant sur la ligne (témoin lumineux clignote au rythme de la sonnerie)
rouge	clignote 1 fois	Appel entrant, MSN ok, port pour appels entrants bloqué

WAN
Chan1
Chan2

Ces témoins lumineux indiquent l'état du canal WAN RNIS logique correspondant (aussi bien en mode routeur qu'en mode CAPI) :

inactif		Canal en veille
rouge	clignotant	Appel entrant sur la ligne
vert	clignotant	Appel sortant en cours
rouge		connexion physique établie/échange de protocole en cours
vert		l'échange de protocole correspondante (X.75, PPP, etc.) est achevé; le canal est logiquement en ligne
vert/rouge	flash rouges brefs (durée env. 1/10 s)	indiquent un paquet de données reçu

Les canaux WAN RNIS n'ont pas d'affectation fixe au canaux B !

Tant que le témoin lumineux 'Chan1' ou 'Chan2' est allumé en vert la connexion est active et payante !

Ce témoin lumineux indique si cette connexion RNIS est un regroupement statique ou dynamique de canaux.

inactif	aucune connexion ou aucun regroupement actif de canaux
vert	liaison par regroupement dynamique ou statique active



WAN
Chan 1+2

LAN-Tx, -Rx,
LAN-Coll, -Link
LAN-FDpx, -Fast

Ces témoins lumineux indiquent les états correspondants du contrôleur de réseau :

LAN-Rx/Tx	jaune	Paquet de données émis par le périphérique vers le LAN ou émis du LAN vers l'appareil
LAN-Coll	rouge	Collision émission
LAN-Link	vert	La connexion vers le LAN est réalisée et prête
LAN-FDpx	vert	Le routeur émet et reçoit des données simultanément
LAN-Fast	vert	Le <i>ELSA LANCOM</i> se trouve en mode 100 Mbit

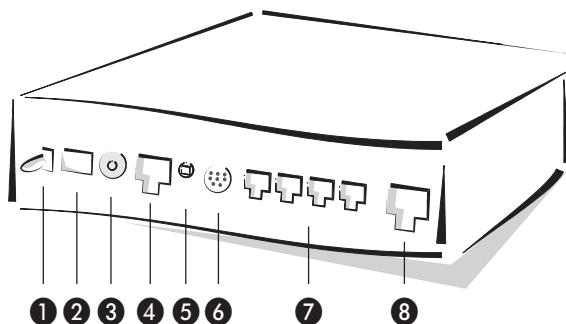


Les deux témoins lumineux LAN-FDpx et LAN-Fast ne sont valables que pour les réseaux 100 Mbps et n'existent donc que sur ELSA LANCOM 1100 Office.

2.4.2

La face arrière de l'appareil

Maintenant retournez le tout et regardez la face arrière. Comme précédemment vous trouvez de gauche à droite :



Exemple modèle :
ELSA LANCOM 2000
Office

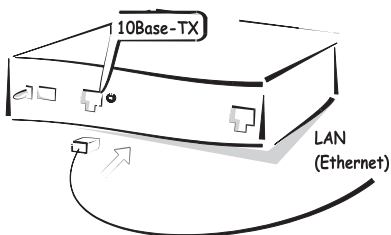
- ❶ Commutateur Marche/Arrêt
- ❷ raccord bloc d'alimentation
- ❸ 10Base-2 (BNC), uniquement *ELSA LANCOM 1000 Office* ou *ELSA LANCOM 2000 Office*
- ❹ 10Base-T (*ELSA LANCOM 800 Office*, *ELSA LANCOM 1000 Office* ou *ELSA LANCOM 2000 Office*) pour réseaux 10 Mbit ou 10/100Base-TX (*ELSA LANCOM 1100 Office*) pour réseaux 10Mbit ou 100 Mbit

- ⑤ commutateur nœud/concentrateur
- ⑥ interface de configuration V.24 (ELSA LANCOM 1000 Office, ELSA LANCOM 2000 Office ou ELSA LANCOM 1100 Office)
- ⑦ quatre raccordements analogiques (POTS, ports a/b, uniquement ELSA LANCOM 2000 Office)
- ⑧ raccordement RNIS S_0

2.5

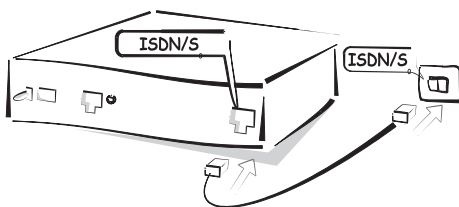
Pour raccorder l'appareil

- ① Connectez votre station de base ELSA LANCOM Office au réseau local LAN. Pour cela, enfichez un côté du câble réseau joint dans le connecteur de réseau 10/100 Base-TX 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).



Exemple modèle :
ELSA LANCOM 800 Office

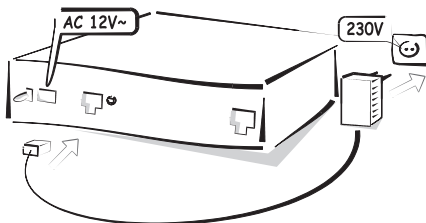
- ② Connectez votre ELSA LANCOM Office au réseau RNIS. Pour cela enfichez le câble de connexion RNIS dans le connecteur fourni dans connecteur RNIS/ S_0 de l'appareil et à un connecteur multiple RNIS/ S_0 ou à un connecteur de standard (configuration point-à-multipoint ou configuration point-à-point).



Exemple modèle :
ELSA LANCOM 800 Office

- ③ Alimentez l'appareil en tension nécessaire via le bloc d'alimentation et mettez-le en circuit. Après un autotest bref de l'appareil le témoin lumineux 'Power/Msg' est allumé en permanence. Le témoin lumineux 'LAN-Link' qu'une liaison correcte est établie avec le réseau local.

Exemple modèle :
ELSA LANCOM 800 Office



Si cette DEL ne s'allume pas, commutez le commutateur nœud/concentrateur. Si la DEL ne s'allume toujours pas, il est possible que la carte réseau ou les câbles soient défectueux.

2.5.1

Installation du logiciel

Le logiciel de configuration *ELSA LANconfig* pour systèmes d'exploitation sous Windows vous permet de régler votre routeur d'une manière simple et conviviale en fonction de vos applications désirées. Sous d'autres systèmes d'exploitation vous pouvez comme alternative procéder à la configuration avec un navigateur HTML.

Pour mettre en service le *ELSA LANconfig* il vous faut un PC Windows dans le réseau local.

- ① Installez tout d'abord le protocole de réseau TCP/IP sur l'ordinateur à partir duquel vous désirez configurer l'appareil.
- ② Installez ensuite *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* et suivez les instructions du programme d'installation.

2.6

Configuration

Dans cet exemple nous vous montrons la liaison simple d'un réseau local à Internet.

La configuration de l'appareil se divise de la façon suivante :

- Réglages de base

● Configurer un accès Internet

Pour chacune des parties de la configuration il y a un tableau d'informations. Il vous indique les informations dont vous avez besoin. Remplissez ce tableau avant de commencer la configuration.

2.6.1

Réglages de base

Dans les réglages de base donnez un nom à l'appareil et déterminez les adresses IP pour l'utilisation dans le réseau local. Dans cet exemple le serveur DHCP dans le routeur donne automatiquement la répartition des adresses IP dans le réseau local.

Navigateur HTML

Si vous ne souhaitez pas ou ne pouvez pas utiliser *ELSA LANconfig* (parce que vous avez installé un autre système d'exploitation p. ex.), vous pouvez également procéder aux réglages de base avec un navigateur HTML normal.

① Démarrez votre navigateur.

- Si vous n'avez jusqu'à présent dans votre réseau local ni de serveur DHCP ni de serveur DNS, le routeur réagit à chaque adresse que vous entrez dans le champ d'adresse. Etant donné que la plupart des navigateurs appellent normalement une page spéciale, le navigateur affichera automatiquement dans la plupart des cas l'écran de démarrage de configuration du routeur.

Si votre navigateur appelle normalement une page vide, entrez un nom quelconque dans le champ d'adresse (p. ex. '*ELSA LANCOM Office*'). L'écran de démarrage sera ainsi automatiquement affiché.

- Si vous utilisez dans votre réseau local déjà un serveur DHCP ou des adresses IP fixes, entrez dans le champ d'adresse du navigateur l'adresse 'x.x.x.254', 'x.x.x' représentant le groupe d'adresses utilisé jusque là dans le réseau.



Si vous ne savez pas si des adresses IP ont été utilisées jusqu'à présent dans votre réseau, cliquez sous Windows 95 ou Windows 98 d'abord sur **Démarrer ► Exécuter**, entrez dans la fenêtre qui s'ouvre l'instruction `winipcfg` et confirmez en cliquant 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`.

- ② Sélectionnez 'Réglages de base'.
- ③ Activez l'option 'Déterminer automatiquement les paramètres IP', 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. Le routeur

déterminera et attribuera automatiquement alors en tant que serveur DHCP les adresses IP pour tous les appareils dans le réseau local.

ou

- Vous ne voulez pas utiliser d'adresses IP parce que vous utilisez p.ex. uniquement un réseau Windows.
- ④ Désactivez l'option 'Déterminer automatiquement les paramètres IP', 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 pour le nouvel appareil et lui attribuer une adresse quelconque dans les zones d'adresse réservées à des fins personnelles comme p. ex. '10.0.0.1' avec le masque de réseau '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 au nouvel appareil une adresse libre se trouvant dans la zone d'adresses utilisée jusque là et déterminez si le routeur 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.

- ⑤ Attribuez un mot de passe pour l'accès à l'appareil et déterminez s'il doit servir de serveur DHCP ou non dans votre réseau local.



Désactivez la 'Configuration automatique des stations de travail via DHCP' uniquement si vous voulez utiliser des adresses IP fixes dans votre réseau ou si vous exploitez déjà un autre serveur DHCP. Le fonctionnement du serveur DHCP est décrit plus loin dans ce manuel.

- ⑥ Entrez pour chaque bus S_0 les numéros d'appel auxquels le routeur doit réagir et le préfixe nécessaire pour accéder à la tonalité extérieure si vous connectez votre appareil à un mini-standard.

Indiquez aussi si les informations de taxation sont transmises à votre accès RNIS.

Si vous ne remplissez pas le champ pour les numéros d'appel, le routeur réagit à tous les numéros d'appel qui sont valables pour cet accès.

Avec ces réglages vous avez fait connaître votre nouveau routeur dans le réseau local. Il répond lui-même à l'adresse IP '10.0.0.1'. Après un redémarrage tous les appareils dans le réseau local obtiennent leur adresse IP du serveur DHCP dans le routeur. Le pool d'adresses de '10.0.0.2' à '10.0.0.253' est automatiquement utilisé.

En cas d'appel à partir du réseau RNIS, l'appareil réagit seulement aux numéros d'appel que vous avez enregistrés pour chaque bus S_0 .

ELSA LANconfig

Au premier lancement d'*ELSA LANconfig*, un nouveau périphérique est reconnu dans le réseau TCP/IP et peut être immédiatement configuré. Un assistant sera lancé automatiquement pour vous aider à procéder au réglage de base de l'appareil, ou pour vous en télécharger 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, le routeur 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**. Si dans la fenêtre suivante figure la valeur '0.0.0.0' dans le champ 'Adresse IP', l'ordinateur n'a jusqu'à présent pas encore d'adresse IP.*

- ③ Choisissez l'option 'Je désire effectuer les réglages moi-même' si vous êtes familiarisé avec les réseaux et les adresses IP et si l'une des 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 routeur 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 au routeur une adresse libre se trouvant dans la zone d'adresses utilisée jusque là et déterminez si le routeur 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. Le fonctionnement du serveur DHCP est décrit plus loin dans ce manuel.

Telnet

Si vous ne voulez ou ne pouvez pas utiliser *ELSA LANconfig* ou un navigateur HTML (parce que vous avez installé un autre système d'exploitation sans navigateur p. ex.), vous pouvez également procéder aux réglages de base 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 10.0.254` dans la fenêtre s'ouvrant.

- ② Modifiez la langue de la configuration avec l'instruction :

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

- ③ Adresse Intranet et masque réseau :

```
set /Setup/Module TCP-IP/Adresse Intranet
10.0.0.1
set /Setup/Module TCP-IP/Masque Intranet
255.255.255.0
```

La connexion Telnet est interrompue avec la modification de l'adresse Intranet.

- ④ Désactiver éventuellement la fonction DHCP :

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

Même si ici les enregistrements sans autre explication ne vous disent pas grand-chose, vous avez atteint le même but qu'avec la configuration via ELSA LANconfig!

Avec ces réglages vous avez fait connaître votre nouveau routeur dans le réseau local. Il répond lui-même à l'adresse IP '10.0.0.1'. Après un redémarrage tous les appareils dans le réseau local obtiennent leur adresse IP du serveur DHCP dans le routeur. Le pool d'adresses de '10.0.0.2' à '10.0.0.253' est automatiquement utilisé.

ELSA LANconfig

- ① Lancez *ELSA LANconfig* **Démarrer** ► **Programmes** ► **ELSAIlan** ► **ELSA LANconfig**.
- ② Sélectionnez votre *ELSA LANCOM Office* dans la liste des appareils et appelez les assistants.
- ③ Sélectionnez l'assistant pour l'accès à Internet, votre pays et puis un des fournisseurs d'accès à Internet déterminés ou un accès général via PPP.
- ④ Entrez dans les fenêtres suivantes les données de connexion tels les numéros d'appel, le nom d'utilisateur, le code et quitter l'assistant en cliquant sur **Terminer**.

Terminé !

Avec ces quelques clics de souris vous avez entièrement configuré l'appareil pour un accès à Internet via une ligne RNIS. Tous les ordinateurs dans votre réseau local qui obtiennent de votre *ELSA LANCOM Office* leurs propres adresses IP et les adresses IP pour la passerelle peuvent maintenant à plein rendement surfer sur Internet ...

3 Configurations possibles

Les routeurs ELSA sont toujours livrés avec le logiciel actuel dans lequel certains réglages ont déjà été préparés pour vous.

Il vous faut cependant compléter les informations et les adapter à vos besoins spécifiques. 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.

FR

3.1 De nombreux chemins mènent au **ELSA LANCOM**

En principe, il y a différentes possibilités d'accès au routeur d'ELSA :

- Par l'interface de configuration (interface config.) sur la face arrière du routeur (également nommé outband)

L'interface de configuration est à votre disposition sur les modèles *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1000 Office* et *ELSA LANCOM 1100 Office*.

- Par le réseau LAN ou WAN (inband)
- Par une connexion PPP sur l'Accès réseau à distance ou similaire (configuration à distance)

Quelle est donc la différence entre ces possibilités ?

D'une part l'accessibilité des appareils : la configuration par Outband est toujours disponible. La configuration Inband n'est plus possible quand par ex. le réseau transmetteur est perturbé. La téléconfiguration est également tributaire du milieu transmetteur, par ex. la connexion RNIS.

D'autre part les exigences envers des logiciels ou du matériel supplémentaire(s). La configuration Inband nécessite l'un des ordinateurs présent dans le réseau LAN ou WAN ainsi qu'un logiciel approprié. La configuration Outband nécessite en plus du logiciel l'un des ordinateurs (avec interface série) ainsi que le câble de configuration correspondant. La téléconfiguration nécessite un ordinateur avec PPP-Client, carte RNIS ou adaptateur de terminal. La solution la plus simple est la configuration à distance en se servant de l'Accès réseau à distance et d'*ELSA LANconfig*.



3.2

La voie directe : Outband

La configuration Outband vous permet d'accéder directement au routeur par l'interface de configuration.

Vous n'avez besoin de la configuration outband que si vous ne pouvez pas accéder à votre périphérique par TCP/IP.

3.2.1

Conditions pour la configuration Outband

Que vous faut-il pour cela ?

- un routeur avec interface de configuration, *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1000 Office* ou *ELSA LANCOM 1100 Office*
- Un ordinateur avec Windows 95, Windows 98 ou Windows NT 4.0 et *ELSA LANconfig*.
ou
un ordinateur avec un système d'exploitation quelconque et un émulateur de terminal (par ex. *Telix* ou *Hyperterminal*).
- Le câble de configuration livré et, le cas échéant l'adaptateur 9/25 broches pour relier l'ordinateur au routeur (port COM du PC à l'interface de configuration du routeur).

3.2.2

Configuration outband avec *ELSA LANconfig*

Lancez *ELSA LANconfig* par ex. à partir de la barre de Windows par **Démarrer ► Programmes ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* cherchera alors automatiquement des périphériques *ELSA LANCOM* dans le réseau local (mais pas sur l'interface série). Pour trouver un nouvel appareil sur l'interface série tapez **Appareil ► Recherche ► Rechercher sur toutes les interfaces**. *ELSA LANconfig* affiche les nouveaux routeurs avec leur désignation.

Dans le cas d'un nouveau périphérique non encore configuré sur l'interface de configuration, vous pouvez appeler différentes aides de configuration par **Outils ► Assistant de configuration**. Choisissez l'un des assistants proposés et répondez simplement à ses questions. Après cela, votre *ELSA LANCOM* sera réglé pour la tâche sélectionnée.

Afin de pouvoir modifier la configuration actuelle, il suffit de double-cliquer sur la désignation de l'appareil dans la liste des appareils trouvés.

3.2.3 Configuration Outband avec programme de terminal

Dès que l'émulateur de terminal est lancé, appuyez plusieurs fois la touche Retour afin de reconnaître automatiquement le taux de transmission (jusqu'à 230 Kbps, 38,4 Kbps en version standard).

Après l'introduction du mot de passe, toutes les instructions décrites au paragraphe 'Instructions de configuration' seront à votre disposition.

3.3 La voie confortable : Inband

La configuration Inband vous permet d'accéder au routeur à partir de n'importe quel ordinateur du LAN ou WAN. L'accès pourra toutefois être restreint ou bloqué entièrement par la liste d'accès IP. Pour cette configuration, utilisez Telnet (fait partie de la livraison de la plupart des systèmes d'exploitation) ou *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.

3.3.1 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 routeur requérir une adresse IP, afin que vous puissiez le 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 192.168.130.1, vous pourrez alors contacter votre périphérique avec l'adresse 192.168.130.254.



Si vous avez déjà un ordinateur avec l'adresse XXX.XXX.XXX.254 dans votre réseau, donnez une nouvelle adresse au périphérique par la configuration Outband avant de l'installer dans le LAN.

3.3.2 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'). Le routeur peut, en outre, déterminer pour lui-même l'adresse IP côté réseau local.

3.3.3

Configuration par *ELSA LANconfig*

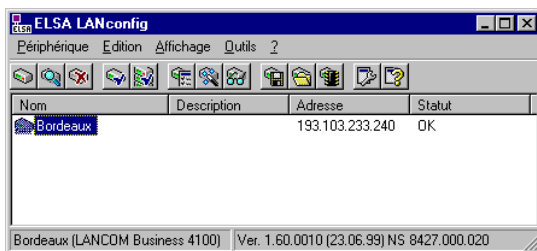
Appelez *ELSA LANconfig* p.ex. à partir de la barre de Windows avec **Démarrer ► Programmes ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* cherchera automatiquement des périphériques dans le réseau local. Si un périphérique non configuré est trouvé dans le réseau local, *ELSA LANconfig* lance automatiquement l'assistant de configuration.

Choisissez l'un des assistants proposés et répondez simplement à ses questions. Après cela, le routeur sera réglé pour la tâche sélectionnée.



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 disponibles. 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 **Édition ► 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.

3.3.4 Configuration par Telnet

Lancez la configuration par telnet, par ex. à partir d'une boîte DOS avec la commande :

```
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'.

3.4 L'accès à distance : Configuration par Accès réseau à distance

Le réglage de routeurs distants est particulièrement simple à l'aide de la configuration à distance par l'Accès réseau à distance. Après la mise en marche et l'accès à RNIS, l'administrateur pourra accéder immédiatement au périphérique sans faire un seul réglage. En connectant ainsi d'autres réseaux à votre LAN, vous économisez beaucoup de temps et d'argent pour les déplacements vers le site du réseau ou l'instruction d'un collaborateur sur place pour la configuration des routeurs.

Vous pouvez en outre réserver un numéro d'appel particulier pour la configuration à distance. De cette manière, un technicien SAV pourra toujours accéder au routeur, même si des erreurs de réglage le rendent inaccessible.

3.4.1 Ce dont vous avez besoin pour la configuration à distance

- un ordinateur avec client PPP, par ex.

- un logiciel pour la configuration Inband, par ex. *ELSA LANconfig* ou Telnet
- une carte RNIS, un adaptateur de terminal ou un routeur *ELSA LANCOM* avec *ELSA LANCAP*

3.4.2

Préparation de la configuration à distance

- ① Appliquez la tension d'alimentation nécessaire au routeur.
- ② Raccordez le périphérique à un accès RNIS.

3.4.3

La première connexion à distance par Accès réseau à distance (*ELSA LANconfig*)

- ① Sélectionnez dans *ELSA LANconfig* **Périphérique ► Nouveau**, activez le type de raccordement 'Connexion réseau (TCP/IP)' et entrez le numéro d'appel de l'accès RNIS sur lequel *ELSA LANCOM* est branché. Réglez le cas échéant le délai après lequel une connexion sans transfert de données devra être interrompue automatiquement.
- ② *ELSA LANconfig* génère automatiquement une nouvelle inscription dans l'Accès réseau à distance. Sélectionnez pour la connexion un périphérique supportant PPP (par ex. le pilote de NDIS WAN livré avec *LANCAP*) et confirmez avec **OK**.
- ③ Ensuite, *ELSA LANconfig* affichera dans la liste des appareils un nouveau périphérique avec le nom 'Inconnu' et le numéro d'appel de transmission téléinformatique en tant qu'adresse.



L'entrée dans la liste des appareils effacera aussi la connexion dans l'Accès réseau à distance.

- ④ Par la connexion à distance, vous pouvez régler le routeur comme tous les autres périphériques. Pour lire la configuration, *ELSA LANconfig* établira une connexion par l'Accès réseau à distance.

3.4.4

La première connexion à distance avec un client PPP et Telnet

- ① A l'aide de votre client PPP, établissez une connexion vers le *ELSA LANCOM* en utilisant les données suivantes :
 - nom d'utilisateur 'ADMIN'

- mot de passe comme sur le routeur *ELSA LANCOM*, aucun mot de passe à la livraison
 - une adresse IP pour la connexion, uniquement en cas de besoin
- ② Lancez une connexion Telnet vers le routeur *ELSA LANCOM*. Utilisez pour cela l'adresse IP suivante :
- '172.17.17.18', si vous n'avez pas défini d'adresse IP pour le client PPP. Le *ELSA LANCOM* utilisera automatiquement cette adresse s'il n'a pas été convenu autre chose. Le PC appelant réagira à l'IP '172.17.17.17'.
 - Si vous avez défini une adresse, incrémentez l'adresse IP du PC de 1. Exemple : Pour le client PPP vous avez défini l'adresse IP '10.0.200.123', le *ELSA LANCOM* réagira sur '10.0.200.124'. Exception : Si l'IP finit par '254', le routeur réagira sur 'x.x.x.1'.
- ③ Par la connexion à distance, vous pouvez régler le routeur *ELSA LANCOM* comme tous les autres périphériques.

3.4.5

Restriction de la configuration à distance

La connexion PPP à partir d'un correspondant quelconque vers le routeur ne réussit que si le périphérique répond à chaque appel avec la configuration correspondante pour le mode PPP. Ceci est également possible dans l'état à la livraison, puisque le protocole standard (default layer) est réglé sur PPP.

Mais peut-être voulez-vous régler le default layer sur un autre protocole après la première configuration, par ex. pour une connexion LAN-LAN ? Dans ce cas, le périphérique ne prendra plus les appels des connexions téléinformatiques en PPP. Pour y remédier, il suffit de convenir un numéro d'appel spécifique pour accéder à la configuration. Si l'appareil reçoit un appel sur ce numéro, les réglages PPP seront utilisés, et ceci indépendamment des autres configurations du routeur. Durant cet échange PPP, il ne sera accepté que le nom d'utilisateur qui aura été enregistré automatiquement par *ELSA LANconfig* lors de l'établissement de la communication.

- ① Passez dans la zone de configuration 'Gestion' sur l'onglet 'sécurité'.



- ② Sélectionnez dans la zone 'Accès à configuration' si l'accès à partir de réseaux distants est possible en totalité, en lecture seule ou pas du tout.

Dans le cas d'une connexion Telnet ou terminal, entrez alternativement l'instruction suivante :

```
set/Setup/Config-module/Wan-config
[on][read][off]
```

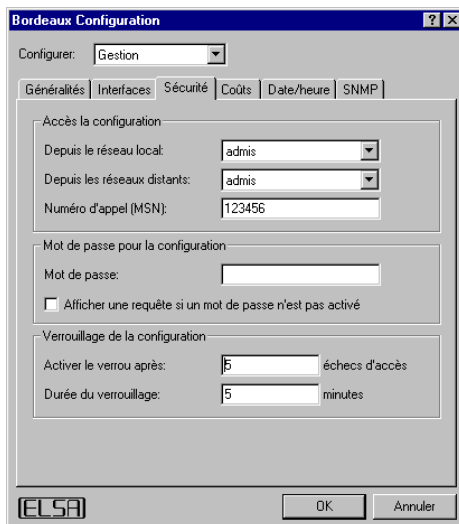
Si vous voulez bloquer entièrement l'accès au routeur via le WAN, mettez l'accès à la configuration à partir de réseaux distants sur 'interdit'.

- ③ Dans la zone 'Accès la configuration', entrez comme numéro d'appel un MSN ou EAZ de votre accès RNIS qui n'est pas utilisé pour le routeur, le *LANCAPI* ou les ports A/N.

Entrez alternativement l'instruction suivante :

```
set/Setup/Config-module/Farconfig      ( EAZ-MSN )
123456
```

- ④ Protégez les réglages de l'appareil au besoin avec un mot de passe.



Entrez alternativement l'instruction suivante :

passwd

De cette manière, on vous demandera d'entrer un nouveau mot de passe et de le confirmer.

3.5 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, 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 !

3.5.1 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.

3.5.2 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) :

- *ELSA LANconfig* (conseillé)
- Emulateur de terminal
- 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 **Édition ► Sauvegarder la configuration dans un fichier**).

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

ELSA LANconfig



Dans l'outil de configuration *ELSA LANconfig* marquez l'appareil souhaité dans la liste de sélection et cliquez sur **Édition ► 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 **Édition ► Gestion du microprogramme ► Activation du microprogramme durant le test**.

Emulateur de terminal (par ex. *Telix* ou Hyperterminal sous Windows)

Dans le menu 'microprogramme' des émulateurs de terminal déterminez d'abord à l'aide de l'instruction 'set Mode-Firmsafe', dans quel mode vous voulez charger le nouveau microprogramme (immédiatement, login ou manuel). Fixez aussi en cas de besoin, la durée de la période de test du microprogramme à l'aide de 'set Timeout-Firmsafe'.

L'instruction 'Télécharger microprogramme' commute ensuite le routeur en réception. Lancez ensuite le téléchargement à partir de votre émulateur de terminal :

- Avec *Telix*, cliquez sur le bouton **Upload**, sélectionnez 'XModem' pour la transmission et choisissez le fichier souhaité pour le téléchargement.
- Avec Hyperterminal, cliquez sur **Transmission ► Envoi fichier**, choisissez le fichier, sélectionnez le protocole 'XModem' et appuyez ensuite **OK**.



TFTP

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

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

*Cette instruction envoie le fichier correspondant avec **writelflash** à l'adresse IP indiquée. Pour cela, TFTP doit être commuté sur transmission de données binaires. Le format ASCII est toutefois 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 la mémoire flash, erreur de transmission TFTP etc.), FirmSafe activera le micrologiciel précédent. La configuration sera conservée.

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

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

3.6 Supervision de la ligne ?

Une fois la configuration de base des appareils achevée, on obtient des informations supplémentaires importantes sur les paramètres devant encore être modifiés, et ce avant tout grâce à l'observation du trafic des données sur les différentes interfaces du routeur.

D'autres possibilités sont à votre disposition en plus des statistiques sur l'appareil que vous pouvez par exemple lire durant une séance Telnet ou terminal.

3.6.1

ELSA LANmonitor

Avec l'outil de surveillance *ELSA LANmonitor* vous pouvez sous les systèmes d'exploitation Windows, toujours afficher à l'écran les informations les plus importantes sur l'état de votre routeur. Un grand nombre des messages internes du périphérique sont traduits en clair et vous indiquent l'état actuel du périphérique et vous assistent lors du dépannage.

Installation de ELSA LANmonitor

En général *ELSA LANmonitor* est installé automatiquement avec *ELSA LANconfig* sur l'ordinateur à partir duquel vous voulez procéder au réglage de votre routeur.

Si *ELSA LANmonitor* n'est pas encore installé sur votre ordinateur, engagez le CD *ELSA LANCOM*. 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* et suivez les instructions du programme d'installation.

Lors de l'installation, activez l'option pour 'LANmonitor'.

ELSA LANmonitor ne vous permet de surveiller que les périphériques auxquels vous accédez par Inband ou par le réseau local. Pour cela, le protocole réseau TCP/IP doit être installé sur votre ordinateur. Avec ce logiciel, vous ne pouvez pas vous adresser aux routeurs branchés sur l'interface série.

Contrôle de la connexion Internet avec ELSA LANmonitor

En tant qu'exemple des fonctions de *ELSA LANmonitor*, nous vous montrons d'abord les informations fournies par *ELSA LANmonitor* sur l'établissement de la liaison vers votre fournisseur d'accès Internet.

- ① Réglez donc le routeur pour la communication vers votre fournisseur d'accès, par ex. à l'aide de l'assistant de configuration d'*ELSA LANconfig*.
- ② Lancez *ELSA LANmonitor* avec **Démarrer ► Programmes ► ELSAlan ► LANmonitor**. Définissez un nouveau périphérique avec **Périphérique ► Nouveau** et entrez dans la fenêtre suivante l'adresse IP du routeur que vous voulez surveiller. Si la configuration du



périphérique est protégée par un mot de passe, entrez celui-ci par la même occasion.

En alternative, vous pouvez sélectionner l'appareil dans *ELSA LANconfig* et démarrer la surveillance d'un appareil par **Outils ► Surveillance d'appareil**.

- ③ *ELSA LANmonitor* crée automatiquement un nouvel enregistrement dans la liste des appareils et indique tout d'abord l'état des canaux de transmission. Lancez votre explorateur Internet et entrez un site quelconque. *ELSA LANmonitor* montre alors comment une connexion est établie sur un canal et quel correspondant est appelé. Dès que la communication est établie, un signe '+' devant l'inscription du canal B indique qu'il y a des informations supplémentaires sur ce canal. En cliquant sur le signe '+' vous ouvrez une arborescence dans laquelle vous pourrez lire les différentes informations.



Dans cet exemple vous pouvez voir dans les informations du protocole PPP quelle adresse IP a été assignée à votre routeur par le fournisseur d'accès pour la durée de la communication, et quelles adresses pour serveurs DNS et NBNS ont été transmises.

Dans les informations générales vous pouvez observer les taux de transfert avec lesquels les données sont actuellement transmises avec l'Internet.

- ④ Un clic de la touche droite de la souris sur le canal actif vous permet de couper manuellement la communication. Il vous faut le cas échéant le numéro de passe de configuration.
- ⑤ Si vous souhaitez en plus des informations dans la liste des appareils de *ELSA LANmonitor* une fenêtre d'info réduite sous forme d'un écran à cristaux liquides LCD, cliquez de la touche droite de la souris sur le nom de l'appareil et sélectionnez **Affichage des canaux**.



Un clic de la touche droite de la souris sur la zone d'affichage des canaux arrange cet affichage virtuel de manière à toujours être en avant-plan sur votre écran.

- ⑥ Si vous souhaitez un protocole des sorties du *ELSA LANmonitor* sous forme de fichier, sélectionnez dans le menu 'Affichage' les 'Options' et passez à l'onglet 'Journal'. Activez la journalisation et choisissez si le *ELSA LANmonitor* doit établir un fichier protocole tous les jours, tous les mois ou continuellement.

3.7 Éditions des tracés

Les éditions des tracés permettent de contrôler les processus internes du routeur pendant ou après la configuration. Un tracé révèle p. ex. toutes les étapes d'une négociation du PPP. L'interprétation de ces tracés permet aux utilisateurs expérimentés de découvrir d'éventuelles erreurs lors de l'établissement d'une connexion. Particulièrement positif : les erreurs peuvent être détectées à la fois dans la configuration des propres routeurs et chez le correspondant.



Les éditions des tracés sont légèrement décalées dans le temps par rapport à l'événement effectif, mais sont toujours dans l'ordre correct. Ceci ne gêne en aucun cas l'interprétation des affichages, il faut tout de même en tenir compte lors d'analyses plus approfondies.

Lancement d'un tracé

La syntaxe de l'appel d'un tracé est la suivante :

```
trace [Code] [Paramètre]
```

L'instruction tracé, le code, les paramètres et les instructions combinées sont séparés par des espaces. Que se cache-t-il derrière Code et Paramètre ?

Ce code provoque avec tracé la réaction suivante :
?	affiche un texte d'aide
+	active une sortie de tracé
-	désactive une sortie de tracé
#	commute entre différentes éditions des tracés (Bascule)
pas de code	affiche l'état actuel du tracé

Ce paramètre affiche avec tracé :
Statut	messages d'état des connexions
Error	messages d'erreurs des connexions
ELSA	négociation du protocole ELSA
PPP	négociation du protocole PPP
routeur IPX	roulage IPX
RIP	IPX Routing Information Protocol
SAP	IPX Service Advertising Protocol
IPX-watchdog	IPX-Watchdog-Spoofing
SPX-watchdog	SPX-Watchdog-Spoofing
NetBIOS	Gestion NetBIOS
Routeur IP	roulage IP
IP-RIP	IP Routing Information Protocol = protocole d'information de rou- tage IP
ICMP	Internet Control Message Protocol = protocole Internet de mes- sage de contrôle
ARP	Address Resolution Protocol = protocole de résolution d'adresse
SCRPT	Négociation de script
Masquerading IP	processus dans le module Masquerading
DHCP	Dynamic Host Configuration Protocol
D-channel-dump	tracé du canal D du bus RNIS branché

Cette instruction combinée affiche avec tracé :
All	toutes les éditions des tracés
Display	éditions d'état et d'erreurs
Protocol	éditions ELSA et PPP
TCP-IP	éditions IP-Rt., IP-RIP, ICMP et ARP
IPX-SPX	éditions IPX-Rt., RIP, SAP, IPX-Wd., SPX-Wd., et NetBIOS
Time	affiche l'heure système avant même l'édition du tracé
Source	affiche le protocole ayant demandé le tracé avant même l'édition du tracé

Les paramètres rajoutés sont exécutés de gauche à droite. Ceci permet la restriction d'un paramètre venant d'être appelé.

Exemples :

Ce code provoque avec tracé la réaction suivante :
trace	affiche tous les protocoles pouvant provoquer des sorties durant la configuration, ainsi que l'état des sorties correspondantes (ON ou OFF).
trace + all	active toutes les éditions des tracés.
trace + protocol display	active la sortie de tous les protocoles de liaison et des messages d'état et d'erreurs.
trace + all - icmp	active toutes les éditions des tracés à l'exception du protocole ICMP.
trace ppp	affiche l'état du ppp
trace # ipx-rt display	commute l'édition des tracés du routeur IPX et des affichages sur écran.
trace - time	désactive la sortie de l'heure système avant la sortie du tracé même.

3.8**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.

4 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 :

- Sécurité de la configuration
- Sécurité pour le réseau local
- Gestion des coûts de communication
- Connexions via le RNIS
- Prise en charge de PPP
- Routage IPX (seulement *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1100 Office*, *ELSA LANCOM 1000 Office*)
- Routage IP
- Bridging (seulement *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1100 Office*, *ELSA LANCOM 1000 Office*)
- Gestion d'adresses automatique via DHCP
- Agent de relais *DHCP*
- Serveur DNS
- NetBIOS-Proxy (seulement *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1100 Office*, *ELSA LANCOM 1000 Office*)
- Rerouteur téléphonique (least-cost router)
- *ELSA LANCAPI*
- Gestion des temps
- Mini-standard (seulement *ELSA LANCOM 2000 Office*)
- Comptabilisation

Seulement sur CD !

Seulement sur CD !

Seulement sur CD !

Seulement sur CD !

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.

4.1 La sécurité de votre configuration

En configurant le périphérique, vous fixez une série de paramètres essentiels pour l'échange de données : la sécurité de votre propre réseau, le contrôle

des coûts de communication et les droits d'accès des utilisateurs font par exemple partie de ces paramètres.

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

4.1.1 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 d'entrée du mot de passe se trouve dans *ELSA LANconfig*, dans le dossier de configuration 'Management' sur l'onglet 'Sécurité'. Au cours d'une session sur terminal ou telnet, activez la demande de mot de passe dans le menu `/Setup/Config-Module/passw.prompt`. Dans ce cas, le mot de passe en soi est activé au moyen de la commande `passwd`.

4.1.2 Le verrouillage des accès

La configuration du *ELSA LANCOM Office* est protégée contre les « attaques en force brute » par un verrouillage d'accès. Dans le cas d'une attaque en force brute, un utilisateur non autorisé cherche à trouver un mot de passe et à trouver un accès à un réseau, à un ordinateur ou à un autre périphérique. A cet effet, un ordinateur peut par exemple simuler automatiquement toutes les combinaisons possibles de lettres et de chiffres jusqu'à ce qu'il trouve le bon mot de passe.

Pour se protéger contre de telles manipulations, il est possible de prescrire un nombre maximum d'essais d'ouverture de séance infructueux. Une fois que cette limite est atteinte, l'accès est bloqué pour un certain temps.

Ces paramètres s'appliqueront globalement à toutes les variantes de configuration (Outband, Telnet, TFTP/*ELSA LANconfig* et SNMP). Le verrouillage 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/Config-module` :

- 'Blocage actif après' (Login-errors)
- 'Durée du blocage' (Lock-minutes)

4.1.3 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.

4.2 La sécurité de votre LAN

Vous n'appréciez certainement pas qu'une personne externe puisse en toute liberté consulter ou modifier les données sur vos ordinateurs. Un *ELSA LANCOM Office* offre différentes possibilités pour limiter un accès de l'extérieur :

- Protection de l'accès par un nom d'utilisateur, un mot de passe et un numéro d'appel
- Rappel automatique de numéros définis
- Filtrage des paquets de données
- Masquering IP (NAT, PAT)

4.2.1 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 :

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

- par nom : Seuls les appels des correspondants dont le nom figure dans la liste des noms sont acceptés.
- numéro : Seuls les appels des correspondants figurant dans la liste des numéros sont acceptés.
- par nom ou numéro : Seuls les appels des correspondants figurant dans la liste des numéros **ou** 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

L'utilisation de la couche ELSA ou PPP sur le canal B permet également la transmission du nom du correspondant appelant. Pour cela il faut d'abord établir une connexion, car le nom ne peut pas être transmis sur le canal D.

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.

Le protocole ELSA vérifie si le nom transmis par le correspondant figure dans la liste des noms.

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 en guise de 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 ? Si, cette particularité est proposée par PPP : Ici on peut demander en supplément une protection spéciale pour ce protocole selon PAP (PPassword Authentication Protocol), CHAP (CChallenge Handshake Authentication Protocol) ou MS-CHAP (variante Microsoft du CHAP). 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, CHAP ou MS-CHAP si vous voulez accéder vous-même par 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 ?

Si le protocole ELSA est utilisé pour le canal B, l'identification ne portera que sur le nom, sans mot de passe. Le nom sera le nom du périphérique du routeur 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 routeur *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).

4.2.2

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.

En modifiant les réglages dans la liste des noms et des numéros ainsi qu'en sélectionnant le protocole (ELSA ou PPP) vous pourrez déterminer la réaction de votre routeur pour les rappels :

- 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 unités de taxation 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.

FR

4.2.3

La cachette – masquerading IP (NAT, PAT)

Aujourd'hui, l'une des tâches les plus fréquentes des routeurs est la connexion d'un grand nombre de postes de travail dans un LAN au réseau des réseaux, l'Internet. Chacun doit, dans la mesure du possible, avoir la possibilité d'accéder à partir de son poste de travail au WWW et pouvoir y chercher les informations actuelles pour son travail.

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 de poste de travail 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. L'adresse IP peut être attribuée de manière fixe, ou être attribuée de façon dynamique par le fournisseur d'accès. Les ordinateurs dans le LAN se servent alors du routeur comme d'un passerelle et ne peuvent pas être reconnus eux-mêmes. Le routeur sépare Internet et Intranet comme par un mur. On désigne donc masquerading IP comme une « technique de coupe-feu » (firewall).

L'utilisation du masquerading IP est fixée séparément pour chaque route dans le tableau de routage. 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/IP-router-module/IP-routing-table.

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

4.3

Gestion des unités de taxation

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 naviguant sans cesse sur Internet) peuvent occasionner des frais de téléphone élevés.

Pour limiter ces coûts, le logiciel offre différentes possibilités :

- Les unités de taxation pour la connexion RNIS peuvent être limitées pour une période déterminée.
- Les unités de taxation pour la connexion RNIS peuvent être limitées pour une période déterminée.

4.3.1 Limitation des communications RNIS en fonction des unités de taxation

Si les informations de taxation sont transmises à un accès RNIS les coûts de connexion peuvent être limités de façon très simple. La configuration par défaut permet p. ex. d'utiliser au maximum 830 unités de taxation en six jours. Dès que cette limite est atteinte, le routeur interdit tout établissement actif d'une connexion.



*Vous pouvez profiter au mieux de la surveillance des unités de taxation du routeur après activation des « unités de taxation **durant** la connexion » dans le réseau RNIS (selon AOCD). Demandez le cas échéant l'activation de cette caractéristique auprès de votre opérateur. Une surveillance des unités de taxation avec la caractéristique « Unités de taxation **après** la liaison » est en principe aussi possible, mais il se pourrait que les communications permanentes ne soient pas reconnues !*



Si vous avez mis le Least Cost Routing en service pour les modules routeur, des communications pourraient être établies via des fournisseurs d'accès ne transmettant pas d'informations de facturation !

4.3.2 Limitation des communications RNIS en fonction de la durée

Le mécanisme de surveillance des coûts ne fonctionne pas s'il n'y a pas d'informations de taxation qui sont transmises à l'accès RNIS. Tel est bien le cas par ex. si la transmission de ces informations n'a pas été demandée, ou si la société téléphonique ne transmet en aucun cas les informations en question.



Afin de pouvoir limiter les coûts des connexions même quand il n'y a pas d'informations de taxation, on peut contrôler le temps de connexion maximale à l'aide de la durée de connexion. Pour ce faire, on fixe un budget en fonction du temps pour une période déterminée. La connexion par défaut p. ex. permet d'établir des connexions actives pendant 210 minutes au maximum en l'espace de six jours.

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.

La protection unités ou durées ne vaut que pour les fonctions de routage ! En revanche, les connexions via LANCAPAPI ou les ports a/b ne sont pas concernés.



4.3.3

Configuration dans le gestionnaire des coûts

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`.

Ce gestionnaire des coûts de communication vous permet d'effectuer tous les paramétrages nécessaires portant sur les durées de connexion et sur le contrôle des unités de taxation.

- Période
Durée d'une période de surveillance spécifiée en jours
- Unités de budget, budget de minutes RNIS
Nombre maximal d'unités RNIS ou de minutes RNIS en ligne pour une période de surveillance
- Budget restant, minutes RNIS restantes
Unités RNIS disponibles ou minutes RNIS en ligne pour la période actuelle

- Unités du routeur, minutes RNIS du routeur
Unités RNIS ou minutes RNIS en ligne sur l'ensemble des périodes
- Nombre total d'unités
Toutes les unités de taxation générées par le périphérique
- Tableau du budget, Tableau des durées
Tableaux contenant les unités de taxation ou les durées pour chaque module



Les informations relatives aux unités et aux durées de connexion sont sauvegardées lors d'une procédure de lancement (par ex. lors de l'installation d'un nouveau micro-logiciel) et ne disparaissent que lorsque le périphérique est éteint. Toutes les indications de durée reportées ici sont exprimées en minutes.

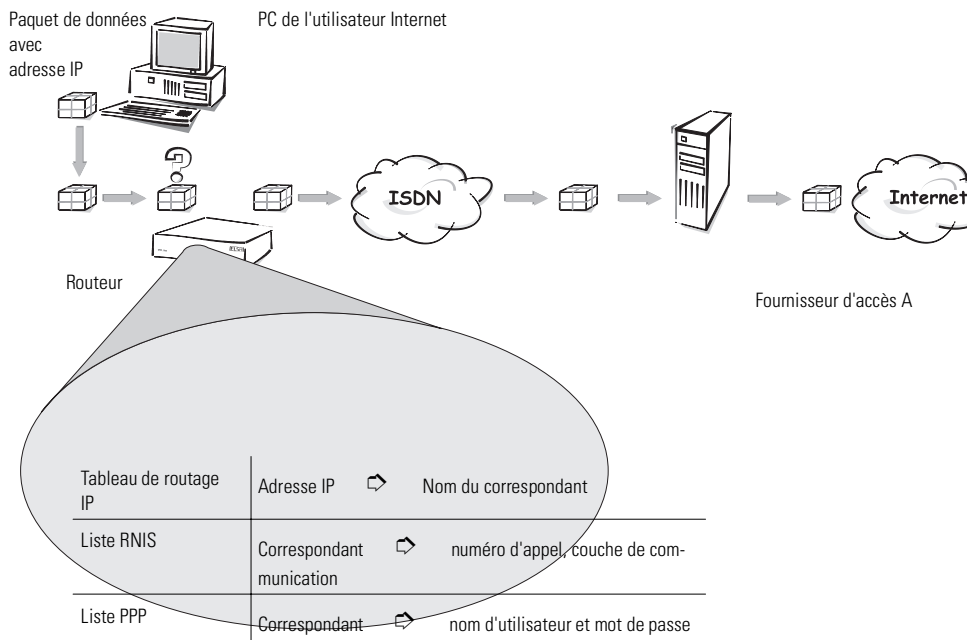
4.4

Connexions 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 qui permettent d'établir les connexions requises.

Nous allons expliquer cette procédure à l'aide d'un exemple simplifié.



Un paquet de données en provenance d'un ordinateur trouve en premier lieu sa voie vers Internet via l'adresse IP du destinataire. Avec cette adresse l'ordinateur envoie le paquet au routeur via le réseau local. A l'aide de l'adresse IP le routeur regarde tout d'abord dans le tableau de routage IP et trouve le correspondant qui correspond à cette adresse, le 'fournisseur_d'accès_A' p. ex. A l'aide de ce nom il contrôle la liste RNIS des noms et trouve le numéro d'appel du correspondant, qui peut être joint via le réseau RNIS, y compris la couche de communication qui doit être utilisée. Par ailleurs le routeur obtient à partir de la liste PPP le nom d'utilisateur et le mot de passe qui sont nécessaires pour établir la communication avec le fournisseur d'accès A.

Le routeur peut alors établir sur la ligne RNIS une connexion avec le routeur du fournisseur d'accès. Dès que la connexion est établie, le routeur peut transmettre le paquet de données à Internet via la ligne RNIS.

Vous trouverez des informations supplémentaires sur les réseaux IP, etc., dans les bases techniques de la documentation électronique sur le CD.

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

La liste PPP sera décrite dans un chapitre spécial (voir liste 'PPP').

Vous trouverez des informations sur le tableau de routage IP dans le paragraphe 'Routage IP'.

4.4.1

Liste RNIS 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 RNIS`.

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 canaux 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 le rappel du correspondant

4.4.2 Configuration des interfaces

Vous trouverez la configuration des interfaces dans *ELSA LANconfig* dans la zone de configuration 'Gestion' sur l'onglet 'Interfaces' ou pour les sessions 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 routeurs. En particulier, il s'agit des paramètres suivants :

- Protocole de canal D utilisé pour l'accès S_0 considéré
Automatique, DSS1 (Euro-ISDN), DSS1 Point à point, 1TR6 (RNIS allemand), Liaison permanente GRPO
- Canal de liaison permanente
Canal B à utiliser éventuellement pour la liaison permanente
- Préfixe du numéro
Préfixe du numéro d'appel des appels sortants, par ex. le numéro du standard dans les entreprises.

4.4.3 Configuration des Interfaces du routeur

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

- Numéro d'appel (MSN)

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.

- Autoriser plusieurs connexions simultanées

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

- Inhiber l'affichage de mon numéro chez le correspondant

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.

4.4.4 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 :

- Numéro d'appel (MSN)
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 l'interface *LANCAPi*
 Vous pouvez désactiver ici les fonctions de *LANCAPi*, les limiter aux appels sortants, ou les activer pour les appels sortants et 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.

4.4.5 Couche communication

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 de 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.

4.4.6

Liste round-robin

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 round-robin`.

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.

- Correspondant
Nom du correspondant tel qu'il a été indiqué 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 avec :
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.

4.4.7 Liste des scripts

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.

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

4.4.8 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.
- par 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).

- par nom ou numéro

L'appel est accepté si l'une des deux vérifications aboutit.

4.4.9

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 quand le routeur prend des appels 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).

- Correspondant

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.

4.5

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, qui permet de router les paquets de données des adresses inaccessibles localement.

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

Dans un tel cas de figure, DHCP (Dynamic Host Configuration Protocol) est la réponse la mieux adaptée. Ce protocole permet à un serveur DHCP dans un réseau local basé TCP/IP d'attribuer dynamiquement les adresses nécessaires aux différentes stations.

4.5.1 Le serveur DHCP

ELSA LANCOM Office peut gérer les adresses IP en tant que serveur DHCP dans son réseau TCP/IP. Pour ce, il communique aux ordinateurs 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.

4.5.2 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 cet état, le périphérique cherche d'autres serveurs DHCP après la mise en service

dans le réseau local. Cette recherche est reconnaissable au bref clignotement de la DEL Tx après la mise en service.

- Si au moins un autre serveur DHCP est détecté, le périphérique déconnecte son propre serveur DHCP. Ceci a pour effet d'éviter, entre autres, qu'un périphérique non configuré une fois activé attribue des adresses dans le réseau qui ne se trouvent pas dans le réseau local.
- Si aucun autre serveur DHCP n'est détecté, le périphérique active son propre serveur DHCP.

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

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

4.5.3

Attribution des adresses

Attribution d'adresses IP

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

- L'adresse IP peut être extraite à partir du pool d'adresses (pool d'adresses de départ – pool d'adresses d'arrivée). Ici, des adresses quelconques valables dans le réseau local peuvent être entrées.
- Si '0.0.0.0' est entré à la place, le serveur DHCP déduit par lui-même les adresses respectives (départ ou arrivée) à partir des configurations de l'adresse IP ou de l'adresse Intranet dans le 'module TCP/IP'. La procédure se déroule comme suit :
 - Si uniquement l'adresse IP ou l'adresse Intranet est entrée, le départ ou l'arrivée du pool est déterminé à l'aide du masque de réseau correspondant.
 - Si les deux adresses sont indiquées, l'adresse Intranet a alors la priorité pour la détermination du pool.

A partir de l'adresse utilisée (adresse IP ou Intranet) et du masque de réseau associé, le serveur DHCP calcule la première et la dernière adresse IP possible dans le réseau local comme adresse de départ ou adresse d'arrivée du pool d'adresses.

- Si le routeur n'a ni une propre adresse IP ni une adresse Intranet, le périphérique se trouve dans un état de service particulier. Il utilise alors lui-même l'adresse IP '10.0.0.254' et le pool d'adresses '10.x.x.x' pour l'attribution 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'attribution d'une adresse. Une adresse valable issue du pool est choisie comme adresse IP. Si une adresse IP a déjà été attribuée 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 attribuée 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. L'ordre est le même que pour l'attribution d'adresses.

Attribution de l'adresse de diffusion

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

Seuls des spécialistes de réseau expérimentés devraient procéder à la modification de la préconfiguration de l'adresse de diffusion. Une configuration erronée dans cette zone peut entraîner des établissements de connexion non désirés et payants !

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 attribution

Les adresses attribuées à l'ordinateur ne sont valides que pour une certaine durée. Une fois cette période écoulée, l'ordinateur ne doit plus les utiliser. Afin de ne pas perdre les adresses (en particulier ses adresses IP), l'ordinateur demande, suffisamment à temps, une prolongation qui lui est normalement accordée. Ce n'est que 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, 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 – Demande d'attribution

De manière standard, la presque totalité des paramètres dans le voisinage réseau de Windows sont définis de manière que les paramètres nécessaires

soient demandés par le DHCP. Vérifiez les paramètres en cliquant sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau**. Sélectionnez l'entrée pour 'TCP/IP' au niveau de votre adaptateur de réseau et ouvrez les **Propriétés**.

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

Sur l'onglet 'Configuration WINS', l'option 'Utiliser DHCP pour la résolution WINS' doit être activée lorsqu'on veut utiliser les réseaux Windows par IP avec résolution du nom par le serveur NBNS. Le serveur DHCP doit en outre avoir une entrée NBNS dans ce cas.

Priorité pour l'ordinateur au poste de travail – Écraser l'attribution

Si un ordinateur utilise d'autres paramètres que ceux qui lui sont attribués, (une autre passerelle par défaut p. ex.), ces paramètres doivent être réglés directement sur l'ordinateur du 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 du voisinage réseau.

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

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

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

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

- new

L'ordinateur au poste de travail a fait une première demande. Le serveur DHCP vérifie si l'adresse 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.

4.5.4

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. Si vous raccordez l'appareil à un concentrateur, le commutateur nœud/concentrateur doit être en position 'nœud'. En revanche, si vous connectez directement le routeur sur la carte réseau d'un ordinateur du réseau, le commutateur nœud/concentrateur doit se trouver en position 'Hub'.
- ② Mettez le routeur sous tension. Le routeur ne trouve pour commencer aucun autre serveur DHCP sur le réseau et active ses propres fonctions DHCP.
- ③ Si rien ne se produit, installez le protocole 'TCP/IP' sur tous les ordinateurs du réseau local.

- Lors de l'installation du protocole, les ordinateurs sont généralement réglés de manière standard de façon à aller chercher automatiquement l'adresse IP sur un serveur DHCP. Suite à un redémarrage dans le cadre de cette installation, les ordinateurs font automatiquement une demande d'adresse IP auprès du serveur DHCP.
- Si vous avez déjà installé le protocole, activez la fonction DHCP sur tous les ordinateurs sur le réseau local. Sous Windows 95 par ex., ouvrez pour cela la fenêtre de configuration des propriétés du réseau en cliquant sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau**. Double-cliquez sur l'entrée pour protocole 'TCP/IP'. Activez l'option 'Obtenir automatiquement une adresse IP'. Passez à l'onglet 'Configuration DNS' et effacez toutes les adresses DNS existantes. Effacez ensuite sur l'onglet 'Passerelle' toutes les entrées éventuelles, puis fermez toutes les fenêtres avec **OK**. Après un redémarrage dans le cadre de ce paramétrage, les ordinateurs font automatiquement une demande d'adresse IP auprès du pool d'adresses du serveur DHCP.



- ④ Installez *ELSA LANconfig* sur l'un des ordinateurs du réseau.
- ⑤ Démarrez le programme dans le groupe de programmes 'ELSAIan'. Au démarrage, *ELSA LANconfig* remarque qu'il y a un routeur non configuré sur le réseau et démarre l'assistant de paramétrage par défaut.
 - Si vous n'avez encore utilisé aucune adresse IP sur votre réseau, sélectionnez dans cet assistant l'option 'Effectuer tous les réglages automatiquement', puis confirmez dans la fenêtre suivante avec le bouton **Terminer**.

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 de forme de messages diffusés, un serveur DNS, une passerelle par défaut etc.

Configuration manuelle

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

4.6

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.com'. 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.

4.6.1

Que fait un serveur DNS ?

Les noms demandés au serveur DNS se composent de plusieurs parties : une partie est le nom propre du 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'.

Sans serveur DNS dans le réseau local, chaque nom inconnu au niveau local est recherché 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 qui se trouve dans le réseau. Les raisons suivantes, cependant, nous amènent à envisager une implantation du serveur DNS directement dans le routeur *ELSA LANCOM Office* :

- Un routeur *ELSA LANCOM Office* faisant fonction de serveur DHCP est en mesure d'affecter les adresses IP aux ordinateurs au sein du réseau local de façon autonome. Le serveur DHCP connaît donc déjà tous les ordinateurs de son propre réseau, qui reçoivent leur adresse IP via DHCP, par leur nom d'ordinateur et par leur adresse IP. 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 Office* connaît les noms d'ordinateur et les adresses IP au sein des autres réseaux NetBIOS connectés. Les ordinateurs avec adresse IP fixe, en outre, du fait qu'ils s'identifient sur le tableau NetBIOS, sont connus par leurs noms et leurs adresses.
- Le serveur DNS dans le routeur *ELSA LANCOM Office* peut être utilisé en même temps comme mécanisme filtrant très confortable. 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 en 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.

4.6.2

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/DNS-module/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/DNS-module/domain yourdomain.com
```

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

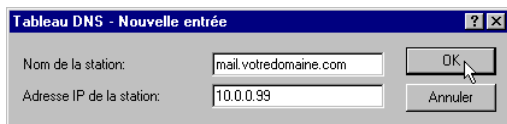
```
set setup/DNS-module/dhcp-usage yes
```

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



- ④ Le serveur DNS sert avant tout à séparer les requêtes relatives à des noms sur Internet d'avec les 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,
 - qui ne font pas partie de votre réseau local,
 - qui ne se trouvent pas sur Internet, et
 - qui sont 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.yourdomain.com, IP : 10.0.0.99) via le routeur, entrez :



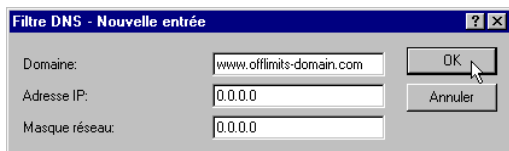
```
cd setup/DNS-module/DNS-table
```

```
set mail.yourdomain.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/DNS-module/Filter-list
```

```
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 COM, entrez :

```
set 002 *.COM 10.0.0.123 255.255.255.255
```



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

Choissant bien les adresses IP et les masques de réseau, vous pouvez filtrer également 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.

4.7

Proxy NetBIOS

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



Cette fonction n'est à votre disposition que sur les modèles ELSA LANCOM 2000 Office, ELSA LANCOM 1100 Office et ELSA LANCOM 1000 Office.

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.

4.7.1

En quelques mots : définition de NetBIOS

NetBIOS sert à interconnecter plusieurs ordinateurs simplement et sans complication. Un représentant courant des réseaux NetBIOS est le réseau Windows dans lequel plusieurs ordinateurs Windows 3.11, 9x et 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 par 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 noir » sur lequel tous les ordinateurs inscrivent uniquement leur nom et leur adresse IP. Dans ce cas, les ordinateurs sont eux-mêmes responsables pour la cohérence des noms dans le réseau.

Un *ELSA LANCOM Office* dispose d'un tel « tableau noir ». 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 noir de ce réseau.

4.7.2 Traitement des paquets NetBIOS

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

Dans le but d'éviter ces connexions inutiles, un *ELSA LANCOM Office* 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 noir 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 noir) 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 DEFALT dans Internet, le filtre IP préconfiguré pour les ports NetBIOS intercepte ces paquets et empêche l'établissement de la connexion.

4.7.3 Quelles conditions doivent être satisfaites ?

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 routable, par ex. sur IP dans ELSA LANCOM Office!

Le routage des paquets NetBIOS dans *ELSA LANCOM Office* 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' en guise de 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' en guise de constructeur, puis 'Client pour les réseaux Microsoft'.

- Service

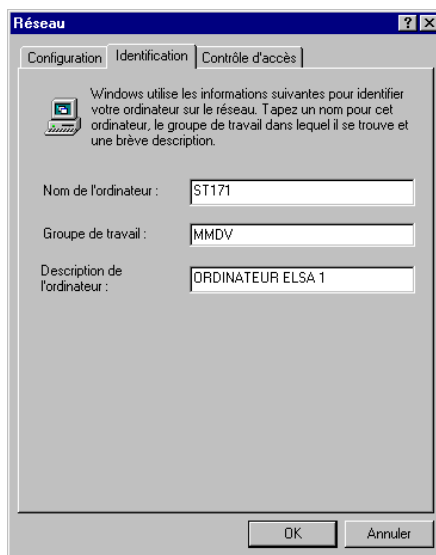
Le partage de fichiers et d'imprimantes permet à d'autres utilisateurs d'utiliser les lecteurs et les imprimantes du réseau Microsoft.

Pour installer le partage de fichiers et d'imprimantes, cliquez sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau ► Ajouter ► Service**. Sélectionnez 'Microsoft' en guise de constructeur, puis 'Fichier et imprimante partagés pour les réseaux Microsoft'.

Paramétrages dans le réseau Windows

- Noms et désignation des groupes

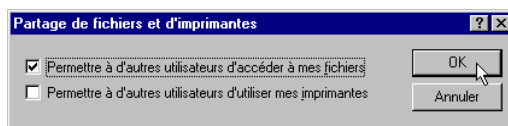
Cliquez sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau**, et sélectionnez l'onglet 'Identification'.



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.

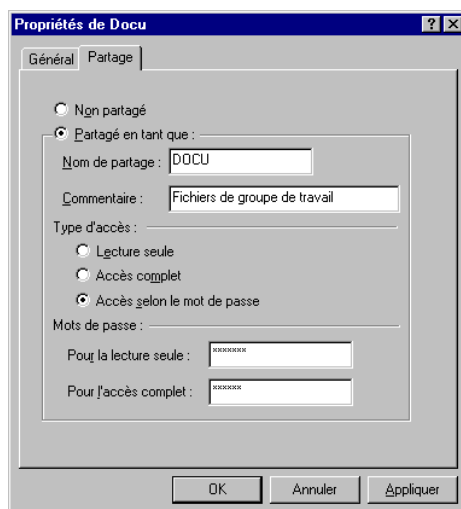
- Partage de fichiers et d'imprimantes

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**. Sélectionnez si les autres utilisateurs dans le réseau Windows peuvent 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 le voisinage réseau.

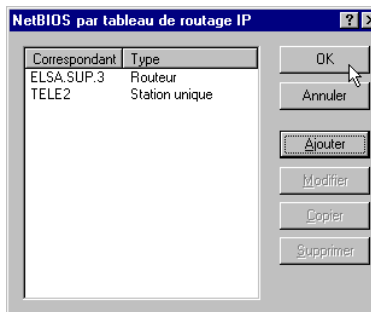
4.7.4 Interconnecter deux réseaux Windows

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 l'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 DEFAULT afin que les paquets NetBIOS ne conduisent pas à l'établissement d'une connexion via la route par DEFAULT. Ce filtre est préconfiguré de cette façon au départ usine des périphériques.

Filtre pour le réseau local						
Du port dest.	Au port dest.	Du port src.	Au port src.	Adresse IP	Masque de réseau	Protocole
0	0	137	139	255.255.255.255	0.0.0.0	tous

- 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 par tableau de routage IP'.



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

```
cd /Setup/NetBIOS-Modul/Gegenstellen-Tab.  
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 et/ou 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 Activez la fonction NetBIOS une fois que tous les correspondants sont saisis.

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

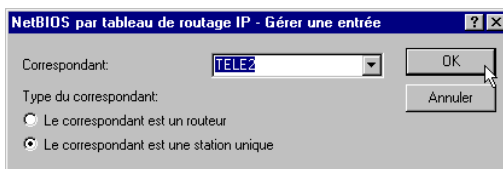
Après la mise sous tension, une connexion est établie (après un délai d'attente aléatoire) avec tous les correspondants qui ne sont pas mis en évidence comme nœud d'accès. Les informations nécessaires sur les ordinateurs dans les réseaux sont échangées lors de cette première connexion. Ce n'est qu'après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



4.7.5 Accès par les ordinateurs distants

L'accès par un ordinateur distant à un réseau Windows via un accès à distance est également configuré rapidement.

- ① *ELSA LANCOM Office* 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 Office* (voir 'Interconnecter deux réseaux Windows').
- 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 pour les correspondants distants également dans le tableau de routage IP NetBIOS.



```
cd /Setup/NetBIOS-Modul/Gegenstellen-Tab.  
set nhamel.ras workstation
```



Mettez cette entrée en évidence en tant que 'station isolée' pour que ce correspondant ne soit pas appelé automatiquement après que le module NetBIOS ait été activé.

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

4.7.6 Qui cherche trouve : le Voisinage réseau

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

Routage NetBIOS via le couplage LAN-LAN

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*

Office. Via Telnet, on peut consulter la liste des ordinateurs accessibles actuellement en sélectionnant

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

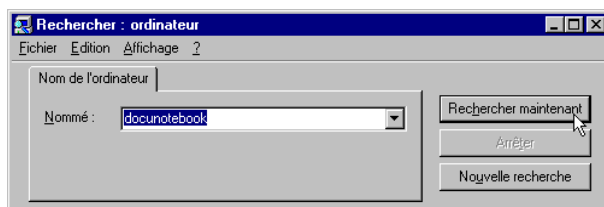
Cette liste a par ex. l'aspect suivant :

Nom	Type	Adresse IP	Correspondant	Timeout	Flags
DOCUNOTEBOOK	00	10.10.0.53	NHAMEL.MOBIL	4939	0020
DOCUNOTEBOOK	20 seco ndes	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	192.168.100.1 62	4997	0000	
NHAMEL.MOBIL	00	10.10.0.1	NHAMEL.MOBIL	0	0020

Par 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**

► **Rechercher** ► **Ordinateur**.



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

Routage NetBIOS via accès RAS

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

- Il n'existe pas, du côté du nœud d'accès, une liste des hôtes qui permette 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 Office* au moyen de l'Accès réseau à distance.

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

4.8 Le rerouteur téléphonique (least-cost router)

Depuis la libéralisation du marché téléphonique en Europe, les utilisateurs des services de télécommunication ont le choix, à part l'opérateur institutionnel, entre une série de provider (opérateurs réseaux privés qui se distinguent par des tarifs en partie 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 (préselection). Pour router un appel via un opérateur alternatif, on compose d'abord le préfixe pour accéder dans le réseau correspondant et on ne compose le numéro de téléphone du correspondant appelé qu'après ce numéro de code de réseau.

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. *ELSA LANCOM Office* 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.

Le rerouteur téléphonique (least-cost router) dans le *ELSA LANCOM* travaille de la façon suivante

Le rerouteur téléphonique analyse les numéros composés par ex. par le routeur ou l'interface *LANCAPi*. Dans le cas du *ELSA LANCOM 2000 Office*, les chiffres composés sur un terminal raccordé (par ex. un téléphone ou un télécopieur) sont pris en compte.

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 d'opérateur privé est ajouté devant le numéro (avant l'indicatif) du correspondant. Ce n'est que 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 par ex. que le reroutage permet d'économiser en particulier sur les appels longue distance et sur les appels internationaux avec call-by-call. Une situation similaire s'applique aux communications avec des téléphones mobiles. Vous vous êtes renseignés 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 par 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
06	1603	tous les jours	0:00h à 23:59h
00	1601	Di	0:00h à 23:59h

Ces quatre entrées signifient que toutes les communications vers l'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. Les appels dans le réseau mobile, donc d'un numéro commençant par 06, sont réacheminés via l'opérateur avec le préfixe 1603. 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 Office*. Vous devrez faire preuve d'une certaine méthodologie :
- Vous pouvez saisir directement les préfixes uniques qui ne risquent pas d'être confondus :
 - Préfixes pour les réseaux de radiotéléphonie
 - '00' pour les communications internationales
- Il serait très simple de rerouter tous les appels qui commencent 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

rou tage. 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 rapprochés, 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. Une entrée vierge signifie également « pas de reroutage ».
- Éventuellement, la plupart de vos connexions RNIS sont 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.
- Étudiez les diverses zones tarifaires.

Une fois que vous avez déterminé les préfixes à rerouter, vous pourrez choisir l'opérateur. Vous aurez bien sûr besoin de tous leurs tarifs à jour. Là aussi, Internet peut vous aider à trouver ces tarifs. Une fois que vous aurez ces informations, 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 Office* 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 :

- ☐ Routeur
- ☐ Ports A/N (uniquement *ELSA LANCOM 2000 Office*)
- ☐ LANCAPI

Si vous avez activé le Least Cost Routing également pour les modules de routage, des connexions seront éventuellement établies via des routeurs qui ne transmettent 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. Au besoin, utilisez dans ce cas les budgets-durées.

- ③ Sélectionnez l'onglet 'Plages horaires et jours fériés'. Ouvrez la **Table 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 ! Par 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 (par ex. France Télécom) lorsque tous les opérateurs alternatifs sont débordés. 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).

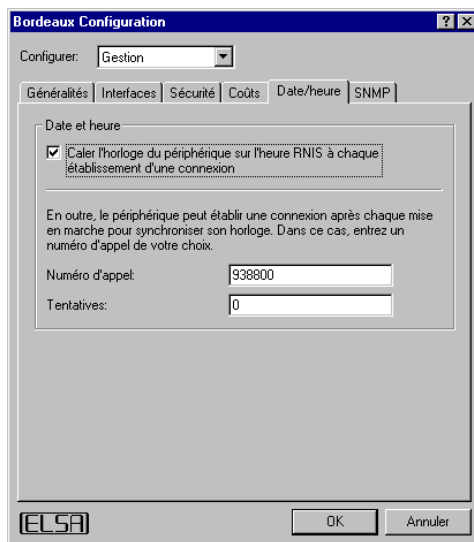
*Élargissez votre tableau de routage étape par étape, et vérifiez le résultat de chaque entrée. A cet effet, exécutez par ex. ELSA LANmonitor et établissez – via ELSA LANCAP – les connexions avec les correspondants dans le tableau de reroutage. Vous pourrez consulter à l'aide du numéro composé si l'entrée 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 Office* 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 (par ex. un babillard ou un FAI) ou analogique (horloge téléphonique ou service vocal).



Contrôlez l'heure après la première connexion. Certaines régions téléphoniques transmettent au routeur des informations incorrectes qui entraînent des erreurs de reroutage !

4.9

ELSA CAPI Faxmodem

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 standard en liaison avec un routeur *ELSA LANCOM Office*.

4.9.1 Installation

ELSA CAPI Faxmodem est proposé sur le CD d'installation. Installez *ELSA CAPI Faxmodem* toujours avec la version actuelle d'*ELSA LANCAPI*. Après le redémarrage, *ELSA CAPI Faxmodem* est disponible dans le système, par ex. sous Windows 95 ou Windows 98 via **Démarrer ► Panneau de configuration ► Modems**.

4.9.2 Transmettre des télécopies via *ELSA CAPI Faxmodem*

Le fax-modem *ELSA CAPI Faxmodem* est détecté automatiquement par les logiciels de télécopie courants lors de l'installation et identifié en tant que fax-modem de la 'Classe 1'. Vous pourrez ainsi envoyer des télécopies jusqu'à 14.400 bps. Au cas où votre programme de télécopie permettrait de différencier (par ex. WinFax ou Talkworks Pro), sélectionnez, lors de la configuration du modem, l'option 'CLASSE 1 (contrôle de flux logiciel)'.



ELSA CAPI Faxmodem n'est prêt à transmettre des télécopies que si ELSA LANCAPI est actif, ce que vous reconnaîtrez par ex. au petit symbole CAPI en bas à droite sur l'écran. Veuillez observer également les réglages du pilote LANCAPI lui-même.

4.10 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.

4.10.1 *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

télécopieur, 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.

Par ex., dans le cas de l'envoi de télécopies, un télécopieur 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.

Installation du client *LANCAPI*

L'interface *LANCAPI* est formée par deux composants, un serveur (dans le *ELSA LANCOM Office*) et un client (sur les PC). Le client *LANCAPI* est installé sur les ordinateurs du réseau local qui souhaitent utiliser les fonctions de l'interface *LANCAPI*.

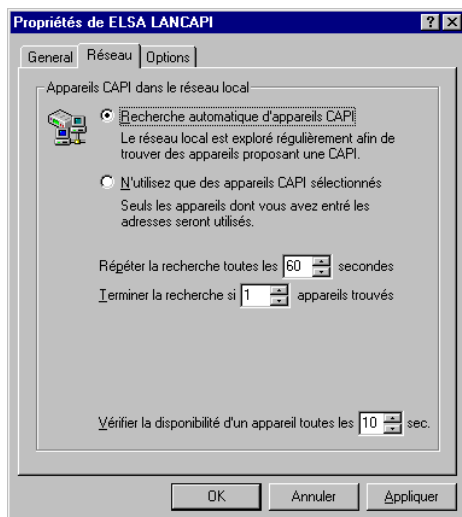
- ① Introduisez le CD-ROM *ELSA LANCOM* dans le lecteur approprié. Lorsque le logiciel d'installation n'est pas exécuté automatiquement quand vous insérez le CD-ROM, ouvrez l'explorateur Windows et cliquez sur 'autorun.exe' se trouvant sur le CD *ELSA LANCOM*.
- ② Sélectionnez 'Installation du logiciel 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 l'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 quels serveurs *LANCAPI* doivent être utilisés par les clients, et de sélectionner la méthode de contrôle. Si vous n'exploitez qu'un seul *ELSA LANCOM Office* dans votre réseau local en guise de 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 'ELSAAn'. Vous trouverez les informations sur le pilote du service mis à disposition dans l'onglet 'Généralités'.
- 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 les serveurs automatiquement, spécifiez dans la liste l'adresse IP des serveurs que le client doit utiliser. L'indication de ces adresses est judicieuse par ex. lorsque vous exploitez plusieurs *ELSA LANCOM Office* 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.



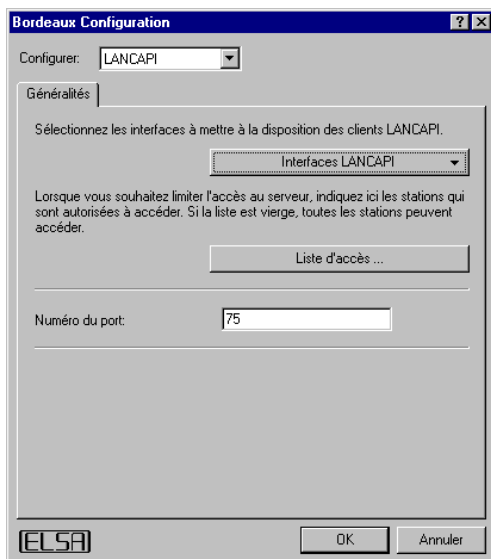
Configuration du serveur *LANCAPI*

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

- A quels numéros d'appel l'interface *LANCAPI* doit-elle réagir ?
- Lequel des ordinateurs du réseau local doit-il 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 'ELSAlan'. 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 *LANCAPI*, ou autorisez uniquement les appels sortants. Dans le deuxième cas, l'interface *LANCAPI* ne réagit pas aux appels entrants et ne peut pas être mis en œuvre par ex. pour la réception de télécopies. Par ex., autorisez uniquement les appels sortants lorsque vous avez déjà attribué tous les numéros d'appel disponibles aux autres appareils de télécommunication.
- ③ Quand le serveur *LANCAPI* est actif, entrez dans le champ 'Numéro d'appel' les numéros de téléphone auxquels *LANCAPI* doit réagir.

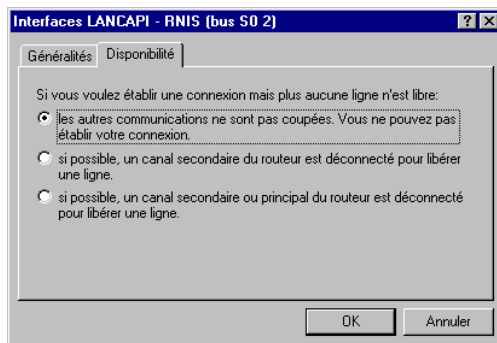
Séparez les numéros par un point-virgule. Pour que *LANCAPi* accepte tous les appels entrants, laissez ce champ vierge.

- ④ Par défaut, le port utilisé par *LANCAPi* 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 *LANCAPi*, spécifiez dans la liste d'accès l'adresse IP des participants autorisés.



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

Sélectionnez l'onglet 'Disponibilité'. Indiquez comment *ELSA LANCOM Office* se comporte lorsqu'une connexion doit être établie via *LANCAPi* (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 *LANCAPi*. Un logiciel de télécopie qui utilise *LANCAPi* fera vraisemblablement une deuxième tentative d'envoi ultérieurement.
- La connexion via *LANCAPi* 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. Lorsque le routeur

établit deux connexions distinctes avec deux correspondants (deux canaux principaux sont occupés), l'interface *LANCAPI* doit attendre.

- La connexion via *LANCAPI* peut toujours être établie, une connexion du routeur sera coupée le cas échéant pour la durée de la communication. Ainsi, la fonction télécopie est toujours accessible.

Utilisation de *LANCAPI*

Vous avez deux possibilités d'utiliser *LANCAPI* :

- Vous utilisez un logiciel qui accède directement à une interface CAPI (dans ce cas : *LANCAPI*), par 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, par 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 *LANCAPI*, sélectionnez 'ISDN WAN Line 1'.

4.11 La régie téléphonique intégrée

Lorsqu'on migre d'un accès analogique (RTC) à un accès numérique (RNIS/Numéris), on se demande souvent si on peut continuer d'utiliser ses anciens appareils. Quatre ports A/N intégrés dans le *ELSA LANCOM 2000 Office* permettent de raccorder téléphone, télécopieur, répondeur ou modem analogiques.

Les terminaux analogiques ne seront donc pas mis au rebut après la migration. On n'aura pas besoin d'acheter les nouveaux appareils numériques. Par ailleurs, les ports A/N du routeur *ELSA LANCOM 2000 Office* permettent d'utiliser les compléments de service du RNIS tels que le renvoi de poste, le double appel, le va-et-vient, ou la conférence à trois.

Les terminaux raccordés aux ports A/N peuvent utiliser les fonctions d'une petite régie téléphonique : vous pourrez, par exemple, faire des appels internes, transférer un appel externe vers un autre appareil ou aller et venir entre un appel externe et un appel interne.

Dans ce contexte, veillez également aux fonctions du least-cost router (fonction de reroutage téléphonique) !



Les fonctions de standard ne sont disponibles que sur ELSA LANCOM 2000 Office !

4.11.1

Raccordement des terminaux analogiques

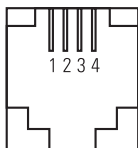
Terminaux pouvant être raccordés

Vous pouvez en principe raccorder aux ports A/N du *ELSA LANCOM 2000 Office* tout terminal analogique :

- Téléphones
- Télécopieurs Groupe 3
- Répondeurs automatiques
- Modems
- Appareils tout-en-un

Adaptateur téléphonique (RJ11)

Pour que vous puissiez continuer d'utiliser vos terminaux analogiques, ELSA fournit les adaptateurs requis.



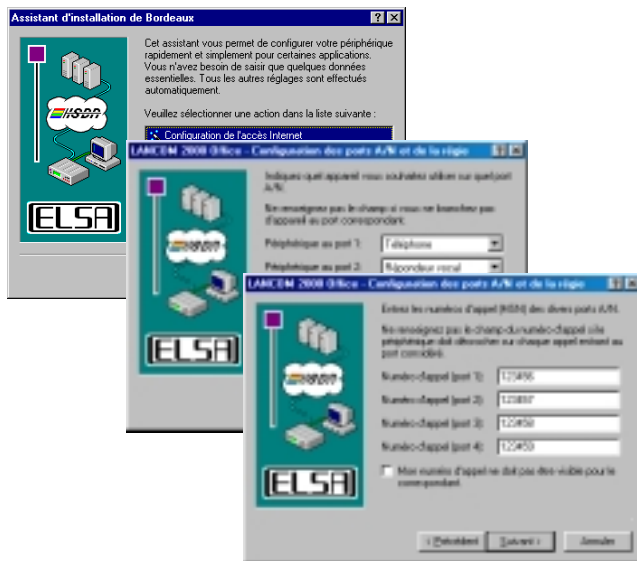
4.11.2

Configuration avec *ELSA LANconfig* et les assistants d'installation

Pour vous faciliter la configuration des ports A/N et de la régie intégrée du *ELSA LANCOM 2000 Office*, *ELSA LANconfig* vous permet d'exécuter un assistant qui modifiera à votre place la configuration du *ELSA LANCOM*. En principe, il vous suffit d'indiquer quel type de terminal est raccordé à quel port et d'affecter à chaque port un numéro d'appel.

- ① Exécutez *ELSA LANconfig* se trouvant dans le groupe de programmes 'ELSAIan'.

- ② Dans la liste des périphériques, sélectionnez le *ELSA LANCOM* à configurer. Cliquez sur **Options ► Assistant de configuration**, et sélectionnez la commande 'Configuration des ports A/N et de la régie ».



- ③ Indiquez quel terminal est raccordé à quel port, et affectez un numéro d'appel aux ports A/N.
- ④ Indiquez ensuite si vous voulez exploiter le *ELSA LANCOM* comme une régie ou comme un accès téléphonique simple.
- ⑤ Voilà, c'est déjà fini ! Cliquez sur **Terminer** dans la fenêtre suivante pour fermer l'assistant et charger la nouvelle configuration dans le *ELSA LANCOM*.

Qu'a donc fait l'assistant pour vous ? Le résultat est différent selon le terminal configuré sur chaque port. Les particularités, outre le numéro d'appel et les numéros internes invariables, sont les suivantes :

- **Téléphone**

Quand vous configurez un port A/N pour un téléphone, un deuxième appel entrant pendant la communication en cours est présenté par un signal d'appel.

- Répondeurs automatiques

Quand vous configurez un répondeur automatique, un signal d'appel n'est pas généré, mais il vous sera possible de prendre l'appel sur un autre terminal. En d'autres termes, si le répondeur est plus rapide que vous et qu'il restitue déjà son message d'accueil, vous pourrez décrocher l'écouteur d'un autre téléphone et parler avec l'appelant.

- Télécopieur et modem

En ce qui concerne les télécopieurs et les modems, l'assistant désactive les compléments de service décrits, puisque ces terminaux ne supportent pas d'être « dérangés ».

- Prise de ligne

- Quand vous exploitez le *ELSA LANCOM 2000 Office* comme une régie téléphonique, vous serez d'abord relié au routeur *ELSA LANCOM* quand vous décrochez le téléphone. Vous pouvez alors faire un appel interne ou composer le zéro pour avoir la tonalité externe et faire un appel externe.



Lorsque votre ELSA LANCOM 2000 Office est relié à un mini-standard, vous accéderez évidemment à ce mini-standard quand vous composez le zéro et devrez éventuellement composer une deuxième fois le zéro pour avoir la tonalité externe !

Tenez compte aussi du fait que vous devrez par exemple faire précéder les numéros dans votre annuaire et dans les listes de distribution des téléphones, des modems et des autres terminaux par le zéro.

- Quand vous exploitez le *ELSA LANCOM 2000 Office* comme un accès téléphonique normal, vous entendez la tonalité externe immédiatement après avoir décroché le combiné (ou la tonalité du mini-standard auquel le *ELSA LANCOM 2000 Office* est relié). Les appels internes via le *ELSA LANCOM 2000 Office* ne sont pas possibles dans cette configuration !

Si le résultat de la configuration au moyen de l'assistant ne correspond pas à vos souhaits, vous pouvez naturellement modifier la configuration vous-même, comme décrit ci-après.

4.11.3

Configuration manuelle avec *ELSA LANconfig*

Vous pouvez régler manuellement le comportement de chacun des quatre ports A/N pour un appel entrant ou sortant.



Sélectionnez la zone de configuration 'Téléphonie', puis l'onglet 'Ports A/N'. Sélectionnez le pays dans lequel vous utilisez le *ELSA LANCOM 2000 Office*. Indiquez ensuite comment les terminaux doivent réagir quand un appel entrant est destiné à plusieurs d'entre eux : les terminaux peuvent sonner l'un après l'autre, deux par deux ou tous en même temps.

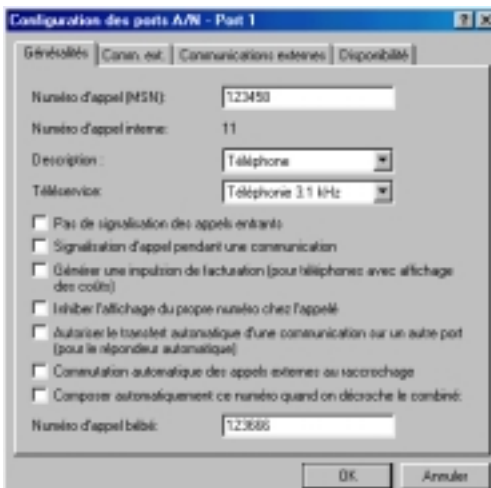
Veillez aussi à la consommation d'électricité élevée en particulier des téléphones d'un certain âge. Quand plusieurs de ces téléphones sonnent en même temps, le bloc d'alimentation du routeur ELSA LANCOM risque d'être surchargé. Dans ces cas, sélectionnez 'isolé' ou 'paire' :



Vous pouvez ouvrir la configuration du port au moyen de la liste déroulante 'Configuration des ports A/N'. Les icônes illustrent quel type de terminal est raccordé à chaque port. Sélectionnez le port dont vous souhaitez modifier la configuration.

Configuration générale

Sur l'onglet 'Généralités', vous saisissez les données suivantes pour chacun des ports A/N utilisés :



- Affectez un numéro d'appel au port : MSN (Multiple Subscriber Number) pour les configurations point-à-multipoint et le protocole DSS1 du canal D, DDI (Direct Dial In) pour les configurations point-à-point et la SDA, ou EAZ pour le protocole 1TR6.
 - Lorsque le port A/N doit réagir à plusieurs numéros d'appel, séparez ces numéros par des point-virgules.
 - Le premier des numéros saisis est affiché sur l'écran du téléphone du correspondant qu'on appelle.
 - Si vous n'entrez pas de numéro d'appel du tout, le port A/N prend tous les appels entrants et vous identifie chez les appelés toujours avec votre numéro d'abonné principal.
- Le numéro d'appel interne est attribué de manière fixe et ne peut pas être modifié :
 - '11' pour le port A/N 1
 - '12' pour le port A/N 2
 - '13' pour le port A/N 3
 - '14' pour le port A/N 4
- Sélectionnez une description du port. Cette description n'a aucune incidence sur les fonctions du port ni du terminal raccordé, elle sert uniquement à identifier rapidement l'utilisation du port. Vous pouvez sélectionner parmi les descriptions suivantes :
 - Pas de description

- Téléphones
- Télécopieurs groupe 3
- Répondeurs automatiques
- Modems
- Appareils tout-en-un
- Sélectionnez le téléservice que le port A/N signale à son correspondant quand il établit une connexion. Ce paramètre ne règle pas la prise des appels entrants par un téléservice donné ! Choisissez l'un des téléservices suivants :
 - Analogique 3,1 kHz (par défaut)
 - Voix
 - Télécopie groupes 2/3
- Suivant les besoins, activez ou désactivez les options suivantes :
 - 'Pas de signalisation...' active ou désactive la sonnerie du terminal raccordé.
 - 'Signalisation d'appel pendant une communication' signale les autres appels pendant une communication (présentation d'appel).
 - 'Générer une impulsion de facturation' : cette fonction génère une impulsion de téléfax sur la base des informations transmises dans le RNIS et envoie cette impulsion au terminal raccordé au port considéré. Ceci permet de contrôler le coût des communications lorsque votre téléphone analogique est équipé pour cette fonction. Désactivez cette option pour les télécopieurs et les modems, car l'impulsion de téléfax risque de perturber la transmission des données.



L'envoi d'impulsions de téléfax ne fonctionne correctement que sur les accès 'AOCD' (transmission des téléfax pendant une communication). Avec la méthode 'AOCE', les téléfax ne sont transmises qu'après le raccrochage, et ainsi le téléphone n'est plus en mesure de compter toutes les impulsions.

- L'option 'Inhiber l'affichage du propre numéro chez l'appelé' empêche que votre numéro soit affiché sur le téléphone du correspondant (non-identification d'appel). Or, le numéro d'appel est toujours transmis à l'autocommutateur public. Par conséquent, l'opérateur pourra toujours ventiler les coûts suivant le numéro d'appel même si la fonction de non-identification d'appel est active.



La non-identification d'appel au cas par cas devra éventuellement faire l'objet d'une demande séparée à l'opérateur.

- 'Autoriser le transfert automatique d'une communication sur un autre port' vous permet de prendre un appel sur un autre port que celui qui a déjà répondu. Cette option n'est en règle générale activée que sur les ports auquel est raccordé un répondeur automatique.
- 'Commutation automatique des appels externes au raccrochage' permet de relier entre eux des appelants externes. Si par exemple vous téléphonez parallèlement avec deux personnes externes, vous pourrez relier vos deux interlocuteurs entre eux simplement en raccrochant le combiné.



De même, la possibilité de relier deux appelants externes entre eux devra faire l'objet d'une demande séparée à l'opérateur.

Songez aussi que vous devrez porter les coûts de communication alors que vous-même ne participez plus à la conversation !

- 'Composer automatiquement ce numéro quand on décroche le combiné' : saisissez le numéro à composer automatiquement quand on décroche le combiné sans composer de numéro. Le numéro enregistré est composé cinq secondes après le décrochage du combiné.

Suivant le modèle du téléphone utilisé, cette fonction de numérotation automatique est configurable directement sur votre téléphone. Dans ce cas, la configuration effectuée dans ELSA LANconfig est écrasée.

Configuration de la prise de ligne

Sélectionnez l'onglet 'Comm. ext.'. Indiquez comment le port A/N doit se comporter quand on décroche le combiné et appuie sur la touche flash (touche R). « Décrocher le combiné » est à prendre au figuré, car un modem ou un télécopieur règle le décrochage d'une autre manière (en émettant un signal).



Trois options vous permettent de choisir le comportement du routeur après le décrochage :

- Quand vous sélectionnez l'option 1, vous établissez une connexion avec le routeur *ELSA LANCOM* après avoir décroché le combiné. Vous pouvez à présent faire un appel interne, donc appeler un terminal raccordé à un autre port A/N. Pour un appel externe, les deux cas suivants se présentent :
 - Quand le routeur *ELSA LANCOM* est relié directement à un accès RNIS, vous pouvez composer le 0 pour faire un appel externe.
 - Si le routeur *ELSA LANCOM* est lui-même relié à un mini-standard, vous devrez éventuellement composer en plus le préfixe du standard pour effectuer des appels externes.
- Dans le cas de l'option 2, vous établissez, quand vous décrochez le combiné, une connexion avec l'accès auquel votre routeur *ELSA LANCOM* est raccordé. Ceci correspond à une liaison interne avec le *ELSA LANCOM* avec numérotation automatique du 0. Vous avez maintenant les possibilités suivantes :
 - Quand le routeur *ELSA LANCOM* est relié directement à l'accès de base, vous pouvez faire un appel externe sans autre préfixe.
 - Si le routeur *ELSA LANCOM* est lui-même relié à un mini-standard, vous devrez éventuellement composer en plus le préfixe du standard pour effectuer des appels externes.

- Dans le cas de l'option 3, vous établissez une ligne via l'accès auquel votre routeur *ELSA LANCOM* est raccordé, c'est-à-dire qu'un 0 est composé automatiquement après la connexion interne avec le *ELSA LANCOM*. En plus, le numéro saisi dans le champ au bas de l'onglet est composé. Cette option vous donne les possibilités suivantes :
 - Lorsque le routeur *ELSA LANCOM* est relié à un standard, le numéro du standard est composé automatiquement et vous pouvez faire des appels externes sans composer de préfixe.
 - Lorsque vous souhaitez faire des appels via un opérateur alternatif proposant le reroutage téléphonique, faites suivre le numéro du standard par le préfixe de cet opérateur (par exemple 16XY). Vous téléphonerez dès lors systématiquement via le réseau de cet opérateur.

Fonction de la touche flash (touche R)

La partie inférieure de l'onglet 'Comm. ext.' vous permet de choisir la fonction de la touche flash.



Sur la plupart des téléphones, la touche flash est la touche R. Sa fonction peut souvent être programmée. Veuillez vérifier la fonction par défaut de cette touche dans le manuel d'utilisation de votre téléphone, et comment vous pouvez la reprogrammer. Le routeur ELSA LANCOM accepte des signaux flash d'une durée comprise entre 70 et 300 ms.

En ce qui concerne l'utilisation de la touche flash, sélectionnez l'une des trois options décrites. Ces options sont comparables à celles qui régissent le comportement après le décrochage du combiné :

- L'option 1 permet d'établir une liaison avec la régie téléphonique interne du routeur *ELSA LANCOM* quand on appuie sur la touche flash. Vous pouvez alors faire un appel interne ou composer le 0 pour faire un appel externe (éventuellement via le standard).
- En activant l'option 2, vous êtes relié directement à l'accès RNIS (ou avec le standard) après avoir appuyé sur la touche flash.
- L'option 3 permet de composer automatiquement le numéro d'appel indiqué quand vous appuyez sur la touche flash.

En combinant les options pour le décrochage du combiné d'une part et pour la fonction de la touche flash d'autre part, vous pouvez adapter la régie téléphonique intégrée dans le *ELSA LANCOM* à vos préférences. Exemples :

- Votre routeur *ELSA LANCOM* est relié directement à un accès RNIS. Activez l'option 2 pour le décrochage et l'option 1 pour la touche flash. Après avoir décroché le combiné, vous pourrez faire un appel externe, ou faire un appel interne en appuyant sur la touche flash.
- Votre routeur *ELSA LANCOM* est relié à un standard de capacité plus importante. Activez l'option 1 pour le décrochage et l'option 3 pour la touche flash. Précisez le numéro du standard à composer pour les appels externes. Après avoir décroché le combiné, vous pourrez faire un appel interne ; une pression sur la touche flash compose automatiquement tous les préfixes introduisant un appel externe.

La touche flash a une signification particulière suivant que vous êtes en train de téléphoner, que la communication est maintenue pendant un va-et-vient, ou que vous êtes en train de numéroté. Le tableau suivant indique ce qui se passe dans les divers cas. En principe, vous pouvez vous baser sur le fait que vous atteindrez intuitivement, en appuyant sur la touche flash, exactement ce que vous voulez faire.

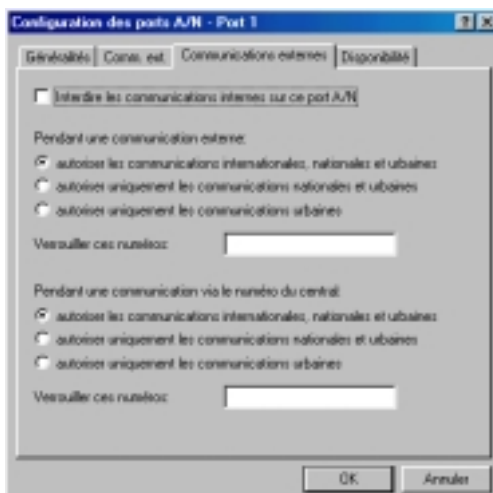
Voici en détail ce qui se passe :

Connexion	Statut	Effet de la touche flash
aucune liaison n'est établie	<ul style="list-style-type: none"> - Tonalité - Numérotation incomplète - Dépassement de délai pendant une numérotation - Le correspondant sonne - Dépassement de délai de la sonnerie 	Interruption de la numérotation/de l'établissement de la connexion, et la fonction configurée est exécutée.
une liaison est établie		La liaison est maintenue, et la fonction configurée est exécutée.

Connexion	Statut	Effet de la touche flash
une liaison est maintenue	- Tonalité	On revient à la communication en attente.
	- Numérotation incomplète - Dépassement de délai pendant une numérotation	Interruption de la numérotation, et la fonction configurée est exécutée.
	- Le correspondant sonne - Dépassement de délai de la sonnerie	Interruption de l'établissement de la connexion, et on revient à la communication en attente.
une liaison est établie, et une communication est maintenue ou un appel est signalé		Flash + 0 : la communication en attente/signalée est coupée. Flash + 1 : la communication en cours est coupée, et la communication en attente/signalée est activée. Flash + 2 : va-et-vient de la communication active à la communication en attente/signalée. Flash + 3 : établissement d'une conférence à trois.
Conférence à trois active		Flash + 2 : la conférence à trois est terminée et séparée en une communication active et une communication en attente.

Définition des droits d'appel

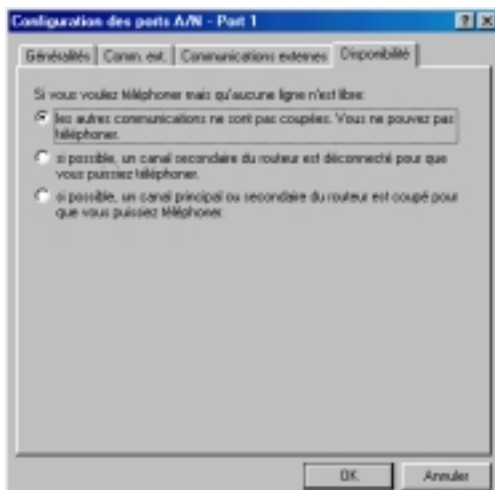
L'onglet 'Communications externes' vous permet d'indiquer pour chaque port A/N si les appels externes sont autorisés avec le terminal relié au port considéré.



Les appels entrants ne sont pas concernés par ces restrictions. Mais les appels externes peuvent être restreints aux communications locales ou nationales. De même, des numéros choisis peuvent être bloqués.

Configuration de la disponibilité

L'onglet 'Disponibilité' vous permet d'indiquer comment le *ELSA LANCOM* se comporte lorsqu'une connexion doit être établie via les ports A/N (appels entrants et sortants) mais que les deux canaux B sont occupés (gestion des priorités). Les options disponibles sont les suivantes :



- Les autres communications ne sont pas coupées. On ne pourra par exemple pas téléphoner quand toutes les lignes sont occupées.
- Une communication via les canaux secondaires peut être coupée, les canaux secondaires étant ceux qui sont par exemple utilisés pour le regroupement des canaux. La connexion via un port A/N peut être établie lorsqu'un canal principal est libre.
- Les communications via les canaux principaux peuvent être coupées. On pourra toujours établir une liaison via le port A/N considéré, et une connexion du routeur sera éventuellement interrompue pendant la durée de la communication. On pourra donc toujours vous joindre au téléphone.

Pour que le ELSA LANCOM 2000 Office puisse identifier les appels entrants même si une communication est en cours, le complément de service « présentation d'appel » doit être activé.

4.11.4 Utilisation de la régie téléphonique avec le téléphone

Le ELSA LANCOM 2000 Office vous permet d'utiliser plusieurs compléments de service pour la téléphonie (par exemple le va-et-vient). Vous avez besoin à cet effet d'un téléphone à numérotation en fréquence vocale (modulation de fréquence, DTMF) et disposant d'une touche R (fonction hook/flash).



Lorsque vous ne savez pas si votre téléphone numérote en fréquence vocale ou en fréquence décimale, décrochez le combiné et composez un numéro : si vous entendez un cliquetis monotone, il s'agit de la numérotation en fréquence décimale ; si vous entendez des sifflements différents, il s'agit de la numérotation en fréquence vocale.

Certains compléments de service (par exemple la présentation d'appel) requièrent un abonnement spécial.

Présentation d'appel

Ce complément de service vous permet de savoir si quelqu'un essaie de vous appeler pendant que vous êtes en train de téléphoner avec un premier correspondant. Vous pouvez décider si vous voulez continuer la première conversation, ou si vous la terminez et prenez le deuxième appel. Pour prendre le deuxième appel, procédez de la manière suivante :

- ① Vérifiez si vous disposez de ce complément de service.
 - Pour vérifier si la présentation d'appel est active, décrochez le combiné du téléphone et tapez ***#43#**.
 - La présentation d'appel est active si vous entendez deux tons aigus. Deux tons graves signifient qu'elle n'est pas active.
- ② Activez la présentation d'appel.
 - Décrochez le combiné et attendez la tonalité.
 - Appuyez sur les touches ***43#**.
 - Attendez le message, puis raccrochez.
- ③ Pour prendre le deuxième appel :
 - Quand vous entendez le signal de la présentation d'appel, appuyez sur la touche **R** dans un délai de 30 secondes.
 - Appuyez ensuite sur **2**. La première communication est mise en attente, et vous pouvez parler avec le deuxième correspondant.
 - Pour passer d'un appel à l'autre (va-et-vient), appuyez sur la touche **R** puis sur **2**.
- ④ Pour terminer la communication en cours :
 - Appuyez sur la touche **R**.
 - Appuyez ensuite sur **1** pour terminer la communication en cours.



Nota : marquez une pause d'une demi seconde entre deux appels (appuyez sur la fourche ou raccrochez le combiné).

- ⑤ Désactiver la présentation d'appel
 - Décrochez le combiné et attendez la tonalité.
 - Appuyez sur les touches **#43#**.
 - Attendez le message, puis raccrochez.

FR

Conférence à trois

Ce complément de service vous permet de téléphoner avec deux personnes en même temps. Vous pouvez soit appeler les deux correspondants vous-même, soit faire participer un deuxième appel (présentation d'appel) à la ronde.



Une conférence téléphonique à trois ne peut être établie qu'entre un correspondant interne et deux correspondants externes. Deux correspondants internes ne pourront donc pas établir de conférence à trois avec un correspondant externe !

Pour établir une conférence à trois, procédez de la manière suivante :

- ① Conférence à trois après une présentation d'appel
 - Quand vous entendez le signal de la présentation d'appel, appuyez sur la touche **R** dans un délai de 30 secondes.
 - Appuyez ensuite sur **2**. La première communication est mise en attente, et vous pouvez parler avec le deuxième correspondant.
 - Appuyez de nouveau sur la touche **R**.
 - Appuyez sur **3** pour réunir les trois personnes.
- ② Conférence à trois avec deux appels différents
 - Appelez d'abord le premier correspondant.
 - Quand la communication est établie, appuyez sur la touche **R**. Suivant la configuration de la prise de ligne, vous entendez la tonalité interne ou externe.
 - Composez le numéro d'appel du deuxième correspondant. La première communication est mise en attente, et vous pouvez parler avec le deuxième correspondant.
 - Appuyez sur **3** pour réunir les trois personnes.

③ Pour terminer la communication active :

- Appuyez sur la touche **R**.
- Appuyez ensuite sur **1** pour terminer la communication en cours.

④ Pour terminer les deux communications :

- Pour terminer les deux communications en même temps, raccrochez le combiné.



Vérifiez si l'option 'Commuation automatique des appels externes au raccrochage' pour le port A/N considéré est active ou non. Lorsqu'elle est active, les communications ne sont pas coupées quand vous raccrochez le combiné, mais les deux correspondants externes sont reliés entre eux. Songez aussi que vous devrez porter les coûts de communication alors que vous-même ne participez plus à la conversation !

Double appel/Va-et-vient

Ce complément de service vous permet de faire un deuxième appel, par exemple pour consulter un collègue. Pour ce double appel, procédez de la manière suivante :

① Établissement d'une deuxième communication

- Appuyez sur la touche **R**.
- Composez le numéro d'appel du deuxième correspondant. La première communication est mise en attente, et vous pouvez parler avec le deuxième correspondant (double appel).



Vous pouvez appeler un correspondant aussi bien interne qu'externe.

② Va-et-vient

- Pour basculer d'un appel à l'autre (va-et-vient), appuyez sur la touche **R** puis sur **2**.

③ Relier les deux correspondants

- Vous pouvez relier les deux correspondants entre eux en raccrochant le combiné.



Vérifiez si l'option 'Commuation automatique des appels externes au raccrochage' pour le port A/N considéré est active ou non. Si cette option est active, vous pouvez aussi relier deux correspondants externes entre eux.

④ Pour terminer la communication en cours :



- Appuyez sur la touche **R**.
- Appuyez ensuite sur **1** pour terminer la communication en cours.

Si vous terminez la communication en cours en raccrochant simplement le combiné, le téléphone sonne immédiatement pour vous rappeler que vous avez quelqu'un sur la deuxième ligne.

FR

Interception des appels

Lorsque vous avez raccordé des téléphones à plusieurs ports A/N, vous avez la possibilité de prendre un appel destiné à un autre appareil sur votre propre téléphone.

- ① Décrochez le combiné quand un autre téléphone que le vôtre sonne.
- ② Quand vous entendez la tonalité interne du *ELSA LANCOM 2000 Office*, composez le numéro interne du port A/N auquel l'autre téléphone est raccordé. Si vous n'entendez pas tout de suite la tonalité interne du *ELSA LANCOM 2000 Office*, appuyez -suivant la configuration- sur la touche **R** pour établir une connexion au *ELSA LANCOM 2000 Office*.
- ③ Composez ensuite le **8** pour intercepter l'appel et le rediriger sur votre téléphone.



*Si vous êtes vous-même en train de téléphoner, appuyez par exemple sur la touche **R** suivant la configuration du *ELSA LANCOM 2000 Office* pour mettre le premier correspondant en attente, et récupérez l'autre appel en composant le numéro interne et le **8**.*

Renvoi de poste

Ce complément de service vous permet de faire suivre les appels où que vous soyez. Il vous faut simplement programmer le numéro d'appel du téléphone où on peut vous joindre. Un appel entrant peut être renvoyé immédiatement, après 15 secondes ou uniquement si votre poste est occupé. Procédez de la manière suivante :



*Avant de pouvoir utiliser cette fonction, vous devrez affecter une adresse MSN à vos ports A/N. Utilisez *ELSA LANconfig* pour attribuer les adresses MSN.*

- ① Activer le renvoi de poste
 - Décrochez le combiné et attendez la tonalité.



- Appuyez sur les touches
 * **2 1** * (pour le renvoi de poste immédiat)
 * **6 1** * (pour le renvoi de poste après 15 secondes)
 * **6 7** * (pour le renvoi de poste quand votre téléphone est occupé)
- Entrez le numéro du poste où l'on peut vous joindre, puis appuyez sur #.
- La fonction est active dès que vous entendez deux tons aigus. Raccrochez.

*Si vous n'avez pas attribué de MSN au port A/N considéré, la combinaison de touches * **x y** * Numéro de destination * MSN du port A/N # vous permet d'activer le renvoi de poste, et # **x y** * MSN du port A/N de le désactiver # de désactiver la fonction (x y est à remplacer par l'option immédiatement, dans 15 secondes ou 'si occupé').*

*Pour vérifier si la fonction est active, décrochez le combiné et composez (après la tonalité) # * **x y** * MSN du port A/N #. La présentation d'appel est active si vous entendez deux tons aigus. Deux tons graves signifient qu'elle n'est pas active.*

- ② Désactiver le renvoi de poste
- Décrochez le combiné et attendez la tonalité.
 - Appuyez sur les touches
 # **2 1** # (pour le renvoi de poste immédiat)
 # **6 1** # (pour le renvoi de poste après 15 secondes)
 # **6 7** # (pour le renvoi de poste quand votre téléphone est occupé)
 - La fonction est inactive dès que vous entendez deux tons aigus. Raccrochez. Si vous entendez un ton grave, soit la fonction n'était pas active, soit vous avez entré le MSN incorrect !

Numérotation directe

Cette fonction vous permet d'appeler un correspondant choisi à l'avance (par exemple police-secours) sans que vous ayez besoin de composer le numéro. Si vous ne composez pas de numéro dans les cinq secondes qui suivent le décrochage, le numéro choisi est composé automatiquement.

Par exemple, si vous sortez le soir, vous pouvez programmer le numéro où votre enfant peut vous joindre en cas d'urgence. Votre enfant aura alors juste besoin de prendre le combiné en mains pour vous joindre.



Vous pouvez également configurer cette fonction avec ELSA LANconfig. Dans ce cas la programmation effectuée au moyen des touches du téléphone est écrasée.

Procédez de la manière suivante :

- ① Vérifiez si vous disposez de ce complément de service.
 - Pour vérifier si la fonction est active, décrochez le combiné et composez (après la tonalité) ***#53#**.
 - La présentation d'appel est active si vous entendez deux tons aigus. Deux tons graves signifient qu'elle n'est pas active.
Nota : suivant la configuration de la prise de ligne pour le port A/N considéré, vous devrez faire précéder le numéro d'appel par 0.
- ② Pour activer la numérotation directe :
 - Décrochez le combiné et attendez la tonalité.
 - Appuyez sur les touches ***53***.
 - Entrez le numéro du poste où l'on peut vous joindre, puis appuyez sur **#**.
 - La fonction est active dès que vous entendez deux tons aigus. Raccrochez.
- ③ Pour désactiver la numérotation directe :
 - Décrochez le combiné et attendez la tonalité.
 - Appuyez sur les touches **#53#**.
 - La fonction est active dès que vous entendez deux tons aigus. Raccrochez.



*Si vous aviez déjà programmé la numérotation directe précédemment et que vous avez désactivé cette fonction, il vous suffit d'entrer ***53#** pour réactiver la fonction.*

Activer/désactiver un port A/N

Cette fonction vous permet d'indiquer si votre téléphone doit sonner quand vous recevez un appel. Utilisez cette fonction par exemple lorsque vous ne voulez pas être dérangé. La personne qui appelle entend la tonalité « occupé ». Procédez de la manière suivante :

- ① Vérifiez si vous disposez de ce complément de service.

- Pour vérifier si la fonction est active, décrochez le combiné et composez (après la tonalité) ***#99#**.
- La présentation d'appel est active si vous entendez deux tons aigus. Deux tons graves signifient qu'elle n'est pas active.

② Activer le port A/N

- Décrochez le combiné et attendez la tonalité.
- Appuyez sur les touches ***99#**.
- La fonction est active dès que vous entendez deux tons aigus. Raccrochez.

③ Désactiver le port A/N

- Décrochez le combiné et attendez la tonalité.
- Appuyez sur les touches **#99#**.
- La fonction est active dès que vous entendez deux tons aigus. Raccrochez.

Non-identification d'appel

Cette fonction interdit l'affichage de votre propre numéro de téléphone sur le terminal de votre correspondant.

La non-identification d'appel devra éventuellement faire l'objet d'une demande préalable à votre opérateur.



Procédez de la manière suivante :

① Vérifiez si vous disposez de ce complément de service.

- Pour vérifier si la fonction est active, décrochez le combiné et composez (après la tonalité) ***#310#**.
- La présentation d'appel est active si vous entendez deux tons aigus. Deux tons graves signifient qu'elle n'est pas active.

② Pour activer la non-identification d'appel :

- Décrochez le combiné et attendez la tonalité.
- Appuyez sur les touches ***310#**.
- La fonction est active dès que vous entendez deux tons aigus. Raccrochez.

③ Pour désactiver la non-identification d'appel :

- Décrochez le combiné et attendez la tonalité.
- Appuyez sur les touches **#310#**.
- La fonction est active dès que vous entendez deux tons aigus. Raccrochez.

4.12

Comptabilisation

La comptabilisation permet de déterminer les temps en ligne et les volumes de données transmis et de les attribuer aux ordinateurs qui en sont à l'origine. Les données de comptabilisation sont enregistrées dans une liste pour les connexions actuelles et dans une liste de totalisation.

Les données suivantes sont enregistrées :

- Utilisateur (nom, adresse IP, adresse MAC)

Les temps en ligne et les volumes de données transmis sont d'abord attribués aux adresses MAC des interfaces réseau des ordinateurs dans le réseau local. A partir des modules de serveur DHCP ou DNS le routeur disposent d'informations supplémentaires sur l'attribution des adresses MAC et des noms des ordinateurs. Dans ce cas, le temps en ligne peut directement être attribué aux noms des ordinateurs. Si une attribution de l'adresse MAC au nom de l'ordinateur n'est pas possible, une autre information disponible, l'adresse IP p. ex., est enregistrée pour l'identification de l'utilisateur.

Pour les participants qui ont accès au réseau local via une liaison entrante, l'adresse MAC n'est en général pas connue. Dans ce cas le routeur génère une pseudo-adresse avec laquelle les correspondants entrants sont identifiés lors de la comptabilisation.

- Correspondant avec lequel la connexion a été établie
- Type de la connexion RNIS
- Volume de données dans le sens émission et réception
- Temps en ligne

Pour les connexions par commutation qui sont utilisés par plusieurs utilisateurs, la durée d'une connexion peut être plus longue que celle utilisée réellement par l'utilisateur. C'est pourquoi, dans ces cas-là, la durée de la connexion est calculée à l'aide de la première et de la dernière action d'un utilisateur, plus le temps de garde valable pour la connexion.

- Nombre de connexions

Dans ce champ est indiqué le nombre de fois où l'action d'un utilisateur a conduit à l'établissement d'une connexion

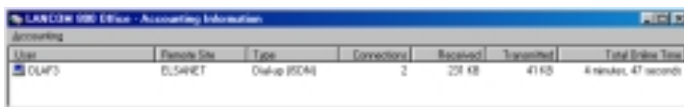
4.12.1

Configuration de la comptabilisation

Vous trouverez les paramètres pour la comptabilisation sous `/Setup/Comptabilisation`. Vous pouvez ici activer ou désactiver la comptabilisation et l'enregistrement dans la mémoire flash. Vous pouvez par ailleurs choisir le tri du tableau de totalisation selon le temps en ligne ou le volume de données.

4.12.2 Lecture des informations de comptabilisation

Un affichage des données enregistrées est possible via *ELSA LANmonitor*. Les données peuvent également être sauvegardées comme fichier sur un support de données.



User	Remote Site	Type	Connections	Received	Transmitted	Total Online Time
CLAF	ELSAHET	On-line (PCAN)	2	228 KB	41 KB	4 minutes, 47 seconds

En cas d'accès via Telnet les données enregistrées peuvent également être consultées sous */Setup/Comptabilisation*.

Les informations suivantes sont listées d'après le nom d'utilisateur et le correspondant :

- Nom d'utilisateur
Nom de l'utilisateur ou son adresse de couche 3 (adresse IP, adresse IPX ou en mode Bridge encore l'adresse MAC)
- Correspondant
Correspondant avec lequel l'utilisateur a échangé des données
- Type de connexion
Genre de connexion
- Octets Rx, octets Tx
Volume de données sur l'interface
- Temps total
Temps total en ligne pour cet utilisateur avec ce correspondant
- Connexions
Nombre de connexions avec ce correspondant comptées pour l'utilisateur

Quand un utilisateur établit une connexion avec un autre correspondant un nouvel enregistrement est généré dans le tableau. Tous les volumes de transfert et les temps en ligne d'un utilisateur avec un correspondant sont regroupés dans un enregistrement.

Selon le tri de la liste, les 512 enregistrements avec le volume de transfert le plus important ou avec le temps en ligne le plus long sont enregistrés dans le tableau.

5 Annexe

5.1 Caractéristiques techniques

Matériel	
Connexion WAN	RNIS-So (BRI), configuration point à point et point à multipoint, I.430 (Autosensing)
Connexion LAN	<p><i>LANCOM 800 Office</i>: Ethernet IEEE 802.3, 10Base-T</p> <p><i>LANCOM 1000 Office</i>: Ethernet IEEE 802.3, 10Base-T, 10Base-2 (BNC), mode bidirectionnel simultané</p> <p><i>LANCOM 1100 Office</i>: Ethernet IEEE 802.3, 10/100Base-T (RJ45, commutateur nœud/concentrateur), autosensing, 10Base-2 (BNC), mode bidirectionnel simultané</p> <p><i>LANCOM 2000 Office</i>: Ethernet IEEE 802.3, 10Base-T, 10Base-2 (BNC), mode bidirectionnel simultané</p>
CPU/mémoire	RISC CPU 32 bits (Hitachi SH3), 60 MHz, Flash ROM 2 Mo, RAM 4 Mo
Alimentation	12 VA avec alimentation enfichable pour 230 V, 12 VA; LANCOM 2000 : 24 VA
Design et dimensions	Boîtier métallique robuste, raccordements sur l'arrière ; dimensions 158 x 40 x 125 mm (l x h x p)
Conditions ambiantes	Température : 5– 40°C, humidité relative : 0– 80%, sans condensation
Homologations	<p>Homologué CE en Suisse et dans tous les pays de la CE :</p> <p><i>LANCOM 1000/1100/2000 Office</i> (pour l'Allemagne XYZ D800110K)</p> <p><i>LANCOM 800 Office</i>: EN 50082 (partie 1), EN 55022 (classe B), EN 60950, NET3</p>
Logiciels	
Modes de fonctionnement	<p>Routeur IP, serveur DHCP, client DHCP, serveur DNS ;</p> <p><i>D800109K, ICT D800110K</i></p> <p><i>LANCOM 2000 Office</i> : routeur IPX, bridge, proxy NetBIOS, standard en plus</p>
Protocoles de réseau	<p>Routeur IP : ARP, PROXY ARP, IP, ICMP, UDP, TCP, RIP-1, RIP-2, DHCP,</p> <p>Routeur IPX : IPX, SAP, Novell NetBIOS, mode Novell-Burst</p>
Protocoles RNIS	<p>Configuration de la connexion : Bus RNIS-So, configuration point à point et point à multipoint, I.430 (autosensing)</p> <p>Canal D : DSS1 ou 1TR6 (autosensing), support optionnel de liaison permanente</p> <p>Canal B : PPP (asynchrone/synchrone), X.75, HDLC, MLPPP pour regroupement des canaux, CAPI 2.0 via <i>LANCAPI</i>, compression Stac</p>
Commande de ligne	Rappel automatique avec ou sans établissement de la communication : ligne sur demande, veille en ligne dyn., canal sur demande en cas de regroupement des canaux, sélection à tour de rôle, reroutage rapide d'appels, connexion prioritaire programmable, BACP

Téléphonie (ports a/b)	seulement <i>LANCOM 2000 Office</i> : 4 raccordements analogiques, RJ11 avec adaptateur RJ11/ RJ11, Fonctions RNIS : communications internes, renvoi d'appel, va-et-vient, mise en garde, double appel, conférence à trois, transfert d'appel, indicateur de taxation, accès réglable à la tonalité externe, connexion prioritaire, numérotation directe
Fonctions Security et Firewall :	PAP et CHAP, MS-CHAP ; mécanismes d'authentification dans le protocole PPP ; possibilités de filtrage en mode IP (<i>LANCOM 1000/1100/2000 Office</i> en plus en mode EPX et bridge), protection de la configuration par listes d'accès et mot de passe, masquering IP, mécanisme de protection RNIS (CLIP, rappel etc.), protection par mot de passe, comptabilisation
Masquering IP (NAT/PAT)	Conversion d'adresse IP et de port via une adresse IP ; affectation statique/dynamique de l'adresse IP via PPP ou DHCP ; masquage de TCP, UDP, ICMP, FTP ; routage par DNS, masquage inverse pour services IP issus de l'intranet comme p. ex. le serveur Web ; masquering NetBIOS
Sécurité de fonctionnement	Chiens de garde matériel, autotests permanents, concept FirmSafe pour mise à jour à distance du logiciel
Contrôle des coûts de communication	Réglage possible pour une période déterminée du coût maximal ou de la durée des communications
Comptabilisation	Mémorisation du nombre et de la durée des connexions
Management	Configuration TFTP et téléchargement du micrologiciel, gestion SNMP via SNMP v.1 ou v.2, accès WAN ou LAN pouvant être activés séparément, éditions de diagnostic pour protocoles et interfaces, outils de diagnostic, affichage d'état <i>ELSA LANmonitor</i> , <i>LANconfig</i> , configuration à distance via RNIS, configuration via HTML, <i>ELSA WEBConfig</i> (<i>LANCOM 1000/1100/2000 Office</i> interface outband V.24/V.28 en plus (Mini-DIN 8 points))
Contenu du coffret :	
Accessoires	Bloc d'alimentation, câble de connexion RNIS, deux câbles LAN à paire torsadée, documentation détaillée et <i>CDELSA LANCOM LANCOM 1000/1100 Office</i> : câble pour interface outband, connecteur BNC-T en plus <i>LANCOM 2000 Office</i> : câble pour interface outband, connecteur BNC-T, 4 adaptateurs RJ11/RJ11 logiciel : <i>ELSA LANCAPI</i> , <i>ELSA LANtools</i> (<i>ELSA LANconfig</i> , <i>ELSA LANmonitor</i> pour l'affichage d'état), <i>ELSA CAPI Faxmodem</i>
Service & Support	6 ans de garantie par hotline et Internet

5.2

Déclarations de conformité

FR



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

Geräteart: ISDN Router
 Type of Device:
 Typenbezeichnung: ELSA LANCOM 800 Office
 Product Name:
 EG-Baumusterprübscheinigungs Nr.: D800109K
 Registration No.:
 Benannte Stelle: CETECOM ICT Services GmbH
 Notified Body: **CE 0682 X**

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:
 This is to confirm that this product meets all essential protection requirements relating to the

Niederspannungs Richtlinie (73/23/EWG)
 Low Voltage Directive (73/23/EEC)
 ISDN Richtlinie (97/346/EWG)
 ISDN Directive (97/346/EEC)
 EMV Richtlinie (89/336/EWG)
 EMC Directive (89/336/EEC)

Zur Beurteilung der Konformität wurden folgende Normen herangezogen:
 The assessment of this product has been based on the following standards

EN 50082-1: 1992
 EN 50081-1: 1992 Teil / part : EN 55022B: 1994
 EN 60950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997
 TBR 3

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:
 On behalf of the manufacturer / importer:

ELSA AG
 Sonnenweg 11
 D-52070 Aachen

abgegeben durch: / this declaration is submitted by:

Aachen, 29. Februar 2000
 Aachen, 29th February 2000

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:	ISDN Router
Typenbezeichnung:	ELSA LANCOM 1100 Office
EG-Baumusterprüfbescheinigungs Nr.:	D800109K
Benannte Stelle:	CETECOM ICT Services GmbH
Notified Body:	CE 0682 X

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:
This is to confirm that this product meets all essential protection requirements relating to the

Niederspannungs Richtlinie (73/23/EWG)
Low Voltage Directive (73/23/EEC)
ISDN Vorschrift (97/346/EG)
ISDN Directive (97/346/EC)
EMV Richtlinie (89/336/EWG)
EMC Directive (89/336/EEC)

Zur Beurteilung der Konformität wurden folgende Normen herangezogen:
The assessment of this product has been based on the following standards

EN 50082: 1992 Teil 1: EN 61000-4-2, 3, 4, 5, 6
EN 50081: 1992 Teil 1: EN 55022B: 1994
EN 60950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997
TBR 3

Diese Erklärung wird verantwortlich für den Hersteller / Importeur
On behalf of the manufacturer / importer

ELSA AG
Sonnenweg 11
D-52070 Aachen

abgegeben durch: / this declaration is submitted by:

Aachen, 8. Februar 1999
Aachen, February 8th 1999


i.V. Peter Wieninger
Bereichsleiter Entwicklung
VP Engineering



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

Geräteart: ISDN Router
 Type of Device:
 Typenbezeichnung: ELSA LANCOM 1000/2000 Office
 Product Name:
 EG-Baumusterprüfbescheinigungs Nr.: D800109K
 Registration No.:
 Benannte Stelle: CETECOM ICT Services GmbH
 Notified Body: **CE 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/EEG)

Low Voltage Directive (73/23/EEG)

ISDN Richtlinie (97/346/EWG)

ISDN Directive (97/346/EEC)

EMV Richtlinie (89/336/EWG)

EMC Directive (89/336/EEC)

Zur Beurteilung der Konformität wurden folgende Normen herangezogen:
 The assessment of this product has been based on the following standards

EN 50082-1: 1992

EN 50081-1: 1992 Teil / part : EN 55022B: 1994

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

TBR 3

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:
 On behalf of the manufacturer / importer:

ELSA AG
 Sonnenweg 11
 D-52070 Aachen

abgegeben durch: / this declaration is submitted by:

Aachen, 8. April 1998
 Aachen, 8th April 1998

i.V. Peter Wieninger
 Bereichsleiter Entwicklung
 VP Engineering

5.3

Conditions générales de garantie

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 :01.06.1998

1 Objet de la garantie

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

2 Durée de la garantie

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

3 Modalités

- a) Si des défauts surviennent pendant la période de garantie, l'acquéreur doit faire valoir son droit de garantie immédiatement, au plus tard 7 jours après l'apparition du défaut.
- b) Toute avarie de transport reconnaissable de l'extérieur (par exemple boîtier endommagé) survenue lors du transport doit être signalée 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 réhibition ou la prétention à diminution. Toute réclamation de dommages-intérêts, quelle qu'en soit la raison, est exclue. Cette garantie ne limite pas les droits de l'acquéreur conformément aux lois sur la responsabilité produit, par exemple dans les cas de dommages corporels ou d'endommagement des objets personnels ou dans les cas de préméditation ou de négligence grossière, dans lesquels ELSA AG engage impérativement sa responsabilité.
- c) En particulier, le remboursement d'un manque à gagner ou de dommages directs ou indirects sont exclus.
- d) Nous n'engageons aucune responsabilité pour la perte de données ou la récupération de ces données en cas de faute légère ou moyenne.
- e) Dans les cas où nous provoquons la destruction de données avec préméditation ou par négligence grossière, nous engageons notre responsabilité pour le rétablissement typique tel qu'il serait à réaliser en cas de création régulière de copies de sauvegarde selon les mesures de sécurité adéquates.
- f) La garantie s'applique uniquement au premier acheteur et ne peut être transférée à un tiers.
- g) Pour toute contestation le tribunal d'Aix-la-Chapelle (Aachen) est seul compétent, si l'acquéreur a la qualité de commerçant et en a tous les droits et obligations. Si l'acquéreur n'a pas d'attribution de juridiction en R.F.A. ou si son domicile ou son lieu de résidence habituel est transféré en dehors du champ d'application territorial de la R.F.A. après la conclusion du contrat, le tribunal de notre siège social est seul compétent. Ceci est valable également si le domicile ou le lieu de résidence habituel de l'acheteur n'est pas connu au moment de l'introduction d'une action.

- h) La loi applicable est la loi de la République Fédérale d'Allemagne. Le droit de l'ONU en matière d'achat n'est pas applicable.

6 Index

Toutes les pages débutant par R se trouvent sur CD.

10/100Base-TX	28
100BASE-T	R-88
100Mbit	28
10Base-2 (BNC)	28
10Base-T	28
1TR6	14, R-80
802.2	R-90
802.3	R-90

A

Accès à distance	12, 43, 87
Accès analogiques	13
Accès réseau à distance	39, 43, 61
Access-list	R-99
Adaptateur	40
Adaptateur pour le câble de configuration	21
Adaptateur téléphonique	109
address pool	R-110
address ranges	R-102
Adressage	86
Adresse d'arrivée	75
Adresse de départ	75
Adresse IP	41, 52, 62
Adresses IP	17
Affectation des adresses	42
Affichage de l'état	17
Affichage des canaux	52
Affichage des unités de taxation	18
Aging-minute(s)	R-94, R-96
AOCD	15, 63
Appel bébé	115
Appels dans le réseau mobile	98
Appels externes	108, 115
Appels internationaux	96

Appels internes	13, 18, 108
Appels longue distance	97
Apple Talk	R-3
APPP	R-84
ARP cache	R-100
ARP-aging-minute(s)	R-100
Assistant de configuration	40
asynchronous PPP	R-84
Auth.	R-85
Authentication	R-15, R-19
Authentification	15
auto mode	R-110

B

Backoff	R-93
BACP	16
B-channel protocols	R-83
Binding	R-90
Bloc transfo	21
Boot system	R-122
Bridge	
configuration	R-39
filtering data packets	R-40
bridge	R-39
Broadcast address	R-5
Broadcast transfer	R-8
Budget en fonction du temps	64
Buffers	R-88
Bureautique	103

C

Cable	R-1
Câble de configuration	21
Câble de raccordement au réseau local	21
Câble de raccordement RNIS	21
Cable network	R-4
Câble RNIS	13

- cache R-100
- Call charge information R-21
- Call charge units R-21
- call numbers R-86
- Callback R-81
- callback R-86, R-88
- Callback options R-82
- Call-by-Call 97
- call-by-call R-117
- Calling Line Identification Restriction
..... R-80
- Canal B 52
 - état de la liaison 16
- Canal D 61
- Canaux principaux 121
- Canaux secondaires 121
- CAPI Faxmodem 102
- Caractères joker 85
- Caractéristiques techniques 133, 135
- CBCP R-18
- CD 21
- Cells R-1
- Challenge Handshake Authentication
Protocol 60, R-85
- Channel bundling R-21
 - dynamic** R-21
 - static** R-21
- channel bundling R-84
- CHAP 60, R-85
- charge R-82
- charger le logiciel 47
- Charges R-95
- charges R-90
- charging information R-81
- charging unit R-81
- CLI 61, R-86
- Client LANCAPI 104
- Client pour réseaux Windows 89
- Client PPP 43
- CLIP 15
- CLIR R-80
- Common ISDN Application
Programming Interface 103
- Communication urbaine 98
- Commutateur nœud/concentrateur 29
- compatibility R-83
- Compression 16
- Compression de données Stac 16
- Comptabilisation 19
- Conditions Outband 40
- Conférence à trois 18, 108, 123
- Config-aging-minute(s) R-115
- Configuration 14
 - Procédé 39
 - SNMP 56
- Configuration à distance 19, 39
- Configuration des ports A/N et de la
régie 110
- configuration Inband 39
- configuration options R-114
- Configuration Outband 39, 40
- Configuration point-à-multipoint 14
- Configuration point-à-point 14
- Configuration WINS 78
- Connect R-87
- Connecteur mini-standard 14
- Connecteur multiple 14
- connection time-outs R-81
- Connector R-88
- Connexion à distance 44
- Connexion à un réseau étendu WAN 14
- Connexion à un réseau local 14
- Connexion par réseau 11
- Connexion PPP 39, 45
- Consultation 13
- Contenu de l'emballage 21
- Contrôle des accès 59
- Contrôle des coûts de communication 15
- Correspondants NetBIOS 87

Coupe-feu	15
Couplage LAN-LAN	12
Courrier électronique	12
Coûts de communication	13, 18, 87

D

data compression	R-84
Data compression procedure	
LZS	R-21
Data packet	R-1
data transfer	R-21
Data transmission in an IPX network	R-24
DDI numbers	R-83
Décrochage du combiné	116
default route	R-103
Dépannage	51
destination network	R-101
Destination port	R-104
destination ports	R-103
device names	R-81
Device-name	R-81
DHCP	17, 73, R-110
DHCP pour résolution WINS	78
DHCP server	R-110
dial prefix	R-82
Dialup-remote	R-81
Disconnect	R-87
Disponibilité	107, 120
Distance of a route	R-29
DNS	81, R-37, R-99
DNS Forwarding	R-37
DNS forwarding	R-100
DNS queries	R-104
DNS-backup-IP-address	R-100
Documentation	21
Documentation électronique	21
Domain Name Service	81, R-37
Domaines	81
Double appel	18, 108, 124
Droits d'appel	119

DSS1	14, R-80
Dst-address	R-105
Dst-netmask	R-105
Durée de communication	16
Durée de validité	74, 77
dynamic assignment of the IP address	
.....	R-101
dynamic bundling	R-81
Dynamic channel bundling	R-21
Dynamic Host Configuration Protocol	R-73
dynamic IP routing table	R-107
Dynamic routing	R-28
dynamic short-hold	R-81

E

Échange PPP	45
Économies sur la facture de téléphone	98
Éditions des tracés	53
ELSA CAPI Faxmodem	17
ELSA-RVS-COM	13
ELSA-ZOC	13
Emulateur de terminal	14
Émulateur de terminal	40
Encaps	R-83
End-address-pool	R-110
Envoi de télécopies	103
Espace d'adressage	86
Essais d'ouverture de séance	58
Établissement d'une connexion	87
Etablissement d'une liaison	18
Etat S0	26
Ethernet	14, R-83
10/100Base-T	14
10Base-2	14
10Base-T	14
Fast Ethernet	14
Ethernet packet format	R-90
EuroFileTransfer (télédisquette)	11
Exclusion routes	R-30
exponential backoff	R-93

● **F**

Fast callback	62
fast callback procedure	R-82
Fast-Ethernet	14
10/100Base-T	14
Fax	11
Fax Class 1	18, 102
Fax-modem	
LANCAPI	103
Faxmodem	17
Fichier et imprimante partagés	89
Filtre	59
Filtre IP	88
Filtres	12
firewall function	R-104
FirmSafe	15, 47
firmsafe	R-121
Firmware	R-120
firmware upload	R-120
Fonction de coupe-feu	62
fonction de rappel	15
Fonctions de sécurité	12
Fonctions RNIS supplémentaires	18
Force brute	15, 58
Fournisseur d'accès Internet	11
Frais de téléphone élevés	63
Fréquence décimale	122
Fréquence vocale	122

● **G**

Gestion d'adresses	73
Gestion des communications	63
Gestion des liaisons	18
Gestion des lignes	12
Gestion des priorités	107, 120
Gestion des unités de taxation	62
Group table	R-113
Groupes	86

● **H**

HDLC packets	R-84
HDLC56K	R-84
HDLC64K	R-84
Heure	97
Heure du réseau RNIS	101
Heure du RNIS	16
hierarchical IP addresses	R-6
Horloge	101
Horloge interne	101
Host	R-1
Host table	R-113
Hôte	82
Hyperterminal	40

● **I**

IANA	R-5
ICMP	R-104, R-106, R-108
Identification	89, R-78
Identification de l'appelant	60
Identification du numéro de l'appelant	15
Inband	39, 41
Avec Telnet	43
Indicatif	97
Informations de facturation	18
Informations de taxation	15
Informations sur le nom	87
Installation	13
Interception d'appel	115
Interception des appels	125
Interconnexion de réseaux locaux	12
Interface	R-1
Interface CAPI	103
Interface de configuration	40
Interface de configuration V.24	29
Interface de configurations	39
Interface list	R-79
Interface SO	14
Interface sérieielle	39
Interfaces	28

- Internet 12, 62, R-3
 - Internet access R-17
 - Internet address R-36
 - Internetwork R-3
 - Interrogation de l'heure 16
 - Intranet R-98
 - intranet address R-36
 - Intranet-mask R-98
 - inverse masquerading R-107
 - IP R-106
 - IP address R-16, R-98
 - IP addresses R-4
 - IP broadcast R-106
 - IP header R-106
 - IP masquerading R-35, R-101, R-107
 - simple masquerading R-37
 - supported protocols R-37
 - IP multicast R-106
 - IP network R-3
 - IP routing
 - Filter R-31
 - FTP R-31
 - Telnet R-31
 - IP routing table R-28
 - IP-netmask R-98
 - IP-routing-table R-101
 - IPX R-3
 - IPX routing
 - backoff R-24
 - Binding R-23
 - binding R-24
 - exponential backoff R-26
 - Filter R-26
 - Hops R-25
 - network R-23
 - propagate R-24
 - Propagate loop function R-26
 - remote station R-23
 - RIP and SAP tables R-25
 - Tics R-25
 - IPX routing table R-23
 - IPX watchdogs R-28
 - IPX-router R-89
 - IPX-watchdog R-90
 - ISDN layers R-83
 - ISDN network R-4
 - ISDN time R-45
- **J**
- Jours de semaine 97
 - Jours fériés 97
- **K**
- Key R-15, R-85
- **L**
- LAN R-3, R-8
 - LANCAPI 11, 13, 17, 44, 103, R-116
 - LAN-Coll 28
 - LANconfig 30, 39, 41, 42, 44, 48, 51
 - Assistants 42
 - LAN-configuration R-115
 - LAN-filter-table R-94, R-96, R-103
 - Langner openISDN config
 - Assistants 42
 - Language R-115
 - LAN-Link 28
 - LANmonitor 16, 101
 - LAN-Rx 28
 - LAN-Tx 28
 - layer name R-81
 - Layer-name R-83
 - LCP echo reply R-16
 - LCP echo request R-16
 - LCR 16, 63, 96, R-117
 - le regroupement statique des canaux 16
 - leased-line connection R-83
 - Least Cost Router 99
 - Contrôle des coûts de communication 100

Modes de fonctionnement	100
Repli automatique	100
Least Cost Routing = rerouteur	
téléphonique	16
least-cost router	96
Least-cost routing	63
Liaison commutée	12
Lignes spécialisées	12
Limitation des communications en	
fonction de la durée	63
Limitation des communications RNIS ..	63
Limitation des unités de taxation	62
Limiter les coûts	63
liste d'accès IP	41
Liste PPP	60
Local Area Network	R-3
local network	R-3
Local-routing	R-91, R-105
location	R-78
Lock-minutes	R-115
Login	48
log-in block	R-115
Login-errors	R-115
LOOP-propagate	R-92
Looser	R-82
LZS data compression	R-21

● M

MAC	R-8
MAC address	R-88
MAC addresses	R-9
MAC protocol	R-9
manual connection	R-87
Masquerading	R-101, R-107
masquerading	R-98
Masquerading IP	12, 15, 59, 62
Masquerading table	R-108
Maximum number of simultaneous con-	
nections	R-115
Mécanisme d'acheminement DNS	83

Media Access Control	R-8
Médias en ligne	41
Medium	R-1
Medium Access Control	R-8
Mémoire flash	14, 47
Microprogramme	15
Mise à jour des microprogrammes	14
Mise en attente	18, 108
MLPPP	16, R-21
Mode automatique	74
Mode DHCP automatique	74
Modem	18
modem operation	R-84
Modes d'exploitation	57
Moniteur LAN	51
Mot de passe	46, 52, 59, 60, 61
Mots de passe	91
Multilink PPP	R-13, R-21
Multipoint cabling	R-8
Multiprotocol capability	R-9

● N

Name	R-78
name server	R-99
name verification	R-86
Name-list	R-81
Naming IP Addresses	R-23
NAT	59, 62, R-35
NBNS	87, R-100
NBNS-backup	R-100
NetBIOS	19, 82, R-91
Accès à distance	94
Correspondant	92
Filtre IP	92
Interconnexion entre deux réseaux	
locaux	92
Protocole réseau	88
TCP/IP	88
NetBIOS name server	R-100
NetBIOS propagated frames	R-92

Netmask R-4
 NetWare server R-90
 Network R-1, R-90
 Network adapter R-1
 Network address R-4, R-92
 Network cable R-1
 network connection R-88
 Network Information Center R-35
 Network protocol R-3
 Networking dans un réseau Windows 94
 NIC R-35
 Node-ID R-89
 Nom d'ordinateur 86
 Nom d'utilisateur 45, 61
 Noms d'ordinateur 81
 Noms de réseau 81
 Noms et désignation des groupes 89
 Non-identification d'appel 114, 128
 Novell R-92
 NT domain R-112
 number R-81
 Number list R-86
 Numéro de code de réseau 96
 Numéro de configuration 46
 Numéro vert 99
 Numérotation directe 126
 numérotation directe 18

● **O**
 Opérateurs 99
 opérateurs réseaux privés 96
 Operating R-89, R-98, R-101
 Ordinateurs accessibles 95
 Other R-122
 Outband 39, 40

● **P**
 Packet R-1
 PAP 60, R-85
 Partage 91

pas d'informations de taxation 63
 Passerelle 62, 73, 77
 password R-99
 Password Authentication Protocol
 60, R-85
 Password-required R-115
 PAT 59, 62, R-35
 Période 63
 physical medium R-1
 Pilote de télécopie 18, 102
 Plage horaire 97
 Point-to-multipoint connection R-2
 Point-to-point connection R-2
 point-to-point protocol R-84
 Pool d'adresses 75, 81
 Port 107
 Port number R-37
 Ports A/N 13, 18, 108
 Configuration 109
 Connexion du routeur 121
 Description 113
 Numéro d'appel 113
 Numéro d'appel interne 113
 Options 114
 Téléservices 114
 Ports NetBIOS 88
 PPP 19, 52, 61, R-21, R-84, R-86
 Assigning IP addresses R-16
 Callback functions R-17
 checking the line with LCP R-15
 PPP LCP Extensions R-20
 PPP negotiation R-98
 PPP-Client 39
 préfixe 96
 Présélection 96
 Présentation d'appel 110, 122
 Priorités d'appel 120
 Prise d'appel 111
 Prise de ligne 111, 115
 Private address spaces R-5

Procédés de sécurisation 60
 Programmes de télécopie standard .. 102
 Prohibited address ranges R-102
 Propagated Frames R-92
 Propagated frames R-26
 protect R-86
 Protection 57, 59
 Protection d'accès 59
 Protection de l'accès 15
 Par nom 60
 Par nom ou numéro 60
 Par numéro 60
 Protection par mot de passe 15, 58
 Protocol R-3
 Protocole de canal B 60, 61
 Protocole ELSA 61
 provider 96
 Proxy 19
 proxy ARP R-101, R-102
 Proxy NetBIOS 86
 Proxy-ARP R-105

R

R1-mask R-107
 Raccordement RNIS SO 29
 Raccordements 28
 Raccordements analogiques 29
 Rappel 61
 Fast Call Back 62
 Rappel automatique 13, 59
 Recherches en ligne 12
 Régie téléphonique 13, 18, 108, 110
 registered IP address R-5, R-98
 Réglage automatique de l'heure 101
 Regroupement des canaux 16, 121
 regroupement des canaux 16
 Dynamique 16
 Statique 16
 regroupement dynamique des canaux 16
 Remote Access R-105

Remote access R-16
 remote access R-93
 remote station verifications R-85
 Remote-table R-112
 Renvoi d'appel 13, 18
 Renvoi de poste 108, 125
 Répondeur téléphonique 13
 Reroutage direct 97
 Réseau 10Mbit 28
 Réseau Windows 78, 86
 Réseaux NetBIOS 82
 Réseaux Peer-to-Peer 19
 Réseaux TCP/IP 81
 Réseaux Windows 19
 Reset system R-122
 Ressources partagées 91
 RIP R-24, R-106
 RIP tables R-25
 RIP-SAP-scaling R-91
 RIP-type R-106
 Round robin list R-82
 round robin list R-82
 Round-Robin R-83
 Routage 87
 Routage téléphonique à la demande .. 96
 Router R-1
 Router des réseaux Windows 86
 Router name R-29
 Routes/FRM R-94
 Routing R-6
 Routing Information Protocol R-24
 Routing table R-6
 IP masquerading R-30
 special entries R-30
 Routing-table R-92

S

SAP R-24, R-95
 SAP services R-96
 SAP tables R-25

- scaling R-91
- Scope ID R-112
- Scopes 86
- Script list R-86
- script processing R-84, R-86
- Sécurité 57, 59, 62
- security procedure R-85
- semipermanent leased-line connection
..... R-82
- server information R-95
- Server list R-114
- Server/FRM R-96
- Serveur de messagerie électronique ..85
- Serveur de noms NetBIOS 87
- Serveur DHCP 41, 74, 82
 - Configuration 79
- Serveur DNS 17, 73, 76, 82
 - information disponible 83
 - liste-filtre 85
 - mécanisme filtrant 82
- Serveur LANCAPI 106
- Serveur NBNS 73, 76, 78
- Serveur WINS 87
- Service 82
- Service Advertising Protocol R-24
- service information R-96
- Service table R-107
- Setup
 - DHCP-module R-110
 - IP-router-module R-101
 - IPX-module R-89
 - LAN-module R-88
 - TCP-IP-module R-97
 - WAN-module R-78
- Shared Medium R-8
- Shared medium R-3
- Short-hold R-81
- Single User Access 62
- SNAP R-90
- SNMP 56, R-109
- Socket filter R-27
- Socket-Filter R-91
- Socket-filter R-93
- Sonnerie 112
- Source port R-104
- Spare-heap-blocks R-89
- special dialing characters R-81, R-82
- speed R-84
- Split horizon R-26
- Spoofing R-95, R-97
- SPX watchdogs R-28
- SPX-watchdog R-91
- Stac R-21, R-84
- Standard 117
- Start-address-pool R-110
- static bundling R-81
- Static channel bundling R-21
- static IP address R-101
- Static routing R-28
- Statistiques 17
- Status R-43
 - Call-info-table . R-73, R-74, R-76, R-77
 - Config-statistics R-70
 - Connection-state R-45
 - Connection-statistics R-71
 - Delete values R-77
 - Info-connection R-72
 - IP-router-statistics R-68
 - IPX-statistics R-57
 - LAN-statistics R-48
 - Layer-connection R-73
 - operating time R-45
 - PPP-statistics R-49
 - Queue-statistics R-70
 - S0-bus R-75
 - TCP-IP-statistics R-62
 - WAN-statistics R-46
- Subnet R-6
- Suppresses the outgoing MSN R-80
- Surveillance 51

System-administrator R-109
 System-location R-109

T

Table-ARP R-100
 Tableau de reroutage 97
 Table-RIP R-93, R-107
 Table-SAP R-95
 Tarif local 98, 99
 Tarifs 96, 98
 Taux de transfert 16, 52
 TCP R-104, R-108
 TCP max. connections R-100
 TCP/IP 30, 41, R-3, R-28
 TCP/IP stack R-3
 TCP-aging-minute(s) R-100
 Téléchargement 15, 48
 Téléchargement de microprogramme
 Avec LANconfig 49
 Téléchargement du microprogramme .48
 avec émulateur de terminal 49
 avec TFTP 50
 Téléconfiguration 39
 Télécopie 13, 102
 Télécopies 18
 Télécopieur 13, 18
 Téléphone 13, 18
 telephone company R-117
 Téléphone mobile 97
 Téléphonie 13
 Télétravail 12
 teleworkers R-105
 Telix 40
 Telnet 14, 36, 44
 Telnet server R-99
 Témoins lumineux 17, 25
 Temps en ligne 19
 Terminaux analogiques 18, 108
 Terminaux numériques 108
 TFTP 41

TFTP server R-99
 throughput R-21
 Time R-45, R-85
 time R-119
 Time-out R-21
 Timeout R-111
 TOS R-106
 Touche Flash 117
 Touche R 117
 Tracé
 Code et paramètres 54
 Exemples 56
 Lancement 53
 Transfert d'appel 13
 Transfert de fichiers 12
 Transfert EuroFile 18
 Trap-IP R-109
 Traps-active R-109
 Travail à domicile 12
 trunk seizure R-82
 Type d'accès 91
 Type of Service R-38
 Type-of-service R-106

U

UDP R-104, R-108
 Unités de taxation 63
 Unités pour la connexion RNIS 63
 Upload-system R-122
 User name R-15
 Username R-85

V

Va-et-vient 13, 18, 108, 124
 verification attempt R-85
 Verrouillage 58
 Verrouillage d'accès 58
 Verrouiller domaines 85
 Version-table R-120
 Voisinage réseau 94

Volume de données 19

● **W**

WAN-Chan1 27

WAN-Chan2 27

WAN-configuration R-115

WAN-filter-table R-94, R-96, R-104

WAN-update-minute(s) R-95, R-97

watchdog R-90

Watchdogs R-28

Windows Internet Name Service-Server
..... 87

winipcfg 32, 35

Wireless links R-1

WWW 62

● **X**

X.75 data protection R-84

X.75 secured format R-84

● **Y**

Y connection R-21

Y connections R-80

● **Z**

Zone tarifaire 98

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.

Network technology



*This section 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 cover the topic 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 cable or radio link, for example, that is connected to the computers using special interfaces (e.g. network adapters).



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

*Packets
Cells*

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, a host is not responsible for the task of forwarding information. A host normally has exactly one interface to the network.

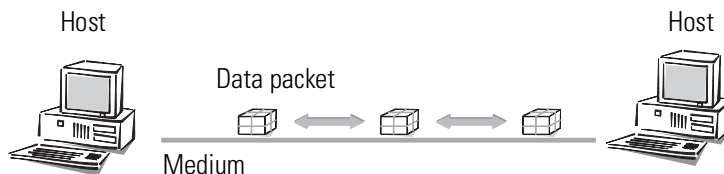
Router

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.

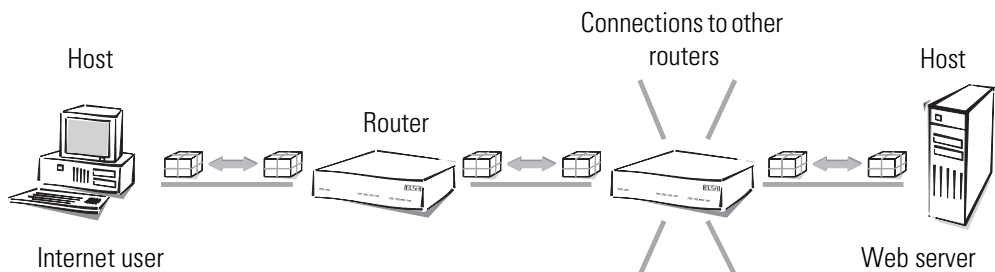
Connection modes

Point-to-point connection

The connection of exactly two hosts via a medium is called a “point-to-point connection”. In this case a host sends packets that can only be received by **one** specific recipient (unambiguous connection).



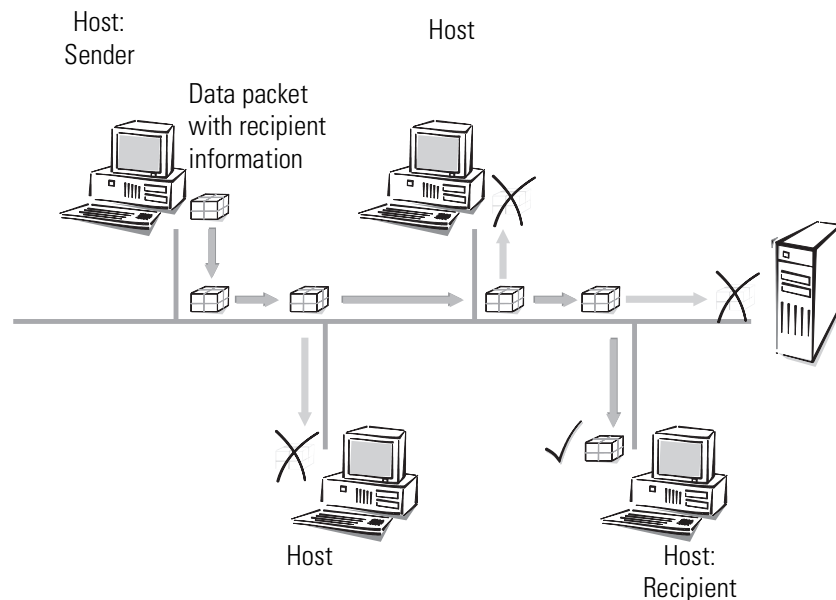
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers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



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

Point-to-multipoint connection

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



Kinds of networks

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

IP addressing

<i>Packet-oriented transfer</i>	In IP networks the communication between computers takes place in a packet-oriented fashion. This means that data or messages are packed together in packets 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 consists of four bytes separated by dots, 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. 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 netmask. You know what masks are: they cover up one part of something and only allow a different part to be visible. This is exactly how a netmask operates. It is a number which is identical in structure to the IP address, i.e. 32 zeros or ones. The netmask 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, serious consequences may result if such IP packets are released on the Internet.

IP routing and hierarchical IP addressing

Routing

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

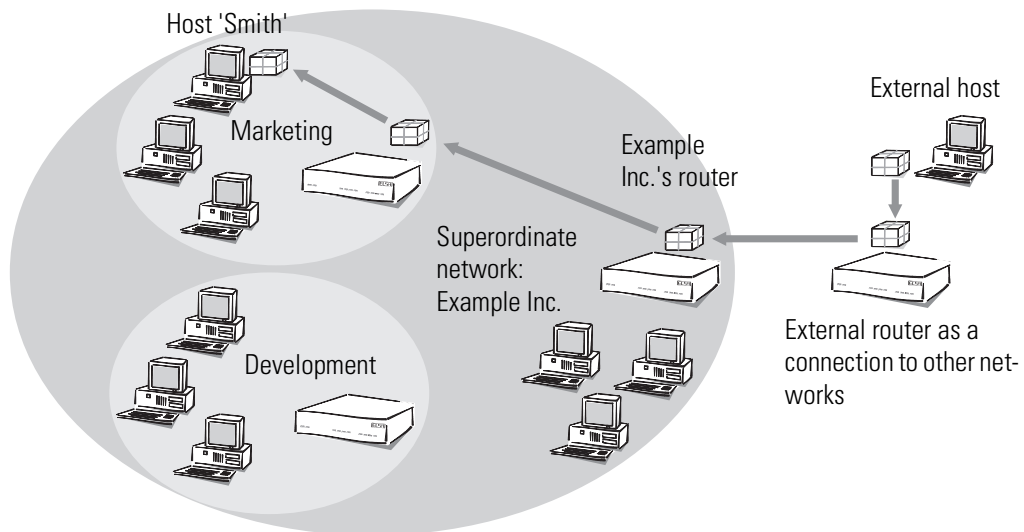
Every router manages a table (routing table). This table indicates the quickest interface connection to the host for every host in the network. You can imagine that, as they grow, these tables may exceed the capacity of the router—the Internet, as a worldwide linking up of publicly accessible IP computers 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 All an external router that establishes the connections to other networks has to know is 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 at 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 at the Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division, where the packet is passed on to the recipient.

Expansion through local networks

Media access control

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

LAN and IP network

The connection of all computers communicating through a shared medium using a MAC protocol is called a LAN. A LAN forms an independent network and is subordinate to the IP network, i.e. IP networks can use the physical connections of the LAN to establish connections between the hosts and the routers. LAN refers to a limitation of the area covered by the network, not a restriction of the number of workstations connected to it.

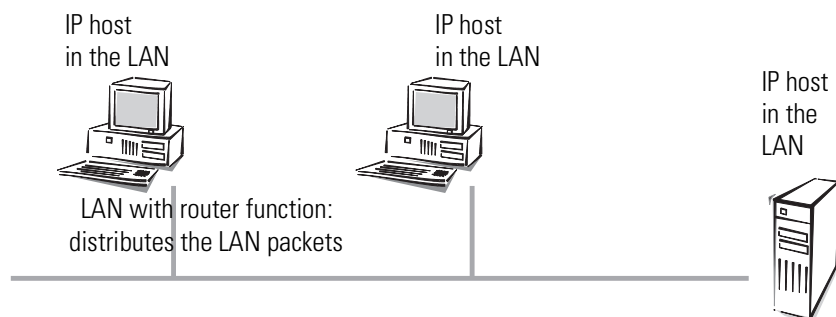
MAC address Specific LAN addresses hardwired into the interfaces by their manufacturers are used to manage the transfer in the LAN. Since the LAN addresses are used for communication via the MAC protocol, they are called MAC addresses. They can be thought of as the fingerprint of the interface hardware.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

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

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

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

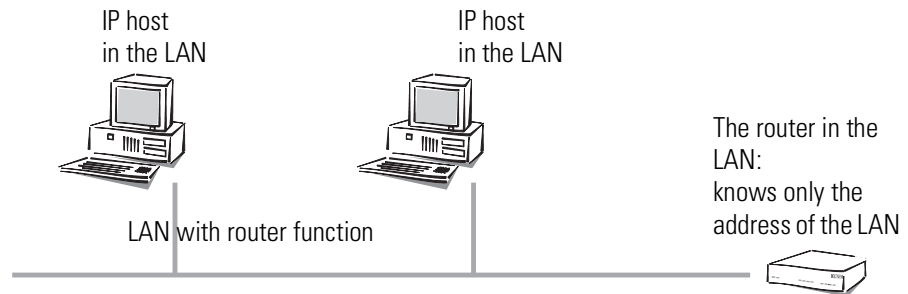
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts gives the packets to the LAN which handles the further distribution of the data packets. This is why only IP addresses from the numerical space of the specific network should be used for the internal communication of the hosts in a LAN 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 an interface with a point-to-point cable, 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 router in the LAN that takes care of the further processing of the packet.
- The sending host must send a packet with an address within the LAN directly 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'.

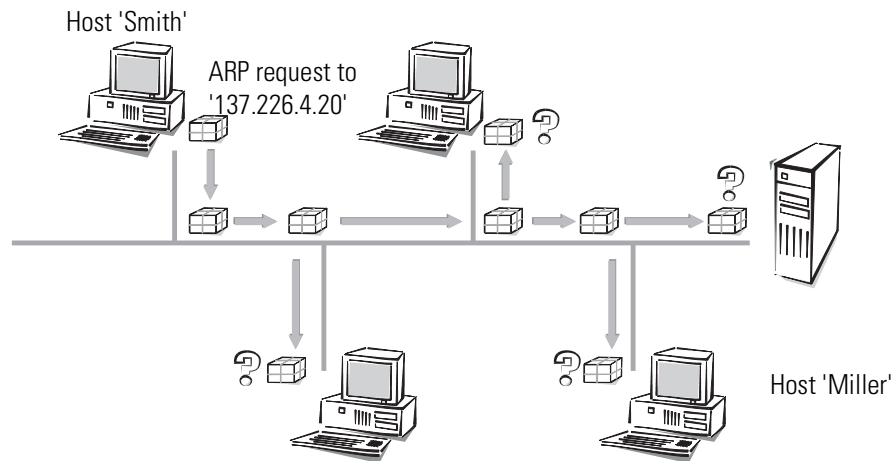
Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). Using the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located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

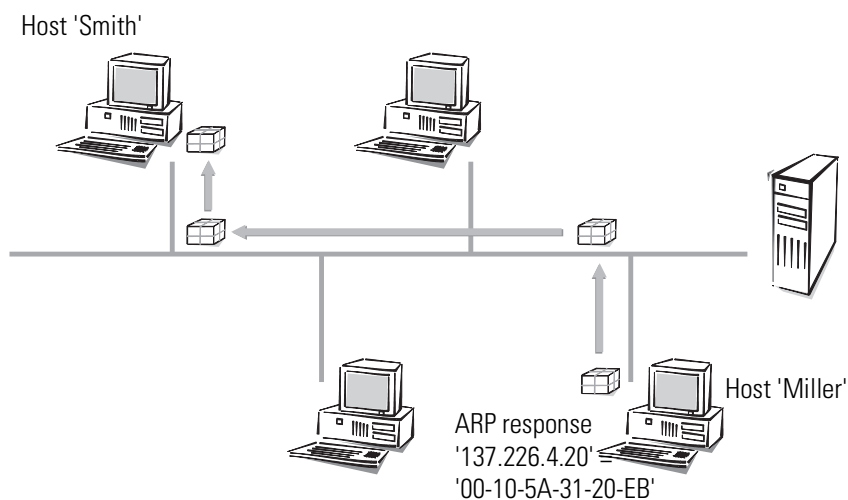
ARP

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, feels addressed and answers with an ARP response packet that it sends directly to host 'Smith' (the MAC address '00-10-5A-31-20-DF' of host 'Smith' is extracted from the sender field in the ARP request packet). Host 'Smith' recognizes this as an answer to its request, extracts the MAC address '00-10-5A-31-20-EB' from the ARP response packet and enters it into its 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 its 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 its network address and realizes that host 'External' is located outside the LAN. So host 'External' can only be reached through the router. Host 'Smith' finds out the MAC address of the router '00-80-C7-6D-A4-6E' by looking up the router's IP address in 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 cable 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 entire 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 an infinite number of LANs. 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".

Point-to-point protocol

ELSA routers also support the Point-to-Point Protocol (PPP). PPP is a generic term for a whole series of WAN protocols which enable the interaction of routers made by different manufacturers since this protocol is supported by practically all manufacturers.

Due to the increasing importance of this protocol family and the fact that PPP is not associated with any specific operating mode of the routers, we will be introducing the functions of the devices associated with the PPP here in a separate section.

The protocol

What is PPP?

The point-to-point protocol was developed specifically for network connections via serial channels and has asserted itself as the standard for connections between routers. It implements the following functions:

- Password protection according to PAP or CHAP
- Callback functions
- Negotiation of the network protocol to be used over the connection established (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP/IPX addresses. This process is carried out using IPCP and IPXCP (IP Control Protocol and IPX Control Protocol).
- Verification of the connection through the LCP (Link Control Protocol)
- Channel bundling (Multilink PPP)

PPP is the standard used by router connections for communication between devices or the WAN connection software of different manufacturers. Connection parameters are negotiated and a common denominator is agreed using standardized control protocols (LCP, IPCP, IPXCP, CCP) which are contained in PPP, in order to ensure successful data transfer where possible.

What is PPP used for?

It is best to use the point-to-point protocol in the following applications:

- for reasons of compatibility when communicating with external routers, for example
- remote access from remote workstation computers with ISDN adapters
- Internet access (when sending addresses)

PPP as implemented in the *ELSA MicroLink Cable* can be used synchronously or asynchronously and over both a transparent HDLC connection and an X.75 connection.

The phases of PPP negotiation

Establishment of a connection using PPP always begins with a negotiation of the parameters to be used for the connection. This negotiation is carried out in four phases which should be understood for the sake of configuration and troubleshooting.

- Establish phase

Once a connection has been made at the data communication level, negotiation of the connection parameters begins through the LCP.

This ascertains whether the remote station is also ready to use PPP, and the packet sizes and authentication protocol (PAP, CHAP or none) are determined. The LCP then switches to the opened state.

- Authenticate phase

Passwords will then be exchanged, if necessary. The password will only be sent once if PAP is being used for the authentication process. An encrypted password will be sent periodically at adjustable intervals if CHAP is being used.

There may also be negotiation on a callback using CBCP (Callback Control Protocol) during this phase.

- Network phase

The IPCP and IPXCP protocols have been implemented in the *ELSA MicroLink Cable*.

The IPCP and/or IPXCP network layers can be established following a successful transfer of the password.

IP and/or IPS packets can be transferred from the router modules to the opened line if the negotiation of parameters is successful for at least one of the network layers.

- Terminate phase

In the final phase the line is cleared, when the logical connections for all protocols are cleared.

PPP negotiation in the *ELSA MicroLink Cable*

The progress of a PPP negotiation is logged in the devices' PPP statistics and the protocol packets listed in detail there can be used for checking purposes in the event of an error.

The PPP trace outputs offer a further method of analysis. You can use the command

```
trace + ppp
```

to begin output of the PPP protocol frames exchanged during a terminal session. You can perform a detailed analysis once the connection has been broken if this terminal session has been logged in a log file.

The PPP list

You can specify a custom definition of the PPP negotiation for each of the remote stations that contact your net. The PPP list can be found in the *ELSA LANconfig* in the 'Communication' configuration section on the 'Protocols' tab, or in the `/Setup/WAN-module/PPP-list` menu.

The PPP may have up to 64 entries, containing the following values:

In this column of the PPP list...	...enter the following values:
Remote site	Name the remote station uses to identify itself to your router
Auth.	Security method used on the PPP connection ('PAP', 'CHAP' or 'none'). Your own router demands that the remote station observes this procedure. Not the other way round. This means that 'PAP' or 'CHAP' security is not useful when connecting to Internet service providers, who may not wish to provide a password. Select 'none' as the security attribute for connections such as these.
Password	Password transferred by your router to the remote station (if demanded). A string of asterisks (*) in the list indicates that an entry is present.
Time	Time between two checks of the connection with LCP. This is specified in multiple of 10 seconds (i.e. 2 for 20 seconds, for instance). Simultaneously the time between two checks of the connection according to CHAP. This time is entered in minutes. The time must be set to '0' for remote stations using Windows 95, Windows 98 or Windows NT.
Retries	Number of retries for the check attempt. You can eliminate the effect of short-term line interference by selecting multiple retries. The connection will only be dropped if all attempts are unsuccessful. The time interval between two retries is 1/10 of the time interval between two checks. Simultaneously the number of the "Configure requests" that the router maximum sends before it assumes a line error and clears the connection itself.
Conf, Fail, Term	These parameters are used to affect the way in which PPP is implemented. The parameters are defined in RFC 1661 and are not described in greater detail here. You will find troubleshooting instructions in this RFC in connection with the router's PPP statistics if you are unable to establish any PPP connections. The default settings should generally suffice. These parameters can only be modified via SNMP or TFTP (using the <i>ELSA LANconfig</i> configuration program)!
Username	The name with which your router logs onto the remote station. The device name of your router is used if nothing is specified here.
Rights	Network protocols to be routed over this connection: IP, IPX, NTB (NetBIOS). NetBIOS always requires one of the other two protocols.

Everything ok? Checking the line with LCP

The devices involved in the establishment of a connection through PPP negotiate a common behavior during data transfer. For example, they first decide whether a

connection can be made at all using the security procedure, names and passwords specified.

The reliability of the line can be constantly monitored using the LCP once the connection has been established. This is achieved within the protocol by the LCP echo request and the associated LCP echo reply. The LCP echo request is a query in the form of a data packet which is transferred to the remote station along with the data. The connection is reliable and stable if a valid response to this request for information is returned (LCP echo reply). This request is repeated at defined intervals so that the connection can be continually monitored.

What happens when there is no reply? First a few retries will be initiated to exclude the possibility of any short-term line interference. The line will be dropped and an alternative route sought if all the retries remain unanswered. This may be found in the form of a backup line, for example.



We recommend that you switch off regular LCP queries in the case of remote access from individual workstation computers using Windows 95, Windows 98 or Windows NT since these operating systems do not respond to LCP echo requests.

The LCP request behavior is configured in the PPP list for each individual connection. The intervals at which LCP requests should be made are set by the entries in the 'Time' and 'Retries' fields, along with the number of retries that should be initiated without a response before the line can be considered faulty. LCP requests can be switched off entirely by setting the time at '0' and the retries at '0'.

Assigning IP addresses via PPP

In order to connect computers using TCP/IP as the network protocol, all participating computers require a valid and unique IP address. In the event that a remote station does not have an IP address of its own (e.g. an individual computer belonging to a teleworker), the *ELSA MicroLink Cable* can assign an IP address for the duration of the connection to permit communications.

This mode of assigning addresses is run during the PPP negotiation and is used only for connections over the WAN. The assignment of addresses via DHCP, on the other hand, is used only within the LAN.



Assignment of an IP address will only be possible if the ELSA MicroLink Cable can identify the remote sites by its call number or name when the call arrives, i.e. the authentication process has been successful.

- For example: Remote access

Address assignment is made possible by a special entry in the IP routing table. 255.255.255.255 is specified as the network mask as the IP address to be assigned to the remote station in the 'Router' field. In this case the router name is the name

the remote station uses to identify itself to the *ELSA MicroLink Cable*.

In this configuration, the addresses of the DNS and NBNS servers (Domain Name Server and NetBIOS Name Server), including those of the backup servers based on the entries in the TCP/IP module are sent to the remote station in addition to the IP address.

For the whole thing to work it follows that the remote station should be configured to take the IP address and the name servers (DNS and NBNS) from the *ELSA MicroLink Cable*. This can be done under Windows Dial-Up Networking, for example, using the 'TCP-settings' under 'IP-address' or 'DNS-configuration'. Enable the 'Server-assigned IP-address' and 'Server-assigned name server addresses' options.

■ For example: Internet access

The assignment of IP addresses can take place the other way round if the *ELSA MicroLink Cable* is used to provide access to the Internet for a local area network. In this case it is possible to configure the *ELSA MicroLink Cable* so that it has no valid Internet IP address of its own but has one assigned to it by the Internet provider for the duration of the connection. The *ELSA MicroLink Cable* also receives information on DNS servers at the provider in addition to the IP address during PPP negotiation.

The *ELSA MicroLink Cable* is only known by its internally valid intranet address on the local area network. This means that all workstation computers on the local area network can access the same Internet account and reach the same DNS server, for example.

Windows users can view the assigned addresses in the *LANmonitor*. In addition to the name of the remote station, the current IP address as well as the addresses of DNS and NBNS servers can be found there. Options such as channel bundling or the duration of the connection are also displayed.



The ELSA LANmonitor is generally installed automatically during the installation of the ELSA LANconfig. Its description can be found in the 'Configuration modes' chapter in the 'What's happening on the line?' section.

Callback functions

In addition to callback via the D channel and via the ELSA protocol, the *ELSA MicroLink Cable* also supports callback via CBCP as specified by Microsoft and via PPP in accordance with RFC 1570 (PPP LCP extensions). There is also the option of a particularly fast callback using a process developed by ELSA.

PCs running Windows 95, Windows 98 or Windows NT can only be called back through the CBCP. The following values have been made available to you in the name list for the

callback entry so that additional call number verification is also possible on the *ELSA MicroLink Cable*:

This entry is used to...	...to set the callback so that:
Off	No callback occurs.
Auto (not Windows 95, Windows 98 or Windows NT, see below)	If the remote station is found in the number list, it will be called back. The call is initially rejected and the return call placed as soon as the channel is free (approx. 8 seconds later). If the remote station is not found in the number list, the call is initially accepted as the DEFAULT remote station and the callback is negotiated during the callback protocol negotiation. A charge of one unit is incurred for this.
Name	A protocol negotiation is always performed before the return call is placed, even if the remote station is found on the number list (e.g. for computers using Windows that have dialed into the device). A charge of one unit is incurred for this.
ELSA	If the remote station is found in the number list, a fast callback is performed; i.e. the <i>ELSA MicroLink Cable</i> sends a special signal to the remote station and returns the call immediately once the channel is free. The connection is established in approx. 2 seconds. If the remote station does not cancel the call immediately upon receiving the signal, a fallback to the standard callback procedure is performed after 2 seconds (duration of call establishment approx. 8 seconds). This process is only available for DSS1 connections.
Looser	Use the 'Looser' option if a return call is being expected by the remote station. This setting simultaneously fulfills two tasks. It ensures that the call establishment is canceled locally for incoming calls from a remote station just called, as well as enabling the response to the fast-callback process. In other words, to take advantage of the fast callback, the caller must be in 'Looser' mode, while the station being called must be set to the 'ELSA'.



Greatest security is offered by the 'Name' setting if an entry exists in both the number list and the PPP list. The 'ELSA' setting ensures the fastest callback method between two ELSA routers.

*The 'Name' setting **must** be selected for Windows remote stations.*

Microsoft CBCP callback

Microsoft CBCP provides a number of options to determine callback numbers:

- The party called does not call back.
- The party called allows the caller to specify the callback number itself.
- The party called knows the callback numbers and **only** calls these back.

It is possible to use the CBCP from a PC running Windows 95, Windows 98 or Windows NT to establish a connection to the *ELSA MicroLink Cable* have it call you back.

The callback entry and the call numbers entry in the name list are used to select these three possible settings.

Liste des noms - Nouvelle entrée

Nom:

Numéro d'appel:

Time-out: secondes

Time-out pour regroupement: secondes

Nom de la couche: ▼

Rappel automatique en retour:

- ☒ Pas de rappel
- ☐ Rappeler le correspondant
- ☐ Rappeler le correspondant (procédure rapide)
- ☐ Rappeler le correspondant après vérification du nom
- ☐ Attendre que le correspondant rappelle

No callback

For this setting, the callback entry must be set to 'Off' during configuration with a terminal program or via telnet.

Choose select callback number

The remote station is called back after the name has been verified. The callback entry must have the value 'Name' for this setting and **no** call number may be specified in the name list.

Following the authentication process, the dialog box below will appear in Windows 95 in which the user can specify his call number:

Convenience Callback

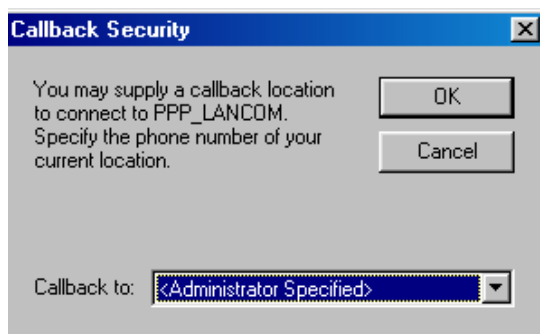
You may supply a callback location to connect to PPP_LANCOM. Enter a phone number where PPP_LANCOM can call you back.

Location:

Callback number specified by the *ELSA MicroLink Cable*

The remote station is called back after the name has been verified. The callback entry of the appropriate remote station must have the value 'Name' for this setting and **one** call number must be specified in the name list.

Following the authentication process, the message below will appear in Windows 95 which the user can only confirm:



Callback to a Windows 95, Windows 98 or Windows NT workstation is initiated approximately 15 seconds after the connection is dropped. This delay is specified by Windows and cannot be shortened.

Fast ELSA callback

This fast, ELSA-specific process is ideal if two *ELSA MicroLink Cable* are to communicate with one another via callback.

- The caller who would like to be called back sets 'Wait for callback from remote site' in the name list ('Looser' when configuring via a terminal program or Telnet).
- The return caller selects 'Call back the remote site (fast procedure)' in the name list and sets the number ('ELSA').

Callback as specified in RFC 1570 (PPP LCP extensions)

There are five methods of demanding a callback specified in RFC 1570. All versions are accepted by the *ELSA MicroLink Cable*. All versions will be processed in the same way, however:

The *ELSA MicroLink Cable* drops the connection to the remote station after authentication and then calls it back three seconds later.

Channel bundling with MLPPP

If you are establishing an ISDN connection to a party supporting PPP you can really speed up your data: You can compress the data and/or use several B channels for the transfer (channel bundling).

Connections using channel bundling differ from "normal" connections inasmuch as they use not only one, but several B channels in parallel for transmitting the data.

MLPPP (Multilink PPP) is used for channel bundling. Of course, this procedure is only available if PPP is being used as the B-channel protocol. MLPPP is ideal, for example, for accessing the Internet via a provider which also supports MLPPP on its dial-up nodes.

■ Static channel bundling

If a connection is established with static channel bundling, the router tries to establish the number of B channels specified as 'Minimum' in the channel list. Either the channels specified in the channel list or random free channels are used.

■ Dynamic channel bundling

In the case of dynamic channel bundling, the router initially establishes the number of B channels specified as 'Minimum' in the channel list and starts the data transfer. If the router determines that the throughput stays above a certain threshold for a given period of time, it will attempt to add further channels until the number specified as 'Maximum' in the channel list has been reached. Either the channels specified in the channel list or random free channels are also used in this case.

If the dynamic channels are established and the data throughput rate drops below the threshold value, the router waits for the set B2 timeout period and then automatically closes the channels again. Any partly used call charge units are used up fully if call charge information is transmitted during the connection. Therefore, the router only uses the dynamic channels if and as long as it really needs them.

How to configure channel bundling

Three settings are required to configure a channel-bundled connection:

- ④ Create an entry in the name list for the connection to be established with channel bundling. Select a layer which has set the bundling in the layer-2 options.
 - **compr.** When using the LZS data compression procedure (Stac), the data volume is reduced provided it was not already compressed before. This process is also supported by routers from other manufacturers and by ISDN adapters under Windows operating systems.
 - **bundle** uses several B channels per connection. The channel bundling method is determined by the configuration of the layer 2 options in the layer list, the timeouts in the names list, the setting for the Y connection in the interface table and the setting for the channel table.

- **bnd+compr** uses both compression and channel bundling and therefore provides maximum possible transmission performance.
- ⑤ Enter the holding times for this connection in the name list as well. Please observe the following rules:
- Depending on the application, the B1 holding time should be long enough to ensure that the connection is not prematurely terminated by the brief absence of data packets. Experience has shown that values between 60 and 180 seconds are a good basis which can be adapted as required during operation.
 - The B2 hold time determines the delay time after which the dynamic channels are terminated once the data throughput drops below the threshold value.
- ⑥ Use the channel list to determine the number of channels to be used for the connection. You may also specify the channels to be used, thus keeping certain channels free for dial-up connections via RAS, for example.

The channel list entry determines whether static or dynamic channel bundling will be used (see above). More than one minimum channel results in static bundling, whereas a difference between the minimum and maximum number of channels permits dynamic channel bundling.

- ⑦ Use the entry for the Y connection in the interface list to determine what should happen if an additional connection to a different remote station is requested during an existing connection using channel bundling, but no further B channels are available.
- Y connection **On**: The router interrupts the bundled connection on this interface to establish a connection to the other remote station. When the channel is free again, the originally bundled connection automatically takes the channel back (always in the case of static bundling, only as required when using dynamic bundling).
 - Y connection **Off**: The router holds the existing bundled connection on this interface, the other connection must try a different interface or wait if none of the interfaces with active channel bundling permit a channel to be terminated.

IPX routing

The IPX router transmits data from networks using IPX/SPX as the network protocols (e.g. Novell networks). A remote network is notified to the computers in the local network by its entry in the IPX routing table. A maximum of 16 different networks can be entered in the routing table.

Naming IPX addresses

A complete IPX network address comprises three parts: A network number, the MAC address of the network adapter and the socket number.

- The network number can be freely selected. It must, however, be unique on all the addressable IPX networks to ensure correct assignment.
- The MAC address is burnt into each network component. A different address is only used inside the network in special cases.
- An IPX network uses the socket numbers to address a specific service on a computer rather than just the computer itself. Socket numbers identify the various services uniquely.

Information about the LAN

Several separate LANs required at one location do not necessarily need to have their own cabling. Different logical networks can share one cable. They use different formats for the Ethernet packets to ensure that the data belonging to the various networks does not clash and that one network remains invisible to the others. These formats are determined by the binding belonging to a unique network number on this cable.

You must provide the router with the network number and the binding associated with it to ensure that it too now knows which network it belongs to. If we leave the network address at the default setting '00000000', the router provides the address and the binding itself. It does this by searching on the attached cable for the network from which it receives the most SAP replies.

IPX routing table

Use the IPX routing table to determine which remote stations (i.e. which other routers or computers) can be reached by the local network and to give it some parameters for connection purposes. The table, which can hold up to 16 entries has the following structure:

Remote site	Network	Binding	Propagated	Backoff
BRANCH01	00000245	802.3	Route	On
BRANCH02	00000320	SNAP	Filt.	On
HEAD OFFICE	00000420	802.2	Filt.	Off

- Remote site:
The name of the remote station registered as the device name in the corresponding router on the remote side.
- Network:

The address of the WAN. This is not the address of the destination network, but a third address which represents the network between the two networks to be connected. Thus the following applies:

LAN address 1 \neq WAN address 1 = WAN address 2 \neq LAN address 2 \neq LAN addr.1

■ Binding:

This is where you set which Ethernet binding is to be used on the WAN. This entry is only effective if the layer for this connection supports Ethernet encapsulation. 802.3 is assumed if the entry is missing.

■ Propagated:

A filter for type 20 IPX packets (NetBIOS propagated frames). The Network Basic Input/Output System was originally developed for IBM, and has since also been used by Microsoft in a modified form. This protocol provides services such as name resolution, data protection and correct packet sequencing (secure protocol) in layers 3 and 4 of the OSI model. NetBIOS packets have a special packet type and socket (propagated packets). NetBIOS is primarily used to exchange data between stations on a local network (LAN).

These IPX packets can be excluded from transmission or routed using the 'Filter' property. The 'Route' property transmits the packets if a connection to the remote station concerned is active or a free channel is available for the establishment of an additional connection. The propagated frames are rejected if all the lines to other remote stations are busy.

■ Backoff:

The IPX router uses a special algorithm (exponential backoff) to keep the connection costs arising in the case of erroneous configurations as low as possible.

The backoff function should be switched off if there is no server available on the remote station network (e.g. in the case of remote access from a workstation) (see also exponential backoff).

The default setting is 'On'.

What happens when data is transmitted on an IPX network?

When a device logs on to an IPX network, it first sends a request for the Service Advertising Protocol (SAP) and locates the nearest available server (get nearest server request) in the network numbered '00000000'. A router or server located on this network responds to this request and sends the correct network number.

The servers also regularly transmit information regarding which services they offer and which other networks they can reach. They use the special data packets complying with the Service Advertising Protocol or the Routing Information Protocol (RIP).

Once the IPX router is fully configured and is ready for operation, it proceeds to establish connections to all remote stations which can be reached via the routing tables and then exchanges SAP and RIP information with these networks. The router saves this data to its internal SAP and RIP tables.

RIP and SAP tables

RIP and SAP information is sorted alphabetically in the relevant tables. RIPs are thus only ordered by network and SAPs by service type first, then by server name.

The RIP and SAP tables are updated with each new RIP or SAP packet. The router only incorporates in its table SAP information for which it also has a corresponding RIP entry to ensure that only those services are offered (SAP) which can also be reached (RIP). The entries on the tables indicate, in addition to the information on reachable routes and services, how many routers the path to the destination (hops) passes through or how much time a data packet needs in the destination network (tics = approx. 1/18 of a second), for instance. The router selects the path with the fewest tics and the lowest hop count from the tables and stores only this route if the RIP information offers several different routes to a destination network, for instance.

RIP tables can hold 64 entries and SAP tables 128. If each new packet updates the tables, it stands to reason that the old entries must also disappear at some stage. Entries are artificially aged to do this. The age of all entries on RIP/SAP tables derived from local data transfers is incremented by 1 point every 60 seconds. A new RIP or SAP packet for an entry resets the age to zero. The route or service can be designated unreachable (down) once a selectable age of between 1 and 60 is reached. The entry is deleted when this elapsed time doubles. Additionally, any RIP and SAP information related to this remote station is deleted from the tables and replaced with new information when a connection is established.

So many routers around here...

If the establishment of simultaneous network connections to a greater number of remote stations is required than the number of B channels available, then it's time for a second (third...) router. The same entries are made in the routing tables for all routers to ensure that the brothers function in perfect harmony with each other and that the network really can always find a contact. The same routing information is then sent in the RIP packets to each router, albeit with a higher tic and hop count (`Setup/IPX-module/LAN-config/RIP-SAP-scal . activate`). This marks these routes as a sort of stand-by in the event that all channels are busy on the device addressed.

Redundant routes

A router receiving information in a RIP packet relating to routes with the same tic and hop counts as its own routes (redundant routes) does not, of course, have to reannounce

these routes itself to the sender. Therefore, it only sends these routes to the routers which did not propagate the route. This procedure is known as a "split horizon".

The Propagate loop (`Setup/IPX-module/LAN-Config/LOOP-Prop.`) can be used if it is nevertheless necessary to notify redundant routes to the local network. The routes learned in this way are then flagged in the RIP table with 'LOOP'. Although the propagation of redundant routes is not prohibited by the Novell specification, it should still be avoided as much as possible. Therefore, the default setting is 'Off'.

Exponential backoff

When switched on, the unit's IPX router attempts to establish suitable connections to receive routing information (RIP and SAP information) required for operation from the remote IPX stations. If this is not possible, due perhaps to a faulty configuration of the IPX router, the exponential backoff algorithm prevents connections constantly being established and thus saves charges.

The router will attempt to reach a remote station again with ever increasing wait times if the first attempt is unsuccessful. The wait time for this is determined as follows:

- The first attempt takes place after $10 + x$ seconds. x being a number from 0 to 10.
- The second attempt will be made $10 + x$ seconds after the first attempt has failed. x now standing for a number from 0 to 20 seconds.
- The higher value for x will now be doubled with each repeated attempt. The router finally gives up after the 16th unsuccessful attempt. The continual increase in the wait time means that 16 attempts will take a maximum of one day.

The route will be blocked if all attempts to call the remote station are unsuccessful. You can then only make further attempts at connection by amending the entry in the routing table.



The time to the next attempt and the number of attempts to establish a connection can be found in the network statistics using (`Status/IPX-module/IPX-router/Networks`).

IPX packet filters

The entries in the routing table determine which other networks will be accessible. However, they are then also accessible for data packets which are not actually required in the network of the remote station. These packets can also lead to unwanted connections being established which cost money.

Suitable filters are therefore required. These enable you to exclude from transmission over the WAN or at least restrict data packets which are only used in internal network communications, for example:

- Propagated frames

These special data packets use protocols which cannot in fact be routed. This data is encapsulated in normal IPX packets and sent as broadcast so that they can nevertheless participate in common routing.

These packets are sometimes not desirable in routing. For this reason, you can specify explicitly whether this type of packet is to be routed or filtered.

■ Socket filter

Every packet in an IPX network contains destination and source sockets along with destination and source addresses. Sockets identify the processes for which the data in the packet is intended.

There is a filter table each for sockets from local and remote networks containing the filters which can be used to exclude individual or entire groups of destination sockets. Certain sockets which are known frequently to be the cause of unwanted connections have already been entered in the socket filter table as default settings.

■ RIP and SAP information

A router uses the RIPs to inform the other routers of all the routes (paths to the other networks) known to it using the split horizon principle. This includes the entries from its own routing table and all routes which the router has derived from other routers. It gets its information for this purpose from routers on both local and remote networks. The router enters all available routing information in its internal RIP table.

The servers offer their services in the SAP information. The various services are represented within the SAP information as numbers. Each service (e.g. file server or print server) has a unique number. The router incorporates the information on the services available in its internal SAP table and registers which service is available on which network at which MAC address. At the same time it also establishes whether the service offered is located in a local or remote network and whether it can propagate the service without first establishing a connection.



You can look at the RIP and SAP tables and their current values in the IPX module (setup/IPX-module/RIP-config or SAP-config) of the router.

RIP and SAP information are extremely important for devices communicating on a network, which is why there are various different options for setting up the transmission of these packets.

- A LAN and WAN filter table can be used to tell the router not to include information on routes to particular networks or on certain available services in internal or external tables. The affected routes are thus not used, information on them is not provided and the services are not offered in the local network.
- RIP and SAP packets are always transmitted, i.e. no filters are used. These packets, however, must occupy a part of the connection.

- RIP and SAP packets will only be sent if the information they contain has been modified in some way.
- RIPs and SAPs can be transferred at regular, selectable intervals. Information is usually sent out in one minute intervals. The time interval between blocks can be stretched to up to 60 minutes.
- The most economical handling of RIP and SAP packets involves transmitting the information only once, when a connection is established.

■ IPX and SPX watchdogs:

These data packets are used by the server to determine whether workstation computers, for example, are still active or if they can be logged off. To ensure that these "Are you there?" packets for computers on a remote network do not continually result in connections being established, you can set the responses to these requests as follows:

- IPX watchdogs receive no response. The computers are logged off after a time specified on the server.
- IPX and SPX watchdogs can be responded to locally. This procedure is known as spoofing. The router responds in place of the computers addressed, which are then never logged off. It is also recommended that a time is set on the server after which the devices in question are always logged off.
- IPX and SPX watchdogs may of course be routed as normal but this frequently results in a connection being established.



Further information on IPX, the IPX router and the associated parameters can be found in chapter 'Setup/IPX-module' in the reference manual.

IP routing

An IP router works between networks which use TCP/IP as the network protocol. This only allows data transmissions to destination addresses entered in the routing table. This chapter explains the structure of the IP routing table of an ELSA router, as well as the additional functions available to support IP routing.

The IP routing table

Use the IP routing table to tell the router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a "route" since it is used to describe the path of the data packet. This procedure is also called "static routing" since you make these entries yourself and they remain unchanged until you either change or delete them yourself. Naturally, there is "dynamic routing", too. The routers use the routes in this way to exchange data between themselves and continually update it automatically. The static

routing table can hold up to 64 entries, the dynamic table can hold 128. The IP router looks at both tables when the IP RIP is activated.

You also use the IP routing table to tell the router the length of this route's path so that it can select the most suitable route in conjunction with IP RIP where there are several routes to the same destination. The default setting for the distance to another router is 2, i.e. the router can be reached directly. All devices which can be reached locally, such as other routers in the same LAN or workstation computers connected via Proxy ARP are entered with the distance 0. The "quality level" of this route will be reduced if the entry addressed has a higher distance (up to 14). "Unfavorable" routes like this will only be used if no other route to the remote station in question can be found.

The routing table can be found in the *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Routing' tab, or in the `/Setup/IP-router-module/IP-routing-table` menu. This, then, is how an IP routing table might look:

IP address	Netmask	Router	Dis- tance	Mask.
192.168.120.0	255.255.255.0	GLASGOW	2	On
192.168.125.0	255.255.255.0	LONDON	3	Off
192.168.130.0	255.255.255.0	191.168.140.123	0	Static

What do the various entries on the list mean?

■ IP addresses and Network

This is the address of the destination network to which data packets may be sent and its associated network mask. The router uses the network mask and the destination IP address of the incoming data packets to check whether the packet belongs to the destination network in question.

■ Router

The router transmits the appropriate data packets to the IP address and network mask to this remote station. A name is entered at this point if the remote station is a router in another network or an individual workstation computer. This is where the IP address of another router which knows the path to the destination network is entered if the router on the network cannot address the remote station itself.

■ Distance

Number of routers between your own and the destination router. This value is often equated with the cost of the transmission and used to distinguish between inexpensive and expensive call paths for wide-area connections. The distance values entered are propagated as follows:

- All networks which can be reached while a connection is established to a destination network are propagated with a distance of 1.

- All non-connected networks are propagated with the distance entered in the routing table (but with a minimum distance of 2) as long as a free transmitting channel is still available.
- The remaining networks are propagated with a distance of 16 (= unreachable) if there are no longer any channels available.
- Remote stations connected using Proxy ARP are an exception to this. These "Proxy hosts" are not propagated at all.

■ Mask.

Use the 'Masquerade' option in the routing table to inform the router which IP addresses to use when transferring the packets.

- 'Off': No masquerading.
- 'On': This entry requests a random IP address valid in the Internet from your provider which is then used for the connection and masquerading.
- 'stat.': Use this entry to request the assignment of a specific IP address from your provider as entered in the 'TCP/IP' configuration section on the 'General' tab or in the /Setup/TCP-IP-module menu. This address will be used for the connection and masquerading.

For further information see the 'IP Masquerading' section.

■ Following entries have a special meaning:

- IP address 255.255.255.255 with a network mask of 0.0.0.0: This is the default route. Any data packets which cannot be routed by other routing entries are transmitted to the remote station listed here.
- Network mask 255.255.255.255: Entries with completed network masks frequently only identify individual workstation computers (remote access) and not actual networks. A network which is only visible by a single IP address using IP masquerading may sometimes be concealed behind this.
- Router name 0.0.0.0: Exclusion routes. Data packets for this "zero route" are rejected and are not routed any further. This is how routes which are forbidden on the Internet (private address spaces, e.g. 10.0.0.0), for example, are excluded from transmission.

Examples with explanatory notes:

IP address	Netmask	Router	Dist.	This is what happens:
192.168.1.9	255.255.255.255	FIELD SERVICE	2	The FIELD SERVICE remote station can be reached at IP address 192.168.1.9.
192.168.120.0	255.255.255.0	Router01	2	All data packets with destination IP addresses 192.168.120.x are transmitted to ROUTER01.

IP address	Netmask	Router	Dist.	This is what happens:
192.168.125.0	255.255.255.0	Router02	3	All data packets with destination IP addresses 192.168.125.x are transmitted to ROUTER02.
192.168.130.0	255.255.255.0	192.168.140.123	0	All data packets with destination IP addresses 192.168.130.x are transmitted to the router with the IP address 192.168.140.123.
10.0.0.0	255.0.0.0	0.0.0.0	0	Excludes transmission of all data packets to networks using private address spaces.
255.255.255.255	0.0.0.0	HEAD OFFICE	2	All data packets which cannot be allocated to the entries listed above are transmitted to the HEAD OFFICE remote station.



The sequence of the entries is important here: They are processed from top to bottom. The router sorts entries automatically: Firstly by network masks, in descending order. Then by the IP addresses, in ascending order. This places the 'HEAD OFFICE' entry at the very end of the list. If this entry were at the top of the list, the router would send all (!) data packets not belonging to the local network to the network of the head office.

TCP/IP packet filters

You can use your entries in the routing table to determine quite precisely which data should be transferred. Additionally, you can use the '0.0.0.0' entry in the 'Router' field to reject whole groups of IP addresses.

Occasionally, you may wish to restrict a transmission even further. You can do this using a characteristic of TCP/IP, which is to send port numbers for destination and source as well as the source and destination IP addresses with a data packet. The destination port in a data packet stands for the service to be addressed in the TCP/IP network. The destination ports are fixed for the various services on the TCP/IP network (see also 'TCP/IP-ports' in the reference manual). The source ports, on the other hand, may be selected freely within certain ranges.

The router can check the source and destination ports of data packets using the TCP or UDP protocols. It can then deduce the purpose of the data from these ports. For example, FTP accesses or Telnet sessions can be identified. The appropriate filter table can be used to determine that certain data is not to be transferred from the LAN to the remote station. Data for particular ports can also be blocked from entering the LAN from the WAN in the same way. The filter tables can use the filter type along with the definition of the port ranges and associated protocols to determine whether the data in question should never be transmitted or whether it should simply not lead to a call being established (i.e. only be transmitted if a connection already exists).

The IP router has two separate filter tables, for packets coming from the LAN and from the WAN. These filter tables can be found in the *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Filtering' tab, or in the /Setup/IP-router-table/WAN-filter-table or LAN-filter-table menus.

Proxy-ARP

The proxy ARP is a special feature of the IP router. This proxy is used if the transmission of data to IP addresses takes place in the same logical network as the sender, but the destination address is still reached via a router. This is the case when individual workstation computers (teleworkers) are networked via TCP/IP to the company network. The teleworker then has an IP address which is located in the same local network as all the other computers in the LAN. A data packet from LAN to the teleworker would usually only search for a receiver locally, but would not be able to find one.



To take advantage of this function, enable the 'Use Proxy ARP' option (in LANconfig in the 'TCP/IP' configuration section on the 'Routing' tab or in the /Setup/IP-router-module menu for other configuration modes).

The router becomes a proxy for the teleworker with the following entry in the routing table:

IP address	Netmask	Router	Dis- tance	Mask
192.168.110.123	255.255.255.255	Teleworker01	0	off

Proxy hosts are not propagated in an RIP packet because the router responds to an ARP request for the proxy computer with its own MAC address. The distance is set to '0' on the routing table to indicate this clearly.

The router now responds to the request for the MAC address to the IP address 192.168.110.123 with its own MAC address. This ensures that all packets in the LAN for the teleworker are now automatically sent to the router, and that data is sent on to the computer at the other end of the ISDN connection.

Local routing

You know the following behavior of a workstation within a local network: The computer searches for a router to assist with transmitting a data packet to an IP address which is not on its own network. This router is usually notified to the operating system by its property of being the default router or gateway. It is often only possible to enter one default router which is supposed to be able to reach all the IP addresses which are unknown to the workstation computer if there are several routers in a network.

Occasionally, however, this default router cannot reach the destination network itself but does know another router which can find this destination.

How can you assist the workstation computer now?

By default, the router sends the computer a response with the address of the router which knows the route to the destination network (this response is known as an ICMP redirect). The workstation computer then accepts this address and sends the data packet straight to the other router.

Certain computers, however, do not know how to handle ICMP redirects. To ensure that the data packets reach their destination anyway, use local routing (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Routing' tab or in the `/Setup/IP-router-module/Local-routing` menu). This is how you tell the router to send the data packet to the other router itself. The router will then no longer send any ICMP redirects.

This may seem to be a good idea in principle, but local routing should still only be used as a last resort, since this function leads to doubling of the number of data packets being sent to the destination network required. The data is first sent to the default router and is then sent on from here to the router which is actually responsible.

Dynamic routing with IP RIP

In addition to the static routing table ELSA routers also have a dynamic routing table containing up to 128 entries. Unlike the static table, you do not fill this out yourself, but leave it to be dealt with by the router itself. It uses the Routing Information Protocol (RIP) for this purpose. This protocol is used by all routers with RIP in a local network to exchange information regarding the reachable routes.

What information is propagated by IP RIP?

A router uses the IP RIP information to inform the other routers in the network of the routes it finds in its own static table. The following entries are ignored in this process:

- Rejected routes with the '0.0.0.0' router setting.
- Routes running on other routers in the local network.
- Routes linking individual computers to the LAN by proxy ARP.

Although the entries in the static routing table are set manually, this information changes according to the connection status of the router and so do the RIP packets transmitted.

- If the router has established a connection to a remote station, it propagates all the networks which can be reached via this route in the RIPs with the distance '1'. Other routers in the LAN are thus informed by these means that a connection to the remote station has been established on this router which they can use. The establishment of additional connections by routers with dial-up connections can be prevented, thus reducing connection costs.

- If this router cannot establish a further connection to another remote station, all other routes are propagated with the distance '16' in the RIPs. The '16' stands for "This route is not available at the moment". If a router cannot establish a connection, in addition to the present one, this may be due to one of the following causes:
 - Another connection has already been established on all the other channels (also via the *LANCAP* or a/b ports).
 - The existing connection is using all B channels (channel bundling).



To take advantage of this function, enable the 'IP RIP' option (in ELSA LANconfig in the 'TCP/IP' configuration section on the 'Router' tab or in the Setup/IP Router-module menu for other configuration modes).

Routers with RIP capabilities dispatch the RIP packets approximately every 30 seconds. The router is only set up to send and receive RIPs if it has a unique IP address. The IP RIP module is deselected in the default setting using the IP address XXX.XXX.XXX.254.

Which information does the router take from received IP RIP packets?

When the router receives such IP RIP packets, it incorporates them in its dynamic routing table, which looks something like this:

IP address	Netmask	Time	Distance	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

What do the entries mean?

IP addresses and network masks identify the destination network, the distance is taken from the RIP information, the final column indicates the router which announced this route. This leaves the 'Time'. The dynamic table thus shows how old the relevant route is. The value in this column acts as a multiplier for the intervals at which the RIP packets arrive. A '1', therefore, stands for 30 seconds, a '5' for about 2.5 minutes and so on. New information arriving about a route is, of course, designated as directly reachable and is given the time setting '1'. The value in this column is automatically incremented when the corresponding amount of time has elapsed. The distance is set to '16' after 3.5 minutes (route not reachable) and the route is deleted after 5.5 minutes.

Now if the router receives an IP RIP packet, it must decide whether or not to incorporate the route contained into its dynamic table. This is done as follows:

- The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).

- The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.
- The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will always be used.
- The route exists in the table. The new route comes from the same router which notified this route, but has a worse distance than the previous entry. If a router notifies the degradation of its own static routing table in this way (e.g. releasing a connection increases the distance from 1 to 2), the router will believe this and include the poorer entry in its dynamic table.



RIP packets from the WAN will be ignored and will be rejected immediately. RIP packets from the LAN will be evaluated and will not be propagated in the LAN.

The interaction of static and dynamic tables

The router uses the static and dynamic tables to calculate the actual IP routing table it uses to determine the path for data packets. In doing so, it includes the routes from the dynamic table which it does not know itself or which indicate a shorter distance than its own (static) route with the routes from its own static table.

Routers without IP RIP support

Routers which do not support the Routing Information Protocol are also occasionally present on the local network. These routers cannot recognize the RIP packets and look on them as normal broadcast or multicast packets. Connections are continually established by the RIPs if this router holds the default route to a remote router. This can be prevented by entering the RIP port in the filter tables.

Scaling with IP RIP

If you use several routers in a local network with IP RIP, you can represent the routers outwardly as one large router. This procedure is known as "scaling". A router like this, with its supposedly inexhaustible supply of routes is created by the continual exchange of information between the routers.

IP masquerading (NAT, PAT)

One continually growing problem for the Internet is the limited number of generally valid IP addresses available. In addition to this, the allocation of fixed IP addresses for the Internet by the Network Information Center (NIC) is an expensive process. What is more obvious than having several computers share one IP address?

This particular solution is called IP masquerading. This is a procedure whereby only one LAN router appears on the Internet with an IP address. This IP address is allocated to the router either permanently by the NIC or temporarily by an Internet provider. All the other computers on the network then "conceal" themselves behind this one IP address. Aside

from the welcome savings, IP masquerading has the added benefit of guarding very effectively against attacks on the local network from the Internet.

Two addresses for the router

Masquerading pits two opposing requirements of the router against one another: While it must have an IP address which is valid on the local network, it must also have an address valid on the Internet. Since these two addresses may not in principle be located on the same logical network, there is only one solution: two IP addresses are required. The router is therefore assigned an **Internet** address and an **intranet** address, each with its own fitting network mask. Use the 'Masquerade' option in the routing table to inform the router which of the two addresses to use when transferring the packets. If a specific address is requested from the provider, two options are available for the actual address assignment:

- The provider assigns the desired address to the router. The network mask now decides how many computers are masked behind the router.
 - IP address with full '255.255.255.255' network mask: This is your own unique IP address, registered by the NIC. None of the other computers on the network have valid Internet addresses and are masked behind the router's fixed address.
 - IP address with an incomplete network mask, e.g. '255.255.255.248': You have several registered IP addresses, one of which you assign to the router. The remaining IP addresses are assigned permanently to devices on the intranet, which can then use unmasked connections to access the Internet. The other devices can still access the Internet using masked connections.
- The provider assigns another address to the router. Then **all** computers in the local network are masked behind the assigned address.

How does IP masquerading work?

Masquerading makes use of a characteristic of TCP/IP data transmission, which is to use port numbers for destination and source as well as the source and destination addresses. When the router receives a data packet for transfer it now notes the IP address and the sender's port in an internal table. It then gives the packet its unique IP address and a new port number, which could be any number. It also enters this new port on the table and forwards the packet with the new information.

The response to this new packet is now sent to the IP address of the router with the new sender port number. The entry in the internal table allows the router to assign this response to the original sender again.

You can view these tables in detail in the router statistics (see also 'Status').



Simple and inverse masquerading

This masking operates in both directions: The local network behind the IP address of the router is masked if a computer from the LAN sends a packet to the Internet (simple masquerading).

If, on the other hand, a computer sends a packet from the Internet to, for example, an FTP server on the intranet, from the point of view of this computer the router appears to be the FTP server. The router knows the intranet address of the server from the entry in the service table (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Masq.' tab or in the `Setup/IP-router-module/Masquerading/Service-table` menu). The packet is forwarded to this computer. All packets that come from the FTP server in the local network (answers from the server) are hidden behind the IP address of the router.

The only small difference is that:

- Access to a service (port) in the intranet from outside must be defined in advance by specifying a port number. The destination port is specified with the intranet address of, for example, the FTP server, on a service table to achieve this.
- When accessing the Internet from the intranet, on the other hand, the router itself makes the entry in the port and IP address information table.

The table concerned can hold up to 2048 entries, that is it allows 2048 **simultaneous** transmissions between the masked and the unmasked network.

After a specified period of time, the router, however, assumes that the entry is no longer required and deletes it automatically from the table.

Which protocols can be transmitted using IP masquerading?

Naturally, only those which also communicate using ports. Protocols working without port numbers or using ports above IP in the OSI model cannot be masked without special treatment.

The current version of router implements masquerading for the following protocols:

- FTP
- TCP
- UDP
- ICMP

DNS forwarding

Names rather than IP addresses are generally used to access a server over the Internet. Who knows which address is behind 'www.domain.com'? The DNS server, of course.

DNS stands for Domain Name Service and refers to the assignment of domain names (such as domain.com) to the corresponding IP addresses. This information must be

constantly updated and be accessible all over the world at any time. DNS servers holding long tables containing IP addresses and domain names exist for this purpose.

If a computer calls up a home page from the intranet, it first sends out a DNS request: "Which IP address belongs to `www.domain.com`?" If the router has been specified as the DNS server in the workstations, the request is handled as follows:

- Initially the router checks whether a DNS server has been entered in its own settings (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Addresses' tab or in the `/Setup/TCP-IP-module` menu). If it finds one it connects to this server and retrieves the information required.
- If no DNS server is entered in the router, it will attempt to reach a DNS server over a PPP connection (e.g. from the Internet provider) to get the IP address assigned to the name from there. This can only succeed if the address of a DNS server is sent to the router during PPP negotiation.
- If no connection exists, the default route is established and a search is then carried out there for the DNS server.

This procedure does not require you to have any knowledge of the DNS server address. Entering the intranet address of your router as the DNS server for the workstation computers is sufficient to enable you obtain the name assignment. This procedure also automatically updates the address of the DNS server. The router always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

Policy Based Routing

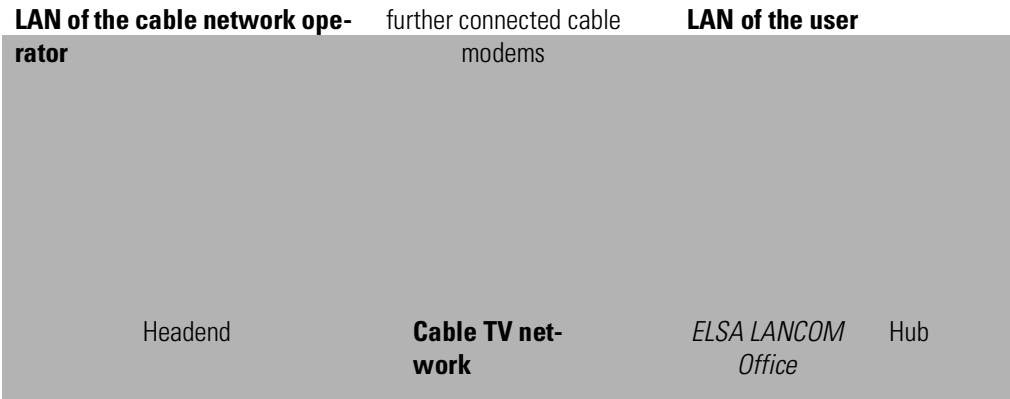
Policy-based routing describes a process in which particular data packets are given preferential treatment. This requires evaluation of a special field within the IP data packet, known as the Type of Service (TOS) field. This preferential treatment of a number of data packets can, for example, simplify the configuration of the router via the WAN when large data volumes are to be transferred simultaneously.



You can find more information on policy based circuit routing in the 'Description of the menu options'.

Bridging

A bridge connects two or more LANs in such a way that they appear to be a single large network. When bridging via cable modems, the LAN of the cable network operator with the headend is on one side and the LAN of the network participants with the cable modem and the local workstations on the other.



In the bridge operating mode, the *ELSA LANCOM Office* transfers all data to computers without locally assigned MAC addresses, between the local network or another local area network (LAN) or a workstation on one side and the cable network on the other side.

The bridge thus learns on its own which MAC addresses are located on its own network and which are located on the other side. After a very high level of data traffic that occurs during the initial negotiations between the two LANs, the network load drops sharply. In this case, the connection will no longer be established so frequently. When receiving data from the cable network, the bridge in the cable modem uses the MAC addresses to determine whether the data is destined for its own LAN. The bridge will only accept data packets that are addressed to MAC addresses in its LAN.

The bridge connects the two participating computers as if they were in fact located in one network. For this reason, however, only those computers which can also theoretically be integrated into a network should be connected. This means that both networks and the network and workstation computer must have the same network addresses.

The bridge is not dependent on the protocol used in layer 3. It operates only with Ethernet addresses (MAC addresses). Please, therefore, ensure that you only use those B-channel protocols in the layer list which have the setting ETHER in the ENCAPS column. Use a protocol other than PPP on layer 3, as this protocol is not supported for the bridge.



It is not possible to use the bridge via 2 B channels, as MLPPP is used for channel bundling.

What do you need to configure the bridge?

First establish which subscriber numbers the *ELSA MicroLink Cable* should listen to and which it should itself transfer externally (Setup/WAN-Module/Interface).

An entry which includes name and subscriber number must exist in the name list for *ELSA MicroLink Cable* to reach the remote station (Setup/WAN-Module/Name-List).

You should specify the correct remote station to the bridge (Setup/Bridge-Module/Remote-ID) since additional remote stations may be entered in the *ELSA MicroLink Cable* over time. This is because the bridge can only connect precisely two

networks together, while one router can manage several remote stations. You should also set (Setup/Bridge-Module/Operating:On) so that the bridge can function.

The process is now completed. The bridge now sets to work transferring all the data packets for non-local MAC addresses to the remote station set.



You can find more instructions on how to configure the ELSA MicroLink Cable as a bridge in the appropriate section of 'Workshop' and in the detailed description of the individual menus in the reference section of the manual.

What are the filter options?

You may not always wish to transfer all data. Much of the data which is bouncing around in the LAN is of no interest to remote networks or computers. For this reason, you can block transfer of the following data packets or only transfer them if the line has been established already: You can thus block transfer of the following data packets via the bridge:

- Broadcast packets: Data directed at all devices accessible in a network (Setup/Bridge-Module/LAN-config/Broadcast).
- Multicast packets: Data which is transferred to all devices accessible in a group (Setup/Bridge-Module/LAN-config/Multicast).
- Unicast packets: This is data directed only at a specific device (meaning a fixed MAC address).

Special filter lists which exclude certain addresses from a transmission or only allow certain addresses can be set up to handle this data. The bridge filters differentiate here between destination and source addresses. You can first establish for both address types whether the associated table contains the addresses to which data is to be transmitted (Setup/Bridge-Module/LAN-config/Dest.-address/Filter-type/pos) or the addresses to be excluded (.../Filter-type/neg). You then enter the MAC addresses to be filtered into the table itself.



This method of filtering by entering the exact MAC address naturally demands a certain degree of maintenance effort. Should the addresses change, when a network adapter is changed for example, the new addresses must be entered to ensure that the bridge continues to function.

Description of the menu options

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

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

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



Some of the features described in this Reference Manual apply only to specific models in the *ELSA LANCOM* family. Restrictions with regard to specific models are indicated by the symbol shown here.







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

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


















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

Symbols







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

Overview of the menus






















Setup

-  Name
-  WAN-module
-  Charges-module
-  LAN-module
-  IPX-module
-  TCP-IP-module
-  IP-router-module
-  SNMP-module
-  DHCP-module
-  NetBIOS-module
-  Config-module
-  LANCAP-Module
-  LCR-module
-  DNS module
-  Time-module





Firmware

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

Status

-  Connection
-  Current-time
-  Operating-time
-  WAN-statistics
-  LAN-statistics
-  PPP-statistics
-  IPX-statistics
-  TCP-IP-statistics
-  IP-router-statistics
-  Config-statistics
-  Queue-statistics
-  Conn.-statistics
-  Info-connection
-  Layer-connection
-  Call-info-table
-  Remote-statistics
-  S₀-bus
-  Channel-statistics
-  Time-statistics
-  LCR-statistics
-  Delete-values

Other







-  Manual-dialing
-  Boot-system
-  Reset-system
-  Upload-system

Status

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

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

The menu has the following layout:

Status		Running status displays
Connection		Status of the WAN route
Current-time		Current time in device
Operating-time		Period of time the device has operated since it was last switched on
WAN-statistics		Displays WAN statistics
LAN-statistics		Displays LAN statistics
PPP-statistics		Point-to-point-protocol statistics
IPX-statistics		Statistics from the IPX and IPX router area
TCP-IP-statistics		Statistics from the TCP/IP area
IP-router-statistics		Statistics from the IP router
Config-statistics		Remote configuration statistics
Queue-statistics		Statistics relating to the packets in the queues of the individual modules
Connections-statistics		Connection information for each interface
Info-connection		Information on the last connection for each interface
Layer-connection		Information on the B-channel protocol used for each interface
Call-info-table		Information on the last 100 calls received
Remote-statistics		Statistics on the last 100 connections
S ₀ -bus		Status of the S ₀ interface
Channel-statistics		Information of the status of the individual channels.
Time-statistics		Time module information
LCR-statistics		Least-cost router information
Delete-values		Deletes all values except tables with substatistics.

Display and keyboard

The display shows status information and error messages issued by the device. The following display modes are available:

- B channel overview (one character per channel)
- B channel status (one line per channel)
- Device status / Device error messages

A total of six keys are available (cursor keys + "Mode" + "Clr"), as well as a two-line display with 40 characters per line, of which 16 characters each are currently displayed. Depending on the devices settings, the text information is displayed in German or English.

B-channel-overview

In the B channel overview the channels are displayed in the form of a table. The individual fields of the table have the following significance:

P : x (status of port 1, first B channel)	P : X	P : X	P : X
1 : x (status of port 1, second B channel)	2 : x	3 : x	4 : x

The following symbols are used for the channel status (shown by x in the table):

.	Channel idle (disabled)
-	Channel idle (enabled)
E (flashing)	An error has occurred on the channel
A (flashing)	Outgoing call
A	Connected (outgoing)
P (flashing)	Incoming call
P	Connected (incoming)
N (flashing)	Negotiation

The cursor keys have no function in this mode.

B channel status display

The B channel status display shows an excerpt from a table with an entry for each B channel. In the event of changes to the status of a channel, the table will jump to the current entry if no cursor key has been used for at least 5 seconds. The status of the channel is displayed in plain text, e.g.:

CH11: Connection LC_PPP

CH12: Remote station LC_PPP not responding

Error messages are retained for 60 seconds. Information with regard to the enabling and disabling of S₀ interfaces is also displayed.

The up and down cursor keys can be used to scroll through the individual lines; use the left and right cursor keys to navigate within the line itself. Although a width of only 16 characters is available, the display has a total width of 40 characters (the visible section can be moved). The display returns to the start 5 seconds after the last horizontal movement.

Device status and device error messages

Channel-independent device status messages and especially error messages (with simultaneous flashing Power/Msg LED) are displayed in this mode. The unit automatically switches to this mode in the event of an error.


The up and down cursor keys permit scrolling through all available messages. The model number (e.g. "Model 4100") and the firmware version always appear as the final message. This display also appears immediately after switching the unit on, before changing to the last current display mode. The error messages in this mode can also be up to 40 characters long.

The Mode key switches between the display modes described above.

The Clr key clears the errors displayed in the device status and device error message display modes.

Status/Connection

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

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

Status/Current-time

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










Status/Operating-time

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

Status/WAN-statistics

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

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

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

Byte-transport-statistics

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

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

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

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

Packet-transport-statistics

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

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:

lfc	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:

lfc	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:

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

Throughput- statistics

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













lfc	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:

lfc	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
Link-active		Display of correct Ethernet connection (data transfer possible). Corresponds to the 'Link' LED on the device.
Negotiation done		The negotiation of the transfer mode between the router and the remote station is complete. This is only relevant if Setup/LAN/Connection is set to 'Auto'.

/LAN-statistics	Running status displays	
Connector		This item shows the connection type currently being used on the Ethernet connection: 10B-TX: 10 MBit, half-duplex FD10B-TX: 10 MBit, full-duplex 100B-TX: 100 MBit, half-duplex FD100B-TX: 100 MBit, full-duplex If 'Auto' is set under Setup/LAN, then this is the connection type the two units have negotiated. This corresponds to the 'Fast' and 'FDpx' LEDs on the unit. If, on the other hand, a fixed transfer mode has been set, this value will be the same as the one in Setup/LAN/Connection.
LAN-rx-bytes		Number of bytes received from the LAN
LAN-tx-bytes		Number of bytes sent to the LAN
LAN-rx-broadcasts		Number of broadcast packets received from the LAN
LAN-rx-multicasts		Number of multicast packets received from the LAN
LAN-rx-unicasts		Number of directly addressed packets received from the LAN
LAN-tx-broadcasts		Number of broadcasts received from the LAN
LAN-tx-multicasts		Number of multicasts received from the LAN
LAN-tx-unicasts		Number of unicasts received from the LAN
Delete-values		Deletes LAN statistics

Status/PPP-statistics

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

/PPP-statistics	Running status displays	
PPP-phases		Statistics relating to the status of PPP protocol negotiation for each interface
LCP-statistics		Displays PPP/LCP statistics
PAP-statistics		Displays PPP/PAP statistics
CHAP-statistics		Displays PPP/CHAP statistics
CBCP-statistics		Displays PPP/CBCP statistics
IPXCP-statistics		Displays PPP/IPXCP statistics
IPCP-statistics		Displays PPP/IPCP statistics
CCP-statistics		Displays PPP/CCP statistics
ML-statistics		Displays PPP/ML statistics

/PPP-statistics		Running status displays
BACP-statistics		Displays PPP/BACP statistics
Rx-options		Displays the LCP, IPCP and IPXCP information received
Tx-options		Displays the LCP, IPCP and IPXCP information sent
Delete-values		Deletes PPP statistics.

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

PPP-phases

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

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

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

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

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

Status/PPP-statistics/LCP-statistics

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

PPP negotiation. Below is a detailed description of the meanings of the parameters for these statistics:

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

Status/PPP-statistics/PAP-statistics

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

Rx-discarded	Number of PAP packets discarded
Rx-request	Number of PAP request packets received
Rx-success	Number of PAP success packets received

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

Status/PPP-statistics/CHAP-statistics

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

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

Status/PPP-statistics/IPXCP-statistics

When IPX is used, the **IPXCP** (Internet Exchange Protocol Control Protocol) indicates the status of the protocol and the packets exchanged in the negotiation. Below is a detailed description of the meanings of the parameters for these statistics:

Rx-discarded	Number of IPXCP packets discarded
Rx-config-request	Number of configure request packets received for IPXCP
Rx-config-ack.	Number of configure acknowledge packets received for IPXCP
Rx-config-nak.	Number of configure negative acknowledge packets received
Rx-config-reject	Number of configure reject packets received for IPXCP
Rx-terminate-request	Number of terminate request packets received for IPXCP
Rx-terminate-ack.	Number of terminate acknowledge packets received for IPXCP
Rx-code-reject	Number of code reject packets received for IPXCP
Tx-config-request	Number of configure request packets sent for IPXCP
Tx-config-ack.	Number of configure acknowledge packets sent for IPXCP
Tx-config-nak.	Number of configure negative acknowledge packets sent
Tx-config-reject	Number of configure reject packets sent for IPXCP
Tx-terminate-request	Number of terminate request packets sent for IPXCP

Tx-terminate-ack.	Number of terminate acknowledge packets sent for IPXCP
Tx-code-reject	Number of code reject packets sent for IPXCP
Delete-values	Deletes IPXCP statistics

Status/PPP-statistics/IPCP-statistics

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

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

Status/PPP-statistics/CBCP-statistics

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

Rx-request	Number of CBCP request packets received
Rx-discarded	Number of CBCP packets discarded
Rx-acknowledge	Number of CBCP acknowledge packets received
Tx-request	Number of CBCP request packets sent
Tx-response	Number of CBCP response packets sent
TX-acknowledge	Number of CBCP acknowledge packets sent
Request-discarded	Number of CBCP request packets discarded

Response-discarded	Number of CBCP response packets discarded
Ack.-discarded	Number of CBCP acknowledge packets discarded
Delete-values	Deletes CBCP statistics

Status/PPP-statistics/CCP-statistics

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

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

Status/PPP-statistics/ML-statistics

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

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

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

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




Rx-options

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

Tx-options

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

The two submenus have the same layout:

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

The LCP table has separate listings for every channel:

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

The IPXCP table shows the negotiated IPX option separately for every channel:








Network	Network number of the WAN network
Node-ID	The Rx options show the node ID assigned to the <i>ELSA LANCOM</i> (generally 000000000000 or the MAC address of the router). The Tx options show the node ID of the remote station (also 000000000000 or the MAC address of the remote station)
Routing-method	The routing protocol in use is given here (RIP/SAP or nothing), in the Rx what the remote station has assigned to us and in the Tx the one that the <i>ELSA LANCOM</i> assigns to the remote station.

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

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

Status/IPX-statistics

The statistics from the IPX area are grouped here and classified by type, socket and router information. The IPX statistics contain the following parameters:

/IPX-statistics	Statistics from the IPX and IPX router area	
MAC-statistics		Statistics from the IPX packet media access control
Watchdog-statistics		Statistics for watchdog packets
Propagate-statistics		Statistics for IPX propagated packets (IPX type 20)
RIP-statistics		Statistics for NetWare RIP
SAP-statistics		Statistics for NetWare SAP
IPX-router-statistics		Statistics on the remote IPX router
Delete-values		Deletes IPX statistics

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

Status/IPX-statistics/MAC-statistics

These statistics include the following values:

IPX-LAN-rx	Number of IPX packets received from the LAN
IPX-LAN-rx-broadcasts	Number of broadcast IPX packets received from the LAN
IPX-LAN-rx-multicasts	Number of multicast IPX packets received from the LAN
IPX-LAN-rx-unicasts	Number of directly addressed IPX packets received from the LAN
IPX-LAN-tx	Number of IPX packets sent to the LAN
IPX-WAN-rx	Number of IPX packets received from the WAN
IPX-WAN-rx-broadcasts	Number of broadcasts received from the WAN
IPX-WAN-rx-multicasts	Number of multicasts received from the WAN
IPX-WAN-rx-unicasts	Number of directly addressed IPX packets received from the WAN
IPX-WAN-tx	Number of IPX packets sent to the WAN
Delete-values	Deletes MAC statistics

Status/IPX-statistics/Watchdog-statistics

These statistics include the following values:

IPX-watchdog-LAN-rx	Number of IPX watchdog packets received from the LAN
IPX-watchdog-LAN-tx	Number of IPX watchdog packets sent to the LAN
IPX-watchdog-WAN-rx	Number of IPX watchdog packets received from the WAN
IPX-watchdog-WAN-tx	Number of IPX watchdog packets sent to the WAN
SPX-watchdog-LAN-rx	Number of SPX watchdog packets received from the LAN
SPX-watchdog-LAN-tx	Number of SPX watchdog packets sent to the LAN
SPX-watchdog-WAN-rx	Number of SPX watchdog packets received from the WAN
SPX-watchdog-WAN-tx	Number of SPX watchdog packets sent to the WAN
Delete-values	Deletes watchdog statistics

Status/IPX-statistics/Propagate-statistics

These statistics include the following values:

Propagate-LAN-rx	Number of IPX propagated packets received from the LAN
Propagate-LAN-filters	Number of IPX propagated packets from the LAN that were received/filtered
Propagate-LAN-tx	Number of IPX propagated packets sent to the LAN
Propagate-LAN-socket-errors	Number of IPX propagated packets from the LAN filtered by socket filter

Propagate-LAN-hop-errors	Number of IPX propagated packet filtered from the LAN by hop count
Propagate-LAN-backroute-errors	Number of IPX propagated packets to be backrouted from the LAN
Propagate-LAN-contention	Number of packets to be routed from the LAN during a defective connection
Propagate-WAN-rx	Number of IPX propagated packets received from the WAN
Propagate-WAN-filters	Number of IPX propagated packets from the WAN that were received/filtered
Propagate-WAN-tx	Number of IPX watchdog packets sent to the WAN
Propagate-WAN-socket-errors	Number of IPX propagated packets filtered from the WAN by socket filter
Delete-values	Deletes IPX propagated packet statistics

Status/IPX-statistics/RIP-statistics

These statistics include the following values:

RIP-LAN-rx	Number of RIP packets received from the LAN
RIP-LAN-errors	Number of RIP packets with defective content received from the LAN
RIP-LAN-tx	Number of RIP packets sent to the LAN
RIP-WAN-rx	Number of RIP packets received from the WAN
RIP-WAN-errors	Number of RIP packets with defective content received from the WAN
RIP-WAN-tx	Number of RIP packets sent to the WAN
Delete-values	Deletes RIP statistics
Table-RIP	Displays RIP table

Table-RIP

There are 256 entries with RIP information in the **RIP table**. It has the following layout:

Network	Hops	Tics	Node ID	Time	Flags
Network address	Number of routers to be passed on the path to the other network	Time required for this route in tics	MAC address of the server	Number of table updates until the entry is deleted	Local, remote, loop or down

Status/IPX-statistics/SAP-statistics

These statistics include the following values:

SAP-LAN-rx	Number of SAP packets received from the LAN
SAP-LAN-errors	Number of SAP packets with defective content received from the LAN
SAP-LAN-tx	Number of SAP packets sent to the LAN
SAP-WAN-rx	Number of SAP packets received from the WAN
SAP-WAN-errors	Number of SAP packets with defective content received from the WAN

SAP-WAN-tx	Number of SAP packets sent to the WAN
Table-SAP	Number of SAP packets received from the LAN
Delete-values	Deletes SAP statistics

Table-SAP There are 512 entries with SAP information in the **SAP table**. It has the following layout:

Type	Server-name	Network	Node ID	Socket	Hops	Time	Flags
Service SAP no.	Server computer name	Network address	MAC address of the server	Socket for the service	Number of routers to the destination network	Number of table updates until the entry is deleted	Local, remote, loop or down

Status/IPX-statistics/IPX-router-statistics

These statistics include the following values:

IPXr-LAN-rx	Number of IPX packets to be routed from the LAN
IPXr-LAN-tx	Number of IPX packets routed to the LAN
IPXr-LAN-hop-errors	Number of IPX packets filtered by hop count to be routed from the LAN
IPXr-LAN-socket-errors	Number of IPX packets filtered by socket filter to be routed from the LAN
IPXr-LAN-net-errors	Number of packets from the LAN to be routed to incorrect networks
IPXr-LAN-backroute-errors	Number of IPX packets to be backrouted from the LAN
IPXr-LAN-contention	Number of packets to be routed from the LAN during a defective connection
IPXr-LAN-down-errors	Number of IPX packets to be routed from the LAN to logged-off networks
IPXr-WAN-rx	Number of IPX packets to be routed from the WAN
IPXr-WAN-tx	Number of IPX packets routed to the WAN
IPXr-WAN-hop-errors	Number of IPX packets filtered by hop count to be routed from the WAN
IPXr-WAN-socket-errors	Number of IPX packets filtered by socket filter to be routed from the WAN
IPXr-WAN-net-errors	Number of packets from the WAN to be routed to incorrect networks
IPXr-WAN-backroute-errors	Number of IPX packets to be backrouted from the WAN
IPXr-WAN-down-errors	Number of IPX packets to be routed from the WAN to logged-off networks
IPXr-intern-rx	Number of packets from internal modules to the IPX router
Networks	Table of networks in the IPX routing table with node IDs
Establish-table	Table of the last 20 packets that required a connection
Delete-values	Deletes IPX router statistics

Establish-table The **establish table** is a further submenu option within router statistics. It contains the last 20 entries, which provide information on the system time, the IPX destination address, and the IPX source address of the data packets that have caused a connection to be established.

An IPX establish table might have the following appearance:

Time	Destination	Source
1T; 16:45:01	00000081 ffffffff 0453	00000001 00a05702000a 0453
1T; 10:45:10	00000081 ffffffff 0452	00000001 00a05702000a 0452

The 'Time' is displayed as the device operating time or the ISDN real time (if this is available from the ISDN terminal). The destination address 'fffffff' might refer, for example, to a broadcast packet. The destination and source addresses both consist of the network number, MAC address and the socket number (all hexadecimal values).

Networks The **network statistics** are also a submenu option within the IPX router statistics. This table provides more extensive information on a static route (remote station). It has the following layout:

Remote-ID	Network	Binding	Propagate	Backoff	Time	Node-ID
Logical remote station	Network address	Binding	Route/Filter	Connection counter	Time remaining until next connection	Node-ID of remote station










The different entries have the following meaning:

Remote-ID	Logical name of the remote station as it is entered in the routing table. An entry for the LAN link is also present; it is located in the first position in the table and has the name "LAN".
Network	Address of the network in which the remote station is located. For remote WAN stations, this corresponds to the entry in the routing table. If the autodetect function is configured in the IPX routing table (/SETUP/IPX-MODULE/LAN-CONFIGURATION/NETWORK), the network that was detected is displayed here.
Binding	Ethernet binding to which the remote station is linked. For remote WAN stations, this corresponds to the entry in the routing table. If the autodetect function is configured in the IPX routing table (/SETUP/IPX-MODULE/LAN-CONFIGURATION/NETWORK), the binding that was detected is displayed here.
Propagate	Filter flag for IPX type 20 (propagated) frames. For remote WAN stations, this corresponds to the entry in the routing table. For the LAN, a route is always entered here.

Backoff	Connection counter for the exponential backoff algorithm. When the connection counter reaches a value of 16, no more attempts are made, meaning that the route is deactivated (also possible for the LAN).
Time	Time remaining (specified in seconds) until the next connection attempt is made by the exponential backoff algorithm. When a connection has been successfully established, the remaining time is set to zero, thus activating the route.
Node ID	Node ID of the responsible router in the WAN network. The node ID of the router is entered here for the LAN entry.

Status/TCP-IP-statistics

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

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

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

Status/TCP-IP-statistics/ARP-statistics

These statistics include the following values:

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

Table-ARP

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

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

Status/TCP-IP-statistics/IP-statistics

These statistics include the following values:

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

Status/TCP-IP-statistics/ICMP-statistics

These statistics include the following values:

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

Status/TCP-IP-statistics/TCP-statistics

These statistics include the following values:

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

Status/TCP-IP-statistics/TFTP-statistics

These statistics include the following values:

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

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

Status/TCP-IP-statistics/DHCP-statistics

These statistics include the following values:












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

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

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

Status/TCP-IP-statistics/NetBIOS

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

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

B-Nodes Broadcast nodes. A B node performs name negotiations exclusively via broadcasts. Such a computer is not visible over a router connection, since broadcasts may not be routed.












P-Nodes Point-to-point nodes. For name negotiations, a P node requires a NetBIOS nameserver (NBNS) as well as a NetBIOS datagram distribution server (NBDD) to transfer datagrams over a router.

M-Nodes Mixed nodes. This type is a mixture of B and P nodes. It acts as a B node in the local network; if the required partner can't be found in the local network, it attempts to locate it using an NBNS query (P node behavior).

W-Nodes This type of node is not permissible according to RFC, but was introduced nevertheless by Microsoft as a hybrid node.

Status/TCP-IP-statistics/DNS-statistics

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

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

The hit list has the following structure:

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






















The individual fields of this list have the following significance:

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

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

Status/IP-router-statistics

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

/IP-router-statistics	Statistics from the IP router area	
IPr-LAN-rx		Number of data packets to be routed from the LAN
IPr-LAN-tx		Number of data packets routed to the LAN
IPr-LAN-local-routings		Number of packets received from the LAN and routed to the LAN
IPr-LAN-network-errors		Number of LAN packets that were not routed
IPr-LAN-routing-errors		Number of LAN packets that must be sent to another router
IPr-LAN-ttl-errors		Number of LAN packets with an expired time-to-live value
IPr-LAN-filters		Number of LAN packets filtered by the filter table
IPr-LAN-discards		Number of LAN packets discarded
IPr-WAN-rx		Number of data packets to be routed from the WAN
IPr-WAN-tx		Number of data packets routed to the WAN
IPr-WAN-network-errors		Number of WAN packets that were not routed
IPr-WAN-ttl-errors		Number of WAN packets with an expired time-to-live value
IPr-WAN-filters		Number of WAN packets filtered by the filter table
IPr-WAN-discards		Number of WAN packets discarded
IPr-WAN-type-errors		Number of packets from the WAN without an IP router ID
IPr-ARP-errors		Number of unsuccessful accesses to the ARP cache
Delete-values		Deletes IP router statistics
Establish-table		Table of the last 20 packets that required a connection
Protocol-table		Table of routed packets arranged by protocol
RIP-statistics		Statistics from the IP/RIP area
Delete values		Deletes IP-router statistics

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

An IP router establish table might have the following appearance:

Time	Dest.-address	Src.-address	Prot.	D-port	S-port
1T; 16:45:01	192.120.131.40	192.120.130.10	tcp	23	4711
1T; 10:45:10	192.120.131.50	192.120.130.10	udp	53	8123

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

Protocol-table

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

A protocol table might have the following appearance:

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

Status/IP-router-statistics/RIP-statistics

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

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

Table-RIP












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

An IP-RIP table might have the following appearance:

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










Status/Config-statistics




















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

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

Status/Queue-statistics

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

/Queue-statistics	Statistics on the queue	
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
WAN-heap-packets		Number of buffers available
WAN-queue-packets		Number of buffers in use
Bridge-internal-queue-packets		Number of bridge packets from the LAN
Bridge-external-queue-packets		Number of bridge packets from the WAN
ARP-query-queue-packets		Number of ARP packets in the query queue
ARP-queue-packets		Number of ARP packets in the normal queue
IP-queue-packets		Number of IP packets in the normal queue

/Queue-statistics		Statistics on the queue
IP-urgent-queue-packets		Number of IP packets in the secured queue
ICMP-queue-packets		Number of ICMP packets
TCP-queue-packets		Number of TCP packets
TFTP-queue-packets		Number of TFTP packets
SNMP-queue-packets		Number of SNMP packets
IPX-queue-packets		Number of IPX packets
RIP-queue-packets		Number of RIP packets
SAP-queue-packets		Number of SAP packets
IPX-watchdog-queue-packets		Number of watchdog-packets
SPX-watchdog-queue-packets		Number of SPX watchdog packets
IPX-router-queue-packets		Number of IPX router packets
Prot-heap-packets		Number of prot heap packets
IPr-queue-packets		Number of packets remaining to be processed by the IP router.
DHCP-server-queue-packets		Number of packets in the receive queue of the DHCP server.
IPR-RIP-queue-packets		Number of packets in the receive queue of the IP-RIP module (for RIP queries, RIP propagations...).
DNS-Tx-queue-packets		Number of packets to be forwarded to DNS or NBNS servers.
DNS-Rx-queue-packets		Number of packets that come from DNS or NBNS servers and are to be forwarded to the host.
IP-Masq.-Tx-queue-packets		Number of packets to be sent masked (to the Internet).
IP-Masq.-Rx-queue-packets		Number of packets received from the Internet and have to be demasked.

Status/Connection-statistics

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

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

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

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

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

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

Status/Info-connection

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

Ifc	Status	Mode	Dialup-remote	Device-name	B1-DT	B2-DT
Ch01	Ready				0	0
Ch02	Ready				0	0

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

Ifc	Designates the associated channel.
Status	Indicates the status of the particular connection. The possible values are: Init , Setup WAN , Ready , Dial , Incoming call , Protocol , Connection , Callback , Bundle and Reserved . The Bundle status is indicated in the display <i>ELSA LANCOM Business 4100</i> by the addition of a "/2" in columns 15 and 16 of the associated display line. Bundle is displayed for the second interface either when a bundle connection has been activated via the first interface or when a leased-line connection with two B channels has been set. Reserved is displayed for the second interface when a connection exists to the first B channel and the Y connection has been deactivated.
Mode	Reflects the type of establishment. The following are possible: Active (active call establishment = dialing) Passive (passive call establishment = call acceptance) CB (call establishment via callback)

Dialup-remote	Indicates the call number of the remote station from the name list.
Device-name	Indicates the logical name of the remote station (if it can be detected). The device name is also displayed on the appropriate display line as soon as a logical connection is established.
B1-DT	Indicates the short timeout for the connection.
B2-DT	Indicates the short timeout for bundled channels for this connection.

Status/Layer-connection

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

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

Status/Call-info-table

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

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

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

The different entries have the following meaning:

System-time	Time when the call came. Either the device operating time or the system time of the ISDN is displayed (if made available from the ISDN terminal).
Ifc	Designates the associated interface.
CLIP-Caller	Call number (CLIP) of the caller

Dial-Caller	The MSN/EAZ dialed by the caller
Capab.	The service requested by the caller. Possible values are HDLC64K, HDLC56K and unknown. An analog call is displayed as unknown here.
B-chan.	The B channel used. A value of 0 means that all channels have already been seized, i.e. call waiting is activated.

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

Status/Remote-statistics

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

The table has the following layout:

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



The different entries have the following meaning:

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

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

Status/S₀-bus

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

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

D-info

This table shows general information related to the D channel:

Channel	B-channel identification.
Protocol	D-channel protocol. Either the protocol fixed in the interface table or the protocol detected in the 'Auto' settings at the ISDN terminal.
Layer-2	Activation of layer 2 of the D channel ('Yes' or 'No')
TEI	TEI assigned ('Yes' or 'No')
S ₀ -activation	Displays activation status ('Yes' or 'No')

D2-statistics

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

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

Status/Channel-statistics

This table shows information on the current status of the two B channels. The information from this table is primarily used for output via *ELSA LANmonitor*. Therefore, some values are shown simply as bits with no further explanation.

The table has the following layout:

Channel	State	App	Mode	Cause	Dialup-remote	Sub-address	Charge	Conn.-time	Extra	ISDN-display
S ₀ -1-ERR	00000000	Router	active	0000	0241123456	00000000	3	0		
S ₀ -1-B1	00000000	a/b	active	0000	0241123457	00000000	2	20		
S ₀ -1-B2	00000000	LAN-CAPI	passive	0000	0241123458	00000000	4	180		





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

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

Status/Time-statistics

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

The menu has the following layout:

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

Status/Time-statistics/ISDN







These statistics include the following values:

Connection	Number of attempts to read time information from the ISDN
Information	Number of time updates received from the ISDN
Info-error	Number of erroneous time updates received from the ISDN
Units	
Delete values	Deletes ISDN statistics

Status/LCR-statistics

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

The menu has the following layout:

/LCR-statistics		Least-cost router statistics
Total calls		Total number of LCR calls
Found-events		Number of calls in which the router found a suitable rule in its tables and successfully rerouted the connection.
Not-found-errors		Number of calls in which the router did not find a suitable rule in its tables and thus could not reroute the connection.
Missing time-errors		Number of calls in which the LCR could not become active due to lack of time
Provider-statistics		A table with all providers used (or their prefixes), the number of successful and unsuccessful calls
Delete values		Deletes LCR statistics









Status/Delete-values








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

```
do delete-values
```

Setup

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

/Setup		System configuration
Name		Entering the device name
WAN-module		WAN settings
Charges-module		Charge management settings
LAN-module		LAN settings
IPX-module		IPX module (IPX router) settings
TCP-IP-module		TCP/IP module settings
IP-router-module		IP router module settings
SNMP-module		Settings for configuration via SNMP

/Setup		System configuration
DHCP-module		DHCP server settings
NetBIOS-module		Settings for the NetBIOS proxy
Config-module		Configuration module settings
LANCAPI-module		<i>ELSA LANCAP</i> i settings
LCR-module		Least-cost router settings
DNS module		DNS server settings
Time-module		Time module settings

Name

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

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

In the default configuration, no name is entered.







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







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

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

Setup/WAN-module

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

/WAN-module		WAN settings
Interface-list		S ₀ interface settings
Router-interface-list		Router module settings
Channel-list		Settings for the use of the available channels
Name-list		Remote station settings
RoundRobin-list		Settings for different remote station numbers
Layer-list		Settings for the layer combinations used

/WAN-module		WAN settings
PPP-list		Parameter settings for PPP connections
Number-list		Settings for call numbers with access authorization
Script-list		Dial script settings
Manual-dialing		Settings for manual connection control
Protect		Protection for answering incoming calls
CB-attempts		Number of callback attempts when the remote station is busy
Backup-delay-seconds		

Interface-list

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

Ifc	Protocol	LL-B-chan.	Dial-prefix
S0	Auto	1	0

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

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

`setup/lancapi-module`

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

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

*Router-
interface-list*

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

Ifc	MSN/EAZ	YC.	CLIP
S0	123456	Off	On

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

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

Channel list

The channel list specifies the number and sequence of the channels to be established.

Device-name	Min	Mx	Order	Backup
LONDON	2	2	1-1;1-2	1
INTERNET	2	2	1-1;1-2;2-1;2-2	0
DEFAULT	1	2	0	

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

Device-name	Name of the remote station that is also used in the name and PPP lists.
Min	Number of static channels. These channels are used during every call establishment to the remote station.

Mx	The maximum number of channels to be used for this remote station. The Max-Min difference is the number of dynamic channels.
Order	This defines which channels are to be established on which S ₀ bus. Syntax: [<BusNo>-<ChannelNo>];<BusNo>-<ChannelNo>]... Possible values: 1 to 4 for the busses, 1 or 2 for the channel. If no entry has been made, a random channel on a random bus will be used. If one or more leased lines are to be used, an entry must be available for each leased line.
Backup	Number of possible backup connections. These connections will be established in the event that all valid leased-line channels are down. Backup connections always use a random channel on a random bus.

Name-list

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

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

Device-name	Dialup-remote	B1-DT	B2-DT	WAN-layer	Callback
GLASGOW	875463	180	0	PPPHDL	On
LONDON	040785647	20	20	DEFAULT	Off

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

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

■ Callback options

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

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

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

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

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

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

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

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

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

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

Layer-list

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

The following table below is provided as an example and also shows the default settings for an *ELSA LANCOM Office*:

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	TRANS	PPP	TRANS	bnd+cmpr	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	none	HDLC64K
MLPPP	TRANS	PPP	TRANS	bnd+cmpr	HDLC64K
RAWHDL	TRANS	TRANS	TRANS	none	HDLC64K

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

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

Lay-3	In the lay-3 column, you can define additional headers for data transmission in ISDN. You can select from among the following settings:	
	TRANS	No additional header is inserted (higher data throughput). Always select this setting if the remote station sends the data transparently via ISDN layer 3 (e.g. transparent HDLC, transparent X.75LAPB).
	PPP	A negotiation is performed according to the point-to-point protocol.
	APPP	A negotiation is performed as per the asynchronous PPP. APPP is then used when synchronous PPP is not possible because the connection does not permit a synchronous transmission (e.g. for analog modem operation).
	SCPPP	Following completion of script processing, a synchronous PPP negotiation is initiated.
	SCAPPP	Following completion of script processing, an asynchronous APPP negotiation is initiated.
	SCTTRANS	Following completion of script processing, a connection exists to the remote station. No further protocol negotiation is performed.
Lay-2	In this column, you can select the protocol for ISDN layer 2:	
	TRANS	The data is packed directly in HDLC packets. Always select this setting if communication is to take place via transparent HDLC.
	X.75LAPB	The data is exchanged in X.75 secured format. Always select this setting if the remote station is to work with X.75 data protection.
L2-Opt.	The L2-opt. enables the setting of an option for the data transfer setting under Lay-2 with an additional <i>ELSA LANCOM</i> .	
	none	No data compression or channel bundling is performed.
	compr.	Stac data compression will be used. Compression as per Stac (Hi/fn) must be used in connection with PPP or multilink PPP. Stac compression may also be used in connection with Windows remote stations.
	bundle	Channel bundling is performed via several B channels. Channel bundling is only possible for the Lay-2 settings of 'PPP'.
	bnd+cmpr	Channel bundling and data compression takes place over two B channels.
Lay-1	The lay-1 column allows you to define the speed at which the data is sent in ISDN.	
	HDLC64K	The data is transmitted at 64,000 bps.
	HDLC56K	The data is transmitted at 56,000 bps. This setting is especially important for connections in the USA.
	V110_9K6	Data is transferred at 9,600 bps in a V.110 connection, when connecting to GSM mobile phones, for example.
	V110_19K2	Data is transferred at 19,200 bps in a V.110 connection.
	V110_38K4	Data is transferred at 38,400 bps in a V.110 connection.

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

For Internet and remote access, PPP is generally specified.

PPP-list

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

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

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

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

Device-name	In the Device-name column, you can enter the name with which the remote station logs onto the router. In the case of connections via the data transmission network, this is the name entered as "Username". For remote access via the data transmission network, the 'Username' field (see below) is not evaluated! Entries are not case-sensitive!	
Auth.	In this column, you can enter the security procedure to be used for verification of the remote station. Default: PAP	
	None	The router does not negotiate authentication with the remote station when establishing a connection. However, the remote station can itself require authentication from the router. This is the case when dialing up a connection to an ISP, for example.
	PAP	The remote station is checked as per the Password Authentication Protocol.
	CHAP	The remote station is checked as per the Challenge Handshake Authentication Protocol.
Key	A password may be entered in this column. Its presence is indicated by the symbol * and it is used to check the remote station. It may consist of 95 characters (7-bit ASCII, including spaces). Default: None. The <code>set ?</code> command shows a list of the allowable characters.	
Time	In this column, you can enter the period of time between two remote station verifications specified in minutes. The CHAP protocol must be set here. Default: 0	
Try	In this column, you can specify the number of times the verification attempt is to be repeated. If verification fails, the connection is immediately terminated. Default: 5	
Conf, Fail and Term	These parameters may be used to influence the operation of the PPP. They are defined and described in RFC 1661. The default values are sufficient for most remote stations. If nothing is entered here, the values 0,0,0 appear in the display but the default values 10, 5, 2 are still used. These parameters can only be changed via SNMP or TFTP (using the <i>ELSA LANconfig</i> configuration program)!	
Username	The user name (max. 64 characters) transmitted to the remote station during PPP negotiation. The router identifies itself to the remote station with it. If no user name is entered, the device name serves as the user name. Entries are case-sensitive here.	
Rights	Network protocols to be routed over this connection: IP, IPX, NTB (NetBIOS). NetBIOS always requires one of the other two protocols. The routing of IP or NetBIOS via PPP always requires a suitable route (in the IP routing table for IP or in the remote-station table for NetBIOS).	

Number-list

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

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

Dialup-remote	Device-name
875463	GLASGOW
040785647	LONDON

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

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

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

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

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

Script-list

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

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




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

The entries in the script list have the following meaning:

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

Setup/WAN-module/Manual-dialing

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

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

Connect

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

You can use the command

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

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

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

Disconnect

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

Setup/WAN-module/protection

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

- If 'Protect' is set to 'none', all pending calls are answered provided that the remote end supports the connection protocol.

- If this option is set to 'name', calls are accepted only from remote stations for which an entry is found in the name list. This verification provides additional protection. This verification is only available when using PPP.
- If this option is set to 'number', calls are accepted only from remote stations that are entered in the number list as authorized remote stations.
- The 'no./name' setting allows you to select combined protection using a name list and number list. First a verification that there is an entry in the number list is made. If this is not possible, the router will attempt to determine the name using the protocol negotiation.

Setup/WAN-module/CB-attempts




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

Setup/WAN-module/Backup-delay-seconds

The backup start time indicates the number of seconds to elapse before the first backup attempt is started after determining that the leased line is down. If the value 0 is entered, no backup connection will be established actively.

Setup/LAN-module

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

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

Connector

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

Connect	Meaning
Auto	Default setting; enables the Autosense function of the network chip. This automatically sets the router to the port in use without requiring manual configuration of this item.
10BTX	10BASE-T in half-duplex mode
FD10BTX	10BASE-T in full-duplex mode
100BTX	100BASE-T in half-duplex mode
FD100BTX	100BASE-T in full-duplex mode

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

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

Node-ID







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

Spare-heap

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

Setup/IPX-module

This menu allows you to enter settings for the IPX module, particularly for the IPX router. The menu has the following layout:

/IPX-module	IPX module (IPX router) settings	
Operating		Activates or deactivates the IPX module.
IPX-router		Activates or deactivates the IPX router.
LAN-config		Settings for the LAN side
WAN-config		Settings for the WAN side
RIP-config		RIP settings
SAP-config		SAP settings

Operating

This option allows you to activate or deactivate the IPX module. In the default configuration, the IPX module is activated.

Remote configuration via DOS/IPX and the IPX router can be used only if the IPX module is activated. For local configuration via a LAN, the router does not have to be activated.










IPX-router

This option allows you to activate or deactivate the IPX router. In the default configuration, the IPX router is deactivated.

When the IPX router is activated, the IPX module is also activated. The IPX router can be activated only if different, permissible network addresses are entered under LAN-configuration and WAN-configuration.

Setup/IPX-module/LAN-configuration

Settings for the LAN data packets may be made here. The menu has the following layout:

/LAN-configuration		Settings for the LAN side
Network		Logical IPX network number of the LAN port
Binding		Ethernet frame type setting for the LAN port
IPX-watch		Settings for IPX watchdog management
SPX-watch		Settings for SPX watchdog management
NetBIOS-watch		Settings for NetBIOS watchdog management
Socket-filter		Filter table for destination socket filtering
Loc.-routing		Activates or deactivates local routing.
RIP-SAP-scal.		Activates or deactivates RIP-SAP scaling.
LOOP-prop.		Activates or deactivates propagation of redundant routes.

Network

The NetWare network number of the network (8-digits, hexadecimal) that is connected to the LAN port under the binding (see below) may be entered here. If there is a NetWare server in the local network, the router can automatically detect the network number and the binding.

The default value is '00000000' and means that the router should automatically detect the network number.

Binding

This option allows you to select the Ethernet packet format (Auto, II, 802.3, 802.2, SNAP) for the LAN port. This format must match the Ethernet format used in the local network under the above-mentioned network number.

The default is 'auto' and means that the router should automatically detect the binding (only if there is a NetWare server in the local network).

IPX-watch

This option allows you to define the type of management used for IPX watchdog packets.

- **Filt.** means that the IPX watchdog packets are neither answered nor transferred locally. Users are always logged off after the period of time set in the NetWare server.
- **Route** causes the watchdog packets to be transferred and, consequently, also causes a regular establishment of connections by means of the server's watchdog packets.
- **Spoof** (default) ensures that IPX watchdog packets are answered locally by the router and therefore that users are no longer automatically logged off. This setting is especially economical but steps must be taken in the server to ensure that users are logged off at specific times in order to prevent the usage of too many user licenses.

- SPX-watch* This option allows you to define the type of management used for SPX watchdog packets.
- **Route** causes the SPX watchdog packets to be transferred and, consequently, also causes a regular establishment of connections by means of the server's SPX watchdog packets.
 - **Spoof** (default) causes SPX watchdog packets to be answered locally. This setting is especially economical.

NetBIOS-watch This item specifies how NetBIOS watchdog packets should be treated. NetBIOS watchdog packets occur, e.g., if Windows networks are connected by IPX. The same options are available as with IPX or SPX watchdog packets (filter, route, spoof).

Socket-filter The socket filter table permits the selective filtering of LAN packets to specific ranges of destination sockets. Filtering is performed for both single IPX packets and propagated IPX packets. The following sockets (which are periodically sent in the network and, therefore, would result in connections being established too frequently) are already entered in the LAN filter table as default values (for details, also see FAQs on the 'IPX router').

Start-socket	End-socket
0455	0457
0550	0555
1401	1402
1480	1481
83ba	83ba
900F	9010

Loc.-routing This setting supports the scaling of multiple routers in a local network. When all the channels for one router are already seized and packets for other remote stations are still being received at this router, other routers in the LAN may still have free channels.

If the 'Loc.-routing' option is activated, the router forwards the packets in the local network to a router that has propagated a route to the remote station desired. The router has saved this route, although it is less efficient than its own, and marked it with the 'reserve' flag in the RIP table.

The default setting for this option is 'Off' since an IPX client sends a RIP request for the relevant route after a timeout, thus automatically finding a different router through which it can access the destination network.

RIP-SAP-scal. Another option for supporting scaling is to propagate every route to which there is an active connection with a somewhat better tic count than the actual one. This will ensure that all clients will send their packets for these routes to the router that has the connection. In addition, in the event that all channels are busy, the routes that are no longer available will be propagated as 'DOWN'. Because one or more broadcasts are

sent on the LAN by this procedure every time a connection is established and released (which may require other routers for additional broadcasts and may result in a high network load), this feature can be activated and deactivated. The default setting is 'Off'.



LOOP-prop.

Redundant routes, i.e. routes with the same tic and hop count, are only sent to the remote station by which they were not received (split horizon). When the 'LOOP-prop.' function is activated, these routes can still be propagated. Redundant routes are identified in the RIP table by means of the LOOP flag.

Although the propagation of redundant routes is not prohibited by the Novell specification, it should still be avoided as much as possible. Therefore, the default setting is 'Off'.

Setup/IPX-module/WAN-configuration

This option allows you to maintain the data packet settings for the WAN port. The menu has the following layout:

/WAN-configuration		Settings for the WAN side
Routing-table		Routing table for IPX network and remote station assignment
Socket-filter		Filter table for destination socket filtering

Routing-table

The routing table can hold up to 16 remote stations and destination networks. It contains the following entries:

Remote-ID	Network	Binding	Propagate	Backoff
Name of the IPX remote station	Network address	802.3, II, 802.2, SNAP	Route / Filter	On / Off

The columns have the following meanings:

- **Remote-ID:** Name of the logical remote station (as specified in /Setup/WAN-module/Name-list).
- **Network:** Address of the network on the WAN side. A standalone network must be used, but it must be same for both of the participating routers!
- **Binding:** The Ethernet binding to be used on the ISDN route. This setting is taken into account only if Ethernet encapsulation is set in the layer used. If no binding is specified, a value of 802.3 is assumed.
- **Propagate:** This entry indicates how IPX type-20 packets (NetBIOS propagated frames) are to be handled. The possible settings are Route and Filter. With **Filter**, no propagated frames are routed to the remote station. If the entry has the value **Route**, the packets are forwarded to all currently available remote stations, i.e., there must be a connection to the remote station, or there must be at least one channel available for establishing a connection the remote station.

If no connection or channel is available, the packet is discarded. As a result, the maximum number of remote stations that can receive propagated frames corresponds to the number of possible simultaneous connections. The default setting is 'Filter'.

- **Backoff:** The IPX router uses a special algorithm (exponential backoff) to keep the connection charges as low as possible in the event of erroneous configurations (see below).

If there is no server in the remote network (e.g. with remote access from a workstation), the router cannot detect this and the corresponding remote station will be deactivated after a day at the latest. In order to prevent this from happening, the exponential backoff algorithm can be deactivated for these remote stations.

The default setting is 'On'.

Socket-filter

The socket filter table permits the selective filtering of WAN packets to specific ranges of destination sockets. Filtering is performed for both single IPX packets and propagated IPX packets.

Setup/IPX-module/RIP-configuration

This option allows you to store settings for RIP data packets (router information). The menu has the following layout:








/RIP-configuration		RIP settings
Table-RIP		Displays the RIP table.
LAN-filter-table		Filter ranges for IPX network addresses (LAN)
WAN-filter-table		Filter ranges for IPX network addresses (WAN)
Routes/Frm		Max. no. of RIP entries per RIP frame sent
Aging-minute(s)		Aging period in update units
Spoofing		Sets RIP spoofing procedure
WAN-update-min.		RIP update period; effectiveness depends on spoofing

Table-RIP

This option allows you to display the entries in the current RIP table. The table contains a maximum of 256 entries.

The entries in the RIP table might, for example, look like the entries shown below with the networks 00000001, 00000002, 00000010, 00000081, where these networks can be accessed via different routers. The flags can be used to determine where these networks are located with relation to the particular router (**local** or **remote**). The entry **direct** indicates whether this network is directly the local or remote network. **DOWN** indicates

a network that is known but is not currently available. The table is sorted by the network numbers.

Network	Hops	Tics	Node-ID	Time	Flags
00000001	0	1	00a05702000a	0	local, direct
00000002	1	2	00608c70ab56	1	local
00000010	2	7	00A057020014	1	local, DOWN
00000081	1	6	00a05702000b	0	remote, direct

LAN-filter-table The LAN filter table permits the selective filtering of routes that are 'learned' via the local network. Filtered routes do not appear in the IPX-RIP table.

A LAN filter table for filtering routes in the range from 00001000 to 00001fff might, for example, have the following appearance:

Start-net	End-net
00001000	00001fff

WAN-filter-table The WAN filter table permits the selective filtering of routes that are 'learned' via the wide-area network. Filtered routes do not appear in the IPX-RIP table.

A WAN filter table for filtering routes in the range from 00002000 to 00002fff might, for example, have the following appearance:

Start-net	End-net
00002000	00002fff

Routes/FRM This parameter sets the maximum number of routes that can be included in a RIP frame. The specified value originally defined by Novell is 50. Today, however, it is common practice to pack a higher number of routes in each frame in order to reduce network utilization. If all participating devices in the network support a higher number, this value can be raised as high as 182.

Aging-minute(s) This option allows you to set the number of times the RIP table will be updated until an entry in the RIP table ages, i.e. until the route recorded there is marked as 'not reachable (down)'. You can enter a value from 1 to 60; the default value is 3.

Spoofing

This option allows you to determine how the router will handle RIP packets.

- If you select **Off**, RIP packets are handled in the WAN in precisely the same manner as in local networks. RIP data are sent to the remote side in the event of new information and at intervals of one minute, i.e. a connection is established.
- With the **Trig** setting, the RIP data is sent to the remote end any time changes are detected.
- With the **Time** setting, the RIP data is sent to the remote end at selectable intervals (see below).
- **pBack** (default) is the most economical setting. In this case, the RIP data is sent to the remote end only when a connection is activated.

*When spoofing is set to **pBack**, entries in the RIP table age only when a new connection is established and an entry has been explicitly marked as 'not reachable'.*

WAN-update-min.

The periodic transfer interval for a spoofing time control in which RIP data can be transferred to the remote side is given here. You can enter a value from 1 to 60 minutes; the default value is 5.

Setup/IPX-module/SAP-configuration

This option allows you to store settings for SAP data packets (server information).








/SAP-configuration		SAP settings
Table-SAP		Displays the SAP table.
LAN-filter-table		Filter ranges for IPX service addresses (LAN)
WAN-filter-table		Filter ranges for IPX service addresses (WAN)
Server/Frm		Max. no. of SAP entries per SAP frame sent
Aging-minute(s)		Aging period in update units
Spoofing		Sets SAP spoofing method.
WAN-update-min.		SAP update period; effectiveness depends on spoofing.

Table-SAP

This option allows you to display the entries in the current SAP table. The table contains a maximum of 512 entries. It is sorted first by service type and then by server name. A SAP table might, for example, have the following appearance:

Type	Server-name	Network	Node-ID	Socket	Hops	Time	Flags
0004	Y	000000c1	000000000001	0451	1	1	local
0047	X	00000001	0000c0123456	8060	1	0	local
0107	Z	000000c1	000000000001	8104	2	1	local

Different SAP types are stored in the table. The server name, the applicable network, the server MAC address (000000000001 for internal server networks), the socket number and information on the location of the server must be read.

LAN-filter-table Entries in the LAN filter table make it possible to exclude specific service information ranges of a Novell network from being included in the SAP table and therefore to make better use of the resources of the IPX router. This also prevents unwanted connections from being established by these SAPs (services).

None of the service information located within a range of filters entered in the LAN filter table is transferred by the local network to the IPX router's SAP table. They are also not transferred to the remote station of the IPX router and therefore are also not available there.

For example, the service information for the printer server is often unnecessary for the remote station of the IPX router. If this information is to be excluded from the SAP table by means of the LAN filter table, the following entry is required:

Start-service	End-service
030c	030c

For a list and description of SAP services, please refer to the section entitled 'Novell SAP Numbers'.

WAN-filter-table As with the LAN filter table, you can use the WAN filter table to prevent ranges of service information from being transferred from the WAN to the SAP table.

Therefore, the blocked services have resulted in the establishment of a connection to the remote station before the destination router could filter them on the WAN side.

The layout and function of the WAN filter table are exactly the same as that of the LAN filter table. A WAN filter table for filtering file services might, for example, have the following appearance:

Start-service	End-service
0004	0004

Server/FRM This parameter sets the maximum number of services that can be included in a SAP frame. The specified value originally defined by Novell is 7. Today, however, it is common practice to pack a higher number of services in each frame in order to reduce network utilization. If all participating devices in the network support a higher number, this value can be raised as high as 22.

Aging-minute(s) This option allows you to set the number of times the SAP table will be updated until an entry in the SAP table ages, i.e. until the service recorded there is marked as "not reachable (down)". You can enter a value from 1 to 60; the default value is 3.

Spoofing

This option allows you to determine how the router will handle SAP packets.

- If you select **Off**, SAP packets are handled in the WAN in precisely the same manner as in local networks. SAP data are sent to the remote side in the event of new information and at intervals of one minute, i.e. a connection is established.
- With the **Trig** setting, the SAP data is sent to the remote end any time changes are detected.
- With the **Time** setting, the SAP data is sent to the remote end at selectable intervals (see below).
- **pBack** (default) is the most economical setting. In this case, the SAP data is sent to the remote end only when a connection is activated.















*When spoofing is set to **pBack**, entries in the RIP table age only when a new connection is established and an entry has been explicitly marked as 'not reachable'.*

WAN-update-min.

The periodic transfer interval for a spoofing time control in which SAP data can be transferred to the remote side is given here. You can enter a value from 1 to 60 minutes; the default value is 5.

Setup/TCP-IP-module

This menu allows you to enter settings for the TCP/IP module. The menu has the following layout:

/TCP-IP-module	TCP/IP module settings	
Operating		Activates or deactivates the TCP/IP module.
IP-address		Local IP address
IP-netmask		Local network's matching IP network mask
Intranet addr.		Local Intranet address
Intranetmask		Local network's matching Intranet network mask
Access-list		Restricts access to internal functions via TCP/IP.
DNS-default		Domain name server
DNS-backup		Backup domain name server
NBNS-default		NetBIOS name server
NBNS-backup		Backup NetBIOS name server
Table-ARP		ARP table for mapping an IP address onto a MAC address
ARP-aging-min.		Dwell time for entries in the ARP table
TCP-aging-min.		Time limit for configuration connections that are inactive
TCP-max.-conn.		Max. number of simultaneous configuration connections to the <i>ELSA LANCOM</i>

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

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

IP address The IP address for the router may be entered here. The default address on delivery is '0.0.0.0'.

If IP masquerading is used, this address takes on a special meaning in connection with the Intranet address:

If the IP address is assigned to the router by the Internet provider by PPP, all computers in the network linked by IP address and IP network mask are normally routed. These computers can then also be accessed directly from the Internet.

IP-netmask The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network). A network mask of 255.255.255.255 means that there is only one computer in this network (the router itself). This setting (an IP address registered in the Internet with a fully assigned network mask) can be used for masquerading via a raw IP access, such as that offered by the provider of the individual network. With such an access an IP address is not assigned to the router by a PPP negotiation, but it must have a fixed IP address registered in the Internet.

Intranet-address A second IP address for the router may be entered here. This enables the router to be used as a router for two logical IP networks and also this address has a specific meaning with the use of IP masquerading:

In this case, all computers that are in the network linked by Intranet address and Intranet mask are hidden behind the address assigned by the provider (or the Internet address (IP address)).

The default address on delivery is '0.0.0.0'.

Intranet-mask The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network).



If neither an IP nor an Intranet address has been specified, the device responds to a default IP address, the first three digits of which are identical to the first three digits of the sending device XXX.XXX.XXX.YYY. The device can then be reached by dialing the IP address XXX.XXX.XXX.254.

In the event that such an address already exists in the network, a different address must be entered via outband configuration (terminal program).



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

Access-list

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



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

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

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

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

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

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

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

IP-address	IP-netmask
192.234.222.0	255.255.255.0

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

DNS-default

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

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

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

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

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

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

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

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

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












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

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

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

Setup/IP-router-module

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

/IP-router-module		IP router module settings
Operating		Activates or deactivates the IP router module.
IP-routing-table		Router table for IP network and remote station assignment
LAN-filter-table		Negative/connect filter table for the TCP/UDP destination ports of LAN packets
WAN-filter-table		Negative filter table for the TCP/UDP destination ports of WAN packets
Proxy-ARP		Activates/deactivates the proxy ARP function
Loc.-routing		Activates/deactivates local routing
Start-WAN-Pool		Start of the address pool for dynamic address assignment for remote access
End-WAN-Pool		End of the address pool.
Routing-method		Routing method for IP packets
RIP-config		Settings for IP-RIP operation
Masquerading		Settings for IP masquerading

Operating

This option allows you to activate or deactivate the IP router module. In the default configuration, the IP router module is activated.

Activating the IP router module also activates the TCP/IP module.

IP-routing-table

The routing table can contain a maximum of 128 entries of destination network addresses or direct IP addresses with netmasks, and the names or IP addresses of other local routers. Alternatively, you can enter a setting by means of which packets to specific destination IP addresses are discarded and are not answered by proxy ARP. This is done by entering 0.0.0.0 for the name of the responsible router.

The 'Masquerade' field indicates whether the route should be masked or not. The following options are offered here:

- **On:** IP masquerading is switched on and functions with dynamic assignment of the IP address by the remote station. In this procedure the router queries the IP address '0.0.0.0' at the remote station and is assigned a random IP address by the remote station, which is then used for further processing.
- **Off:** Masquerading is switched off.
- **Static:** IP masquerading is switched on and functions with assignment of a static IP address previously assigned by the remote station. In this procedure the router queries the IP address entered under 'Setup/TCP-IP-module' at the remote station

and is assigned this address by the remote station. Use this setting when the remote station (e.g. your Internet provider) has assigned you a fixed IP address in the access data. Of course, this procedure will only function when this address has also been entered in the router as the IP address.

The IP routing table is generally sorted as shown below:

- The longest network mask is placed on top.
- For network masks of equal length, the one with the smallest IP address is placed on top.

In order to identify the correct remote station, the router searches the routing table from top to bottom using the destination IP address received. If a matching entry is found, the router name found is used for establishing the connection.

Address ranges that are prohibited in the Internet are excluded from transmission by preset entries in the IP routing table (the router name 0.0.0.0 means that packets to these addresses are not transmitted). The IP routing table below is provided by way of example and also shows the default settings:

IP-address	IP-netmask	Router-name	Distance	Masquerade
192.168.0.0	255.255.0.0	0.0.0.0	0	Off
172.16.0.0	255.240.0.0	0.0.0.0	0	Off
10.0.0.0	255.0.0.0	0.0.0.0	0	Off
224.0.0.0	224.0.0.0	0.0.0.0	0	Off

However, if these addresses are required for Intranet use, for example, it is possible to delete the predefined entries at any time. If the routing table contains no entries with the router name 0.0.0.0, the router processes all IP addresses with valid routes.

- Example
 - The local network address is 192.120.130.0.
 - Three terminal units must be available via proxy ARP with the IP addresses 192.120.130.10, 192.120.130.11 and 192.120.130.12 via an *ELSA LANCOM* 'Leeds'.
 - Two destination networks 192.120.131.0 and 192.120.132.0 can be accessed by the remote stations 'GLASGOW' and 'LONDON'.
 - Data packets for the destination network 193.140.300.0 are to be sent to another local router with the IP address 192.120.130.200.
 - Absolutely nothing is to be transmitted to the destination network 193.140.200.0.
 - All other non-local data packets must be sent to the router 'PROVIDER' at the Internet service provider.

In this example, the router table would contain the following entries:

IP-address	IP-netmask	Router-name	Distance	Masquerade
192.120.130.10	255.255.255.255	LEEDS	0	Off
192.120.130.11	255.255.255.255	LEEDS	0	Off
192.120.130.12	255.255.255.255	LEEDS	0	Off
192.120.131.0	255.255.255.0	GLASGOW	0	Off
192.120.132.0	255.255.255.0	LONDON	0	Off
193.140.200.0	255.255.255.0	0.0.0.0	0	Off
193.140.300.0	255.255.255.0	192.120.130.200	0	Off
255.255.255.255	0.0.0.0	PROVIDER	0	On

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

The last line is an entry for the "default route". The IP address 255.255.255.255 means the same as 0.0.0.0 (for technical reasons, 0.0.0.0 cannot be entered in the first column). Because it contains the IP network mask 0.0.0.0, this line is always appropriate after the rest of the table has been searched. Therefore, the router sends everything that it cannot transfer over other routes and should not discard or that comes from a WAN terminal and is not local to the router at the provider.

LAN-filter-table This table allows you to filter specific ranges of destination ports. In addition, you can determine how the packets are to be filtered. If packets with the entered ports are received from the LAN side, they will not be forwarded (always filter) unless a connection is currently in place (connect filter) or unless they can be routed over other than the DEFAULT route (I-Net filter).

The LAN port filters are defined in a table with the following layout:

Idx.	D-st.	D-end	S-st.	S-end	Src.-addres	Src-netmask	Prot	Type
WIN	0	0	137	139	255.255.255.255	0.0.0.0	TCP and UDP	Always s-filt.

The table fields have the following meaning:

■ **Idx.**

Unique index. This entry is required to enable the filters to be distinguished. The index may be four characters long and selected as desired.

- **D-st., D-end**
Destination port range that is to be filtered. A range of 0 to 0 means that no destination port is affected by this filter.
- **S-st., S-end**
Source port range that is to be filtered. A range of 0 to 0 means that no source port is affected by this filter.
- **Src-address, Src-netmask**
A subnetwork of the local network for which the filter is valid can be entered here. A source address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).
- **Prot**
Protocol that is to be filtered. Possible entries are **TCP**, **UDP**, **ICMP** and **all**.
The setting **all** filters out every packet from the specified source network or to the destination network.
- **Type**
Filter type. The possible values are Always-filt., Connect-filt. and Internet-filt.
 - **Always** filter: The packet is discarded.
 - **Connect** filter: The packet is discarded if there is no connection to the remote station.
 - **Internet** filter: The packet is discarded if its destination can be accessed only via the default route.

The default filter is entered in the above table. It suppresses the unwanted and cost-intensive connections in Windows networks on IP. These networks regularly send items such as DNS queries to the local network, which are routed to the Internet without this filter.

WAN-filter-table

This table allows you to enter specific ranges of destination ports. If packets with the entered ports are received from the WAN side, they will not be forwarded (firewall function).

The WAN port filters are defined in a table similar to the LAN filter table:

Idx.	D-st.	D-end	S-st.	S-end	Dst.-address	Dst-netmask	Prot
WIN	53	53	137	139	0.0.0.0	0.0.0.0	TCP and UDP

The fields in the table have the same meaning as in the LAN filter table, with the following exception:

■ Dst-address, Dst-netmask

A subnetwork of the local network for which the filter is valid can be entered here. A destination address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).

The table entries are sorted in a similar fashion to the IP router table:

■ Longest network mask is placed on top.

■ For two network masks of equal length, the one with the smaller IP address is placed on top.

Network masks and IP addresses of 0.0.0.0 can be used as "wildcards". Specified computers and networks may be simultaneously subjected to targeted filtering while others pass the router unfiltered.

The tables are processed from top to bottom. As soon as a matching filter is found, the packet is handled accordingly.

Proxy-ARP

This option allows you to activate or deactivate the proxy ARP mechanism (default: 'Off'). This function permits data to be transmitted to IP addresses within the same logical network as the sender, e.g. when linking individual workstation computers (teleworkers) to the corporate network via TCP-IP.

Loc.-routing

Local routing enables the router to forward data packets via the local network. The local routing is necessary if the router, as the default gateway for the workstations receives packets for destination networks to which it cannot establish a connection itself. If the router cannot return the address of the appropriate router to the workstation via IMCP, it will forward the data to the corresponding router itself (see also 'Local Routing'). Since this setting increases network utilization in the LAN, the default setting is 'Off'.

Start-address-pool

Start of the address pool used for the dynamic assignment of IP addresses for devices dialing in. This function is also known as IP pooling and can be used for remote access by several field staff members, for example.

The address pool should be in the same address range as the router. If possible, ensure that the address pool is large enough that an IP address can be assigned to every device dialing in (e.g. one address for each of the available B channels).

If the device dialing in can initially establish a connection, only to have it terminated again during the protocol negotiation, this is a sign of insufficient free IP addresses in the IP pool.



End-address-pool

End of the address pool for IP pooling.

Setup/IP-router-module/Routing-method

The router offers two methods for IP routing, which can be separately set for IP and ICMP packets. Both methods are based on the evaluation of the field 'Type-of-service' in the IP header.

The menu has the following layout:

/Routing-method		Routing method settings
Routing-method		Routing method for IP packets
ICMP-routing-method		Routing method for ICMP packets

Routing-method This option allows you to define the routing method used for IP packets:

- If you select 'Normal', all IP packets are handled in the same way as per the routing specifications of the Internet protocol.
- If you select 'Type-of-service', IP packets are placed in the urgent queue or reliable queue, depending on the contents of the 'Type-of-service' field. All other packets are placed in the normal send queue. In this way, transmission is guaranteed, provided that it is possible.




ICMP-routing-method

This option allows you to define the routing method used for ICMP packets:

- If you select 'Normal', the ICMP packets are handled like any other IP packets as per the routing specifications of the Internet protocol.
- If you select 'Reliable', all ICMP packets received are placed in the reliable queue.

Setup/IP-router-module/RIP-configuration

This option allows you to enter settings for the management of IP-RIP packets. The menu has the following layout:

/RIP-configuration		Settings for IP-RIP operation
RIP-Type		RIP compatibility switch
R1-mask		Management of network masks
Table-IP-RIP		Dynamic IP routing table

RIP-type

This option allows you to select the method to be used for handling the IP-RIP packets. The different settings have the following meaning:

- **Off:** IP-RIP is not supported (default).
- **RIP-1:** RIP-1 and RIP-2 packets are received but only RIP-1 packets are sent.
- **R1-comp:** RIP-1 and RIP-2 packets are received. RIP-2 packets are sent as an IP broadcast.
- **RIP-2:** Same as **R1-comp** except that all RIP packets are sent to the IP multicast address 224.0.0.9.

R1-mask

If **RIP-1** is set, this option allows you to influence the management of network masks. Therefore, these settings are required only for subnetting under **RIP-1**. The different settings have the following meaning:

- **Class** (default): The network mask used in the RIP packet is derived directly from the IP address class, i.e. the following network masks are used for the network classes:
 - Class A: 255.0.0.0
 - Class B: 255.255.0.0
 - Class C: 255.255.255.0
- **Address**: The network mask is derived from the first bit that is set in the IP address entered. This and all high-order bits within the network mask are set. Thus, for example, the address 127.128.128.64 yields the IP network mask 255.255.255.192.
- **Cl+Addr**: The network mask is formed from the IP address class and a part attached after the address procedure. Thus, the above-mentioned address and the network mask 255.255.0.0 yield the IP network mask 255.128.0.0.

Table-IP-RIP






This option allows you to display the entries in the current dynamic IP routing table.

An IP-RIP routing table might, for example, have the following appearance:

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

Setup/IP-router-module/Masquerading

This menu allows you to enter settings for the masking function. The menu has the following layout:

/Masquerading	Settings for IP masquerading	
TCP-aging-second(s)		Time in seconds after which a TCP masking becomes invalid
UDP-aging-second(s)		Time in seconds after which a UDP masking becomes invalid
ICMP-aging-second(s)		Time in seconds after which an ICMP masking becomes invalid
Service-table		Static masquerading table
Table-masquerading		Dynamic masquerading table

Service-table

The use of inverse masquerading makes 'services' (e.g. a file server) selectively visible in the Internet by entering specified ports in the service table in the IP network, while all other services and computers remain invisible from the local network (see also 'IP Masquerading (NAT, PAT)').

The service table (also called the static masquerading table) can contain up to 16 entries and has the following layout:

D-port	Intranet addr.
20	10.1.1.10
21	10.1.1.10

The different columns have the following meaning:

- D-port: Destination port for the particular entry
- Intranet-addr.: Destination IP address for the computer in the local network

Through this assignment, it is possible, for example, to address the relevant service directly via telnet. Enter the IP address of the router and attach the port number, separated by a double point, to the address.

You can use the command

```
telnet 192.38.50.100:27
```

to connect directly to a news server that can be reached via a router with the IP address 192.38.50.100.

*Table-
masquerading*

With IP masquerading, the IP addresses of computers in the local network are rendered invisible to external devices by means of a conversion of addresses and ports in the router. The dynamic masquerading table displays the IP addresses from the local network that the router is currently masking. The dynamic masquerading table can contain up to 2048 entries and has the following layout:








Intranet addr.	S-port	Protocol	Timeout
10.1.1.10	1234	TCP	10

The different columns have the following meaning:

- Intranet-addr.: IP address of the computer in the local network
- S-port: Source port for this entry
- Protocol: Protocol used (TCP/UDP/ICMP)
- Timeout: Time in seconds until the entry is removed from the table

Setup/SNMP-module

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

/SNMP-module	SNMP module settings	
Send-Traps		Switch for issuing SNMP traps
IP-Trap-Table		Table with 20 destination addresses for trap messages
Administrator		Device administrator
Location		Device location
Register-monitor		Command to set a destination address to which the traps are to be sent
Delete-monitor		Command to delete an address that was set with 'Register-monitor'
Monitor-table		Table with all currently active destination addresses that were set with 'Register-monitor'

Send-Traps This entry controls trap output (No/Yes).

IP -Trap-Table Enters the IP addresses to which the trap messages will be sent.

Administrator Administrator's name

Location Device location

You can also query the last two parameters via SNMP (MIB-2).

Register-monitor This command logs on applications with the router to retain targeted trap information. The *ELSA LANmonitor*, for example, queries the channel statistics in this way and converts them to a graphic display (under Windows).

In principle, any SNMP manager can use this command to obtain information from the router. The syntax

```
register-monitor IP-address:port mac address timeout
```

is used to direct the router to enter the given address in the monitor table and to send traps to it. If the traps are not received within the set hold time, the address will be automatically deleted from the table. A hold time of '0' permanently retains the entry in the table.

Delete-monitor This command removes the entries from the monitor table.









Monitor-table The monitor table has the following structure:

IP-address	Port	MAC-Address	Timeout
10.0.0.53	1057	0080c76da46e	1

This entry indicates, for example, that an *ELSA LANmonitor* has logged on to the router.

Setup/DHCP-module

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


/DHCP-server-module	DHCP server settings	
Operating		Switch for activating the DHCP module
Start-address-pool		Start address for the address pool
End-address-pool		End address for the address pool
Netmask		Network mask for the address pool
Broadcast-address		Broadcast address for the LAN
Max.-lease-time-minute(s)		Maximum period of validity for the address assignment via DHCP
Default-lease-time-minute(s)		Default period of validity for the address assignment via DHCP
Table-DHCP		Table of current assignments via DHCP

Operating

On: The device operates as a DHCP server

Off: The device does not operate as a DHCP server

Auto: The device regularly checks whether there is another DHCP server in the LAN. If not, it operates as a DHCP server and issues IP addresses to local clients.



If there is no IP or Intranet address entered in the TCP/IP module (e.g. delivery status), the router will issue IP addresses from the address range 10.0.0.2 - 10.0.0.253 to all DHCP clients in auto mode.

Start-address-pool
End-address-pool

The IP address assigned is taken from the address pool selected ('Start-address-pool' to 'End-address-pool'). Any valid addresses in the local network can be entered here.

If 0.0.0.0 is entered instead, the device will determine the appropriate addresses (start or end) from the settings under 'Setup/TCP module'. The procedure is as follows:

- If only the IP address or only the Intranet address is entered, the start or end of the pool is determined by means of the associated network mask.
- If both addresses have been specified, the Intranet address has priority for determining the pool.
- The start address of the pool is either the address given in the DHCP module or the first valid address in the local network.
- The end address of the pool is either the address given in the DHCP module or the last valid address in the local network.

A valid address is then taken from the pool for the IP address. If the computer was already assigned an IP address at some point in the past, it requests this same address and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

The DHCP server also checks whether the address that is to be assigned to the computer is unique in the local network. It does this by issuing an ARP request to the address. If the ARP request is answered, the DHCP server begins the procedure again with a new address. As soon as the uniqueness of an address has been established, the requesting computer is assigned the address found.

Netmask The network mask is assigned in the same way as the address:

The system either assigns the network mask entered in the DHCP module or uses the network mask that belongs to the local network (determined during address assignment).

Broadcast The broadcast mask is assigned in the same way as the address:

The system either assigns the broadcast address entered in the DHCP module or uses the broadcast address that belongs to the local network (determined during address assignment).

Max.-lease-time-minute(s) Here you can enter the maximum period of validity that the DHCP server assigns a host. The DEFAULT value of 6000 minutes equals approximately 4 days.

Default-lease-time-minute(s) Here you can enter the period of validity that is assigned if the host makes no request. The DEFAULT value of 500 minutes equals approximately 8 hours.

Table-DHCP In the DHCP module, the 'Table-DHCP' option allows you to verify (or look up) the assignment of IP addresses to the relevant computers. This table has the following layout:

IP-address	Node-ID	Timeout	Hostname	Type
10.1.1.10	00a0570308e1	500	ELSA	new

- IP-address: IP address assigned
- Node-ID: Computer's Ethernet address
- Timeout: Time remaining until the assignment becomes invalid
- Hostname: Computer's name in plain text if it was transmitted in the request
- Type: This field contains additional information on the assignment.








The 'Type' field specifies how the address was assigned. This field can assume the following values:

- **new**: The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.

- **unkn.:** While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.
- **stat.:** A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.
- **dyn.:** The DHCP server assigned an address to the computer.

Setup/NetBIOS-module

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

Operating		On or off
Scope-ID		NetBIOS scope in which the router is located.
NT-Domain		Workgroup/domain in which the router is located.
Remote-table		All remote stations with which NetBIOS information is to exchanged must be entered in the remote-station table.
Group-list		All workgroups known to NetBIOS are recorded in the group list.
Host-list		All computer names known to NetBIOS are recorded in the host list.
Server-list		All servers that have logged onto the network are recorded in the server list.
Watchdogs		
Update		
WAN-Update-Min.		

Scope-ID

The Scope-ID menu item can be used to specify the NetBIOS scope in which the device is located. It then sees only those NetBIOS packets originating in the same NetBIOS scope; all other packets are automatically rejected. The scope ID is only used in conjunction with Windows name servers (WINS). This entry can generally be left blank.

NT-Domain

A workgroup/domain can be specified in the NT domain item to trigger the search procedure when starting the NetBIOS module. This is required if the network does not contain any computers running Windows 95 or Windows 98.

Remote-table

All remote stations that are to provide or receive NetBIOS information must be entered in the remote-table. When the NetBIOS module is switched on, NetBIOS packets from remote stations other than those specified will be rejected automatically. The remote-table has the following structure:

Name	Type
GLASGOW	Router or workstation

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 station	Timeout	Flags
REMOTE	00	10.0.1.100	GLASGOW	5000	xx20
WORKSTATION	00	10.0.0.10		5000	xx00

Group table

The group table thus looks like this:

Group/Domain	Type	IP-address	Remote station	Timeout	Flags
WORKGROUP	1e	10.0.0.10		5000	xx00
WORKGROUP	1e	10.0.1.100	GLASGOW	5000	xx20

The fields of the table have the following significance:

Name	Name of the host in the host table.
Group/Domain	Name of the group or domain in the group list. Groups and NT domains are handled in the same manner from the NetBIOS point of view.
Type	WINS type of the host. The type is not relevant for NetBIOS, but Microsoft Networks assign certain properties to the name on the basis of the type.
IP-address	IP address of the owner of the name. The same name can be assigned to multiple IP addresses in the group list.
Remote station	Name of the remote station for which the name became known.
Timeout	Time until the name is no longer valid. The time-out is also associated with an aging counter in the flags.
Flags	The flags contain additional information pertaining to the name.

Flags

The flags have the following significance:

0x0003	This counter increments up each time the validity expires. The entry will be deleted if the name is not refreshed after the second expiration at the latest.
0x0004	This identifies an entry that still needs to be transferred.
0x0008	This identifies an entry that is queued for deletion, i.e. the name has not yet been refreshed after the establishment of a connection.
0x0010	Reserved

0x0020	This identifies a remote station.
0x0040	Reserved
0x0080	Reserved

The server list has the following structure:

Host	Group/ Domain	UPD	IP-address	OS- Ver	SMB- Ver	Server- type	Remote station	Time- out	Flags
REMOTE	WORKGROUP	00	10.0.1.100	0400	010f	0004140b	GLASGOW	13	0020
WORKSTATION	WORKGROUP	07	10.0.0.10	0400	0415	00452003		31	0000






Unlike the host and group lists, this table fills gradually, as the NetBIOS module depends on messages from the servers themselves.





The individual fields have the following significance:

Host	Name of the server
Group/Domain	Workgroup or domain in which the server is located.
UPD	Update counter: indicates the number of times that the server has already propagated itself
IP-address	Address of the server
OS-Ver	Operating system version number
SMB-Ver	Version number of the SMB protocol used
Server-type	Bit mask in which the services of the server are coded
Remote station	Name of the remote station from which the server was announced
Timeout	Time until the entry loses its validity (for entries from the LAN) or time until the router propagates a remote entry.
Flags	Corresponds to the flags in the host or group tables.

Setup/Config-module

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

/Config-module		Configuration module settings
LAN-config		Switch for configuring from the LAN side
WAN-config		Switch for configuring from the WAN side
Password-required		Password required on/off if there is no password
Farconfig-(EAS-MSN)		Subscriber number for remote configuration via PPP
Maximum-connections		Maximum number of simultaneous connections

/Config-module		Configuration module settings
Config-aging-minute(s)		Time limit for remote configuration connections
Login-errors		Number for failed log-in attempts before the log-in block is activated
Lock-minutes		Duration of block and period until old log-in errors are forgotten
Display contrast		
Language		Configuration language

LAN-config This option allows you to define whether remote configuration from the LAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **On**.

WAN-config This option allows you to define whether remote configuration from the WAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **Off**.

Password-required This specifies whether a new password should be requested every time a remote configuration is begun (**On**), or the password request should be suppressed (**Off**). The default setting for this option is **On**.

Farconfig-(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.

Maximum connections This option allows you to display the maximum number of remote configuration sessions that can occur simultaneously for the device.

Config-aging-minute(s) If data transmission halts during a remote configuration session, e.g. because the user is no longer entering data, the device automatically releases the connection at the end of the time period specified here. Possible settings are from 1 to 99 minutes; the default setting is 5 minutes.

Login-errors This entry specifies the number of failed attempts allowed before the log-in block is activated. An empty password (simply pressing <ENTER> at the password prompt) is not considered an attempt and therefore does not activate the block.



The default value is 5. A lower value may cause the log-in block to be activated with only one access on an older ELSA LANconfig! In this case obtain an updated ELSA LANconfig version over our online media.

Lock-minutes This entry has two meanings. It indicates how long the access is blocked if the log-in block has been activated. It also sets the period after which the device forgets all prior login errors.





Language This option allows you to select whether you will use the German or English version of the software for performing the configuration.

Setup/LANCAPI-module

Configuring *LANCAPI* basically involves answering two questions:

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

The *LANCAPI* module has the following layout:

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

Access-list

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

Interface-table

The interface table appears as follows:

lfc	Operating	EAZ-MSN(s)	Force-Out-MSN
S0-1	Outgoing	123456	no

The fields of the table have the following significance:

lfc	Designates the associated interface
Operating	This item determines whether <i>LANCAPI</i> operation is permitted on this interface for outgoing calls, incoming and outgoing calls (On) or whether <i>LANCAPI</i> operation is disabled completely (Off).
EAZ-MSN(s)	Enter the EAZs or MSNs on which the <i>LANCAPI</i> should respond to incoming calls here; these EAZs/MSNs will also be displayed to the exchange during outgoing calls.
Force-Out-MSN	If no outgoing MSN has been configured for the CAPI application, this item can be used to determine whether the <i>LANCAPI</i> transfers the first EAZ/MSN on the list.

Priority-table





The priority for a port controls the option for breaking outgoing connections via the *LANCAPI* router connections. Option '1' does not break router connections, the setting '2' breaks only auxiliary connections of a router connection with channel bundling, the selection '3' also breaks main channels of a router connection.

Setup/LCR-module

Enter the following information when setting the least-cost router:

- For which modules in the device should the LCR functions be active?
- Which area codes should be diverted when via which call-by-call provider?

The LCR module has the following layout:

/LCR module		Least-cost router settings
Router-usage		Activate LCR for the router modules, On or Off
Lancapi-usage		Activate LCR for the <i>LANCAPI</i> , On or Off
Timetable		Call forwarding table
Celebration-day-table		List of holidays affecting the timetable.

Timetable

The table has 256 entries and the following structure:

Index	Prefix	Days	Start	Stop	Number-list	Fallback
1	0171	192	0:00	23:59	01013;01070	On

The individual entries have the following meaning:

Index	Continuing index of entries in the table.
Prefix	Area code to be diverted.
Days	Validity of the entry for week days and holidays shown in an 8-bit mask: Bit 0 represents Monday, bit 7 holidays. The entry '31' therefore designates all business days, '192' Sundays and holidays.
Start	Beginning time for the validity of the entry on the defined days.
Stop	Termination time for the validity of the entry on the defined days.
Number-list	Network identification number of the call-by-call providers.
Fallback	Automatic fallback to your own telephone company if all call-by-call numbers are busy.

Example:

`set 1 02 31 1:00 11:59 01030;01090;01070 On` diverts all long-distance calls to region '02' between one and twelve o'clock to the provider with the network identification number '01030'. If this number is busy, the network identification numbers '01090' and '01070' will be attempted. If they are also not available, the connection will be made via the normal telephone company.

Celebration-day-table

The celebration-day-table has 256 entries and the following structure:








Index	Date
1	01010000
2	01050000
3	03100000
4	25120000
5	26120000
6	02041999
7	13051999

The individual entries have the following meaning:

Index	Continuing index of entries in the table
Date	Dates of holidays. Enter the index and the date in full without separators, e.g. 'set 8 13041999' for April 13, 1999 as the eighth entry in the list. Enter '0000' as the year for annually occurring holidays.

Setup/DNS-module

The settings for the DNS server can be modified here as required. The menu contains the following items (incl. their default settings):

Operating		On (default) or off
Domain		Own domain, optional, 32 characters max.
DHCP-usage		Yes (default) or no
NetBIOS-usage		Yes (default) or no
DNS-table		Static DNS table for the manual association of IP addresses to names, 64 entries
Filter-list		Filter list for the exclusion of prohibited domains, 64 entries
Leasetime		Specifies the name validity information to be given to a requesting computer. Default: 2000

DNS-table

The DNS table contains a simple association of local names to IP addresses. The table is sorted alphabetically by names.

The table is restricted to 64 entries, as large networks are configured more effectively using the DHCP server, which can also be used to handle name requests. The table has the following layout:

Hostname	IP-address
Host10	10.0.0.10

The name is restricted to a maximum of 32 characters. Longer names are not necessarily practical in a local network.

Filter-list

The filter list contains the entries for prohibited domains. In addition, it is possible to specify for whom a given domain will be prohibited. This is set using an IP address/netmask pair. An IP address of 0.0.0.0 prohibits this domain for all computers. A subnet mask of 0.0.0.0 prohibits the domain for all networks. The table has the following layout:

Idx.	Domain	IP-Address	Netmask
F001	*xxx*	0.0.0.0	0.0.0.0

Clear IDs can be freely selected and assigned to the filters in the 'Idx.' field.

Enter the name of the domain to be prohibited in the 'Domain' field. Wildcards such as '?' and '*' may be used. The wildcard '?' replaces exactly one character, while '*' can stand for a random number of characters. Multiple instances of the wildcard '*' can be used. For example, *xxx* filters all names containing the letters xxx in any position within the name.

The IP address and subnet mask fields can be used to specify the subnet for which the domain will be prohibited.

The filter table is sorted according to the subnet masks in descending order (the longest at the top); entries with identical subnet masks are sorted according to the IP addresses in ascending order. In the event of identical IP addresses, the entries are sorted in ascending order according to the domain to be prohibited.

The table is searched from top to bottom and an error message is returned to the requesting computer in the event of a match.





Setup/Time-module

The least-cost router in the device requires correct time information to calculate the call number diversions via call-by-call provider. Precise time information is also desirable for some statistics.

The time may be set manually (with the 'time' command) or automatically read from the ISDN network.







For automatic time comparison when the module is switched on, a previously specified remote station is called directly and the time information is taken from the ISDN network. So long as the time module is switched on, the time will be taken from the ISDN every time the router establishes a connection.

The time module has the following layout:

/Time-module	Time module settings	
Operating		Activating the module: On, Off
Current-time		Displays the current time in the device.
Time-call-number		Call number to which a connection must be established to receive time information from the ISDN.
Call-attempts		Number of possible attempts to receive time information

Firmware

The various firmware parameters can be called up and a firmware upload started from this menu:

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

Version table

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

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	<loader>	1.60	07061999	64	0

Enter the following command to activate an inactive firmware version:





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

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

- 'immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
 - The new firmware is successfully loaded and then operates as desired. Everything is then in order.
 - However, if the new firmware does not operate correctly, it may not be possible to communicate with the device after the restart. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- 'login': To prevent problems caused by defective firmware, the second option will load the firmware and start it immediately.
 - In contrast to the first option, the firmsafe will wait until it has successfully logged on over outband or inband (by telnet). In contrast to the first option, the firmsafe will wait until it has successfully logged on (by telnet). The new firmware will only be permanently activated when the login occurs successfully within the time set under 'Timeout firmsafe'.
 - If the device no longer responds and it is therefore impossible to log in, the firmware automatically loads the previous firmware version and reboots the device with it.
- 'manual': The third option allows you to set a period (Timeout firmsafe) beforehand for testing the new firmware. The device will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective.

Other

The **Other** menu allows you to manage the following functions:

/Other	Various functions	
Manual-dialing		Connection testing
Boot-system		Boots the device.
Reset-system		Resets to factory settings.
Upload-system		Loads new firmware.

Other/Manual Dialing

Select this option when you wish to establish a connection manually for testing purposes.

Boot-system

This option allows you to reboot the device.
Before executing the command all open connections (ISDN or TCP) will be released or closed.

Reset-system

This option resets all the settings that have been entered. The device is reset to the delivery version.

For safety's sake, the system asks you to enter the configuration protection password in order to ensure that you have not mistakenly selected this command instead of the `Boot-system` command. If no password has been assigned, you must press Enter a second time.

Upload-system

This option starts a firmware upload (refer to chapter 'How to set up new software').

The flash ROM technology permits flexible and service-friendly handling of the system software by allowing different firmware versions to be read in. It also allows devices can be retrofitted for all future options.