

# ***ELSA LANCOM™ Business***

## **Manuel de l'utilisateur**

© 1999 ELSA AG, Aachen (Germany)

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

La transmission et la reproduction de la documentation et des logiciels faisant partie de ce produit, ainsi que l'exploitation de leur contenu 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.

## Marques

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

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

ELSA se réserve le droit de modifier les données mentionnées sans préavis et décline toute responsabilité quant à des inexactitudes et/ou manques techniques.

ELSA AG

Sonnenweg 11

52070 Aix-la-Chapelle

Allemagne

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

Aachen, octobre 1999

# Avant-propos

## Merci de votre confiance !

Avec *ELSA LANCOM Business* vous vous êtes décidé pour un routeur qui vous permet de connecter des réseaux locaux ou des postes de travail à d'autres réseaux par une connexion RNIS.

De très hautes exigences de qualité de fabrication et un contrôle de qualité sévère forment la base d'un standard de production élevé, conditions nécessaires pour garantir la qualité constante des produits ELSA.

## Documentation

La documentation jointe comprend :

- Guide d'installation  
Installation du matériel et premiers exemples de configuration
- Manuel de l'utilisateur  
Description détaillée des fonctions et des modes de service du routeur
- Documentation électronique sur CD-ROM  
Références, description détaillée des menus



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

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



# Contenu

<b>Introduction .....</b>	<b>1</b>
Champs d'application du routeur .....	1
Avantages d'un routeur <i>ELSA LANCOM Business</i> .....	3
Lever de rideau sur <i>ELSA LANCOM Business</i> .....	8
Voyons voir ce périphérique ! .....	8
Nœud ou Concentrateur (« Node » ou « Hub ») ? .....	10
Conformité CE .....	10
<b>Configurations possibles .....</b>	<b>13</b>
De nombreux chemins mènent au <i>ELSA LANCOM</i> .....	13
La voie directe : Outband .....	14
Conditions pour la configuration Outband .....	14
Configuration Outband avec <i>ELSA LANconfig</i> .....	14
Configuration Outband avec programme de terminal .....	14
La voie confortable : Inband .....	16
Conditions pour la configuration Inband .....	16
Alternative : gestion des adresses à l'aide du serveur DHCP .....	16
Lancement de la configuration Inband par <i>ELSA LANconfig</i> .....	16
Lancement de la configuration Inband par Telnet .....	17
L'accès à distance : configuration par Accès réseau à distance .....	17
Ce dont vous avez besoin pour la configuration à distance .....	18
Préparation de la configuration à distance .....	18
La première connexion à distance par Accès réseau à distance ( <i>ELSA LANconfig</i> ) .....	18
La première connexion à distance avec un client PPP et Telnet .....	19
Restriction de la configuration à distance .....	19
Instructions de configuration .....	21
Nouveau microprogramme avec firmsafe .....	22
Comment fonctionne firmsafe ? .....	22
Comment charger le nouveau logiciel ? .....	23
Configuration par SNMP .....	26
Généralités .....	26
Accès aux tableaux et paramètres par SNMP .....	26
La Management Information Base (MIB) .....	28
Supervision de la ligne ? .....	30
Éditions des tracés .....	30
<i>ELSA LANmonitor</i> .....	32

<b>Fonctions et modes d'exploitation .....</b>	<b>35</b>
La sécurité de votre configuration .....	35
Protection par mot de passe .....	36
Le verrouillage des accès.....	36
Contrôle des accès via TCP/IP .....	36
La sécurité de votre LAN .....	37
Le contrôle.....	37
Le rappel.....	38
La cachette – Masquering IP (NAT, PAT) .....	39
Gestion des unités de taxation .....	39
Limitation des communications en fonction des unités de taxation.....	40
Limitation des communications en fonction de la durée.....	40
Configuration dans le gestionnaire des coûts .....	41
Connexions RNIS .....	41
Liste des noms .....	42
Configuration des interfaces.....	43
Interfaces du routeur.....	43
Configuration de l'interface <i>LANCAPi</i> .....	44
Couche communication .....	44
Liste RoundRobin .....	45
Liste des canaux.....	46
Liste PPP.....	47
Liste des scripts .....	47
Prise d'appel.....	48
Liste des numéros .....	48
Liaisons permanentes et canaux secours.....	48
Voici comment configurer la liaison permanente.....	49
Connexion via GSM .....	51
Protocole PPP .....	52
Le protocole.....	52
Liste PPP.....	54
Vérification de la ligne avec LCP .....	55
Attribution des adresses IP avec PPP .....	56
Fonctions de rappel automatique .....	57
Rappel rapide via le protocole ELSA.....	60
Rappel automatique selon RFC 1570 (extensions LCP PPP) .....	60
Regroupement des canaux avec MLPPP.....	60
Routage IPX.....	62
Adressage IPX .....	62
Informations sur le réseau local .....	62
Tableau de routage IPX.....	63
Que se passe-t-il pendant la transmission des données dans	

le réseau IPX ?.....	64
Tableaux RIP et SAP.....	64
Tant de routeurs ici.....	65
Routes redondantes.....	65
Exponential Backoff .....	66
Filtrage des paquets IPX .....	66
Routage IP .....	68
Le tableau de routage IP .....	68
Filtrage des paquets TCP/IP .....	72
Proxy-ARP.....	73
Routage local .....	73
Routage dynamique avec IP-RIP .....	74
Masquerading IP (NAT, PAT) .....	77
Routage par DNS .....	79
Policy Based Routing : routage stratégique.....	80
Gestion d'adresses automatique via DHCP.....	80
Le routeur en tant que serveur DHCP .....	80
DHCP – 'Actif', 'Inactif' ou 'Auto' ?.....	81
Attribution des adresses.....	81
Configuration des routeurs en tant que serveur DHCP.....	85
DNS.....	87
Que fait un serveur DNS ? .....	87
Configurer le serveur DNS .....	88
Proxy NetBIOS.....	90
En quelques mots : définition de NetBIOS .....	91
Traitement des paquets NetBIOS .....	91
Quelles conditions doivent être satisfaites ? .....	92
Interconnecter deux réseaux Windows via le RNIS .....	94
Accès par les ordinateurs distants .....	96
Qui cherche trouve : le Voisinage réseau .....	96
Pooling IP pour les accès commutés .....	98
Bureautique et <i>ELSA LANCAPI</i> .....	98
<i>ELSA LANCAPI</i> .....	98
<i>ELSA CAPI Faxmodem</i> .....	102
Installation .....	103
Transmettre des télécopies via <i>ELSA CAPI Faxmodem</i> .....	103
Le rerouteur téléphonique (Least Cost Router).....	103
<b>Workshop .....</b>	<b>109</b>
Configuration avec <i>ELSA LANconfig</i> et les assistants .....	109
Configuration sans assistants.....	109
Quel périphérique utilisez-vous ?.....	110
Ajouts.....	110
Applications Internet .....	110

Internet pour tous les PC dans le LAN .....	111
Intranet avec propre serveur Web dans Internet.....	115
Interconnexions LAN-LAN .....	121
Interconnexion des réseaux avec le routeur IP.....	121
Interconnexion des réseaux avec le routeur IPX.....	127
Accès à distance .....	131
Accès à distance avec TCP/IP .....	132
Least Cost Router.....	138
<b>Appendice .....</b>	<b>143</b>
Caractéristiques techniques .....	143
Affectation des connecteurs : .....	144
Conditions générales de garantie du 01.06.1998.....	145
Déclaration de conformité .....	147
<b>Glossaire .....</b>	<b>149</b>
<b>Index .....</b>	<b>157</b>
<b>Description of the menu options .....</b>	<b>R-1</b>
Status.....	R-3
Display and keyboard.....	R-4
Status/Connection .....	R-5
Status/Current-time .....	R-5
Status/Operating-time .....	R-5
Status/WAN-statistics.....	R-6
Status/LAN-statistics.....	R-8
Status/PPP-statistics.....	R-9
Status/IPX-statistics .....	R-17
Status/TCP-IP-statistics .....	R-22
Status/IP-router-statistics.....	R-28
Status/Config-statistics .....	R-30
Status/Queue-statistics .....	R-30
Status/Connection-statistics .....	R-31
Status/Info-connection .....	R-32
Status/Layer-connection .....	R-33
Status/Call-info-table .....	R-33
Status/Remote-statistics .....	R-34
Status/S0-bus .....	R-35
Status/Channel-statistics .....	R-35
Status/Time-statistics.....	R-36
Status/LCR-statistics .....	R-37
Status/Delete-values .....	R-37
Setup .....	R-37
Setup/WAN-module .....	R-38



Setup/LAN-module .....	R-48
Setup/IPX-module .....	R-49
Setup/TCP-IP-module .....	R-57
Setup/IP-router-module .....	R-61
Setup/SNMP-module .....	R-69
Setup/DHCP-module .....	R-70
Setup/NetBIOS-module .....	R-72
Setup/Config-module .....	R-74
Setup/LANCAPI-module .....	R-76
Setup/LCR-module .....	R-77
Setup/DNS-module .....	R-78
Setup/Time-module .....	R-79
Firmware .....	R-80
Other .....	R-82
<b>Novell SAP Numbers .....</b>	<b>83</b>
<b>TCP/IP Ports .....</b>	<b>87</b>
<b>ELSA LANCOM Business Internal .....</b>	<b>91</b>
Script Processing .....	91
General .....	91
The Script List .....	92
CompuServe Select .....	92
Online Trace Outputs .....	93
General .....	93
Control of Trace Outputs .....	94
Examples for Control of Trace Outputs .....	95
Supported Protocols and Functions .....	95
Policy Based Routing .....	105
General .....	105
Examples .....	106



# Introduction

Avec les moyens de communication modernes, les applications Internet et Intranet prennent une place de plus en plus importante dans les entreprises des divers secteurs. Les services en ligne sont de plus en plus utilisés sur un mode professionnel. On interconnecte les filiales pour que la communication entre les divers sites soit plus efficace et plus rapide, et même le télétravail gagne du terrain.

Toutes ces applications rendent la mise en œuvre des solutions de routage RNIS de plus en plus intéressante. Les routeurs RNIS d'ELSA relient les réseaux locaux à l'Internet et forment dans les petites et moyennes entreprises la centrale de communication via laquelle les services tels que la télécopie ou la fonction de répondeur téléphonique sont implémentés.

En outre, les routeurs relient les réseaux locaux (Local Area Networks) aux autres RVA et permettent d'accéder aux informations de l'entreprise via un accès à distance.

## 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 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.

Mais les routeurs sont encore plus performants. Grâce à *ELSA LANCAPI*, une interface spéciale, les fonctions de bureautique modernes telles que la télécopie, le répondeur téléphonique, la banquique etc. peuvent être utilisées dans tout le 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.

Le routeur est intégré dans le réseau local comme un PC normal. Toutes les données transitant par le câblage du réseau aboutissent donc aussi au routeur. Celui-ci décide ensuite tout seul si les données sont destinées à un autre réseau et, le cas échéant, 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.

- Nœud d'accès pour fournisseur d'accès Internet

Avec les quatre connexions  $S_0$  disponibles, donc huit canaux B, un *ELSA LANCOM Business* se prête également comme périphérique d'accès pour Provider. La fonction IP-Pooling offre un grand confort de gestion d'un grand nombre de correspondants télécommandés pouvant se brancher sur le routeur.

## Avantages d'un routeur *ELSA LANCOM Business*

Pour vous donner un petit aperçu des fonctionnalités de votre périphérique, voici les propriétés essentielles.

### Simplicité d'installation

- Mettre le routeur *ELSA LANCOM* sous 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. Un *ELSA LANCOM Business* est raccordé à un réseau (Fast) Ethernet via le connecteur 10/100Base-T.

### Connexion à un réseau étendu WAN

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

### Regroupement des canaux et compression

Sur la ligne RNIS, l'appareil prend en charge les regroupements statique et dynamique des canaux par MLPPP et BACP. Le *ELSA LANCOM Business 4100* permet de regrouper jusqu'à huit canaux. La compression de données Stac (hi/fn) permet d'augmenter jusqu'à 400% le taux de transmission.

### **Gestion multicanaux**

Le *ELSA LANCOM Business 4100* met à votre disposition quatre connexions RNIS, donc en tout huit canaux B. Vous pouvez déterminer l'ordre d'utilisation des canaux pour chaque connexion. De cette manière, vous pouvez par ex. réserver certains canaux pour les accès RAS ou alors n'activer que certains canaux pour l'accès Internet.

### **Affichage de l'état**

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

### ***ELSA LANmonitor***

D'autres instruments que les témoins lumineux permettent de reconnaître l'état du routeur. Les utilisateurs des systèmes d'exploitation Windows ont là un instrument supplémentaire. Grâce à *LANmonitor*, les informations sur l'état de routeurs *ELSA LANCOM* sont toujours visibles à l'écran. *LANmonitor* montre les informations les plus importantes sur chaque périphérique dans le réseau local, par ex. :

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

En outre, *LANmonitor* permet la journalisation et la sauvegarde des messages pour l'exploitation ultérieure avec le PC.

### **Statistiques**

Grâce aux nombreuses fonctions de statistique, vous avez le routeur dans votre poche. Ces fonctions vous fournissent par ex. toutes les informations sur les dernières connexions qui vous permettent alors d'optimiser la configuration du routeur.

### **Contrôle des coûts de communication**

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

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

## Least Cost Routing

Même si le nombre d'opérateurs offrant les services de télécommunication est important, le Least Cost Router permet d'effectuer un appel via l'opérateur le moins cher. Vous définissez pour commencer les opérateurs ayant les tarifs les plus avantageux pour vos besoins, et le routeur fait passer chaque appel (peu importe qu'il soit effectué par le routeur ou l'interface *LANCAP*) automatiquement par le fournisseur offrant le meilleur tarif.

## 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.

## Configuration avec *ELSA LANconfig*

Le réglage et l'adaptation des routeurs 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 devront utiliser Telnet ou un logiciel 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 d'installation intégrés vous aident à mettre les périphériques en service avec un minimum d'efforts.

## Protection de l'accès

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

## Compatibilité par PPP

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

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

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

### **Mise à jour des logiciels**

Afin de rester à jour question logiciels, ces routeurs sont équipés d'une mémoire flash ROM. On télécharge tout simplement le nouveau microprogramme dans le routeur 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 (par ex. suite à une erreur de transmission), le routeur réutilise automatiquement la version précédente en état de fonctionner.

### **ELSA LANCAPI et ELSA CAPI Faxmodem**

La mise en œuvre de l'interface *LANCAPI* apporte des avantages surtout économiques. *LANCAPI* est une variante spéciale de l'interface CAPI-2.0 via laquelle divers logiciels de communication (par 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 la télécopie 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 télécopie, 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 standard en liaison avec un routeur *ELSA LANCOM Business*.

## **DHCP**

*ELSA LANCOM Business* dispose aussi 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, l'*ELSA LANCOM Business* peut aussi déterminer toutes les adresses dans le réseau lui-même et les attribuer aux unités.

## **NetBIOS-Proxy**

Les routeurs ELSA sont spécialement conçus pour la liaison des réseaux d'égal à égal (Peer-to-Peer) Microsoft. Le routage intégré de paquets IP-NetBIOS rend enfantin le couplage de deux réseaux Windows. Les correspondants avec lesquels des informations NetBIOS doivent être échangées sont inscrits dans une liste afin d'éviter que chaque paquet NetBIOS ne produise l'établissement d'une communication.

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

## **Serveur DNS**

Le *ELSA LANCOM Business* dispose aussi des fonctions d'un serveur DNS. Cela vous permet d'associer des adresses IP à des noms d'ordinateurs ou de réseaux afin de pouvoir affecter directement la route correcte suite à une demande de nom d'ordinateur.

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

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

## **Accès par GSM**

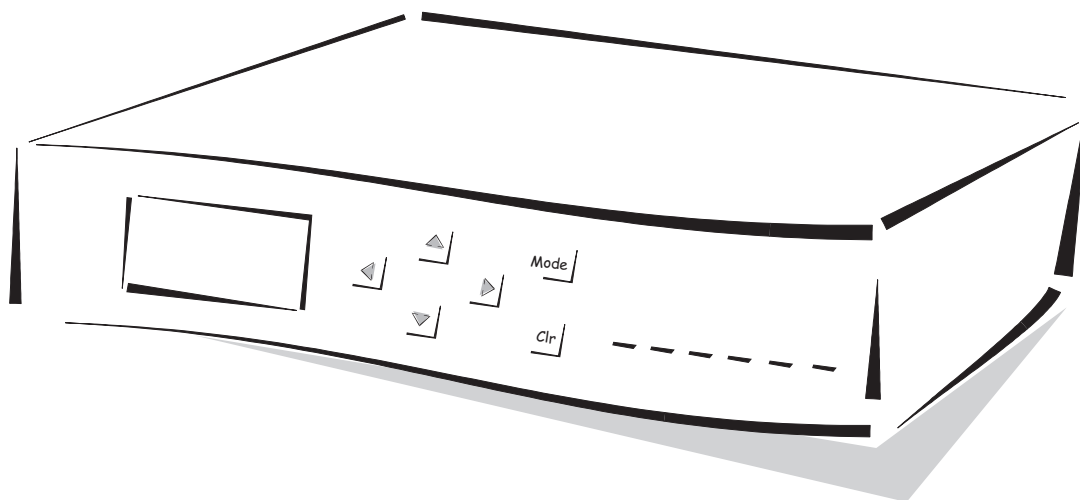
*ELSA LANCOM Business* permet également l'accès par téléphones portables GSM. Le routeur reconnaît l'appel par le protocole V.110 et ajuste automatiquement le niveau utilisé à ce procédé de transmission. De cette manière, les accès RAS par GSM et par RNIS peuvent utiliser le même niveau.

## Lever de rideau sur *ELSA LANCOM Business*

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.

### Voyons voir ce périphérique !

Tout d'abord, nous voulons vous familiariser avec le routeur. Sur la face avant vous trouvez les éléments d'affichage et de commande : un écran, quelques touches et quelques témoins lumineux.



L'écran affiche les différents états de service et les messages de l'appareil. Les états de service et les messages sont affichés sous trois formes différentes. Les touches vous permettent de sélectionner le mode d'affichage, de confirmer les messages et de faire défiler l'affichage. La fonction exacte de chaque touche dans les différents états de service des *ELSA LANCOM* est décrite au chapitre « Configurations possibles ».

*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.

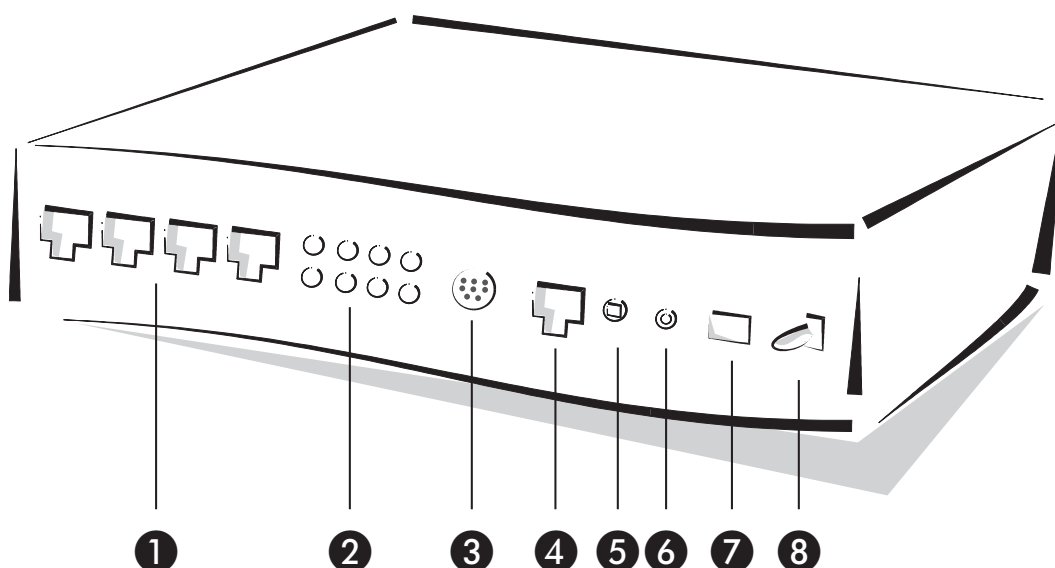
inactif		Périphérique hors circuit mais toujours sous tension
rouge	1 x brève.	Le lancement (test et chargement) a commencé
rouge	clignotant	Affichage d'une erreur de lancement (codé sous forme de clignotement)
rouge		Périphérique prêt au service
rouge	interruption	Message d'erreur ou appels sortants empêchés par un blocage des unités de taxation

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

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



- ❶ Quatre RNIS-S<sub>0</sub>-raccordements (*ELSA LANCOM Business 4100*)
- ❷ LED d'état pour les quatre connexions S<sub>0</sub> :

S <sub>0</sub> Status	inactif	Bus non activé
	clignote rapidement	Bus activé avec canal D, pas de TEI
		Canal D reconnu, Bus non activé
	vert	Bus activé avec canal D, TEI assigné
S <sub>0</sub> Line	inactif	Aucun appel, aucune connexion
	clignote lentement (1x par sec., en tout 2 à 3x)	Appel entrant, mais le routeur n'est pas compétent ou le routeur établit une connexion lui-même
	clignote rapidement (3x par sec.)	Appel entrant, le routeur est compétent, mais n'a pas (encore) pris la communication
	jaune	La connexion va être/est établie

- ❸ Interface de configuration V.24
- ❹ 10/100Base-TX pour réseaux 10-Mbit ou 100-Mbit
- ❺ Commutateur node/hub
- ❻ La touche Reset provoque une remise à zéro du matériel ou remet l'appareil dans l'état à la livraison (appuyer durant env. 5 sec.).
- ❼ Raccord au bloc transfo.
- ❽ Commutateur Marche/Arrêt

## Nœud ou Concentrateur (« Node » ou « Hub ») ?

Tenez compte de la position du commutateur node/hub lors du raccordement au réseau :

- A la livraison, le commutateur est en position 'Node'. Dans cette position, le périphérique se comporte comme un nœud dans un réseau. Il ne pourra alors être branché qu'à un concentrateur, et non pas directement à la carte réseau d'un ordinateur.
- Mettez le commutateur en position 'Hub' si vous ne voulez pas brancher le périphérique à un concentrateur, mais directement à un ordinateur. Dans cette position, les lignes émission et réception de données sont croisées.



*Vous pouvez vérifier la position correcte du commutateur node/hub à l'aide de la LED état du lien (link).*

## Conformité CE

Cet appareil a été testé et répond en pratique aux exigences de protection selon les directives du conseil de la CE pour l'harmonisation des prescriptions juridiques des pays membres sur la compatibilité électromagnétique (89/336/CEE) selon les normes EN55022 classe B et EN50082-1.



*L'utilisation non conforme de l'appareil ou son service à proximité d'émetteurs puissants peuvent provoquer des défaillances provisoires admissibles.*

Ces exigences garantissent une protection appropriée contre les perturbations de réception dans les zones d'habitation. L'appareil génère, utilise et pourrait émettre des signaux situés dans la plage de fréquence de radiodiffusion et de télévision. Des perturbations de réception peuvent survenir si l'appareil n'est pas installé ou exploité conformément aux instructions. Il ne peut toutefois pas être garanti qu'une installation conforme empêche toute perturbation de réception. Si l'appareil occasionne des perturbations de réception de radiodiffusion ou de télévision, ce qui peut être vérifié aisément en mettant l'appareil brièvement hors service, essayez de remédier à la perturbation par l'une des mesures suivantes :

- Modifiez l'orientation ou le lieu d'installation de l'antenne de réception.
- Augmentez l'écart entre l'appareil et votre récepteur radio ou de télévision.
- Branchez l'appareil sur un circuit interne d'alimentation différent de celui de votre récepteur radio ou de télévision.
- Adressez-vous à votre revendeur ou à un technicien radio/télévision professionnel.



# Configurations possibles

*ELSA LANCOM Business* sont toujours livrés avec le logiciel actuel dans lequel certains réglages ont déjà été préparés pour vous.

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

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

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

## 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)
- 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*.

## 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.*

### Conditions pour la configuration Outband

Que vous faut-il pour cela ?

- Un ordinateur avec Windows 95, Windows 98 ou Windows NT 4.0 et le logiciel de configuration *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).

### 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 **Périphérique ► Recherche ► Rechercher à 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 doublecliquer sur la désignation de l'appareil dans la liste des appareils trouvés.

### 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.

## La voie confortable : Inband

La configuration Inband vous permet d'accéder au routeur à partir de n'importe quel ordinateur du LAN ou WAN. Mais cela uniquement si le routeur le permet, car l'accès à partir du WAN ou du LAN peut être restreint ou bloqué entièrement par la liste d'accès IP. Pour la configuration Inband, utilisez Telnet (fait partie de la livraison de la plupart des systèmes d'exploitation) ou le programme de configuration *ELSA LANconfig* pour Windows. *ELSA LANconfig* est compris dans la livraison de votre routeur. Les versions actuelles sont toujours à votre disposition dans nos médias en ligne.

### Conditions pour la configuration Inband

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 192.110.130.1, vous pourrez alors contacter votre routeur avec l'adresse 192.110.130.254.



*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.*

### 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 toutes les adresses IP dans le réseau, y compris celle du serveur (cf. chapitre 'Affectation automatique des adresses avec DHCP').

### Lancement de la configuration Inband par *ELSA LANconfig*

Après l'installation, (en double-cliquant sur 'autorun.exe') vous appelez l'outil de configuration *ELSA LANconfig* par ex. à partir de la barre de Windows **Démarrer** ► **Programmes** ► **ELSA** ► **ELSA LANconfig**. *ELSA LANconfig* cherchera automatiquement des périphériques *ELSA LANCOM* dans le réseau local. Si un périphérique non configuré est trouvé dans le réseau local, *ELSA LANconfig* lance automatiquement l'assistant de configuration.

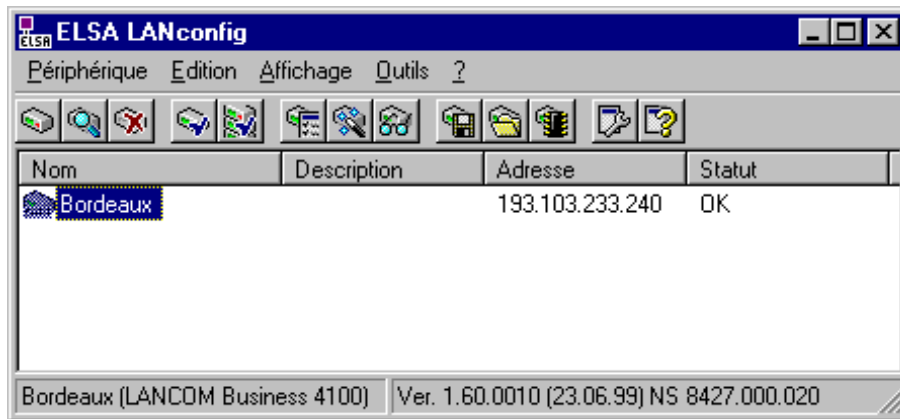
Choisissez l'un des assistants proposés et répondez simplement à ses questions. Après cela, le routeur sera réglé pour la tâche sélectionnée.



Pour lancer une recherche de routeur 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.



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

La suite de la conduite du programme est auto-descriptive, ou alors sélectionnez l'aide en ligne. Vous pouvez à tout moment appeler l'aide contextuelle en cliquant sur le point d'interrogation en haut à droite de chaque fenêtre, ou alors avec un clic de la touche droite de la souris sur un terme qui ne vous paraît pas clair.

## Lancement de la configuration Inband par Telnet

Avec Telnet vous lancez la configuration Inband par ex. à l'aide de l'instruction :

```
telnet 10.1.80.125
```

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

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

## 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.

## 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 LANCAPI*

## Préparation de la configuration à distance

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

## 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 le *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 *LANCAPI*) 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.

## 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.

## 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 Dans la zone de configuration 'Gestion', passez à l'onglet 'Security'.
- 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 à 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.

## Instructions de configuration

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

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

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

Cette instruction...	... signifie...	... par ex. :
? ou help	appelle les textes d'aide.	-
dir, list, ll, ls <MENU>, <VALUE> ou <TABLE>	affiche le contenu de MENU, VALUE ou TABLE.	statistique dir/status/wan affiche la statistique actuelle WAN.
cd <MENU> ou <TABLE>	passse au MENU indiqué ou au TABLE.	cd setup/tcp-ip-module (ou cd se/tc en bref) passe au module TCP/IP.
set <VALUE>	Nouvelle définition du VALUE.  Séparez toutes les entrées dans les lignes des tableaux par des espaces. Un * ne modifie pas l'inscription.	set ip-adresse 192.110.120.140 définit une nouvelle adresse IP.  set /setup/name BORDEAUX nomme l'appareil 'BORDEAUX'
set <VALUE> ?	vous affiche les valeurs que vous pouvez entrer ici.	
del <VALUE>	efface une ligne dans un tableau.	del /se/wan/nam/BORDEAUX efface l'inscription vers le correspondant BORDEAUX
do <ACTION> (paramètre)	exécute l' ACTION, éventuellement avec les paramètres indiqués.	do /firmware/firmware-upload lance le chargement d'un nouveau microprogramme.
passwd	permet l'introduction d'un nouveau mot de passe. Pour cela, il faut d'abord entrer l'ancien mot de passe, s'il en existe un. Ensuite, il faut entrer le nouveau mot de passe deux fois de suite et confirmer chaque fois avec  .	
repeat <sec> <ACTION>	répète l' ACTION avec un délai égal aux secondes indiquées. N'importe quelle touche achève la répétition.	repeat 3 dir/status/wan-statistics affiche la statistique actuelle WAN toutes les 3 secondes.
time	règle la date et l'heure-système.	time 24.12.1998 18:00:00

Cette instruction...	... signifie...	... par ex. :
language <Langue>	définit la langue de la séance actuelle de configuration.	langues prises en charge actuellement. English (language english) Deutsch (language deutsch)
exit, quit, x	fin de la configuration.	

Les textes contenant des espaces ne seront acceptés qu'entre guillemets, par ex. `set /se/snmp/admin "The Administrator"`.

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

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

## Nouveau microprogramme avec firmsafe

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

### Comment fonctionne firmsafe ?

Firmsafe rend le chargement du nouveau logiciel sûr : le 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 routeur 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 routeur attendra ensuite durant cinq minutes un Login correct auprès du périphérique par Outband ou Inband (avec Telnet). 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, le routeur activera automatiquement l'ancien microprogramme et relancera le périphérique.
- 'Manuel' : La troisième possibilité vous permet de déterminer auparavant vous-même une durée, durant laquelle vous voulez tester le nouveau microprogramme. Le routeur démarre avec le nouveau microprogramme et attend pendant la durée réglée que le microprogramme soit activé manuellement pour être actif en permanence.

## Comment charger le nouveau logiciel ?

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

- Outil de configuration *ELSA LANconfig* (conseillé)
- Émulateurs 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** par ex. avec **Edition ► Sauvegarder la configuration dans un fichier**).

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

### **ELSA LANconfig**



Dans l'outil de configuration *ELSA LANconfig* marquez l'appareil désiré dans la liste de sélection et cliquez sur **Edition ► Gestion des microprogrammes ► Télécharger un nouveau microprogramme** ou directement sur le bouton **Télécharger le microprogramme**. Sélectionnez ensuite le répertoire dans lequel se trouve la nouvelle version et marquez le fichier correspondant.

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

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

### Émulateur 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 désiré 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, se trouvant par ex. dans le fichier 'LC\_1000U.130' dans un routeur avec l'adresse IP 194.162.200.17, entrez par 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** au routeur. 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 durant les téléchargements, (erreur d'écriture dans le flash ROM, erreur de transmission TFTP ou autres) la connexion TFTP sera interrompue afin de fournir à l'utilisateur une indication sur un problème. Dans ce cas, le périphérique ne procédera à aucune relance et continuera l'exploitation avec le microprogramme actuel jusqu'à l'arrêt/remise en marche suivant. L'utilisateur a donc la possibilité de sauvegarder par ex. la configuration actuelle du périphérique.

Si le périphérique est coupé durant un téléchargement TFTP, il ne pourra plus être configuré qu'en local, c.a.d. par l'interface Outband. Lors d'une nouvelle mise en marche, le périphérique attendra un nouveau téléchargement du microprogramme par l'interface série.



*Veillez pour cela à ne faire un téléchargement de microprogramme que par une connexion sûre (stable).*

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

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

## Configuration par SNMP

### Généralités

Le simple protocole de management de réseau (SNMP V.1 selon RFC 1157) permet la surveillance et la configuration des périphériques dans un réseau à partir d'une instance centrale. Cette instance est nommée communément « Gestionnaire », tandis que les périphériques sont nommés « Agents ». La structure permise de l'échange des informations SNMP est relativement simple. Dans un réseau, une application « Gestionnaire » a accès à tous les appareils et services adaptés aux SNMP (les agents). Les droits d'accès sont régis par des « Communautés ».

Le tableau suivant montre que SNMP v.1 ne dispose que d'un jeu d'instructions très limité :

Instruction	But/Source	Fonction
GetRequest	Gestionnaire – Agent	sollicite une information de l'agent
GetNextRequest	Gestionnaire – Agent	sollicite de l'agent l'information suivante dans la MIB
SetRequest	Gestionnaire – Agent	modifie un réglage chez l'agent
GetResponse	Agent – Gestionnaire	retourne la valeur demandée au gestionnaire
Trap	Agent – Gestionnaire	signale une erreur ou un état particulier

Ces instructions permettent la surveillance et la configuration centrale dans un réseau des périphériques adaptés aux SNMP. L'aptitude SNMP des agents est définie dans des MIB = Management Information Bases.

Un agent pour SNMP V.1 (selon RFC 1157) est implémenté dans le microprogramme d'ELSA. Le soutien s'étend sur une partie de la MIB-2 et sur une MIB privée jointe au produit dans un fichier séparé. Afin de pouvoir gérer entièrement un routeur par SNMP, cette MIB devra être chargée et traduite par un gestionnaire SNMP (par ex. HP-OpenView). Après cela, tous les menus et paramètres de la configuration seront disponibles dans une propre branche de l'arborescence du management SNMP :

iso/org/dod/internet/private/enterprises/elsa/isdn-devices/isdn-router/...  
ou 1.3.6.1.4.1.2356.400.1...

### Accès aux tableaux et paramètres par SNMP

Tous les tableaux et paramètres peuvent être lus et, le cas échéant, modifiés via l'interface SNMP. En outre il sera défini dans la MIB, à quelle variable sera attribué l'état 'lecture seule' ou 'lecture-écriture'. Dans les gestionnaires SNMP usuels, les deux états

'lecture seule' et 'lecture-écriture' sont repérés, en règle générale, par des couleurs différentes.

### Sécurité d'accès sous SNMP v.1

L'accès aux objets SNMP s'effectue à l'aide de communautés. Une communauté est en fait un mot de passe permettant de gérer l'accès à certaines classes d'informations. Dans le routeur, la communauté 'publique' autorise un accès lecture à tous les paramètres et tableaux. Cette communauté ne permet en effet aucun accès écriture.

Si des données doivent être écrites via SNMP, il faut utiliser comme communauté le mot de passe du périphérique. Si aucun mot de passe n'a été entré pour un routeur, il ne sera autorisé par principe aucun accès écriture via SNMP.

Lors d'un accès sur un routeur via SNMP, les réglages sous 'Setup/Config-module' seront évalués comme suit :

Inscription	Valeur	Signification
Password-required	On	l'accès par la Communauté 'publique' est bloqué.
Password-required	Off	l'accès par la Communauté 'publique' ne permet que la lecture. Si le mot de passe est entré comme Communauté, toutes les actions peuvent être exécutées.
LAN/WAN-Config	Off	tout accès via LAN/WAN est bloqué.
LAN/WAN-Config	On	l'accès par la Communauté 'publique' ne permet que la lecture. Si le mot de passe est entré comme Communauté, toutes les actions peuvent être exécutées.
LAN/WAN-Config	Read	l'accès par la Communauté 'publique' et par le mot de passe est lecture seule.

Après une tentative d'accès infructueuse, une interception (Trap) 'Authentification échouée' est déclenchée et envoyée au(x) gestionnaire(s) dans le tableau interception SNMP, à condition que le mécanisme interception ait été mis en service.

Le mécanisme communauté dans le SNMP v.1 ne représente qu'une sécurité d'accès très restreinte, car les données, les ID MIB et la communauté dans les Demandes et les Réponses sont transmises sans codage dans le bloc de données UDP.

### Effacer des lignes dans les tableaux à l'aide de SNMP

SNMP-même ne dispose d'aucun mécanisme d'effacement spécifique. Il faut donc faire appel à une astuce pour effacer des inscriptions ou créer de nouvelles lignes dans un tableau.

Si une ligne doit être effacée, il faut modifier l'index de cette ligne, c.a.d. la valeur de la première colonne, en entrant sa valeur actuelle.

- Exemple : la 3ème ligne doit être effacée dans le tableau de routage IP suivant.

Adresse IP	Masque de réseau	Router	Distance
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.240.0.0	0.0.0.0	0
10.0.0.0	255.0.0.0	ROBERT	0
224.0.0.0	224.0.0.0	0.0.0.0	0

Via le gestionnaire on modifie l'inscription '10.0.0.0' (donc le premier élément de la troisième ligne) en entrant sa valeur actuelle, donc '10.0.0.0' et on lance l'instruction Set. L'instruction SetRequest du SNMP contient l'ordre de modifier le premier élément de la troisième ligne sur '10.0.0.0'. Le logiciel SNMP reconnaît cette assignation d'index redondante et l'interprète comme instruction d'effacement.

### Ajouter des lignes au tableau à l'aide de SNMP

Si une ligne doit être rajoutée à un tableau, il faudra modifier un index de ligne quelconque sur l'index de la nouvelle ligne. La ligne servant de source pour la modification restera inchangée.

### Messages d'erreur par interception SNMP

Le mécanisme des interceptions SNMP permet d'envoyer des messages d'erreur ou d'avertissement à une instance de gestion. L'agent SNMP contenu dans le routeur permet d'envoyer des interceptions à jusqu'à 20 gestionnaires SNMP. Les adresses IP de ces gestionnaires sont configurées dans le menu de configuration sous `/setup/SNMP-module/IP-Trap-Table`. En général, l'envoi d'interceptions peut être activé et désactivé à l'aide du commutateur `/setup/SNMP-module/Send-Traps`.

### SNMP et *ELSA LANmonitor*

Les trois entrées `/setup/SNMP-module/ ...Register-monitor`, `.../Delete-monitor` et `.../Monitor-table` ne servent qu'à l'inscription automatique de *LANmonitor* et n'ont aucune autre signification pour l'utilisateur. Ils ne sont affichés au menu qu'à des fins de contrôle.

### La Management Information Base (MIB)

Une représentation textuelle de la structure de la configuration (ce que l'on appelle la MIB privée) doit être livrée avec le périphérique afin de permettre à un système de gestion SNMP d'accéder à la configuration *ELSA LANCOM*. La syntaxe de cette MIB s'oriente sur l'ASN.1 (Abstract Syntax Notation One, ISO 8824). Le logiciel de gestion

SNMP comprend généralement un compilateur MIB. Ce compilateur traduit ce fichier MIB en une forme pouvant être utilisée par le gestionnaire.

La MIB ELSA actuelle se trouve sur le CD-ROM joint au produit ainsi que dans les médias en ligne ELSA.

## 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 ex. lire durant une séance Telnet ou terminal.

### Éditions des tracés

Les sorties de tracés se prêtent au contrôle des déroulements internes du routeur durant ou après la configuration. Un tracé révèle par 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. Un aspect particulièrement positif : Les erreurs peuvent tout aussi bien être trouvées dans la configuration des propres routeurs *ELSA LANCOM* que 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



Ce paramètre...	... affiche avec tracé :
IPX-router	routage IPX
RIP	IPX Routing Information Protocol
SAP	IPX Service Advertising Protocol
IPX-watchdog	IPX-Watchdog-Spoofing
SPX-watchdog	SPX-Watchdog-Spoofing
NetBIOS	administration du NetBIOS IPX
IP-router	routage IP
IP-RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
SCRPT	négociation Script
IP-masquerading	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-Tr., 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.



*Vous trouverez des informations sur l'interprétation des éditions des tracés dans la partie Référence du manuel.*

**ELSA LANmonitor**

Avec *ELSA LANmonitor* vous disposez d'un petit outil de surveillance sous Windows qui vous affiche en permanence 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 le logiciel de configuration *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 'ELSA LANmonitor'.



*ELSA LANmonitor ne vous permet de surveiller que les périphériques auxquels vous accédez Inband ou par le réseau local. Pour cela, le protocole réseau TCP/IP doit être installé sur cet 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*. Pour cet exemple, nous avons choisi l'accès Call-by-Call (sans abonnement) de l'entreprise Arcor.
- ② Lancez *ELSA LANmonitor* avec **Démarrer ► Programmes ► ELSAlan ► ELSA 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 ► Monitoring**.

- ③ *ELSA LANmonitor* génère automatiquement une nouvelle inscription dans la liste des appareils et affiche d'abord l'état des deux canaux B. Lancez votre explorateur Internet et entrez un site quelconque. Avec *ELSA LANmonitor* vous pouvez alors suivre l'établissement d'une communication sur un canal et voir quel est le correspondant 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.
- ⑤ Si vous désirez 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 désirez un protocole des sorties du *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 *LANmonitor* doit établir un fichier protocole tous les jours, tous les mois ou continuellement.



# 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
- Liaisons permanentes et procédures de canaux secours
- Connexions via le réseau GSM
- Prise en charge de PPP
- Routage IPX
- Routage IP
- Serveur DHCP
- Serveur DNS
- Proxy NetBIOS
- Pooling IP
- ELSA LANCAPI
- Gestion des durées
- Rerouteur téléphonique (Least Cost Router)

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

Vous trouverez des exemples de configuration détaillés dans le chapitre 'Workshop'.

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

## 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 ex. partie de ces paramètres.

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

## Protection par mot de passe

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

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

## Le verrouillage des accès

La configuration d'*ELSA LANCOM Business* est protégée contre les « attaques en force brute » par un verrouillage d'accès. Il est possible de définir le nombre maximal de tentatives d'accès infructueuses ainsi que la durée du verrouillage.

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`)

## 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 'Généralités' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou dans le menu `/Setup/TCP-IP-module/Access List`.

## La sécurité de votre LAN

Vous n'appréciez certainement pas qu'une personne externe puisse en toute liberté consulter ou modifier les données sur votre serveur d'entreprise. Un *ELSA LANCOM Business* 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)

## Le contrôle

« L'identificateur » à utiliser pour identifier l'appelant est fixé dans l'onglet 'Prise d'appel' du dossier de configuration 'Communication', ou dans le menu `/Setup/WAN-module/Protect`. 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.
- par 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

Si les connexions sont établies avec PPP, le nom du correspondant peut aussi être transmis.

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.

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/WAN-module/PPP List`.

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



*Il est évident que vous n'utiliserez pas les procédures de sécurité PAP ou CHAP si vous voulez accéder vous-même 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 ?

- Avec PPP, on entre le nom et le mot de passe lors de l'établissement de la communication avec le correspondant, par 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).

### 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 (PPP), vous pourrez déterminer la réaction de vos routeurs 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 ne 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 pas facturée à l'appelant.

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

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

Aujourd'hui, l'une des tâches les plus fréquentes des routeurs tels que des routeurs est la connexion d'un grand nombre de postes de travail dans un LAN au réseau des réseaux, 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 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'.

## 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 confortable à Internet ou à des ordinateurs et réseaux à distance. Cependant, lors de la transmission de données via les lignes commutées RNIS, une mauvaise configuration du routeur (par ex. celle relative aux

filtres) ou l'usage excessif de services (par ex. en navigant sans cesse sur Internet) peuvent occasionner des frais de téléphone élevés.

## Limitation des communications en fonction des unités de taxation

Pour limiter ces frais, le logiciel dans le routeur offre, depuis longtemps déjà, la possibilité de limiter les unités disponibles sur une période déterminée. La configuration par défaut permet par ex. de ne consommer que 830 unités au maximum par semaine. 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 !*

## Limitation des communications en fonction de la durée

Ce mécanisme, cependant, n'entre plus en jeu si l'accès RNIS ne transmet pas d'informations relatives aux frais. 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.

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



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

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



*La protection unités ou durée ne vaut que pour les fonctions de routage ! En revanche, les connexions via LANCAPI ne sont pas concernées.*

## Configuration dans le gestionnaire des coûts

Vous configurez ces paramètres en sélectionnant l'onglet 'Coûts' du dossier de configuration 'Gestion' de *ELSA LANconfig*, ou lors d'une session Telnet ou de terminal `SOUS / Setup / Charges-module`.

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-budget, Minutes-budget  
Nombre maximal d'unités ou de minutes en ligne pendant une période de surveillance
- Budget résiduel, minutes résiduelles  
Nombre d'unités ou de minutes en ligne disponibles pendant la période courante
- Unités-routeur, Minutes-routeur  
Nombre d'unités ou de minutes en ligne de toutes les périodes
- Nombre total d'unités  
Toutes les unités de taxation générées par le périphérique
- Budget-tableau, 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 durées reportées ici sont exprimées en minutes.*

## 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.

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

## Liste des noms

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

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 RoundRobin.  
  
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

## Configuration des interfaces

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

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.

## Interfaces du routeur

Vous configurez les paramètres 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/WAN-module/Router-interface-list`.

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.*

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

Vous trouverez les éléments de configuration de l'interface **LANCAPI** en sélectionnant l'onglet 'Généralités' du dossier de configuration 'LANCAPI' de *ELSA LANconfig*, ou lors d'une session Telnet ou de terminal sous `/Setup/LANCAPI-module/Interface-list`.

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.

## Couche communication

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

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

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

## Liste RoundRobin

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

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 RoundRobin.

- **Correspondant**  
Nom du correspondant tel qu'il a été indiqué dans la liste des noms.

- RoundRobin  
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.

## Liste des canaux

Vous trouverez la liste des canaux en sélectionnant l'onglet 'Correspondants' du dossier de configuration 'Communication' de *ELSA LANconfig*, ou lors des sessions Telnet ou de terminal sous `/Setup/WAN-module/Channel-list`.

La liste des canaux sert à fixer le nombre minimal et maximal de canaux B à utiliser, l'ordre des canaux utilisés, et combien de canaux doivent être utilisés pour une ligne de secours par liaison commutée pour épauler une liaison permanente.

- Correspondant  
Nom du correspondant tel qu'il a été indiqué dans la liste des noms.
- Min  
Nombre minimal de canaux à utiliser pour la connexion.  
  
Si vous choisissez d'utiliser plus d'un canal, la connexion se fera toujours avec un regroupement de canaux statique. La couche utilisée doit être paramétrée pour le regroupement de canaux dans les options de la couche 2.
- Max  
Nombre maximal de canaux à utiliser pour la connexion.  
  
Si vous indiquez un nombre maximal supérieur au nombre minimal, la connexion considérée se fera avec un regroupement de canaux dynamique. La couche utilisée doit être paramétrée pour le regroupement de canaux dans les options de la couche 2.
- Ordre  
La syntaxe permettant d'indiquer l'ordre dans lequel les canaux sont utilisés est [Interface]-[Canal] ; [Interface]-[Canal] etc.
- Canaux secours  
Dans le cas d'une liaison permanente, nombre de canaux devant être activés pour une liaison commutée si la liaison permanente est dérangée.



## Liste PPP

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

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

- Correspondant  
Nom du correspondant tel qu'il a été indiqué dans la liste des noms.
- Nom d'utilisateur  
Nom d'utilisateur utilisé pour s'annoncer chez le correspondant.
- Mot de passe  
Mot de passe utilisé pour s'annoncer chez le correspondant.
- IP, NetBIOS, IPX  
Protocoles pouvant être utilisés pour la connexion considérée.
- Vérification  
Procédure d'authentification que le routeur doit demander au correspondant.
- Durée, Rép., Conf., Fail, Term  
Paramètres modifiant le comportement de la connexion.

## 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/WAN-module/Script-list`.

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.
- Script  
Entrez ici le script, comme décrit dans le manuel de référence de la documentation.

## Prise d'appel

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

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.
- par 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.

## 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/WAN-module/Number-list`.

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.

## Liaisons permanentes et canaux secours

Lorsque vous maintenez des connexions pendant des durées très importantes ou établissez des connexions répétitivement, une liaison permanente dans le RNIS peut

s'avérer plus économique. Comme le canal D n'est pas utilisé pour le transfert de données dans le cas des liaisons permanentes, mais que la simple mise à disposition du canal de signalisation est facturée, les liaisons permanentes sans canal D représentent le meilleur rapport prestation/prix.

Lorsqu'un seul canal suffit à long terme, il est préférable de choisir D64S. Si ce débit ne suffit pas, on peut opter pour D64S2. Pour les connexions avec deux correspondants différents, utilisez deux fois D64S. Cette combinaison est également appelée D64SY :

Liaison permanente	Version
D64S	Un canal B, pas de canal D, un correspondant
D64S2	Deux canaux B, pas de canal D, un correspondant
D64SY	Deux canaux B, pas de canal D, deux correspondants

Toutes les trois variantes sont paramétrées dans le routeur en tant que liaison permanente du groupe 0 dans le tableau des interfaces. On distingue les variantes au moyen du flag 'YV.' dans le tableau des interfaces, au moyen de l'entrée 'Options de couche 2' dans la liste des couches et au moyen des entrées dans la liste des canaux.

## Voici comment configurer la liaison permanente

Les paramètres suivants sont requis pour préparer le routeur pour les divers types de liaison permanente.

### Réglages dans le tableau des interfaces

- Sélectionnez le protocole Liaison permanente **GRPO** dans le tableau des interfaces.
- Le flag **YV.** doit avoir la valeur **Inactif** pour une connexion avec un seul correspondant, et la valeur **Actif** pour les connexions avec deux correspondants.
- Pour les connexions avec un seul correspondant dans un canal B, on peut choisir **compr.** en guise d'option de couche 2.

Pour les connexions dans deux canaux B avec un seul correspondant, choisissez **regroupement** et, au besoin, l'option supplémentaire **compr.**

Pour les connexions avec deux correspondants différents dans deux canaux B, vous pouvez choisir **compr.**

### Paramètres dans la liste des canaux

Dans la liste des canaux, vous sélectionnez les canaux à utiliser pour la liaison permanente. Les indications portant sur les canaux et leur ordre doivent être identiques des deux côtés de la liaison. En outre, indiquez ici le nombre de canaux à utiliser le cas

échéant pour une ligne de canaux secours (ce paramètre doit également être identique pour les deux correspondants).

Correspondant	Min	Max	Ordre	Canaux secours
FVG0	2 canaux	2 canaux	1-1 ; 1-2	0

### Paramètres dans la liste des noms

Si vous recourez à une liaison permanente du groupe 0, les périphériques prennent la ligne automatiquement après la mise sous tension et établissent une connexion en utilisant la couche par défaut.

Lorsqu'une couche différente, le mécanisme de canaux secours (Dial-Backup) ou un regroupement dynamique via liaison commutée doivent être employés, le correspondant doit figurer dans la liste des noms.

Nom	Numéro d'appel	Time-out	Time-out2	Nom de la couche	Rappel
FVG0	1234	20 secondes	0 secondes	PPPHDLC	Inactif

Le numéro d'appel est utilisé pour activer des canaux supplémentaires via des liaisons commutées devant être regroupés dynamiquement pour élargir la ligne permanente. Les numéros d'appel supplémentaires éventuellement requis peuvent être ajoutés dans la liste RoundRobin.

Si la ligne permanente n'est pas disponible suite à un dérangement et si les liaisons commutées regroupées dynamiquement sont éventuellement déconnectées suite à un repli du débit, les numéros d'appel saisis sont utilisés pour établir les lignes de canaux secours.

### Paramètres dans la Couche de communication

Une liaison permanente du groupe 0 est d'abord toujours établie vers le correspondant par défaut, c'est-à-dire avec la couche définie chez le correspondant par défaut. Lorsqu'un correspondant par défaut ou la couche du correspondant par défaut n'est pas défini(e), la connexion est établie avec la couche indiquée comme DEFAULT dans la liste des couches. Si cette valeur par défaut manque également dans cette liste, la connexion est établie avec les paramètres de couche suivants :

Nom de la couche	Encapsulation	Couche-3	Couche-2	Options	Couche-1
DEFAULT	Transparent	PPP	Transparent	aucune	HDLC 64000

**Exemple : D64S2, regroupement dynamique (un canal), pas de canaux secours**

Dans la liste des noms, vous affectez la couche 'MLHDLC' à la liaison permanente et entrez le numéro d'appel pour la ligne commutée dynamique :

Nom	Numéro d'appel	Time-out	Time-out2	Nom de la couche	Rappel
FVG0	123456	20 secondes	20 secondes	MLHDLC	Inactif

Dans la liste des canaux, vous entrez le nombre de canaux requis et précisez les canaux à utiliser. Un canal secours n'est pas indiqué.

Correspondant	Min	Max	Ordre	Canaux secours
FVG0	2	3	1-1 ; 1-2 ; 2-1	0

**Exemple : D64S2, regroupement dynamique (un canal), canaux secours (un canal)**

L'entrée dans la liste des noms reste inchangée. Dans la liste des canaux, vous créez un canal secours.

Correspondant	Min	Max	Ordre	Canaux secours
FVG0	2	3	1-1 ; 1-2 ; 2-1	1

**Exemple : D64S2, pas de regroupement dynamique, canaux secours (deux canaux)**

L'entrée dans la liste des noms reste inchangée. Dans la liste des canaux, vous créez un canal secours.

Correspondant	Min	Max	Ordre	Canaux secours
FVG0	2	3	1-1 ; 1-2	2

## Connexion via GSM

Lorsque plusieurs canaux B sont disponibles, *ELSA LANCOM Business* est idéal pour fonctionner comme nœud d'accès (serveur d'accès distant, serveur RAS) dans les petites et les moyennes entreprises. Pour donner aux salariés nomades la possibilité d'accéder au réseau local, le routeur prend en charge également le protocole V.110 et permet aux ordinateurs portables ou ordinateurs de poche d'accéder au moyen d'un téléphone mobile selon la norme GSM.

L'accès via GSM est configuré comme un accès distant normal, par ex. à l'aide de l'assistant convivial de *ELSA LANconfig*. La couche utilisée doit ensuite être paramétrée pour le protocole correspondant.

Nom de la couche	Encapsulation	Couche-3	Couche-2	Options	Couche-1
DEFAULT	Transparent	APPP	Transparent	aucune ou compr.	V.110 9600



*L'utilisation de services de données via un téléphone mobile GSM n'est pas proposée par chaque fournisseur d'accès Internet (FAI) dans un contrat standard et doit éventuellement être souscrite séparément. Certains FAI distinguent aussi entre un abonnement pour des appels de données entrants ou sortants !*

## Protocole PPP

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

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

## Le protocole

### Présentation de PPP

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

- Protection par mot de passe suivant PAP ou CHAP
- Fonctions de rappel automatique en retour
- Négociation des protocoles réseau à utiliser pour les connexions (par ex. IP ou IPX). En font partie les paramètres requis pour ces protocoles, par ex. les adresses IP/IPX. Cette négociation se fait avec les protocoles IPCP et IPXCP (IP Control Protocol et IPX Control Protocol).
- Vérification de la connexion avec LCP (Link Control Protocol)
- Regroupement de plusieurs canaux (multilink PPP)

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

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

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

- Par ex. pour la communication avec les routeurs externes pour des questions de compatibilité
- Accès à distance avec des adaptateurs RNIS depuis des ordinateurs aux postes de travail distants
- Accès Internet (avec la transmission des adresses)

Le protocole PPP implémenté sur le routeur *ELSA LANCOM* peut être utilisé sur un mode synchrone ou asynchrone aussi bien pour une connexion HDLC transparente que pour une connexion X.75.

### Les phases d'une négociation PPP

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

- Establish phase (établissement de la connexion)  
Une fois que les ETCD ont fermé le circuit, ils négocient les paramètres de la connexion via LCP.  
Chacun d'entre eux vérifie si le correspondant est également prêt à utiliser PPP, et ils s'accordent sur la taille des paquets ainsi que sur le protocole d'authentification (PAP, CHAP ou aucun). LCP passe ensuite en état Opened.
- Authenticate phase (phase de l'authentification)  
Au besoin, les mots de passe sont échangés. Pour l'authentification selon PAP, le mot de passe n'est transmis qu'une seule fois. Dans le cas de CHAP, un mot de passe crypté est envoyé périodiquement à des intervalles configurables.  
Eventuellement, un rappel automatique avec CBCP (Callback Control Protocol) est négocié dans cette phase.
- Network phase (phase de réseau)  
Les protocoles IPCP et IPXCP sont implémentés dans le routeur *ELSA LANCOM*.  
Les couches réseau IPCP et/ou IPXCP peuvent être établies après la transmission correcte du mot de passe.

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

■ **Terminate phase (phase de la terminaison)**

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

### La négociation PPP dans le *ELSA LANCOM*

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

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

```
trace + ppp
```

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

### Liste PPP

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

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

Dans cette colonne de la liste PPP...	... vous saisissez les valeurs suivantes :
Correspondant	Nom que le correspondant utilise pour s'annoncer sur votre routeur
Vérification	Procédure utilisée pour sécuriser la connexion PPP (PAP, CHAP ou aucun). Votre propre routeur exige que votre correspondant respecte cette procédure ! (et pas le contraire). C'est pourquoi la sécurisation selon PAP ou CHAP ne s'applique pas aux connexions avec les fournisseurs d'accès Internet qui ne voudront peut-être pas communiquer leur mot de passe. Sélectionnez 'aucune' pour de telles connexions.
Mot de passe	Mot de passe transmis au correspondant par votre routeur (si nécessaire). Les signes * dans la liste indiquent qu'un mot de passe existe.



Dans cette colonne de la liste PPP...	... vous saisissez les valeurs suivantes :
Durée	Délai entre deux vérifications de la connexion avec LCP. Vous exprimez cette durée par un multiplicateur de 10 secondes (par ex. : 2 pour indiquer 20 secondes). Egalement le délai entre deux vérifications de la connexion selon CHAP. Indiquez ce délai en minutes. Cette durée doit être '0' pour les correspondants sous Windows 95, Windows 98 ou Windows NT !
Rép.	Nombre de tentatives de vérification. En choisissant plusieurs tentatives, vous contournez l'effet des perturbations sporadiques de la ligne. Ce n'est que lorsque toutes les tentatives échouent que la connexion est coupée. Le délai entre deux tentatives s'élève à 1/10e du délai séparant deux vérifications. En même temps le nombre maximal de requêtes de configuration (configure requests) que le routeur émet avant qu'il ne suppose une perturbation de la ligne et raccroche lui-même.
Conf, Fail, Term	Ces paramètres permettent d'influencer le mode de fonctionnement de PPP. Ils sont définis dans la recommandation RFC 1661 et ne seront pas décrits ici. Si vous ne pouvez pas établir de connexion PPP, vous trouverez dans cette recommandation et dans les statistiques PPP du routeur des informations sur le dépannage. En général, les paramètres par défaut suffisent. Ces paramètres ne peuvent être modifiés que par l'intermédiaire de SNMP ou de TFTP (avec le logiciel de configuration <i>ELSA LANconfig</i> ) !
Nom d'utilisateur	Nom que votre routeur utilise pour s'annoncer chez le correspondant. Si ce champ n'est pas renseigné, c'est le nom de périphérique de votre routeur qui est utilisé.
Droits	Protocoles réseau qui doivent être routés via cette connexion : IP, IPX, NTB (NetBIOS). NetBIOS réclame toujours l'un des deux autres protocoles.

## Vérification de la ligne avec LCP

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

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

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

de réponse, la ligne est coupée et le périphérique cherche une voie de rechange. Cette alternative peut par ex. être une ligne de canaux secours.



*Dans le cas de l'accès à distance d'ordinateurs aux postes de travail sous Windows 95, Windows 98 ou Windows NT, nous recommandons de désactiver les requêtes LCP régulières, car ces systèmes d'exploitation ne répondent pas aux requêtes d'écho LCP.*

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

## Attribution des adresses IP avec PPP

Pour interconnecter des ordinateurs utilisant TCP/IP comme protocole réseau, tous les participants ont besoin d'une adresse IP unique et valable. Lorsque l'un des correspondants n'a pas son adresse IP (par ex. l'ordinateur d'un télétravailleur), le *ELSA LANCOM* peut lui assigner une adresse pour la durée de la connexion et permettre ainsi l'échange de données.

Ce mode d'attribution de l'adresse est exécuté pendant la négociation PPP et uniquement pour les connexions via le réseau étendu. L'attribution des adresses au moyen de DHCP est utilisée au sein d'un réseau local.



*Une adresse IP peut être attribuée uniquement lorsque le ELSA LANCOM peut identifier le correspondant au moyen de son numéro d'appel ou de son nom, c'est-à-dire si l'authentification a abouti.*

### ■ Exemple : Accès à distance

L'attribution de l'adresse est possible grâce à une entrée spéciale dans la table de routage IP. En plus de l'adresse IP dans le champ 'Routeur' qui doit être attribuée au correspondant, on attribue le masque de réseau 255.255.255.255. Le nom du routeur est dans ce cas le nom sous lequel le correspondant doit s'annoncer chez *ELSA LANCOM*.

En plus de l'adresse IP, on transmet également au correspondant les adresses des serveurs DNS et NBNS (Domain Name Server et NetBIOS Name Server) y compris celle du serveur de backup défini dans le module TCP/IP.

Pour que le tout fonctionne, le correspondant doit naturellement être configuré de manière à ce que *ELSA LANCOM* lui fournisse automatiquement l'adresse IP et les serveurs de noms (DNS et NBNS). Par ex. dans Accès réseau à distance de Windows, cette configuration est réalisée dans la fenêtre 'Propriétés de TCP/IP' (onglets 'Adresse IP' et 'Configuration DNS'), où les options 'Adresse IP attribuée par

serveur' et 'Adresses de serveur de nom attribuées par serveur' doivent être activées.

#### ■ Exemple : Accès Internet

Lorsqu'on réalise un accès Internet pour un réseau local via *ELSA LANCOM*, l'attribution des adresses IP peut prendre le chemin inverse. Dans ce contexte, on peut réaliser des configurations dans lesquelles *ELSA LANCOM* n'a pas d'adresse IP valable dans Internet mais où il s'en fait attribuer une par le FAI pour la durée de la connexion. A côté de l'adresse IP, *ELSA LANCOM* obtient également des informations sur les serveurs DNS pendant la négociation PPP.

Dans le réseau local, *ELSA LANCOM* n'est identifié que par son adresse Intranet. Tous les ordinateurs aux postes de travail dans le réseau local peuvent alors accéder au même compte Internet et accéder aussi par ex. au serveur DNS.

Les utilisateurs peuvent consulter les adresses attribuées dans *LANmonitor*. En plus du nom du correspondant connecté, ils trouveront ici l'adresse IP actuelle ainsi que les adresses de serveurs DNS et NBNS. Même les options telles que le regroupement des canaux ou la durée de la connexion sont affichées.



*ELSA LANmonitor est en règle générale installé en même temps qu' ELSA LANconfig. Pour une description d'ELSA LANmonitor, reportez-vous au chapitre 'Supervision de la ligne'.*

## Fonctions de rappel automatique

*ELSA LANCOM* prend en charge, outre le rappel via le canal D et le rappel via le protocole ELSA, le rappel via le protocole CBCP de Microsoft de même que le rappel via PPP selon RFC 1570 (extensions LCP PPP). Il est également possible d'opérer un rappel rapide au moyen d'une procédure mise au point par ELSA.

Les PC tournant sous Windows 95, Windows 98 ou Windows NT ne peuvent être rappelés que par l'intermédiaire du protocole CBCP. Pour permettre le contrôle des numéros d'appel au sein d'*ELSA LANCOM*, la liste des noms dispose d'un certain nombre d'entrées qui sont :

Avec l'entrée...	... vous réglez le rappel comme suit :
Inactif	Il n'y a pas de rappel.
Auto (ni Windows 95, Windows 98 ni Windows NT, voir ci-après)	Le correspondant est rappelé s'il est trouvé dans la liste des numéros. L'appel est dans un premier temps rejeté. Dès que le canal est de nouveau libre, le numéro est rappelé (durée env. 8 secondes). Dans le cas où le correspondant n'est pas trouvé dans la liste des numéros, il est dans un premier temps accepté en tant que correspondant PAR DEFAUT. Le rappel est ensuite négocié pendant l'échange de protocole. L'utilisateur est ce faisant taxé d'une unité.

Avec l'entrée...	... vous réglez le rappel comme suit :
Nom	Un échange de protocole est systématiquement effectué avant tout rappel, même si le correspondant a été trouvé dans la liste des numéros (par ex. pour les PC avec Windows qui se connectent sur le périphérique). L'utilisateur est ce faisant taxé d'une unité.
ELSA	Un rappel rapide est réalisé si le correspondant a été trouvé dans la liste des numéros : <i>ELSA LANCOM</i> envoie au correspondant un signal spécial et rappelle aussitôt que le canal est à nouveau libre. Environ 2 secondes plus tard, la communication est établie. Si le correspondant ne reprend pas l'appel aussitôt après le signal, la procédure de rappel normale est resélectionnée 2 secondes plus tard (durée env. 8 secondes). Ce mode n'est disponible qu'au niveau des ports DSS1.
Looser	Utilisez l'entrée 'Looser' lorsque le correspondant attend un rappel. Cette entrée a une double rôle : elle annule d'une part toute communication en cours d'établissement dès qu'arrive un appel venant du correspondant en train d'être appelé, et active d'autre part la fonction permettant de réagir à une procédure de rappel rapide. Il faut autrement dit, pour pouvoir opérer un rappel rapide, que l'appelant se trouve en mode 'Looser' et que l'appelé se trouve en mode 'ELSA'.



*L'entrée 'Nom' offre une sécurité maximum lorsqu'un numéro figure à la fois dans la liste des numéros et dans la liste PPP. L'entrée 'ELSA' correspond à la façon la plus rapide pour deux routeurs ELSA d'opérer des rappels automatiques.*

*Les correspondants tournant sous Windows **doivent obligatoirement** être réglés sur 'Nom'.*

### Rappel automatique via le protocole CBCP de Microsoft

Le protocole CBCP de Microsoft offre trois possibilités pour la gestion des numéros de rappel :

- L'appelé ne rappelle pas.
- L'appelé autorise l'appelant à préciser lui-même le numéro de rappel.
- L'appelé connaît le numéro de rappel et ne rappelle **qu'à** ce numéro.

Le protocole CBCP permet d'établir à partir d'un PC tournant sous Windows 95, Windows 98 ou Windows NT une connexion vers *ELSA LANCOM* et de se laisser

rappeler par ce dernier. Les trois options sont sélectionnées à partir de l'option de rappel et du numéro de rappel dans la liste des noms.

Dialogue box titled "Liste des noms - Nouvelle entrée".

Fields:

- Nom: DISTANT01
- Numéro d'appel: 123456
- Time-out: 20 secondes
- Time-out pour regroupement: 20 secondes
- Nom de la couche: PPP

Options for "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

Buttons: OK, Annuler

### Ne pas effectuer de rappel

Il faut pour activer cette option sélectionner l'option 'Pas de rappel' lors de la configuration via un émulateur de terminal ou via Telnet.

### Choisir soi-même le numéro de rappel

Le correspondant est rappelé après contrôle de son nom. Il faut pour activer cette option sélectionner l'option de rappel 'Nom' ; la liste de noms ne doit contenir **aucun** numéro d'appel.

Après authentification, une fenêtre de dialogue invitant l'utilisateur à entrer son numéro d'appel apparaît sous Windows 95.

### Numéro de rappel défini par *ELSA LANCOM*

Le correspondant est rappelé après contrôle de son nom. Il faut pour que cette option soit active que le correspondant ait sélectionné l'option de rappel 'Nom' et que la liste de noms contienne **un** numéro d'appel.

Après authentification, un message ne pouvant qu'être validé par l'utilisateur apparaît sous Windows 95.

Les ordinateurs aux postes de travail Windows 95, Windows 98 ou Windows NT sont rappelés env. 15 secondes après que la connexion ait été coupée. Ce délai est prescrit par Windows et ne peut pas être réduit.

## Rappel rapide via le protocole ELSA

Pour faire communiquer deux *ELSA LANCOM* entre eux dans une configuration où l'un rappelle l'autre, il est conseillé d'utiliser la procédure ELSA de rappel rapide.

- Celui souhaitant être rappelé sélectionne dans la liste des noms 'Attendre que le correspondant rappelle' ('Looser' en cas de configuration via un émulateur de terminal ou via Telnet).
- Celui rappelant sélectionne 'Rappeler le correspondant (procédure rapide)' dans la liste des noms et précise le numéro d'appel ('ELSA').

## Rappel automatique selon RFC 1570 (extensions LCP PPP)

Il existe selon RFC 1570 cinq façons de demander un rappel. Toutes les cinq sont acceptées par *ELSA LANCOM*. La procédure est la même pour chacune des variantes :

Après authentification du correspondant, *ELSA LANCOM* coupe la connexion et rappelle ce dernier trois secondes plus tard.

## Regroupement des canaux avec MLPPP

Si vous établissez une connexion RNIS vers un correspondant adapté à PPP, vous pouvez mettre le turbo à vos données : Vous pouvez compresser vos données et/ou utiliser plusieurs canaux B pour la transmission (Regroupement des canaux).

Une connexion avec regroupement des canaux se distingue d'une connexion « normale » par le fait que l'on a recours pour la transmission de données non pas à un canal B mais à plusieurs canaux B en parallèle.

Pour le regroupement des canaux, on utilise MLPPP (multilink PPP). Pour pouvoir avoir recours à ce procédé, il faut bien entendu avoir choisi le protocole PPP pour le canal B. MLPPP se prête par ex. à l'accès Internet via des fournisseurs d'accès ayant dans leurs nœuds d'accès des correspondants également adapté à MLPPP.

- Regroupement statique des canaux  
Lors de l'établissement d'une connexion avec regroupement statique des canaux, le routeur essaie immédiatement d'établir une connexion avec les canaux B ayant l'option 'Minimal' dans la liste des canaux. Il utilise alors soit les canaux indiqués dans la liste des canaux, soit des canaux libres.
- Regroupement dynamique des canaux  
Pour une connexion avec un regroupement dynamique des canaux, le routeur active d'abord uniquement les canaux B ayant l'option 'Minimal' dans la liste des canaux et commence le transfert des données. Si le routeur constate que le débit se maintient au-dessus d'un seuil donné pendant une certaine période, il tente d'activer des canaux supplémentaires jusqu'à ce que le nombre de canaux indiqué dans 'Maximal' soit atteint. Là aussi, il utilise soit les canaux indiqués dans la liste des

canaux, soit des canaux libres.

Une fois les canaux dynamiques ayant établi la connexion et le débit repassant sous le seuil, le routeur attend la fin du timeout B2 Timeout et libère les canaux automatiquement. Les unités de taxation entamées sont ce faisant consommées jusqu'à la fin lorsque les informations de facturation sont transmises pendant le transfert. Le routeur n'utilise donc les canaux dynamiques que lorsque qu'il en a vraiment besoin et ce, aussi longtemps que nécessaire.

### Procédure de configuration pour le regroupement de canaux :

Le regroupement des canaux se configure en trois temps :

- ① Créez dans la liste des noms une entrée pour la connexion devant recourir au regroupement des canaux. Sélectionnez ce faisant une couche pour laquelle le regroupement des canaux a été paramétré dans les options de la couche 2.
  - **Compression** selon le procédé de compression de données LZS (Stac) ; réduit le volume de transfert dans le cas où les données n'ont pas déjà été comprimées. Ce procédé est également pris en charge par les routeurs d'autres fabricants et par les adaptateurs RNIS compatibles Windows.
  - **Le regroupement des canaux** fait intervenir plusieurs canaux B pour une connexion. La nature du regroupement de canaux est déterminée par la configuration des options de la couche 2 dans la liste des couches, par le réglage des timeouts dans la liste des noms, par le paramètre concernant la connexion en Y dans la liste des interfaces, et par le paramètre dans la liste des canaux.
  - **Compr.+regroupement** utilise les deux (compression et regroupement des canaux) et permet donc de disposer du plus grand débit de transmission possible.
- ② Réglez également dans la liste des noms les timeout pour la connexion. Observez ce faisant les règles suivantes :
  - Le timeout B1 doit être choisi suffisamment grand, de façon à ce qu'il n'y ait pas de coupure prématurée de la connexion en cas de brève absence de paquets. Vous conseillons de choisir au départ une valeur comprise entre 60 et 180 secondes et de corriger par la suite la valeur pendant le service.
  - Le timeout B2 indique au bout de combien de temps les canaux dynamiques sont libérés après le passage du débit sous un certain seuil.
- ③ Dans la liste des canaux, sélectionnez le nombre de canaux à utiliser pour la connexion. Vous pouvez en outre spécifier les canaux à utiliser et ainsi réserver par ex. certains canaux pour les accès distants.

Les options dans la liste des canaux indiquent si le regroupement des canaux est statique ou dynamique (voir plus haut). Si le nombre de canaux « minimal » est supérieur à 1, le regroupement est statique, et si le nombre « maximal » est supérieur au nombre « minimal » de canaux le regroupement peut être dynamique.

- ④ Dans les options pour la connexion en Y de la liste des interfaces, indiquez ce qui doit se passer lorsqu'une connexion avec regroupement des canaux est en cours et qu'une deuxième connexion doit être établie, mais qu'aucun canal B n'est disponible.
- Connexion en Y **active** : le routeur interrompt le regroupement des canaux sur l'interface considérée, afin d'établir la seconde connexion avec l'autre correspondant. Une fois le canal à nouveau libre, le routeur rétablit automatiquement le regroupement de canaux (en cas de regroupement statique toujours, en cas de regroupement dynamique, seulement en cas de besoin).
  - Connexion en Y **inactive** : le routeur maintient la connexion sur l'interface considérée et l'autre connexion doit être établie via une autre interface, ou le routeur doit attendre si aucune interface n'autorise la libération d'un canal lorsqu'une connexion avec regroupement de canaux est en cours.

## Routage IPX

Le routeur IPX transmet les données de réseaux utilisant le protocole réseau IPX/SPX (par ex. les réseaux Novell). Une entrée dans le tableau de routage IPX sert à déclarer un réseau distant aux ordinateurs du réseau local. On peut déclarer jusqu'à 16 réseaux différents dans le tableau de routage.

## Adressage IPX

Une adresse complète dans un réseau IPX comporte trois parties : un numéro de réseau, l'adresse MAC de la carte réseau et le numéro de Socket.

- Le numéro de réseau peut être choisi librement. Il doit néanmoins être unique et se distinguer de tous les autres réseaux IPX adressables pour garantir une affectation correcte.
- L'adresse MAC est fixe. Chaque composant du réseau a une adresse MAC. Ce n'est que dans certains cas particuliers que l'on utilise aussi une adresse différente à l'intérieur du réseau.
- Afin de pouvoir activer non seulement un ordinateur, mais aussi un service particulier sur cet ordinateur, un réseau IPX utilise les numéros de Socket. Ceux-ci permettent d'identifier clairement les divers services.

## Informations sur le réseau local

Lorsqu'on a besoin d'exploiter plusieurs réseaux locaux (LAN : Local Area Network) distincts sur le même site, ces réseaux ne doivent pas obligatoirement avoir chacun leur propre câblage. Plusieurs réseaux logiques différents peuvent se partager un câble. Afin que les données des divers réseaux ne se gênent pas mutuellement et pour qu'un réseau reste invisible pour les autres, ils utilisent des formats différents pour les paquets



Ethernet. Ces formats sont déterminés par la liaison (binding) appartenant à un numéro de réseau unique sur ce câble.

Pour que le routeur sache à quel réseau il appartient, vous devez lui indiquer le numéro de réseau et la liaison correspondante. Lorsque vous laissez l'adresse du réseau à la valeur par défaut '00000000', le routeur détermine l'adresse et la liaison lui-même. A cet effet, il sélectionne sur le câble connecté le réseau sur lequel il reçoit le plus grand nombre de réponses SAP.

## Tableau de routage IPX

Dans le tableau de routage IPX, vous déclarez au routeur quels correspondants (donc les autres routeurs ou ordinateurs) sont accessibles pour le réseau local, et vous indiquez plusieurs paramètres pour la connexion. Ce tableau, pouvant contenir 16 entrées au maximum, a la structure suivante :

Correspondant	Réseau	Liaison	Propagated	Backoff
FILIALE01	00000245	802.3	Router	Actif
FILIALE02	00000320	SNAP	Filtrer	Actif
CENTRALE	00000420	802.2	Filtrer	Actif

### ■ Correspondant :

Le nom du correspondant tel qu'il est enregistré comme nom de périphérique dans le routeur du correspondant.

### ■ Réseau :

Adresse du réseau étendu WAN (Wide Area Network). Il ne s'agit pas de l'adresse du réseau cible, mais d'une troisième adresse représentant le réseau entre les deux réseaux devant être relié entre eux. La règle est la suivante :

Adresse LAN 1  $\neq$  Adresse WAN 1 = Adresse WAN 2  $\neq$  Adresse LAN 2  $\neq$  Adr. LAN 1

### ■ Liaison :

On détermine ici la liaison Ethernet devant être utilisée dans le réseau étendu WAN. Cette définition est uniquement pertinente si la couche pour cette liaison prend en charge l'encapsulation Ethernet. Lorsque cette définition manque, le système utilise 802.3 par défaut.

### ■ Propagated :

Filtre pour les paquets IPX du type 20 (NetBIOS Propagated Frames). A l'origine, le NetBIOS (Network Basic Input/Output System) a été développé pour IBM, et il est entre-temps utilisé aussi par Microsoft sous une forme modifiée. Ce protocole met à disposition des services tels que le décodage du nom, la sécurisation des données et le transfert des paquets dans l'ordre correct dans les couches 3 (réseau) et 4

(transport) du modèle OSI (protocole sécurisé). Les paquets NetBIOS ont un type de paquet et un Socket spéciaux (Propagated Pakets). NetBIOS est utilisé avant tout pour l'échange de données entre des postes de travail dans un réseau local.

Ces paquets IPX peuvent être exclus de la transmission à l'aide du paramètre 'Filtre' ou être routés. Avec le paramètre 'Route', les paquets sont transmis si une connexion est établie avec le correspondant voulu, ou si un canal libre est encore disponible pour établir une connexion supplémentaire. Lorsque toutes les lignes sont occupées, les trames propagées sont rejetées.

■ Backoff :

Le routeur IPX utilise un algorithme spécial (Exponential Backoff) pour réduire, autant que possible, les coûts de communication en cas d'erreur de configuration.

Lorsqu'il n'existe pas de serveur dans le réseau du correspondant (par ex. dans le cas d'un accès réseau à distance depuis un ordinateur au poste de travail), la fonction 'Backoff' devrait être désactivée (voir aussi 'Exponential Backoff').

Par défaut, ce paramètre est 'On'.

## **Que se passe-t-il pendant la transmission des données dans le réseau IPX ?**

Lorsqu'un périphérique s'annonce dans un réseau IPX, il envoie d'abord une requête pour déterminer le protocole SAP (Service Advertising Protocol) et interroge qui est le premier serveur accessible dans le réseau (Get Nearest Server Request) ayant le numéro '00000000'. Lorsqu'un routeur ou un serveur se trouve dans ce réseau, celui-ci répond à la requête et communique le numéro de réseau correct.

Les serveurs transmettent en outre régulièrement des informations sur les services qu'ils mettent à disposition et sur les autres réseaux auxquels ils peuvent accéder. Ils utilisent à cet effet des paquets de données spéciaux suivant le protocole SAP ou RIP (Routing Information Protocol).

Lorsque le routeur IPX est entièrement configuré et mis sous tension, il établit d'abord des connexions avec tous les correspondants accessibles définis dans les tableaux de routage et échange des informations SAP et RIP avec ces réseaux. Le routeur enregistre ces données dans ses tableaux SAP et RIP internes.

## **Tableaux RIP et SAP**

Les informations RIP et SAP figurent par ordre alphabétique dans les tableaux correspondants. Les protocoles RIP sont triés uniquement d'après le réseau, les protocoles SAP sont triés par type de service puis par nom de serveur.

Les tableaux RIP et SAP sont mis à jour après chaque nouveau paquet RIP ou SAP. Afin de proposer uniquement les services (SAP) qui sont vraiment accessibles (RIP), le routeur

admet dans son propre tableau uniquement les informations SAP auxquelles correspond une entrée RIP. À côté des informations sur les routes et les services utilisables, les entrées des tableaux indiquent aussi par ex. combien de routeurs se trouvent sur le chemin (hops) ou combien de temps un paquet met à arriver dans le réseau de destination (tics = environ 1/18ème de seconde). Si par ex. les informations RIP proposent plusieurs routes menant à un réseau cible, le routeur choisit la route ayant le nombre de tics et de hops le plus bas sur la base des tableaux, et enregistre uniquement cette route.

Les tableaux RIP peuvent contenir jusqu'à 64 entrées, les tableaux SAP 128 entrées. Étant donné que les tableaux sont remis à jour après chaque nouveau paquet, il faudra naturellement que les anciennes entrées fassent de la place aux nouvelles. À cet effet, les entrées obtiennent une information artificielle de vieillissement. L'âge de chaque entrée des tableaux RIP/SAP qui a été ajouté suite à un échange de données local est incrémenté de un toutes les 60 secondes. Un nouveau paquet RIP ou SAP correspondant à une entrée entraîne la remise à zéro de l'âge. Une route ou un service est considéré comme inaccessible (down) quand ils ont atteint un âge compris entre 1 et 60 (configurable). L'entrée est supprimée quand elle atteint le double de cette valeur. En outre, toutes les informations RIP et SAP concernant ce correspondant sont supprimées dans les tableaux suite à l'établissement d'une connexion et remplacées par des nouvelles informations.

## Tant de routeurs ici...

Lorsqu'on souhaite établir des connexions vers plus de correspondants qu'il y a de canaux B disponibles, il est temps d'installer un deuxième (troisième...) routeur. Afin que la coordination entre les deux frères fonctionne sans problème et pour que le réseau trouve toujours un interlocuteur, tous les routeurs contiennent les mêmes entrées dans leur tableau de routage. Au moyen des paquets RIP, les informations de routage identiques sont envoyées à chaque routeur, mais avec un nombre de tics et de hops plus élevé (`Setup/IPX-module/LAN-config/RIP-SAP-scal.`). Ces routes sont alors pour ainsi dire mises en réserve, et sont utilisées lorsque tous les canaux du périphérique adressé sont occupés.

## Routes redondantes

Lorsqu'un routeur reçoit des informations (dans un paquet RIP) sur des routes avec un nombre de tics et de hops identique à celui de ses propres routes (routes redondantes), il n'a évidemment pas besoin de déclarer une nouvelle fois ces routes à l'expéditeur. Il communique donc ces routes uniquement aux routeurs qui n'ont pas propagé la route. Cette procédure est appelée « split horizon ».

Lorsqu'on a besoin exceptionnellement de déclarer des routes redondantes dans le réseau local, on peut utiliser la fonction 'Loop propagated' (`Setup/IPX-module/LAN-Config/LOOP-Prop.`). Les routes déclarées ainsi sont mises en évidence

dans le tableau RIP par 'LOOP'. Comme la définition des routes redondantes n'est pas interdite selon les spécifications Novell, mais qu'on devrait si possible les éviter, la configuration par défaut est 'Off'.

## Exponential Backoff

Afin d'obtenir les informations de routage nécessaires (informations RIP et SAP) des correspondants IPX, le routeur IPX essaie d'établir les connexions adéquates après la mise sous tension. En cas d'échec, par ex. à cause d'une configuration incorrecte du routeur IPX, l'algorithme Exponential Backoff empêche la répétition des tentatives de connexion et contribue donc à économiser des coûts de communication infructueuse.

Si la première tentative de communication avec un correspondant échoue, le routeur essaie de se connecter à nouveau après un intervalle de plus en plus long. Cet intervalle est calculé de la manière suivante :

- La première tentative est faite après  $10 + x$  secondes,  $x$  étant compris entre 0 et 10.
- La deuxième tentative est faite au bout de  $10 + x$  secondes après l'échec de la première tentative.  $x$  est maintenant compris entre 0 et 20 secondes.
- La valeur supérieure de  $x$  est à présent doublée à chaque nouvelle tentative. Finalement, le routeur abandonne au bout de la 16ème tentative infructueuse. Suite à l'allongement constant de l'intervalle, la période maximale couverte au bout des 16 tentatives est de 1 journée.

Si aucune tentative de connexion n'a abouti, la route est verrouillée. Une nouvelle tentative de connexion n'est alors possible qu'après avoir modifié l'entrée correspondante dans le tableau de routage.



*Vous avez la possibilité de consulter la durée restant jusqu'à la tentative suivante ainsi que le nombre de tentatives de connexion dans les statistiques réseau (status/IPX-module/IPX-router/Networks).*

## Filtrage des paquets IPX

Les entrées du tableau de routage vous servent à indiquer les autres réseaux accessibles. Mais à partir de ce moment, ces réseaux sont alors accessibles aussi aux paquets qui n'ont rien à voir dans le réseau du correspondant. Ces paquets provoquent des tentatives de connexion inutiles qui génèrent des coûts superflus.

Par conséquent, il faut des filtres adaptés. Ces filtres permettent par ex. d'exclure des paquets, utilisés pour la communication interne entre les réseaux, de la transmission via le réseau étendu ou du moins les limiter.

- Propagated

Ces trames spéciales utilisent des protocoles qui ne peuvent en fait pas être routés. Pour pouvoir tout de même participer au routage commun, ces données sont

encapsulées dans des paquets IPX normaux et envoyés sous forme de messages diffusés.

Le routage de ces paquets n'est parfois pas souhaité. C'est pourquoi vous pouvez indiquer explicitement pour le type de paquet considéré s'il doit être routé ou filtré.

#### ■ Filtre de Socket

Chaque paquet dans un réseau IPX contient, en plus de l'adresse de l'expéditeur et de l'adresse du destinataire, les Sockets source et cible. Par Sockets, on entend les processus auxquels les données du paquet sont destinées.

En ce qui concerne les Sockets du réseau local aussi bien que des réseaux distants, il existe respectivement un tableau de filtrage définissant les filtres au moyen desquels un Socket cible ou des groupes entiers peuvent être exclus la transmission. Certains Sockets connus pour être fréquemment à l'origine de connexions non souhaitées figurent déjà par défaut dans le tableau de filtrage.

#### ■ Informations RIP et SAP

Un routeur communique aux autres routeurs toutes les routes (chemins menant aux autres réseaux) qu'il connaît au moyen des RIP selon le principe « split horizon ». Il s'agit aussi bien des entrées du propre tableau de routage que des routes que les autres routeurs ont communiquées au routeur. Il tire ses routes aussi bien des routeurs du réseau local que de ceux des réseaux distants. Il enregistre toutes les informations de routage disponibles dans son tableau RIP interne.

Les serveurs proposent leurs services dans les informations SAP. Les divers services sont représentés dans les infos SAP par des numéros. Chaque service (par ex. un serveur de fichiers ou un serveur d'impression) est identifié par un numéro. Le routeur reprend les informations sur les services disponibles dans son tableau RIP interne et note quels services sont disponibles dans quels réseaux à quelle adresse MAC. Dans ce contexte, il sait aussi si le service proposé est local ou s'il se trouve dans un réseau distant, et peut alors propager le service sans établir de connexion.



*Vous pouvez consulter les tableaux RIP et SAP avec les valeurs à jour dans le module IPX (setup/IPX-module/RIP-config ou SAP-config) des routeurs.*

Les informations RIP et SAP sont naturellement essentielles pour la communication entre les périphériques dans un réseau, et c'est pourquoi il existe diverses possibilités de configurer la transmission de ces paquets :

- Un tableau de filtres du réseau local ou du réseau étendu permet d'indiquer au routeur de ne PAS faire figurer les informations sur les routes vers certains réseaux ou sur certains services dans le tableau RIP ou SAP interne. Les routes concernées ne sont alors pas utilisées et ne sont pas non plus communiquées, les services ne sont pas proposés dans le propre réseau.
- Les paquets RIP et SAP sont transmis sans filtre, c'est-à-dire toujours. Or, ces paquets occupent dans tous les cas une partie de la ligne de communication.

- Les paquets RIP et SAP sont transmis uniquement si l'information a été modifiée.
  - Les RIP et les SAP peuvent être transmis par intervalles réguliers configurables. Normalement, les informations sont envoyées chaque minute. Ce délai peut être rallongé jusqu'à 60 minutes.
  - Le moyen le plus économique d'envoyer les paquets RIP et SAP est de n'envoyer les informations qu'une fois qu'une connexion a été établie.
- Chiens de garde IPX et SPX :
- Avec ces paquets, les serveurs demandent par ex. aux ordinateurs aux postes de travail s'ils sont encore actifs ou s'ils peuvent être déconnectés. Afin que ces paquets « bonjour-est-ce-que-tu-es-réveillé ? » ne conduisent pas constamment à un établissement de la connexion avec des réseaux distants, vous pouvez configurer la réponse à ce questionnement de la manière suivante :
- Les chiens de garde IPX restent sans réponse. Les ordinateurs sont déconnectés au bout de la période configurée sur le serveur.
  - Une réponse locale peut être donnée aux chiens de garde IPX et SPX. Cette procédure est appelée spoofing. Le routeur répond alors à la place des ordinateurs adressés, et ceux-ci ne sont naturellement jamais déconnectés. Il est donc pertinent de fixer sur le serveur un délai au bout duquel les périphériques correspondants sont déconnectés.
  - Les chiens de garde IPX et SPX peuvent naturellement être routés tout-à-fait normalement, mais entraînent dans ce cas souvent l'établissement d'une connexion.



*Vous trouverez des informations supplémentaires sur IPX, sur le routeur IPX et sur les paramètres correspondants dans le chapitre 'Configuration/Module IPX' du Manuel de référence.*

## Routage IP

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

### Le tableau de routage IP

Dans le tableau de routage IP, vous déclarez au routeur à quels correspondants (donc les autres routeurs ou ordinateurs) il doit envoyer les données destinées aux adresses ou aux plages d'adresses IP. L'entrée dans ce tableau est donc appelée la « route », puisqu'elle décrit le chemin des paquets. Comme vous créez ces entrées vous-même et qu'elles restent inchangées jusqu'à ce que vous les modifiez manuellement ou les supprimiez, cette politique est aussi appelée « routage statique ». A l'opposé, il existe aussi un

« routage dynamique ». Dans ce cas les routeurs échangent leurs informations sur les routes et mettent ces informations à jour en permanence. Le tableau de routage statique peut contenir jusqu'à 64 entrées, le tableau dynamique 128. Lorsque IP-RIP est actif, le routeur IP tient compte des deux tableaux.

En outre, le tableau de routage indique aussi au routeur la distance de cette route, ceci afin que la route la plus avantageuse puisse être choisie en association avec IP-RIP. Par défaut, la distance jusqu'à un autre routeur est 2, ce qui veut dire que le routeur peut être atteint directement. Tous les routeurs adressables localement, c'est-à-dire les autres routeurs dans le réseau local ou les ordinateurs aux postes de travail connectés via Proxy-ARP, figurent dans le tableau avec la distance 0. Lorsqu'on déclare une distance plus élevée (14 au maximum), on réduit la « qualité » de cette route. De telles routes de « qualité inférieure » ne doivent être utilisées que lorsqu'aucune autre route vers le correspondant n'est trouvée.

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

Adresse IP	Masque de réseau	Routeur	Distance	IP-Masquerading
192.168.120.0	255.255.255.0	Bordeaux	2	Inactif
192.168.125.0	255.255.255.0	Paris	3	Inactif
192.168.130.0	255.255.255.0	191.168.140.123	0	Statique

Que signifient les diverses entrées de la liste ?

■ Adresse IP et masque de réseau IP

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

■ Routeur

C'est là que le routeur envoie les paquets correspondants à l'adresse IP et au masque de réseau. Lorsque le correspondant est un routeur dans un autre réseau ou un ordinateur au poste de travail isolé, ce champ contient un nom. Lorsque votre propre routeur ne peut pas joindre lui-même le correspondant, ce champ contient l'adresse IP d'un autre routeur qui connaît le chemin vers le réseau de destination.

■ Distance

Nombre de routeurs se trouvant entre le propre routeur et la destination. Pour les connexions longue distance, cette valeur est souvent considérée comme un indicateur du coût de la transmission, et utilisée pour distinguer les voies de transmission économiques ou chères. Les distances enregistrées sont propagées de la manière suivante :

- Pendant qu'une connexion est établie avec un réseau distant, tous les réseaux accessibles au travers de cette connexion sont propagés avec la distance 1.
- Tous les réseaux non connectés sont propagés avec la distance déclarée dans le tableau de routage (mais au moins avec la distance 2) tant qu'un canal de transmission reste disponible.
- Lorsque tous les canaux sont occupés, les réseaux restants sont propagés avec la distance 16 (= inaccessible).
- Les correspondants reliés via Proxy-ARP constituent une exception. Ces hôtes Proxy ne sont pas propagés du tout.



### ■ IP-Masquerading

L'option 'Masquerading' dans le tableau de routage permet d'indiquer au routeur quelle adresse IP il doit utiliser pour la transmission des paquets.

- 'Inactif' : pas de masquage.
- 'Actif' : votre fournisseur d'accès vous attribue une adresse IP quelconque valable dans Internet que vous utilisez ensuite pour la connexion et pour le masquage.
- 'Stat.' : cette option vous permet de demander au FAI de vous attribuer une adresse donnée, indiquée en tant qu'adresse IP dans l'onglet 'Généralités' du dossier de configuration 'TCP/IP' ou dans le menu /Setup/TCP-IP-module. Cette adresse doit également être utilisée pour la connexion et le masquage.

Pour des informations complémentaires, reportez-vous au chapitre 'Masquerading IP'.

### ■ Les entrées suivantes ont une signification particulière :

- Adresse IP 255.255.255.255 avec le masque de réseau 0.0.0.0 : il s'agit de la route par défaut. Tous les paquets ne pouvant pas être acheminés sur la base des autres entrées de routage sont transmises au correspondant indiqué ici.
- Masque de réseau 255.255.255.255 : les entrées ayant un masque de réseau complet identifient souvent des ordinateurs aux postes de travail isolés (accès à distance), pas un réseau. Parfois, elles identifient aussi un réseau identifié de l'extérieur par une seule adresse IP au moyen de la technique du masquerading IP.
- Nom du routeur 0.0.0.0 : Routes exclues. Les paquets destinés à ces « routes zéro » rejetées et pas transmises Ceci permet d'exclure par ex. les routes interdites dans Internet (Private Address Spaces, par ex. 10.0.0.0).

Exemples et explications :

Adresse IP	Masque de réseau	Routeur	Dist.	Voici ce qui se passe :
192.168.1.9	255.255.255.255	SERVCLIENTELE	2	Le correspondant SERVCLIENTELE peut être joint à l'adresse IP 192.168.1.9.
192.168.120.0	255.255.255.0	ROUTEUR01	2	Tous les paquets destinés aux adresses IP 192.168.120.x sont transmis à ROUTEUR01.
192.168.125.0	255.255.255.0	ROUTEUR02	3	Tous les paquets destinés aux adresses IP 192.168.125.x sont transmis à ROUTEUR02.
192.168.130.0	255.255.255.0	192.168.140.123	0	Tous les paquets destinés aux adresses IP 192.168.130.x sont transmis au routeur ayant l'adresse IP 192.168.140.123.

Adresse IP	Masque de réseau	Routeur	Dist.	Voici ce qui se passe :
10.0.0.0	255.0.0.0	0.0.0.0	0	Exclut la transmission des paquets dans les réseaux commençant par 10.
255.255.255.255	0.0.0.0	CENTRALE	2	Tous les paquets ne pouvant pas être attribués aux entrées précédentes sont transmis au correspondant CENTRALE.



*L'ordre des entrées joue un rôle tout aussi important : elles sont traitées par ordre d'apparition ! Le routeur trie les entrées dans l'ordre correct automatiquement : d'abord par masque de réseau, en commençant par le plus élevé ; ensuite par adresse IP, en commençant par la plus basse. Ainsi, l'entrée 'CENTRALE' se retrouve en fin de liste. Si cette entrée figurait en tête de liste, le routeur enverrait dans le réseau de la centrale tous (!) les paquets qui n'ont rien à faire dans le réseau local.*

## Filtrage des paquets TCP/IP

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

Or, vous aurez parfois besoin de restreindre davantage l'adressage. Vous utilisez à cet effet la propriété de TCP/IP de joindre à un paquet les numéros de port de la cible et de la source, en plus des adresses IP de l'expéditeur et du destinataire. Le port cible dans un paquet représente le service adressé dans le réseau TCP/IP. Alors que les ports cibles pour divers services dans le réseau TCP/IP sont définis de façon fixe (voir aussi 'Ports TCP/IP' dans le Manuel de référence), les ports source peuvent être sélectionnés librement dans certaines zones.

Le routeur peut consulter les ports source et cible des paquets qui utilisent le protocole TCP ou UDP. Il peut déduire de ces ports à quoi servent les données. Il détectera donc par ex. des accès FTP ou des sessions Telnet. Les tableaux de filtres adéquats permettent ensuite de déterminer quelles données ne doivent pas être transmises au correspondant. De même, il est naturellement possible de bloquer les données envoyées à certains ports du réseau local. A côté de la définition des ports et des protocoles correspondants, le type de filtre dans les tableaux de filtrage sert à indiquer si les paquets concernés ne doivent jamais être transmis, ou s'ils doivent simplement ne pas déclencher l'établissement d'une connexion (en d'autres termes : s'ils doivent être transmis uniquement si une connexion est déjà active).

Le routeur IP contient deux tableaux de filtrage distincts pour les paquets en provenance du réseau local et pour les paquets en provenance du réseau distant. Vous trouverez ces tableaux de filtres en sélectionnant l'onglet 'Filtre' du dossier de configuration 'TCP/IP'

d'ELSA LANconfig, ou dans le menu

/Setup/IP-router-table/WAN-filter-table or LAN-filter-table

## Proxy-ARP

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



*Pour utiliser cette fonction, l'option 'Intégrer les stations distantes avec Proxy-ARP' doit être active (dans LANconfig, dans zone de configuration 'TCP/IP', onglet 'Routeur', ou dans le menu /Setup/IP-router-module pour les autres possibilités de configuration).*

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

Adresse IP	Masque de réseau	Routeur	Distance	IP-Masquerading
192.168.110.123	255.255.255.255	Télétravailleur01	0	Inactif

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

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

## Routage local

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

inconnues pour l'ordinateur au poste de travail. Or, ce routeur par défaut est lui-même parfois incapable d'atteindre le réseau de destination, mais il connaît un autre routeur qui trouve le chemin.

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

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

Certains ordinateurs sont malheureusement incapables de gérer les redirections ICMP. Pour que les paquets de données puissent malgré tout être acheminés, utilisez le routage local (sur l'onglet 'Routeur' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou dans le menu `/Setup/IP-router-module/Local-routing`). Vous indiquez ainsi au routeur d'envoyer lui-même le paquet à l'autre routeur. En outre, le routeur n'émet plus de redirection ICMP.

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

## **Routage dynamique avec IP-RIP**

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

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

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

- Routes rejetées dans le cas de la configuration avec '0.0.0.0'.
- Routes qui renvoient à d'autres routeurs dans le réseau local.
- Routes qui relient les ordinateurs isolés au réseau local avec Proxy-ARP.

Les entrées du tableau de routage statique sont certes créées manuellement, mais ces informations peuvent malgré tout changer suivant la situation des connexions du routeur, et par conséquent les paquets RIP envoyés changent aussi.

- Tant que le routeur maintient une connexion avec un correspondant, il indique aux autres routeurs dans le réseau local que tous les réseaux accessibles par cette route ont la distance '1'. Ainsi, ces routeurs sont informés qu'ils peuvent profiter de la connexion entre ce routeur et le correspondant pour transmettre leurs données par le même canal. Les tentatives de connexion supplémentaires du routeur peuvent alors être évitées, et par conséquent les coûts de communication peuvent être réduits.
- En outre, quand ce routeur ne peut pas établir de connexion supplémentaire vers un correspondant différent, il signale que toutes les autres routes ont la distance '16'. '16' signifie que « cette route ne peut pas être empruntée actuellement ». Le fait qu'un routeur ne puisse pas établir de connexion supplémentaire à côté de la connexion en cours peut avoir les causes suivantes :
  - Une autre connexion a déjà été établie dans tous les autres canaux (également via *LANCAPI* ou les ports A/N).
  - La connexion en cours utilise tous les canaux B (regroupement des canaux).



*Pour utiliser cette fonction, l'option 'Routeur IP activé' doit être cochée (dans ELSA LANconfig, dans l'onglet 'Routeur' du dossier de configuration 'TCP/IP', ou dans le menu Setup/IP Router-module pour les autres possibilités de configuration).*

*Les routeurs RIP envoient les paquets RIP environ toutes les 30 secondes. Le routeur ne peut envoyer et recevoir des RIP que s'il a une adresse IP unique. Dans la configuration par défaut avec l'adresse IP XXX.XXX.XXX.254, le module IP-RIP est inactif.*

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

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

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

### Signification de ces entrées

L'adresse IP et le masque de réseau identifient le réseau de destination, la distance est extraite des informations RIP, la dernière colonne indique quel routeur a communiqué cette route. La colonne 'Durée' indique l'âge de la route. La valeur figurant dans cette colonne vaut comme multiplicateur de l'intervalle d'arrivée des paquets RIP, c'est-à-dire que '1' signifie env. 30 secondes, '5' environ 2,5 minutes etc. Quand une information arrive par une route donnée, cette route est considérée comme accessible directement et est affectée de la durée '1'. Au bout de la durée correspondante, la valeur dans cette

colonne est mise à jour automatiquement. Au bout de 3,5 minutes, la distance passe à '16' (route inaccessible), et au bout de 5,5 minutes la route est supprimée.

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

- La route n'existe pas dans le tableau, et dans ce cas elle est ajoutée (s'il y a de la place).
- La route figure dans le tableau avec une durée '5' ou '6'. La nouvelle route est insérée dans le tableau si la valeur de la distance est inférieure ou égale à l'ancienne.
- La route figure dans le tableau avec une durée de '7' à '10', donc avec la distance '16'. La nouvelle route est insérée dans le tableau dans tous les cas.
- La route figure dans le tableau. Une nouvelle route vient du même routeur qui avait déjà communiqué la première route, mais celle-ci a une distance plus avantageuse que la nouvelle route. Lorsqu'un routeur communique ainsi la détérioration de sa propre tableau de routage statique (la distance passe par ex. de '1' à '2' après la coupure de la connexion), le routeur lui croit et ajoute la mauvaise entrée dans son tableau de routage dynamique.



*Les paquets RIP du réseau étendu ne sont pas pris en compte et sont rejetés immédiatement ! Les paquets RIP du réseau local sont analysés et ne sont pas retransmis dans le réseau local !*

### **Synergie : tableaux statiques et tableaux dynamiques**

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

### **Routeurs sans prise en charge de IP-RIP**

On retrouve parfois dans les réseaux locaux des routeurs qui ne prennent pas en charge le protocole RIP. Ces routeurs ne peuvent pas détecter les paquets RIP et les traitent comme des paquets diffusés normaux ou des paquets à diffusion restreinte. Si la route standard pour ce routeur passe par un routeur distant, les paquets RIP déclenchent continuellement l'établissement d'une connexion. Pour éviter cela, on peut entrer le port RIP dans les tableaux de filtrage.

### **Mise à l'échelle avec IP-RIP**

Lorsque vous utilisez plusieurs routeurs dans un réseau local avec IP-RIP, vous pouvez présenter ces routeurs au monde extérieur comme un seul grand routeur. Cette procédure est appelée mise à l'échelle (scaling). En raison des échanges importants de données

entre les routeurs, on dispose d'un routeur connaissant en principe un nombre infini de routes.

## Masquerading IP (NAT, PAT)

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

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

### Deux adresses pour le routeur

Pour le masquerading, le routeur doit remplir deux conditions opposées : d'une part il doit avoir une adresse IP valable dans le réseau local pour qu'il puisse être joint à partir de ce réseau, d'autre part il doit également avoir une adresse valable dans Internet. Comme ces deux adresses ne doivent pas se trouver dans un réseau logique, il n'y a qu'une solution : il faut lui attribuer deux adresses IP. Le routeur aura alors une adresse **Internet** et une adresse **Intranet**, naturellement chacune avec un masque de réseau correspondant. L'option 'Masquerading' dans le tableau de routage permet d'indiquer au routeur laquelle des deux adresses il doit utiliser pour la transmission des paquets. Si dans ce cas une adresse donnée est demandée auprès du FAI, il y a deux possibilités d'attribuer l'adresse réelle :

- Le fournisseur d'accès attribue au routeur l'adresse souhaitée. Le masque de réseau détermine combien d'ordinateurs peuvent être masqués derrière le routeur.
  - Adresse IP avec masque de réseau complet 255.255.255.255 : il s'agit de votre propre adresse, la seule à être enregistrée par le NIC. Aucun autre ordinateur dans le réseau n'a d'adresse valable dans Internet, et ils sont masqués derrière l'adresse fixe des routeurs.
  - Adresse IP avec un masque de réseau incomplet, par ex. 255.255.255.248 : vous avez plusieurs adresses IP enregistrées, et vous en attribuez une au routeur. Les autres adresses IP sont attribuées de façon fixe à des périphériques dans Intranet, ces périphériques pouvant alors accéder à Internet sans masquage. Les autres périphériques peuvent accéder à Internet par des connexions masquées.
- Le fournisseur d'accès attribue au routeur une autre adresse. Dans ce cas, **tous** les ordinateurs du réseau local sont masqués derrière cette adresse.

### Comment fonctionne le masquerading IP ?

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

La réponse à ce paquet est envoyée à l'adresse IP du routeur avec le nouveau numéro de port de l'expéditeur. Le routeur peut ensuite associer cette réponse à l'expéditeur initial sur la base de l'entrée dans le tableau interne et la lui envoyer.



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

### Masquage simple et masquage inverse

Le masquage fonctionne dans les deux sens. Quand un ordinateur du réseau local envoie un paquet dans Internet, le réseau local est masqué derrière l'adresse IP du routeur (masquage simple).

A l'inverse, lorsqu'un ordinateur envoie un paquet par ex. à un serveur FTP relié à Intranet, il croit que le serveur FTP est le routeur. Le routeur connaît l'adresse Intranet du serveur sur la base de l'entrée dans le tableau de service (dans l'onglet 'Masq.' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou dans le menu *Setup/IP-router-module/Masquerading/Service-table*). Le paquet est retransmis à ce serveur. Ensuite, toutes les réponses émises par le serveur FTP sont masquées derrière l'adresse IP du routeur.

La petite différence :

- L'accès à un service de Intranet (port) depuis l'extérieur doit être défini au préalable par un numéro de port. A cet effet, le port cible est indiqué dans un tableau des services par l'adresse Intranet par ex. du serveur FTP.
- Pour les accès de Intranet à Internet en revanche, le routeur définit lui-même l'adresse IP et le port dans le tableau des services.

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

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

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

Evidemment uniquement ceux qui communiquent via les ports. Les protocoles ne recourant pas aux numéros de port ou qui utilisent les ports à un niveau supérieur à IP



dans le modèle de référence OSI ne peuvent pas être masqués sans appliquer de procédure particulière.

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

- FTP
- TCP
- UDP
- ICMP

## Routage par DNS

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

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

Lorsqu'un ordinateur implanté dans Intranet veut accéder à une page d'accueil, il émet d'abord une requête DNS : « Quelle adresse IP appartient à www.domaine.com ? ». Si le routeur est enregistré en tant que serveur DNS sur les ordinateurs aux postes de travail, cette question est traitée de la façon suivante :

- Le routeur recherche d'abord dans sa propre configuration si un serveur DNS a été défini (dans l'onglet 'Adresses' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou dans le menu /Setup/TCP-IP-module). S'il trouve cette indication, il établit une connexion avec ce serveur et récupère l'information souhaitée.
- Lorsqu'aucun serveur DNS n'est déclaré au routeur, le routeur essaie d'accéder à un serveur DNS via une connexion PPP éventuellement en cours (par ex. avec le fournisseur d'accès), et tire la combinaison adresse IP/nom de ce serveur. Naturellement, cela fonctionne uniquement si l'adresse d'un serveur DNS a été transmise au routeur pendant la négociation PPP.
- Si une connexion n'est pas en cours, le routeur établit une connexion via la route par défaut et recherche le serveur DNS de ce côté.

Avec cette procédure, vous n'avez aucun besoin de connaître les adresses d'un serveur DNS. Il suffit de configurer les ordinateurs aux postes de travail avec l'adresse Intranet de votre routeur en guise de serveur DNS pour permettre l'utilisation des noms à la place des adresses IP. En outre, l'adresse du serveur DNS est aussi mise à jour automatiquement. Par ex., au cas où le fournisseur d'accès modifie le nom de son serveur DNS, ou si vous changez de fournisseur, le routeur obtient toujours l'information à jour.

## Policy Based Routing : routage stratégique

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



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

## Gestion d'adresses automatique via DHCP

Pour une exploitation sans accrocs dans un réseau TCP/IP, tous les périphériques d'un réseau local requièrent des adresses IP bien définies. De plus, ils ont besoin des adresses des serveurs DNS et NBNS ainsi que d'une passerelle par défaut, qui permet de router les paquets de données des adresses inaccessibles localement. Dans le cas d'un petit réseau, il est tout à fait concevable de saisir ces adresses « manuellement » pour tous les ordinateurs présents dans le réseau. Dans le cas d'un réseau important comportant plusieurs ordinateurs aux postes de travail, ceci devient rapidement un travail fastidieux.

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

### Le routeur en tant que serveur DHCP

Le routeur peut gérer les adresses 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 Intranet.

En mode DHCP Auto (DHCP-Automode), un routeur ELSA 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 routeur en état de la livraison à un réseau sans autres serveurs DHCP et à l'activer. Le routeur règle alors en combinaison avec *ELSA LANconfig* via l'assistant toutes les allocations d'adresses supplémentaires dans le réseau local par lui-même.

## DHCP – 'Actif', 'Inactif' ou 'Auto' ?

Le serveur DHCP dans les routeurs ELSA 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 routeur 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 routeur une fois activé recherche d'autres serveurs DHCP dans le réseau local (identifiables à un bref clignotement du témoin lumineux Tx après activation).
  - 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 routeur 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 est finalement connecté ou déconnecté.

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

## Attribution des adresses

### Attribution d'adresses IP

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

- L'adresse IP attribuée 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'. 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'affectation des adresses IP dans le réseau. Dans cet état, le serveur DHCP attribue aux autres ordinateurs dans le réseau uniquement l'adresse IP et sa validité, mais pas les autres informations.

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

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

### **Allocation du masque de réseau**

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



*Il est recommandé que seuls des spécialistes de réseau expérimentés procèdent 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 routeur affecte toujours sa propre adresse IP comme adresse de passerelle à l'ordinateur requérant.

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

### Durée de validité d'une affectation

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

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

- Période de validité maximale en minutes

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

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

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

- Période de validité par défaut en minutes

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

### Priorité pour le serveur DHCP – Demande d'attribution

De manière standard, la presque totalité des paramètres dans le voisinage réseau de Windows sont définis de manière à ce 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 – Ecraser l'attribution**

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

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

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

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

Dans le module DHCP du routeur, 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/Tableau-DHCP'. Ce tableau indique l'adresse IP attribuée, l'adresse MAC, la période de validité, le nom de l'ordinateur au poste de travail (s'il y en a un), ainsi que le type d'allocation d'adresse.

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

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

## Configuration des routeurs en tant que serveur DHCP

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

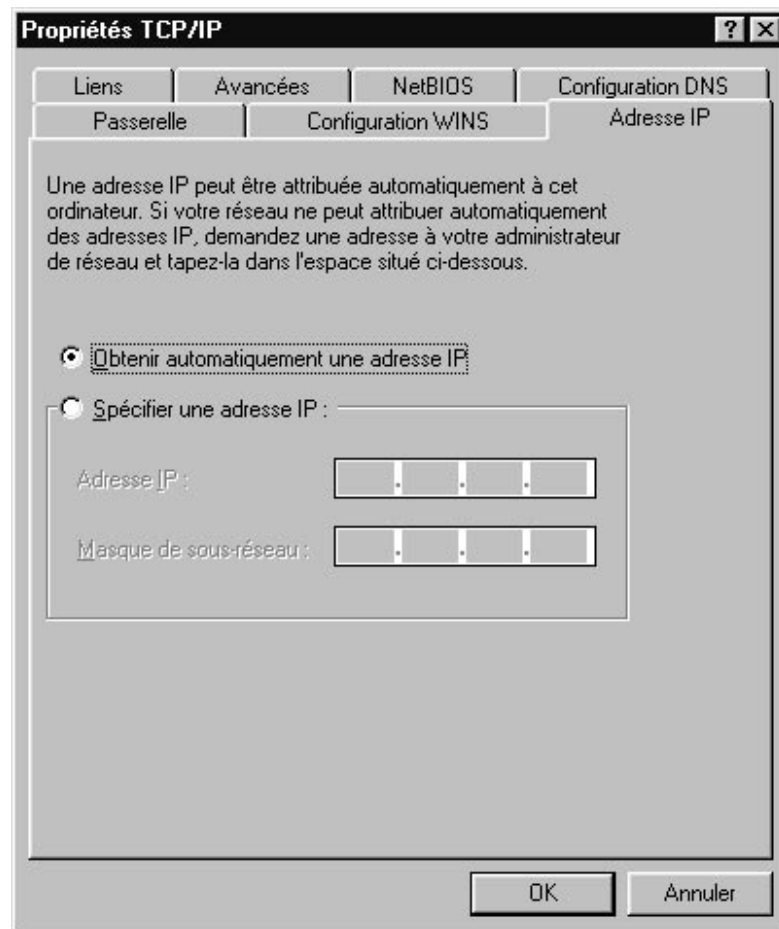
- Jusqu'à maintenant, vous n'aviez pas installé de réseau ou bien votre réseau local n'utilise pas TCP/IP. Grâce au serveur DHCP dans le routeur, vous pouvez d'un coup attribuer des adresses IP à tous les ordinateurs du réseau et au routeur lui-même.
- Vous avez déjà utilisé un réseau avec TCP/IP, mais 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 à votre réseau local à l'aide du câble de réseau. Lorsque vous connectez le périphérique sur un concentrateur, le commutateur node/hub doit se trouver sur 'Node'. En revanche, si vous connectez directement le routeur sur la carte réseau d'un ordinateur du réseau, le commutateur node/hub doit se trouver en position 'Hub'.
- ② Mettez le routeur sous tension. Le routeur ne trouve pour commencer aucun autre serveur DHCP sur le réseau et active ses propres fonctions DHCP.
- ③ Si rien ne se produit, installez le protocole 'TCP/IP' sur tous les ordinateurs du réseau local.
  - Lors de l'installation du protocole, les ordinateurs 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'.  
Dans l'adresse 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 routeur.



*Vous apprendrez dans 'Workshop' comment installer un protocole réseau par ex. sous Windows 95 ou Windows NT. Dans le Guide d'installation, vous trouverez des indications concernant l'installation d'ELSA LANconfig.*

- ④ Installez *ELSA LANconfig* sur l'un des ordinateurs du réseau.
- ⑤ Démarrez *ELSA LANconfig* dans le groupe de programmes 'ELSAlan'. Au démarrage, *ELSA LANconfig* remarque qu'il y a un routeur non configuré sur le réseau et démarre l'assistant de paramétrage par défaut.
  - Si vous n'avez encore utilisé aucune adresse IP sur votre réseau, sélectionnez dans cet assistant l'option 'Effectuer tous les réglages automatiquement' puis confirmez dans la fenêtre suivante avec le bouton **Exécuter**.  
L'assistant attribue alors au routeur l'adresse IP '10.0.0.1' avec le masque de réseau '255.255.255.0' et met le serveur DHCP en marche. A partir de l'adresse IP, le périphérique détermine le pool d'adresses pour l'allocation du DHCP.
  - Si, avant de passer sur le DHCP, vous aviez déjà utilisé des adresses IP sur votre réseau, sélectionnez dans cet assistant l'option 'Je veux effectuer les réglages moi-même'. Indiquez dans la fenêtre suivante une adresse IP libre provenant de



la tranche d'adresses utilisée auparavant et mettez le serveur DHCP en marche. L'assistant attribue au routeur l'adresse IP définie avec le masque de réseau correspondant. A partir de l'adresse IP, le périphérique détermine le pool d'adresses pour l'allocation du DHCP.

- Au bout de quelques secondes, tous les ordinateurs sur réseau font l'objet d'un contrôle et se voient attribuer une nouvelle adresse IP du serveur DHCP le cas échéant. De plus, les ordinateurs reçoivent les autres paramètres tels qu'une adresse de forme de messages diffusés, un serveur DNS, une passerelle par défaut etc.

### Configuration manuelle

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

## 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.

### 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 Business* :

- Un routeur *ELSA LANCOM Business* 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 Business* 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 leur nom et leur adresse.
- Le serveur DNS dans le routeur *ELSA LANCOM Business* 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.

## 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
```

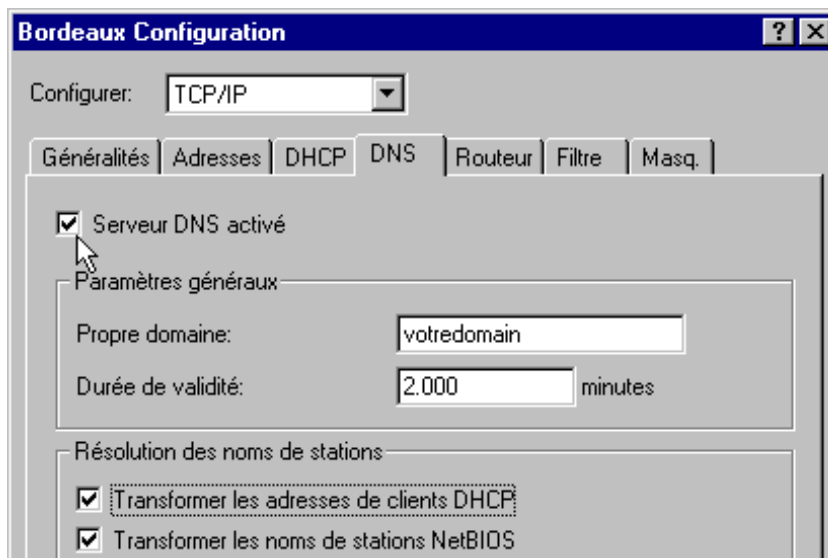
- ② Entrez le domaine auquel appartient le serveur DNS. C'est sur la base de ce domaine que le serveur DNS reconnaît si le nom recherché dans une requête fait partie du réseau local ou non. L'indication du domaine est facultative.

```
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
```

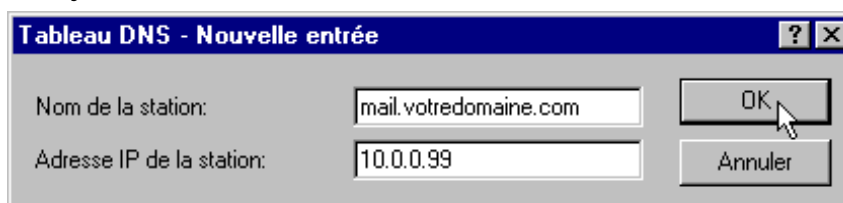
```
set setup/DNS-module/NetBIOS-usage yes
```



- 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 DE, entrez :

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



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

Choisissant 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.

## Proxy NetBIOS

Avec sa fonction de proxy NetBIOS, un *ELSA LANCOM Business* 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.

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

## En quelques mots : définition de NetBIOS

NetBIOS sert à interconnecter 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 Business* 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.

## Traitement des paquets NetBIOS

Le comportement extrêmement loquace des ordinateurs Windows peut entraîner des coûts de communication très élevés dans le cas de connexions via le RNIS, puisque chaque paquet NetBIOS contenant les informations sur le nom conduit automatiquement à l'établissement d'une connexion (par ex. avec le FAI). 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 Business* 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 (du moment qu'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 DEFAUT dans Internet, le filtre IP préconfiguré pour les ports NetBIOS intercepte ces paquets et empêche l'établissement de la connexion.

## 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 Business !*

Le routage des paquets NetBIOS dans *ELSA LANCOM Business* 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 le constructeur Microsoft 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

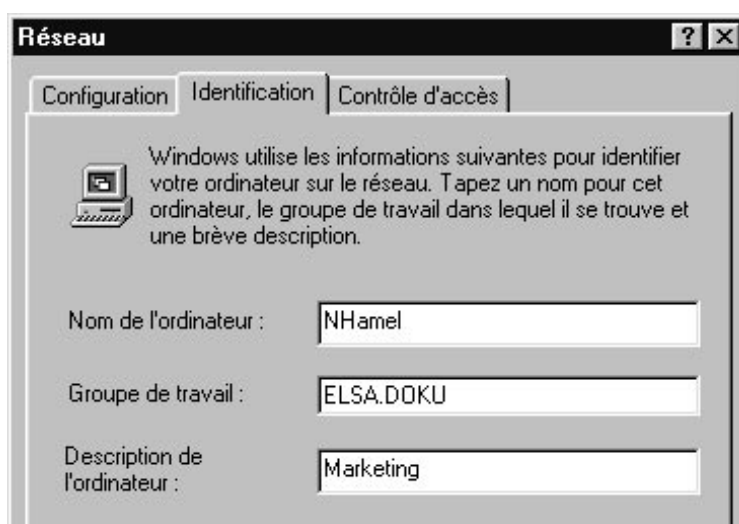
Le partage de fichiers et d'imprimantes permet à d'autres utilisateurs d'utiliser les lecteurs et les imprimantes du réseau Microsoft.

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'.

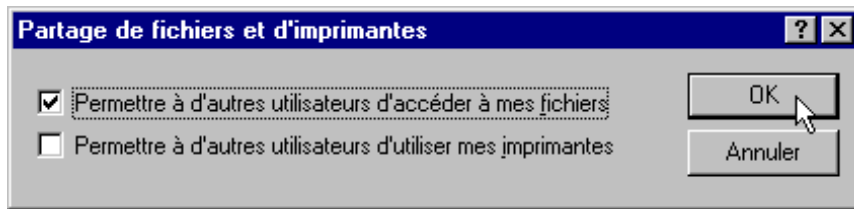


Le nom de l'ordinateur doit être unique. Ceci est valable pour tous les réseaux Windows et tous les groupes de ces réseaux devant être interconnectés via NetBIOS. Par conséquent, le même nom ne doit pas exister plusieurs fois dans des réseaux différents.

#### ■ Partage de fichiers et d'imprimantes

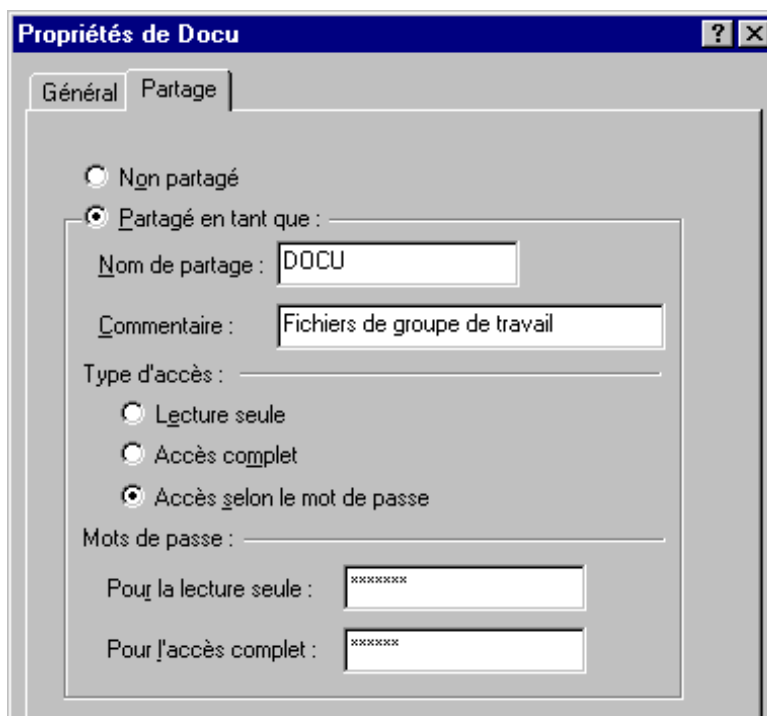
Après l'installation, vérifiez si le partage de fichiers et d'imprimantes est actif. Cliquez à cet effet sur **Démarrer ► Paramètres ► Panneau de configuration ► Réseau ► Partage de fichiers et d'imprimantes**. Sélectionnez si les autres utilisateurs dans le réseau Windows peuvent accéder à l'imprimante 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.



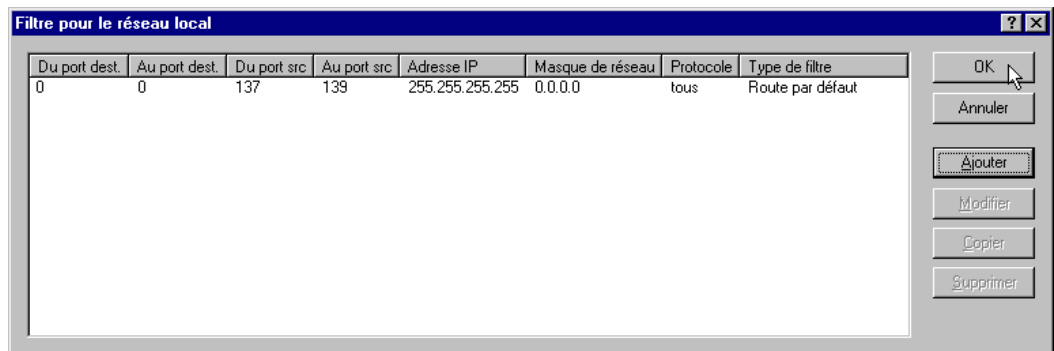
*Vous pouvez vérifier facilement si les paramètres dans le réseau Windows sont corrects : le nom de votre propre ordinateur doit être affiché dans le voisinage réseau.*

## Interconnecter deux réseaux Windows via le RNIS

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



- ① Configurez les deux réseaux pour l'interconnexion entre deux réseaux locaux via TCP/IP, comme décrit dans 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.



- ③ Saisissez ensuite le correspondant pour le routage via NetBIOS. Sélectionnez le dossier de configuration 'NetBIOS' d'*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-module/Remote-table
set nhamel.mobil router
```

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



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

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

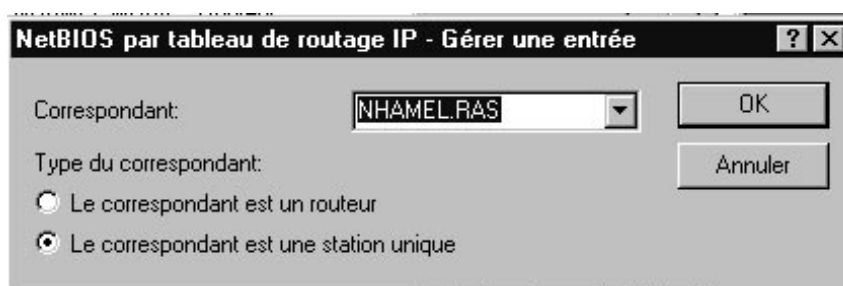
```
cd /Setup/NetBIOS-module
set operating on
```

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.

## 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 Business* 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 Business* (voir 'Interconnecter deux réseaux Windows via le RNIS').
- ② Si les adresses IP du correspondant distant sont attribuées à partir du pool IP, une route supplémentaire doit être créée dans le tableau de routage IP pour ce correspondant.
- ③ Créez une entrée pour les correspondants distants également dans le tableau de routage IP NetBIOS.



```
cd /Setup/NetBIOS-module/Remote-table
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 a été activé.*

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

## 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 après l'interconnexion de réseaux locaux

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

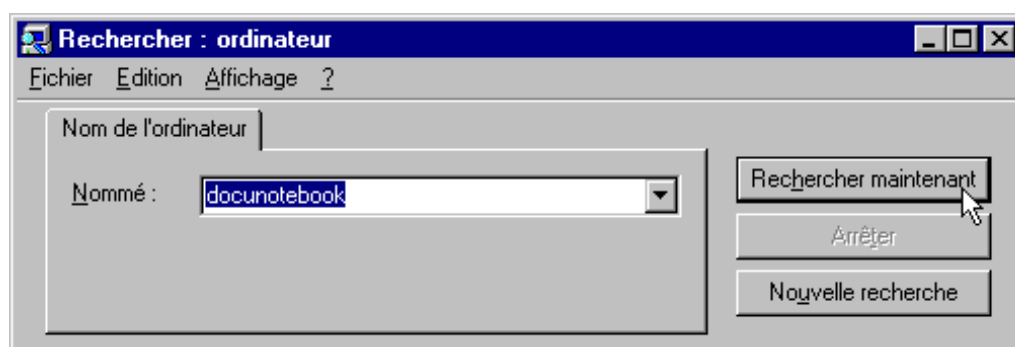
```
dir /Setup/NetBIOS-module/Host-list
```

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	10.10.0.53	NHAMEL.MOBIL	4939	0020
ELSA	1d	10.10.0.53	NHAMEL.MOBIL	4939	0020
ELSA.DOCU	1d	10.1.253.246	4935	0000	
ELSA.DOCU	1d	192.168.100.162	4997	0000	
NHAMEL.MOBIL	00	10.10.0.1	NHAMEL.MOBIL	0	0020

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 Business* 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.

## Pooling IP pour les accès commutés

Lorsque plusieurs canaux B sont disponibles, *ELSA LANCOM Business* est idéal pour fonctionner comme nœud d'accès (serveur d'accès distant, serveur RAS) dans les petites et les moyennes entreprises. Pour éviter de devoir créer une route particulière pour chaque accès commuté, le routeur dispose d'un pool d'adresses IP dans lequel il puise pour attribuer au correspondant une adresse IP valable pour le réseau local pendant la durée de la connexion.

Vous trouverez les paramètres de configuration du pool d'adresses IP sur l'onglet 'Adresses' du dossier de configuration 'TCP/IP' de *ELSA LANconfig*, ou pour les sessions Telnet ou de terminal sous `/Setup/IP-router-module`.

## Bureautique et *ELSA LANCAPI*

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

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

### *ELSA LANCAPI*

#### Avantages de *LANCAPI*

La mise en œuvre de l'interface *LANCAPI* apporte des avantages surtout économiques. Tous les ordinateurs aux postes de travail reliés au réseau local ont, via *LANCAPI*, libre accès aux fonctions de bureautique telles que le 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 RNIS est simulé sur l'ordinateur au poste de travail. Avec l'interface *LANCAPi*, le PC envoie la télécopie à un *ELSA LANCOM Business* via le réseau, et c'est ensuite le routeur qui établit la liaison avec le destinataire via RNIS.

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



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

### Installation du client *LANCAPi*

L'interface *LANCAPi* est formée par deux composants, un serveur (dans le *ELSA LANCOM Business*) 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.

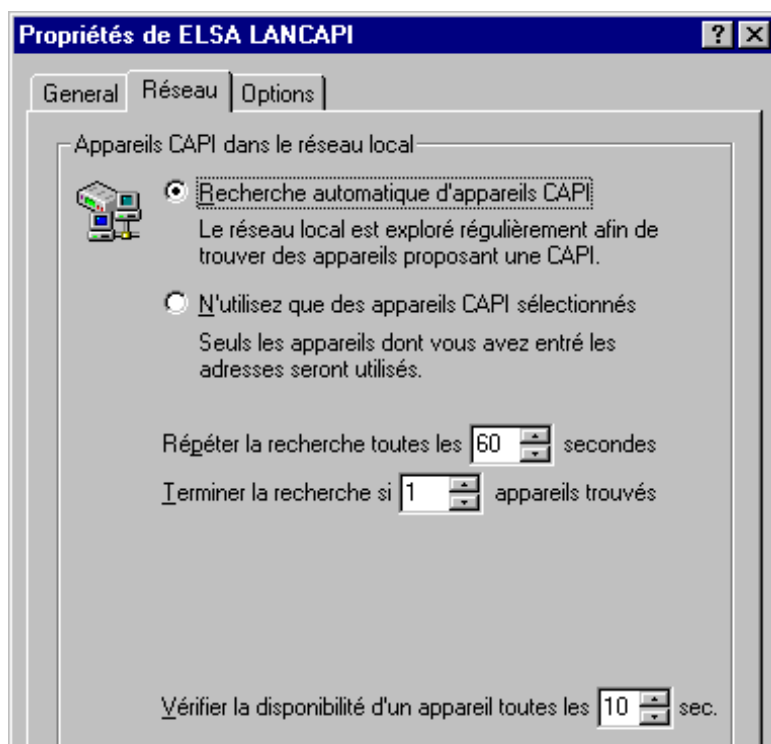
Après un redémarrage de l'ordinateur, l'interface *LANCAPi* est prête à remplir les tâches que lui envoient les logiciels de communication. Après l'installation, l'icône *ELSA LANCAPi* apparaît dans la barre des tâches. Double-cliquez sur cette icône pour ouvrir une fenêtre dans laquelle vous pouvez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



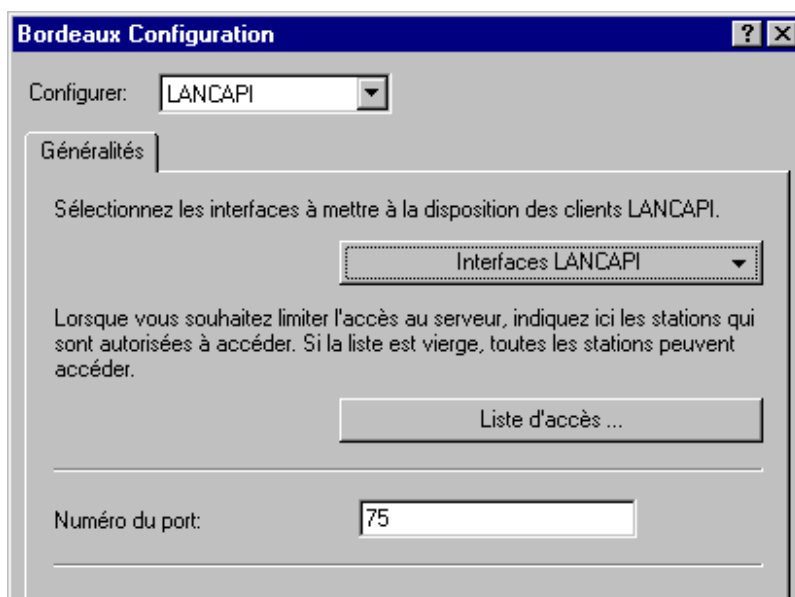
### Configuration du serveur LANCAPI

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 'ELSAIlan'. Ouvrez la configuration du routeur en double-cliquant sur le nom souhaité dans la liste, et sélectionnez la zone de configuration 'LANCAPI'.



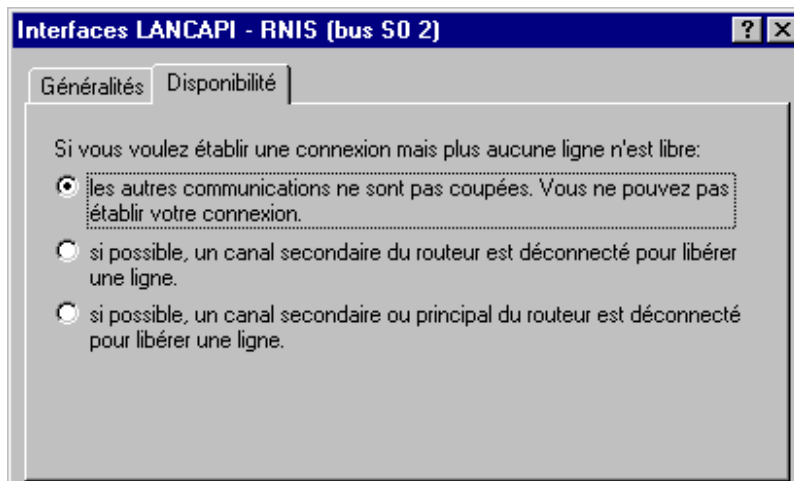
- ② Activez le serveur *LANCAPI*, ou autorisez uniquement les appels sortants. Dans le deuxième cas, l'interface *LANCAPI* ne réagit pas aux appels entrants et ne peut pas être mis en œuvre par ex. pour la réception de télécopies. Par ex., autorisez uniquement les appels sortants lorsque vous avez déjà 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 un *ELSA LANCOM Business* 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 *LANCAP*. Un logiciel de télécopie qui utilise *LANCAP* fera vraisemblablement une deuxième tentative d'envoi ultérieurement.
- La connexion via *LANCAP* peut être établie lorsqu'un canal principal est libre. Un canal principal est le premier canal B utilisé pour une liaison établie par le routeur. Les canaux secondaires sont ceux qui s'ajoutent au canal principal pour un regroupement de canaux.
- Une connexion via *LANCAP* peut toujours être établie, une connexion du routeur sera coupée pour la durée de la communication. Ainsi, la fonction télécopie est toujours accessible.

### Utilisation de *LANCAP*

Vous avez deux possibilités d'utiliser *LANCAP* :

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

## ***ELSA CAPI Faxmodem***

Avec *ELSA CAPI Faxmodem*, vous disposez sous Windows d'un pilote de télécopieur (fax class 1) qui, en tant qu'interface entre *ELSA LANCAP* et l'application, permet d'utiliser



des programmes de télécopie standard en liaison avec un routeur *ELSA LANCOM Business*.

## 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**.

## 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 avec 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.*

## Le routeur 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 d'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 (Présélection). En général, pour router un appel via un opérateur alternatif, on compose d'abord le préfixe de cet opérateur pour accéder à son réseau, et on ne compose le numéro de téléphone du correspondant appelé qu'après ce préfixe.

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

(peu importe qu'il soit effectué par le routeur, l'interface *LANCAPI*, etc.) par l'opérateur le moins cher.

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

Le rerouteur téléphonique (Least Cost Router, LCR) analyse les numéros composés par ex. par le routeur ou l'interface *LANCAPI*.

Après chaque chiffre composé, le routeur vérifie s'il existe dans le tableau de reroutage une entrée (préfixe) correspondante aux premiers chiffres composés. Si une telle entrée existe, et si elle est valable pour l'heure et la date actuelle, le préfixe de l'opérateur privé est ajouté devant le numéro (avant l'indicatif) du correspondant. Ce n'est que lorsque le numéro du correspondant a été complété de cette façon qu'il est envoyé à l'auto-commutateur 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 transporteur 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. Vous vous êtes renseigné chez plusieurs opérateurs privés proposant le reroutage direct et vous avez noté les tarifs les plus avantageux. Les premières entrées dans le tableau de routage ont alors 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
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. 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 Business*. Vous devrez faire preuve d'une certaine méthodologie :
- Vous pouvez saisir directement les préfixes uniques qui ne risquent pas d'être confondus :
  - '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 routage. Songez aussi à tous les numéros spéciaux tels que le numéro vert commençant par '0800'.
- Une stratégie perfectionniste est de gérer tous les reroutages. On commence dans ce cas par les préfixes des zones les plus 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 (par ex. le '8' pour le réseau de France Télécom). Une entrée vierge signifie également « pas de reroutage ».
- Eventuellement, 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.
- Etudiez les diverses zones tarifaires. Adressez-vous par ex. aux opérateurs ou découvrez-les dans Internet.

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. Il s'agit de déterminer : les tarifs par jour, heure, zone, réseau filaire

ou mobile. 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 Business* doivent utiliser ses services de reroutage ?
- Quels appels doivent être routés quand et via quel opérateur ?

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

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



*Si vous avez activé le Least Cost Routing également pour les modules de routage, des connexions seront éventuellement établies via des routeurs 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).



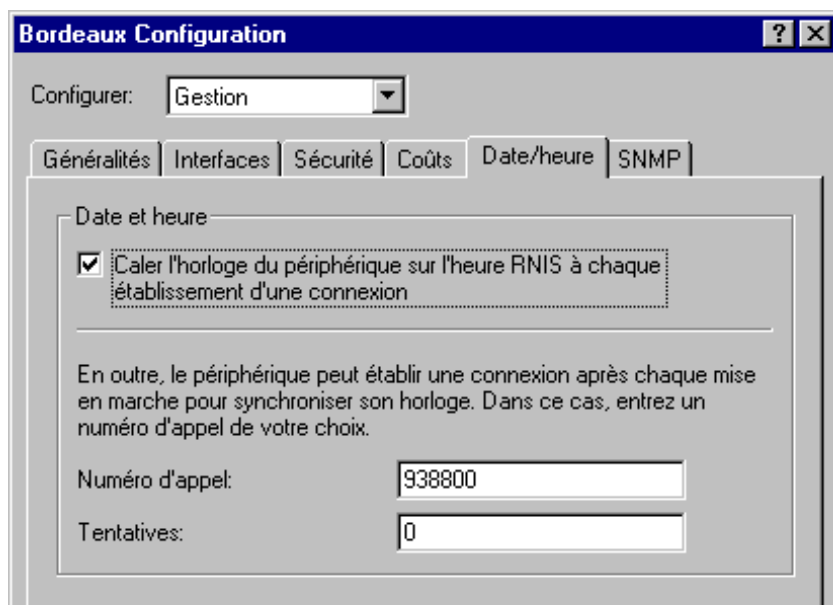
*Elargissez votre tableau de routage étape par étape, et vérifiez le résultat de chaque entrée. A cet effet, exécutez par ex. ELSA LANmonitor et établissez – via ELSA LANCAPI – les connexions avec les correspondants dans le tableau de reroutage. Vous pourrez consulter à l'aide du numéro composé si l'entrée 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 Business* 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).



**Bordeaux Configuration** [?] [X]

Configurer: Gestion

Généralités | Interfaces | Sécurité | Coûts | **Date/heure** | SNMP

Date et heure

☒ Caler l'horloge du périphérique sur l'heure RNIS à chaque établissement d'une connexion

En outre, le périphérique peut établir une connexion après chaque mise en marche pour synchroniser son horloge. Dans ce cas, entrez un numéro d'appel de votre choix.

Numéro d'appel:

Tentatives:



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

# Workshop

Les exemples présentés dans les paragraphes suivants ont pour but de vous montrer comment tirer profit au maximum de votre routeur.

Pour toutes les configurations, nous entendons un périphérique tel qu'il est livré. Si vous voulez suivre un exemple complet, réinitialisez votre routeur le cas échéant avec la configuration au départ usine.

Ce paragraphe a pour objet de vous familiariser avec les signes et les pictogrammes utilisés.

Notre équipe de développement a pour préoccupation constante d'incorporer de nouvelles caractéristiques au logiciel et de concevoir la commande à l'aide d'*ELSA LANconfig* de manière encore plus conviviale. C'est la raison pour laquelle les captures d'écran présentées dans ce chapitre peuvent varier légèrement par rapport à l'affichage de votre logiciel actuel, ce qui n'enlève cependant rien à la fonctionnalité des menus.

Les paramétrages par défaut comme par ex. l'indication des propres numéros d'appel reviennent dans tous les exemples pour faire de chaque paragraphe individuel une description complète. C'est pourquoi des paramétrages qui ne sont pas nécessairement requis pour la fonction de base sont également décrits.





## Configuration avec *ELSA LANconfig* et les assistants

Dans les paragraphes mis en évidence par ce pictogramme, nous vous montrons comment procéder très rapidement et confortablement aux configurations sous les systèmes d'exploitation Windows à l'aide d'*ELSA LANconfig* et de ses assistants.



## Configuration sans assistants

Dans les instructions détaillées, vous trouverez des conseils précis sur les menus dans lesquels les paramétrages doivent être effectués soit à l'aide d'*ELSA LANconfig* ou d'une connexion par terminal ou Telnet.




	Setup/WAN-module	
	Interface	S0 DSS1 0 123456 123456

Vous pouvez entrer directement les valeurs affichées dans une session de configuration par ex. :

```
cd setup/WAN-module/Interface-list
set S0 DSS1 123456 123456
```

Vous trouverez d'autres remarques portant sur la configuration avec Telnet ou les émulateur de terminal dans le chapitre « Possibilités de configuration ».

Dans les instructions détaillées, vous rencontrerez les pictogrammes suivants :

	Menu	Affiche un sous-menu
	Value	Affiche une valeur pouvant être modifiée
	Table	Affiche un tableau dont les entrées peuvent être modifiées.

## Quel périphérique utilisez-vous ?

Les tâches décrites dans le workshop peuvent être résolues avec différents modèles de la famille *ELSA LANCOM*. Les restrictions concernant certains modèles sont indiquées par des pictogrammes à côté du texte.

Toutes les descriptions sont valables pour les routeurs possédant un Bus (interface)  $S_0$ , donc avec 2 canaux B. Sur les appareils équipés de plusieurs Bus  $S_0$  (par ex. *ELSA LANCOM Business 4100*) il faut, le cas échéant, transférer les réglages sur les autres interfaces et canaux.

## Ajouts



Ce pictogramme vous montre les paramétrages optionnels qui ne sont pas obligatoirement nécessaires à la fonction simple de la configuration d'exemple. En font partie entre autres les paramétrages de filtres, les paquets de données spéciaux à l'exception de la transmission ou des mécanismes de protection qui limitent l'accès au périphérique.

## Applications Internet

Dans ce premier paragraphe portant sur les utilisations pratiques des périphériques, nous vous présentons des applications en rapport avec Internet.

Le premier exemple décrit le réseau local d'une entreprise devant être raccordé à Internet via un routeur. Tous les ordinateurs de postes de travail dans le LAN reçoivent un compte de leur fournisseur d'accès leur permettant d'accéder aux services et aux ressources d'Internet. Parallèlement, le routeur doit faire office de coupe-feu dans cette application, protéger le réseau local des accès de l'extérieur, et rendre les ordinateurs de postes de travail inaccessibles depuis Internet.

Dans le deuxième exemple, l'entreprise ne désire pas utiliser exclusivement les offres d'Internet comme participant passif mais mettre aussi à disposition activement sa propre offre d'informations. Pour ce faire, un serveur Web est installé dans le réseau local de l'entreprise qui est raccordé à l'aide d'une liaison permanente au fournisseur d'accès. Ce



serveur doit naturellement être accessible depuis l'Internet, tous les autres ordinateurs du réseau doivent être protégés derrière le coupe-feu.

## Internet pour tous les PC dans le LAN

### Motivation

Beaucoup d'entreprises désirent une connexion à Internet pour tous les ordinateurs dans le réseau local. Jusqu'ici, deux raisons s'opposaient pourtant à cela :

- L'ouverture d'un compte pour chaque ordinateur distinct chez un fournisseur d'accès Internet (FAI) ou même l'achat d'adresses IP enregistrées valables dans Internet sont dans la plupart des cas des solutions beaucoup trop chères. S'y ajoutent les dépenses pour la configuration et la maintenance des accès individuels à Internet.
- Un autre souci lors du raccordement des différents ordinateurs au WWW est l'incertitude existant quant à savoir, si l'accès au réseau de l'entreprise n'est pas trop facile depuis l'extérieur.

Le routeur résout les deux problèmes en une seule fonction : masquerading IP. En résumé, il se produit la chose suivante :

Le routeur est le seul appareil dans le LAN ayant une adresse IP valable dans Internet. Celle-ci peut être affectée par ex. de manière dynamique à l'aide de PPP lors de la sélection d'un fournisseur d'accès Internet (tels que AOL, CompuServe etc.). Les ordinateurs dans le réseau utilisent des adresses issues d'une zone protégée (par ex. adresses par tranches de 10). Grâce au masquerading IP, la totalité du réseau local est « cachée » derrière la seule adresse IP enregistrée du routeur.

Ce procédé présente plusieurs avantages :

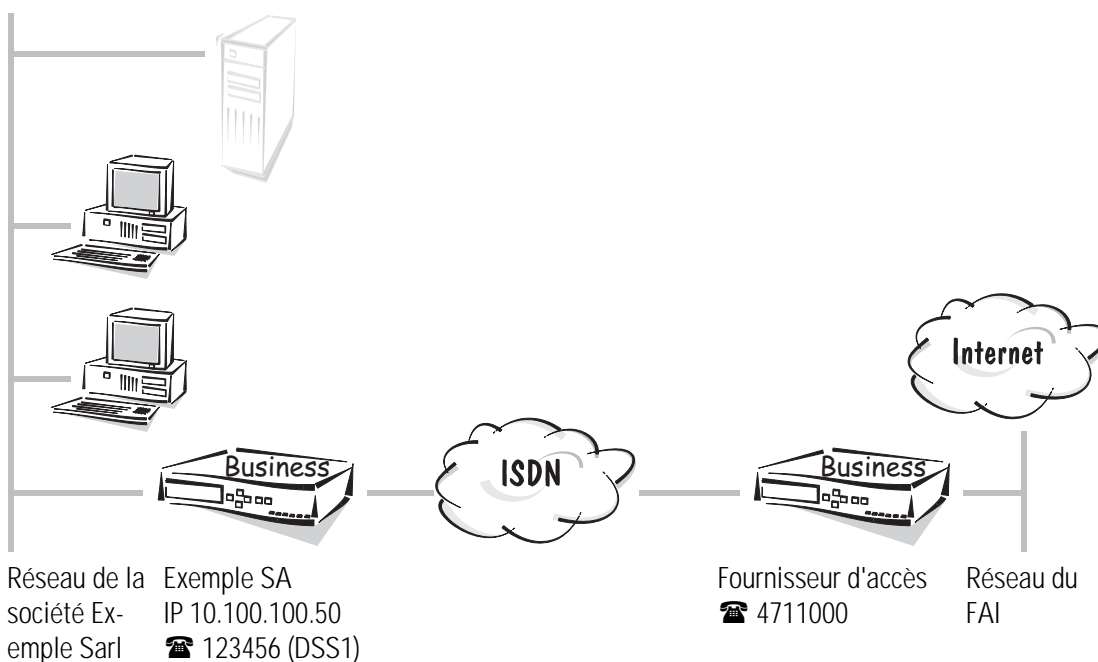
- Masquerading IP facilite l'accès à Internet.  
Seul un périphérique doit être configuré. Et là, les assistants de configuration de *ELSA LANconfig* vous aident.
- Masquerading IP rend l'accès à Internet bon marché.  
Tous les ordinateurs du réseau local peuvent utiliser l'adresse IP du routeur pour accéder à l'extérieur et donc à Internet. Là, un seul compte est nécessaire auprès du fournisseur d'accès pour beaucoup d'utilisateurs. De plus, le routeur gère lui-même la ligne RNIS et n'établit une connexion au fournisseur d'accès qu'à partir du moment où les données peuvent être réellement retransmises.
- Masquerading IP rend l'accès à Internet fiable.  
Les ordinateurs dans le réseau local ne sont pas visibles depuis l'extérieur. Seule l'adresse IP du routeur est connue dans Internet. Un accès de l'extérieur au réseau local s'avère donc impossible, masquerading IP servant de coupe-feu effectif et séparant ainsi Internet et Intranet. Par ailleurs, le routeur est la seule interface à

Internet à être plus facile à contrôler que la plupart des divers périphériques sur les postes de travail.

### Illustration à l'aide d'un exemple

D'un côté, nous avons un réseau local dans une entreprise avec quelques ordinateurs aux postes de travail et un routeur connecté à un accès Euro-ISDN. Un serveur peut exister dans ce réseau, mais ceci n'est pas nécessaire.

De l'autre côté, nous avons un réseau chez un fournisseur d'accès à Internet avec un routeur RNIS comme nœud d'accès pour les utilisateurs. Ce nœud d'accès doit être adressé avec PPP et réclame une sécurité selon 'CHAP'. Les données d'accès sont le nom de l'utilisateur 'WEB\_USER' et le mot de passe 'Surfer'.



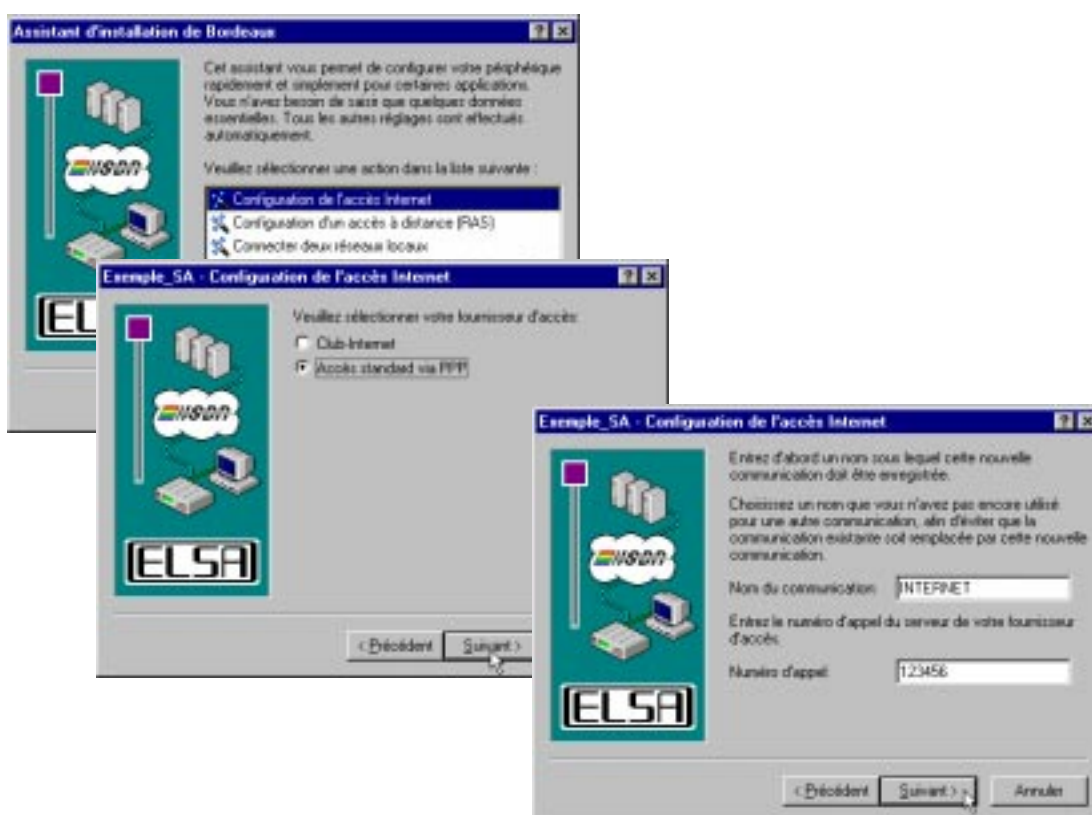
Le tableau suivant montre toutes les données importantes telles qu'elles sont utilisées dans l'exemple. Nous recommandons la création d'un tel tableau pour chaque application. Il vous aide dans votre travail lors de la configuration, lors de la recherche des erreurs et pour les questions relatives au support technique.

	réseau local dans Exemple SA	réseau local du fournisseur d'accès
Adresse IP du LAN	10.100.100.0	
Adresse IP pour le routeur	10.100.100.50	
Masque de réseau IP	255.255.255.0	
Nom du périphérique	Exemple SA	Fournisseur d'accès
Numéro d'appel	123456	4711000



## Internet en toute simplicité avec *ELSA LANconfig* et les assistants

Pour la configuration d'*ELSA LANCOM* pour l'accès à Internet, différents assistants sont disponibles dans *ELSA LANconfig*, qui effectuent à votre place tous les paramétrages nécessaires dans le logiciel *ELSA LANCOM*. Après le démarrage de l'assistant, choisissez l'assistant désiré (automatiquement ou avec **Outils ► Assistant de configuration**). Dans cet exemple, nous n'avons pas opté pour l'un des grands services en ligne mais pour un autre FAI offrant des nœuds d'accès avec PPP. Choisissez ainsi l'option 'Internet via PPP'. L'assistant demande alors les données minimales requises et vous assiste ensuite dans les opérations de paramétrage sur vos ordinateurs aux postes de travail.



## Pas à pas : à quels paramétrages devez-vous procéder dans le routeur ?

- ① Entrez d'abord le numéro d'appel pour les appels entrants et sortants dans le tableau d'interface du routeur (zone de configuration 'Communication', onglet 'Généralités') :

```
cd /Setup/WAN-module/Router-interface-list
S0-1 123456 ON or OFF
```

Si vous avez entré plusieurs numéros d'appels, le premier numéro pour les appels sortants est utilisé.



*Le paramétrage de l'option 'Connexion en Y' se fait en fonction de l'existence simultanée d'une connexion vers un autre correspondant dans le deuxième canal B.*

- ② Une nouvelle entrée dans la liste des noms (zone de configuration 'Communication', onglet 'Correspondants') avec désignation du correspondant et du numéro d'appel associé ainsi que la sélection de la couche prédéfinie 'PPPHDLC' (sans rappel automatique) permet au routeur dans l'entreprise d'appeler le routeur du FAI :

```
cd Setup/WAN-module/Name-list
set Provider 4711000 * * PPPHDLCDLC OFF
```

- ③ Dans la liste PPP sont enregistrés le nom de l'utilisateur et le mot de passe transmis lors de la sélection du correspondant. C'est parce que seul le FAI vous demande votre nom et votre mot de passe, et non l'inverse, que la négociation PPP « n'est pas sécurisée » de ce côté.

```
cd Setup/WAN-module/PPP-list/Default
set Provider no surfing * * WEB_USER IP
```

Le mot de passe 'Naviguer' est remplacé lors de la saisie par quelques \* ! Les autres \* dans cette entrée indiquent les valeurs pouvant être validées sans pour autant les modifier.



*Veillez à respecter l'écriture en majuscules et en minuscules pour le nom de l'utilisateur et le mot de passe.*

- ④ Il ne manque maintenant plus que des adresses. Le routeur a besoin d'une adresse IP libre issue d'Intranet afin d'être trouvé dans son propre réseau TCP/IP. Il la reçoit avec l'entrée de l'adresse Intranet avec le masque de réseau correspondant (zone de configuration 'TCP/IP', onglet 'Généralités').

```
cd Setup/TCP-IP-module
set Intranet IP address 10.100.100.50
set Intranet netmask 255.255.255.0
set operating on
```



*Les entrées pour l'adresse IP et le masque de réseau IP restent libres parce que le routeur se voit attribuer dans cet exemple l'adresse IP de son FAI de façon dynamique. Si par contre des adresses IP enregistrées, valables dans Internet existent, l'une d'entre elles sera enregistrée avec le masque de réseau correspondant (voir également 'Intranet avec propre serveur Web dans Internet').*

- ⑤ Avec les paramétrages effectués jusqu'ici, le routeur est pratiquement devenu partie intégrante d'Internet, mais les ordinateurs dans le LAN ne peuvent pas encore naviguer. Pour y arriver, créez une entrée dans le tableau de routage (zone de configuration 'TCP/IP', onglet 'Routeur'), par lequel sont routées dans l'Internet (route par DEFAULT) tous les paquets pour les adresses localement non accessibles.

```
cd Setup/IP-router-module
```

```
set IP-routing-table 255.255.255.255 0.0.0.0 Provider  
2 ON
```

La route vers l'adresse IP '255.255.255.255' avec le masque de réseau '0.0.0.0' intercepte tous les paquets ne pouvant être affectés localement. 'Fournisseur d'accès' est la désignation du correspondant, auquel les données correspondantes doivent être envoyées. Le correspondant peut être joint directement par votre routeur, c'est pourquoi la distance est mise à '2'. Avec l'option 'On' pour masquering IP, tous les ordinateurs du LAN sont masqués derrière l'adresse du routeur et n'apparaissent pas dans Internet.

- ⑥ A présent, activez uniquement le routeur IP. Le routeur est alors prêt pour le WWW.

```
cd Setup/IP-router-module  
set operating on
```

- ⑦ Que reste-t-il à faire ? Les ordinateurs dans le LAN doivent naturellement aussi savoir que le *ELSA LANCOM* est le central téléphonique pour Internet. Pour ce faire, l'adresse Intranet du routeur est inscrite comme passerelle par défaut et comme serveur DNS sur les ordinateurs aux postes de travail.



*Si vous utilisez le routeur comme serveur DHCP, vous avez la possibilité de faire attribuer ces réglages automatiquement (cf. 'Serveur DHCP').*

## Résultat

Si l'un des collaborateurs démarre maintenant un navigateur sur l'ordinateur à son poste de travail et entre une adresse WEB (par ex. ELSA), une recherche de l'adresse IP correspondante est alors lancée à l'aide du serveur DNS enregistré dans le système d'exploitation (en l'occurrence, ici à l'aide du routeur). Le routeur transmet en tant que passerelle Internet cette interrogation au serveur DNS du FAI, qui finalement détermine l'adresse IP affiliée à ce nom (par ex. 168.192.156.100) et la renvoie à l'ordinateur au poste de travail à l'aide du routeur. Cette adresse n'ayant pas été trouvée dans le réseau local, le routeur envoie ensuite dans Internet tous les paquets destinés à cette adresse IP via la route par défaut.

## Intranet avec propre serveur Web dans Internet

### Motivation

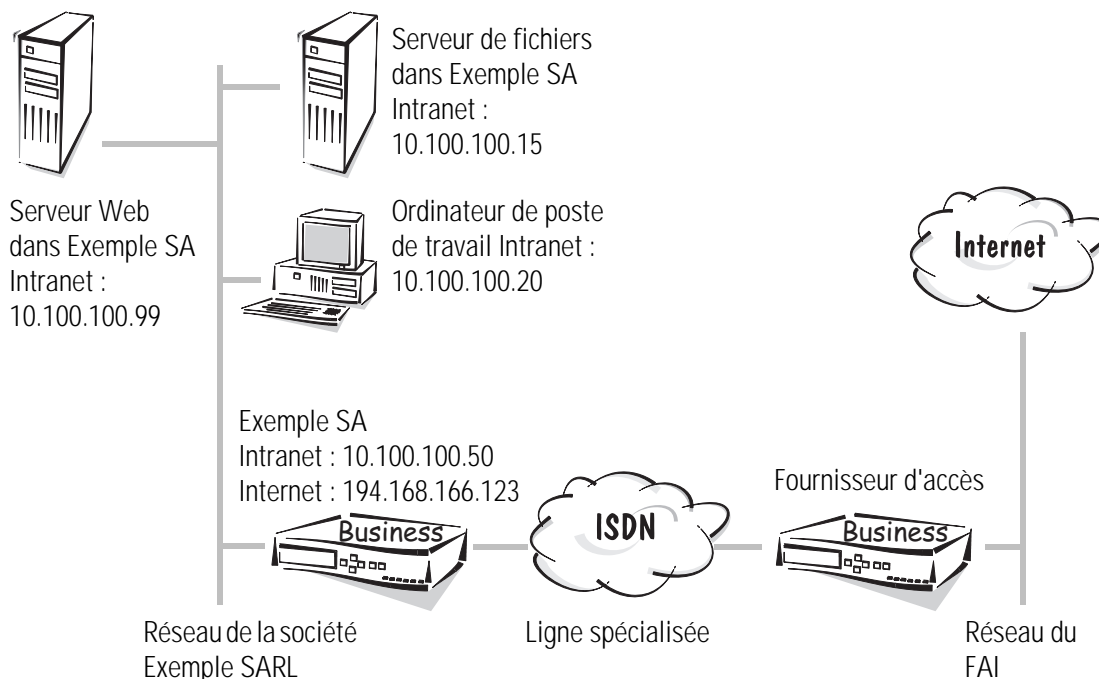
Dans l'exemple 'Internet pour tous les PC dans le LAN', vous avez vu comment raccorder un réseau TCP/IP via un routeur à Internet (avec masquering IP).

Dans l'exemple ci-après, le LAN se voit attribuer dans Exemple SA son propre serveur Web qui peut être accessible depuis l'Internet. Pour ce faire, vous avez besoin outre le compte chez le FAI d'une adresse IP fixe. Cette adresse IP enregistrée est affectée au routeur. Le routeur effectue alors une conversion de l'adresse enregistrée à l'adresse

Intranet du serveur Web. Le serveur Web devient alors visible dans Internet sous l'adresse enregistrée (masquering IP inverse). Tous les autres ordinateurs dans le réseau local restent masqués.

### Illustration à l'aide d'un exemple

Nous avons d'un côté un réseau dans la société Exemple SA avec quelques ordinateurs aux postes de travail et un routeur raccordé à un accès Euro-ISDN. Dans ce réseau, outre les serveurs locaux un serveur Web existe aussi.



De l'autre côté, nous avons le réseau du fournisseur d'accès à Internet. Pour accéder à ce réseau, il existe deux possibilités envisageables :

- Si le serveur Web est très fréquenté, vous désirez peut-être avoir une ligne spécialisée (liaison permanente) vers le fournisseur d'accès (par ex. D64S avec un canal B sans canal D). Dans ce cas, placez un deuxième routeur chez votre FAI et configurez les deux périphériques pour la liaison permanente utilisée.
- Si une liaison permanente s'avère superflue, un routeur suffit dans votre réseau local. Afin que le FAI ne se voit pas facturé pour la connexion à votre serveur Web, configurez votre routeur pour le rappel automatique du fournisseur d'accès.

Dans le deuxième cas, à chaque accès à votre site Web des connexions sont établies au FAI, imputant des coûts à votre facture de téléphone. Ces coûts ne pouvant pas être contrôlés (à l'exception de l'utilisation de budgets qui n'auraient aucun sens ici, nous privilégions dans cet exemple la première variante.

Le tableau suivant montre toutes les données importantes utilisées dans l'exemple. Nous recommandons la création d'un tel tableau pour chaque application. Il vous aide dans

vos travaux lors de la configuration, lors de la recherche des erreurs et pour les questions relatives au support technique.

	réseau local dans Exemple SA	réseau local du fournisseur d'accès
Adresse IP pour le routeur	194.168.166.123	
Masque de réseau IP pour le routeur	255.255.255.255	
Adresse Intranet du LAN	10.100.100.0	
Adresse Intranet pour le routeur	10.100.100.50	
Adresse Intranet pour le serveur Web	10.100.100.99	
Intranetmask	255.255.255.0	
Nom du périphérique	Exemple SA	Fournisseur d'accès



### Ligne permanente : à quels paramétrages devez-vous procéder dans le routeur ?

Le paramétrage dans les deux périphériques est à nouveau très semblable. Nous partons du paramétrage du routeur d'Exemple SA et indiquons le cas échéant les différences pour le routeur chez le fournisseur d'accès.

- ① Premièrement, configurez le routeur dans le tableau Interface d'une liaison permanente selon D64S (zone de configuration 'Gestion', onglet 'Interfaces') :

```
cd Setup/WAN-module/Interface-list
set S0-1 GRP0 1
```

Le canal B utilisé doit être identique pour les deux routeurs !

- ② Avec ces paramétrages, les deux routeurs peuvent établir d'eux-mêmes une connexion dès que vous êtes connecté et relié à la liaison permanente. Utilisez ici automatiquement la couche 'DEFAULT'.

Si la ligne spécialisée doit utiliser une autre couche, définissez une nouvelle couche dans la liste des couches et réglez-la dans cette liste (zone de configuration 'Communication', onglet 'Généralités') selon vos désirs, par ex. avec protocole PPP et compression :

```
cd Setup/WAN-module/Layer-list
set FVG0 TRANS PPP TRANS compr. HDLC64K
```

- ③ Une nouvelle entrée dans la liste de noms (Zone de configuration 'Communication', onglet 'Correspondants') avec désignation des correspondants et de la couche à utiliser permet au routeur d'établir les lignes spécialisées avec les réglages corrects. L'entrée d'un numéro d'appel n'est pas nécessaire :

```
cd Setup/WAN-module/Name-list
set remote connection* 0 0 FVG0 Off
```

La durée de maintien est mise à '0', car des tentatives de connexion superflues pourraient occasionner des retards.

- ④ Dans la liste des canaux, déterminez les canaux devant être utilisés pour la ligne spécialisée. La désignation des canaux et leur ordre doit être identique des deux côtés de la connexion. Entrez ici aussi (de manière identique des deux côtés de la connexion) le nombre de canaux devant être éventuellement utilisés pour un Backup (Zone de configuration 'Communication', Onglet 'Correspondant') :

```
cd Setup/WAN-module/Channel-list
set remote connection 1 1 1-1 0
```

- ⑤ Pour que les noms provenant de la liste des noms des routeurs puissent être transmis et reconnus, le nom du périphérique doit être conforme (zone de configuration 'Communication', onglet 'Généralités') :

```
cd Setup
set Name Exemple
```

- ⑥ Il ne manque maintenant plus que des adresses. Le routeur d'Exemple SA a besoin d'une adresse IP libre dans Intranet afin d'être trouvé dans son propre réseau TCP/IP. Il la reçoit avec l'entrée de l'adresse Intranet avec le masque de réseau correspondant (zone de configuration 'TCP/IP', onglet 'Généralités'). Par ailleurs, il reçoit comme convenu l'adresse IP enregistrée y compris le masque de réseau. Afin que ces entrées deviennent aussi valides, activez le module TCP/IP.

```
cd /Setup/TCP-IP-module
set IP-address 194.168.166.123
set IP-netmask 255.255.255.255
set Intranet address 10.100.100.50
set Intranet netmask 255.255.255.0
set operating on
```

L'autre routeur reçoit, de manière analogique, une adresse IP fixe et (lors de l'utilisation du masquering IP) une adresse Intranet issue de la zone d'adresses du FAI.

- ⑦ Avec l'entrée de l'adresse IP, le routeur d'Exemple SA est pratiquement devenu partie intégrante d'Internet, mais les ordinateurs dans le LAN ne peuvent pas encore naviguer. Pour offrir un accès à Internet à vos propres collaborateurs, créez une entrée dans le tableau de routage (zone de configuration 'TCP/IP', onglet 'Routeur'), par lequel sont routées dans Internet (route par DEFAULT) tous les paquets pour les adresses localement non accessibles.



```
cd Setup/IP-router-module
```

```
set IP-routing-table 255.255.255.255 0.0.0.0 leased-  
line connection 2 ON
```

La route vers l'adresse IP '255.255.255.255' avec le masque de réseau '0.0.0.0' intercepte tous les paquets ne pouvant pas être affectés localement. 'Fournisseur d'accès' est la désignation du correspondant, auquel les données correspondantes doivent être envoyées. Le correspondant peut être joint directement dans Exemple SA par le routeur c'est pourquoi la distance est placée sur '2'. Avec l'option 'On' pour le masquerading IP, tous les ordinateurs du LAN sont masqués derrière l'adresse du routeur et n'apparaissent pas dans Internet.

- ⑧ Le routeur auprès du FAI doit recevoir également une entrée dans le tableau de routage. Cette route contient l'adresse IP du routeur enregistrée dans Exemple SA et le nom du correspondant. Pour cette route, 'IP-masquerading' reste désactivé parce que le routage doit avoir lieu dans cette direction et ne doit pas être masqué.

```
cd /Setup/IP-router-module
```

```
set IP-routing-table 194.168.166.123 255.255.255.255  
Exemple 2 Off
```

Cette adresse IP se situant dans la propre zone d'adresses du fournisseur d'accès, la fonction 'Proxy-ARP' doit être activée :

```
cd /Setup/IP-router-module
```

```
set Proxy-ARP ON
```

- ⑨ Le serveur Web devient visible dans Internet grâce à une entrée dans le tableau des services du périphérique d'Exemple SA (zone de configuration 'TCP/IP', onglet 'Masquerading') :

```
cd /Setup/IP-router-module/Masquerading/Service-table  
set 80 10.100.100.99
```

La valeur '80' indique, que le service visible à l'extérieur est HTTP (WWW), l'adresse '10.100.100.99' choisit l'ordinateur avec cette adresse Intranet spéciale comme serveur Web.



*Vous trouverez une liste avec d'autres services au chapitre 'Ports TCP/IP'.*

- ⑩ A présent, activez uniquement le routeur IP (zone de configuration 'TCP/IP', onglet 'Routeur'). Le routeur est alors prêt pour le WWW.

```
cd /Setup/IP-router-module
```

```
set operating on
```

- ⑪ Que reste-t-il à faire ? Les ordinateurs dans le LAN doivent naturellement savoir que le routeur est le central téléphonique pour Internet. Pour ce faire, l'adresse Intranet du routeur est inscrite comme passerelle par défaut sur les ordinateurs aux postes

de travail. Par ailleurs, l'adresse IP du serveur correspondant est déclarée en tant que serveur DNS auprès du FAI.



*Si vous utilisez le routeur comme serveur DHCP, vous avez la possibilité de faire attribuer ces réglages automatiquement (cf. 'Serveur DHCP').*

Le fournisseur d'accès à Internet doit veiller ensuite à ce que votre serveur Web soit inscrit avec l'adresse IP enregistrée et le nom des domaines dans son serveur DNS, par ex. 'www.exemple\_sa.fr'.

## Résultat

Le but des paramétrages résidait dans la possibilité d'échanger des données avec Internet dans les deux sens : des requêtes depuis le réseau local dans Internet et inversement des requêtes depuis Internet au serveur Web dans le réseau local. Vous y êtes parvenu !

### ■ Internet pour les collaborateurs :

Si l'un des collaborateurs démarre maintenant un navigateur sur l'ordinateur à son poste de travail et entre une adresse Web (par ex. ELSA), une recherche de l'adresse IP correspondante est alors lancée à l'aide du serveur DNS enregistré dans le système d'exploitation. Le routeur transmet en tant que passerelle Internet cette interrogation au serveur DNS du FAI, qui pour finir détermine l'adresse IP affiliée à ce nom (par ex. 168.192.156.100) et la renvoie à l'ordinateur au poste de travail à l'aide du routeur. Cette adresse n'ayant pas été trouvée dans le réseau local, le routeur envoie par la suite tous les paquets destinés à cette adresse IP par le biais de la route par défaut dans Internet.

### ■ Site Web de l'entreprise dans Internet

Lorsqu'un abonné Internet lance quelque part dans le monde son navigateur et entre son adresse Web (par ex. www.exemple\_sa.fr), son ordinateur reçoit à nouveau via le serveur DNS l'adresse IP (194.168.166.123) du routeur dans l'entreprise. L'ordinateur de l'utilisateur Web peut alors, avec cette adresse IP, communiquer directement avec le routeur. Le routeur convertit ensuite automatiquement l'adresse Intranet du serveur Web et facilite ainsi l'accès au site Web de votre entreprise.

Naturellement, d'autres services tels que FTP et Gopher peuvent être offerts dans Internet, si le tableau des services est élargi en conséquence. Il vous appartient de déterminer à votre guise, à l'aide du tableau des services, si un ou plusieurs serveur(s) doivent intervenir pour les différents services.

## Interconnexions LAN-LAN

Lorsque les affaires de la société Exemple SA vont très bien, il est temps pour une filiale ou une centrale d'apparaître sur les marchés globaux. La filiale a elle aussi naturellement son propre réseau local et désire toujours être tenue au courant de ce qui se passe.

L'interconnexion LAN-LAN relie les LAN isolés en un grand réseau et ce si besoin est sur des continents entiers. Dans le cas de liaisons commutées, une gestion intelligente des lignes et des mécanismes de filtrage sophistiqués se charge de réduire les coûts de communication. Naturellement, les lignes spécialisées peuvent coexister avec les liaisons commutées.

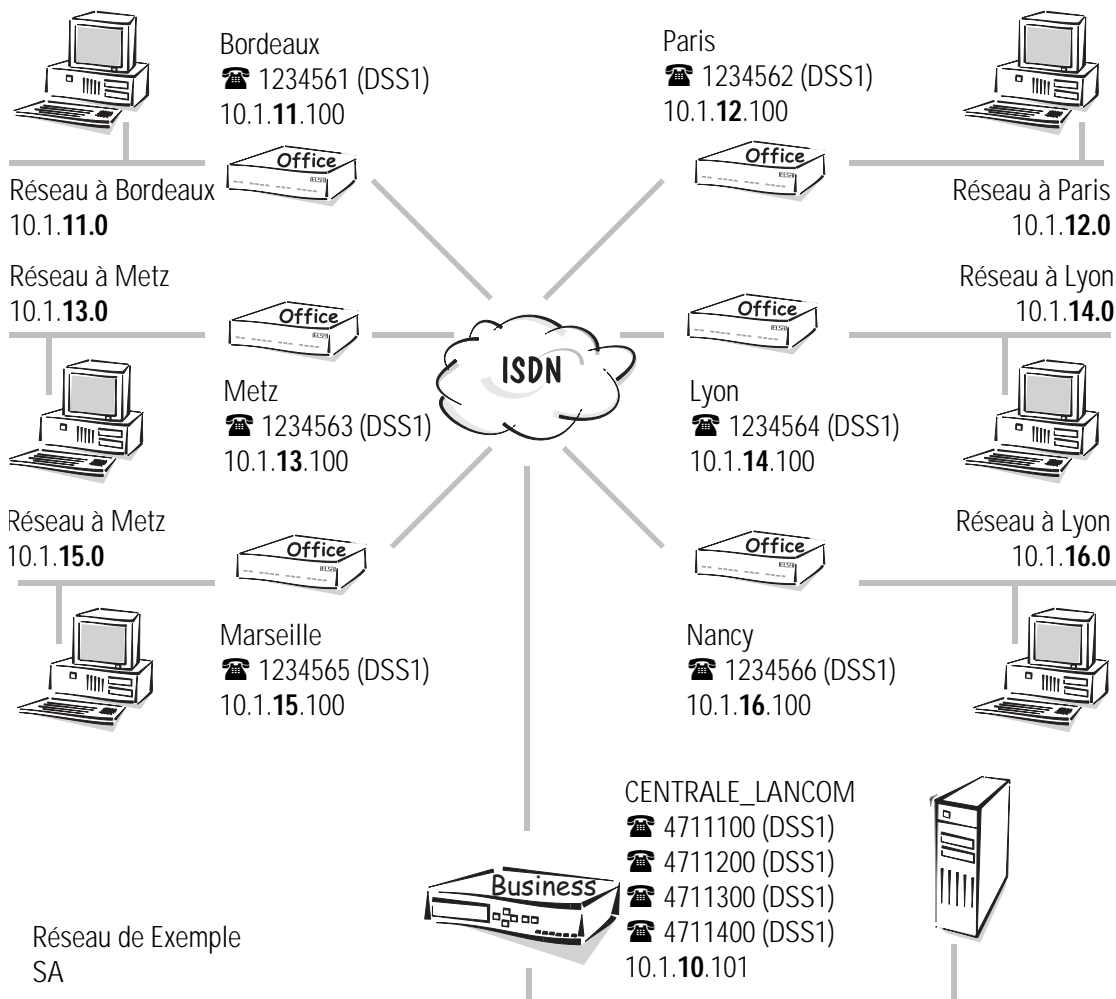
## Interconnexion des réseaux avec le routeur IP

### Motivation

Avec le routeur IP, vous pouvez relier des réseaux qui misent sur TCP/IP en tant que protocole de réseau. Contrairement à l'accès Internet via masquerading IP ('Internet pour tous les PC dans le LAN'), **toutes** les adresses IP des réseaux concernés sont visibles dans les autres réseaux raccordés lors de la connexion de réseaux via le routeur IP et pas seulement celles des routeurs.

### Illustration à l'aide d'un exemple

Dans cette tâche, la centrale a six filiales. Chaque filiale est équipée d'un « petit » routeur. Tous ces routeurs sont raccordés par une liaison commutée RNIS sur un *ELSA LANCOM Business* dans la centrale.



Le tableau suivant montre l'affectation des noms du périphérique, des adresses et des numéros de téléphone tels qu'ils sont utilisés dans l'exemple :

Réseau	Exemple SA	Bordeaux	Paris	Metz	Lyon	Marseille	Nancy
Adresse IP LAN	10.1.10.0	10.1.11.0	10.1.12.0	10.1.13.0	10.1.14.0	10.1.15.0	10.1.16.0
Adresses IP pour les routeurs	10.1.10.101	10.1.11.100	10.1.12.100	10.1.13.100	10.1.14.100	10.1.15.100	10.1.16.100
Masque de réseau IP	255.255.255.0						
Nom du périphérique	Exemple_SA	Bordeaux	Paris	Metz	Lyon	Marseille	Nancy
Numéros d'appel	4711100 4711200 4711300 4711400	1234561	1234562	1234563	1234564	1234565	1234566



## Routage IP en toute simplicité avec *ELSA LANconfig* et les assistants

Pour la configuration à l'interconnexion LAN, un assistant est disponible dans *ELSA LANconfig*, qui effectue tous les paramétrages nécessaires à votre place dans le logiciel et recoupe en même temps les particularités des réseaux TCP/IP. Après démarrage de l'assistant, choisissez (automatiquement ou avec **Outils ► Assistant de Configuration**) l'option 'Connecter deux réseaux locaux'. L'assistant demande alors brièvement les données requises – entre autres aussi le protocole de réseau utilisé – et vous guide ensuite dans le réglage de vos ordinateurs aux postes de travail.

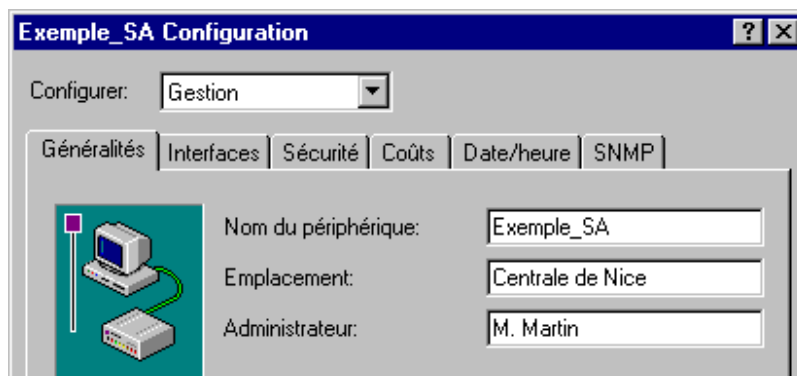
Pour l'interconnexion de plusieurs réseaux, vous devrez faire appel à l'assistant du routeur de la centrale pour chaque réseau à connecter. L'assistant de chaque routeur de filiale devra également être utilisé une fois.



## Pas à pas : à quels paramétrages devez-vous procéder dans les routeurs ?

Les paramétrages sont en principe identiques pour tous les routeurs. Dans les étapes de configuration qui suivent, nous vous indiquerons précisément en partant du routeur de la centrale ce qui doit être réglé immédiatement et nous vous donnerons des indications sur les divergences dans les autres routeurs.

- ① Pour que les noms que vous utilisez dans la liste des noms soient aussi transmis et reconnus par les routeurs, dénommez le périphérique en conséquence (zone de configuration 'Gestion', onglet 'Généralités').



Pour des configurations avec d'autres ressources, spécifiez le nom du périphérique directement dans le menu 'Setup' :

```
set /Setup/Name Exemple_SA
```

Les périphériques dans les filiales reçoivent en conséquence les noms 'Bordeaux' à 'Nancy'.

- ② Puis inscrivez les **propres** numéros d'appel du premier routeur de la centrale (zone de configuration 'Communication', onglet 'Généralités') :

```
cd /Setup/WAN-module/Router-interface-list
set s0-1 4711100 On No
```

Les autres interfaces et périphériques reçoivent en conséquence leurs propres numéros d'appel.

- ③ De nouvelles entrées dans la liste des noms (zone de configuration 'Communication', onglet 'Correspondants') avec désignation du correspondant et du numéro d'appel associé ainsi que la sélection d'une couche définie sur tous les routeurs (ici par ex. la couche prédéfinie 'DEFAULT') permet au routeur dans la centrale d'appeler les routeurs dans les autres réseaux. Avec les valeurs standard pour les durées de maintien B1 et B2 toute connexion est coupée automatiquement si aucune donnée ne circule sur cette ligne pendant 20 secondes. Chaque réseau doit supporter lui-même les coûts téléphoniques, c'est pourquoi l'option de rappel reste désactivée :

```
cd /Setup/WAN-module/Name-list
set BORDEAUX 1234561 * * DEFAULT OFF
```

Les autres appareils n'inscriront que le routeur 'Exemple\_SA' ainsi que le numéro d'appel de l'interface correspondante. Le tiret devant le numéro d'appel signifie que d'autres numéros d'appel existent bien pour ce réseau dans la liste round-robin.

**Liste des noms - Nouvelle entrée**

Nom: EXEMPLE\_SA

Numéro d'appel: -4711100

Time-out: 20 secondes

Time-out pour regroupement: 20 secondes

Nom de la couche: DEFAULT

Rappel automatique en retour: ☒ Pas de rappel

OK Annuler

- ④ Nous poursuivons avec la liste round-robin. Entrez ici dans les routeurs des filiales les numéros d'appel des autres interfaces du routeur de la centrale, que vous n'avez pas encore entrés dans la liste des noms.

**Liste RoundRobin - Nouvelle entrée**

Correspondant: EXEMPLE\_SA

RoundRobin: -4711200-4711300-47114

Commencer avec: ☒ le dernier numéro contacté ☐ toujours le premier numéro

OK Annuler

```
cd /Setup/WAN-module/RoundRobin-list
set Exemple_SA 4711200 last
```

- ⑤ Si les connexions vers les réseaux des filiales ne doivent utiliser que certains canaux B afin de réserver les autres canaux pour les accès par RAS, établissez dans la liste des canaux du routeur central une définition des canaux autorisés pour chaque correspondant.

**Liste des canaux - Gérer une entrée**

Correspondant: BORDEAUX

Minimum: 1 canaux

Maximum: 2 canaux

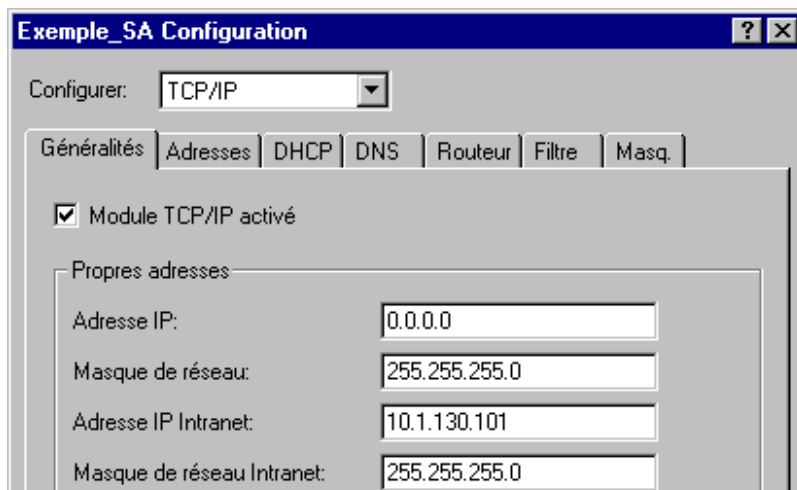
Ordre: 2-1;2-2

Canaux secours: 0

OK Annuler

```
cd /Setup/WAN-module/Channel-list
set BORDEAUX 1 2 2-1;2-2 0
```

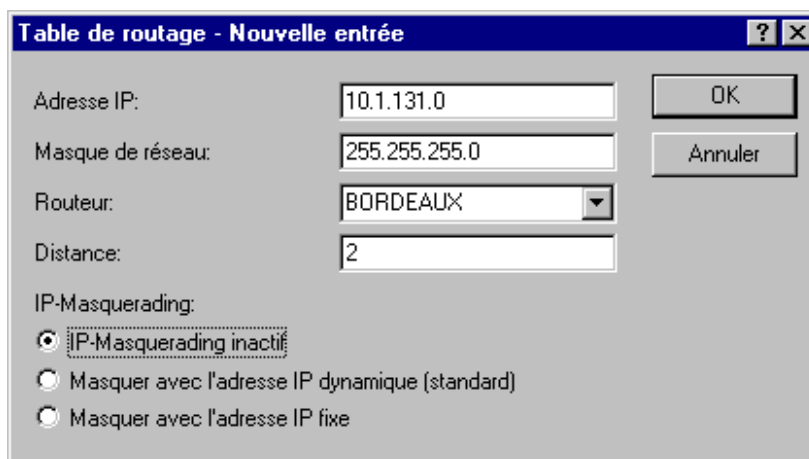
- ⑥ Il ne manque maintenant plus que des adresses. Les périphériques ont besoin d'une adresse IP libre issue d'Intranet afin d'être trouvés dans leur propre réseau TCP/IP. Ils l'obtiennent avec l'entrée de l'adresse Intranet avec le masque de réseau correspondant (zone de configuration 'TCP/IP', onglet 'Généralités'). Afin que ces entrées deviennent aussi valides, activez le module TCP/IP.



```
cd /Setup/TCP-IP-module/RoundRobin-list
set Intranet address 10.1.130.101
set Intranet netmask 255.255.255.0
```

Les routeurs dans les filiales obtiennent les adresses IP 10.131.1.100 à 10.136.1.100, tous avec le masque de réseau 255.255.255.0, tel qu'il est représenté dans l'illustration et dans l'aperçu.

- ⑦ Quelles adresses IP, et vers où les routeurs doivent-ils router ? Dans le tableau de routage des routeurs de la centrale, saisissez les adresses IP et les masques de réseau de toutes les filiales avec le correspondant associé (sans masquerading IP !) :



Enfin, activez le routeur IP et déjà le premier *ELSA LANCOM* est prêt pour la connexion à d'autres réseaux.



```
cd /Setup/IP-router-module/IP-routing-table
set 10.1.131.0 255.255.255.0 Bordeaux 2 OFF
cd /Setup/IP-router-module
set operating on
```

Les routeurs dans les filiales obtiennent chacun une inscription pour la centrale. Ceci permet de router toutes les connexions entre les filiales via le routeur de la centrale.



Alternativement, les centrales peuvent aussi communiquer directement entre elles. Pour ce faire, vous obtenez d'abord les mêmes entrées dans la liste des noms que le routeur dans la centrale. En plus, vous obtenez les mêmes valeurs dans le tableau de routage que les périphériques dans la centrale, où l'entrée de routage pour le propre réseau est remplacée par l'entrée du réseau de la centrale.

- ⑧ Que reste-t-il à faire ? Les ordinateurs dans le LAN doivent naturellement savoir que le routeur est le central téléphonique pour les autres réseaux. Pour ce faire, l'adresse Intranet du routeur est inscrite comme passerelle par défaut sur les ordinateurs aux postes de travail et les serveurs.



*Si vous utilisez le routeur comme serveur DHCP, vous avez la possibilité de faire attribuer ces réglages automatiquement (cf. 'Serveur DHCP').*

## Résultat

Dans une filiale, lors d'un accès d'un ordinateur au réseau de la centrale, il est possible de bifurquer via l'entrée dans la liste RoundRobin sur une autre interface, lorsque le premier qui a été contacté est occupé.

## Interconnexion des réseaux avec le routeur IPX

### Motivation

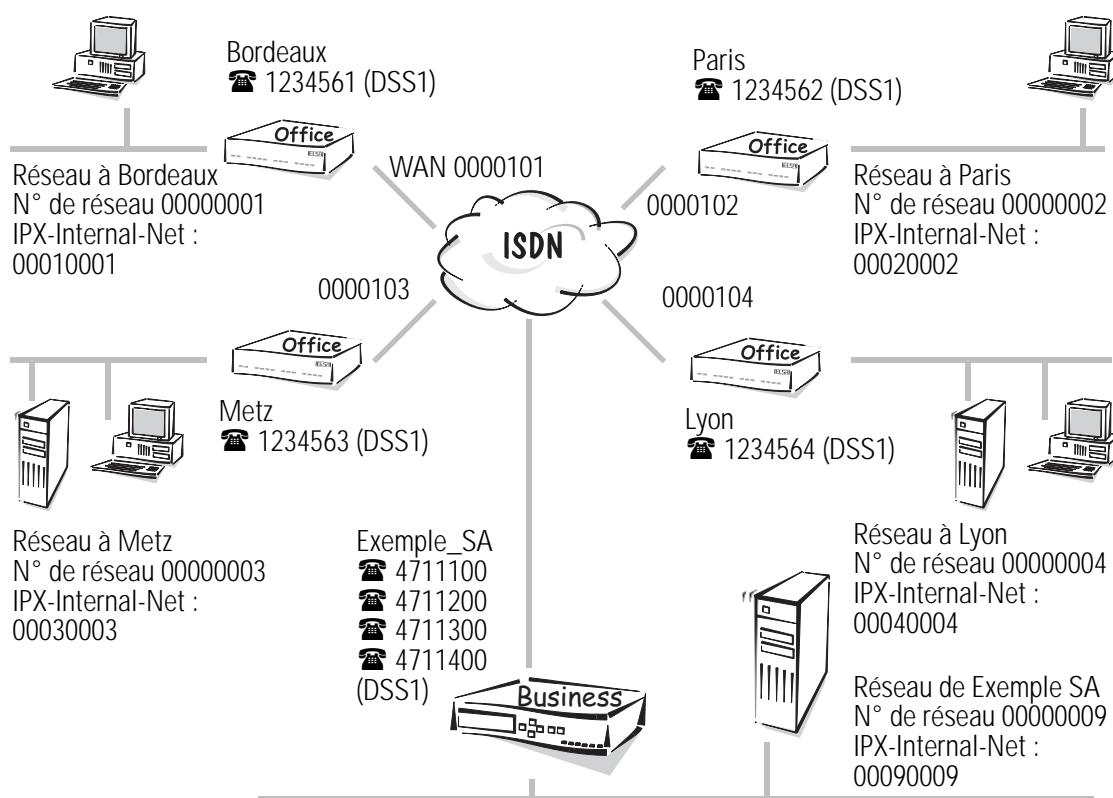
Avec le routeur IPX, vous pouvez relier des réseaux qui misent sur IPX/SPX en tant que protocole de réseau. Vous pouvez par ex. connecter la centrale de l'entreprise sur les réseaux de plusieurs filiales.

### Illustration à l'aide d'un exemple

Dans cette tâche, la centrale a quatre filiales. Chaque filiale est équipée d'un « petit » routeur. Ces routeurs sont raccordés par une liaison commutée RNIS sur un *ELSA LANCOM Business* dans la centrale.

Le tableau suivant montre l'affectation des noms du périphérique, des adresses et des numéros de téléphone tels qu'ils sont utilisés dans l'exemple :

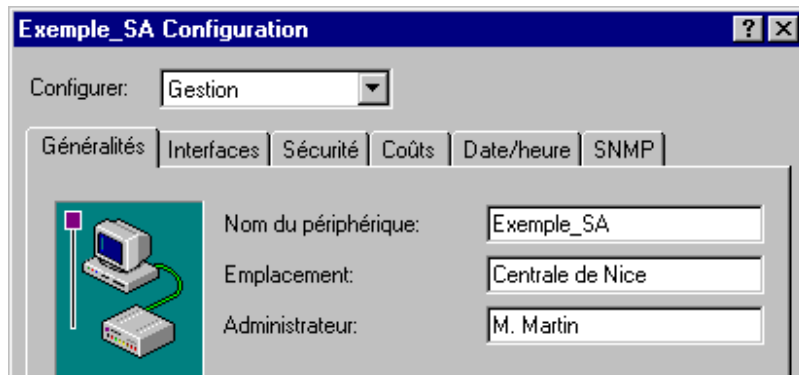
Réseau	LAN Exemple SA	LAN Bordeaux	LAN Paris	LAN Metz	LAN Lyon
Adresse du réseau	00000009	00000001	00000002	00000003	00000004
IPX-Internal-Net	00090009	00010001	00020002	00030003	00040004
Binding	802.3	SNAP	SNAP	802.3	802.3
Nom du périphérique	Exemple_SA	Bordeaux	Paris	Metz	Lyon
Numéro d'appel	4711100 4711200 4711300 4711400	1234561	1234562	1234563	1234564
Réseaux WAN		00000101	00000102	00000103	00000104



### **Pas à pas : à quels paramétrages devez-vous procéder dans les routeurs ?**

Dans les étapes de configuration qui suivent, nous vous indiquerons précisément en partant du routeur de la centrale ce qui doit être réglé et nous vous donnerons des indications sur les divergences dans les autres routeurs.

- ① Pour que les noms que vous utilisez dans la liste des noms soient aussi transmis et reconnus par les routeurs, dénommez le périphérique en conséquence (zone de configuration 'Gestion', onglet 'Généralités') :

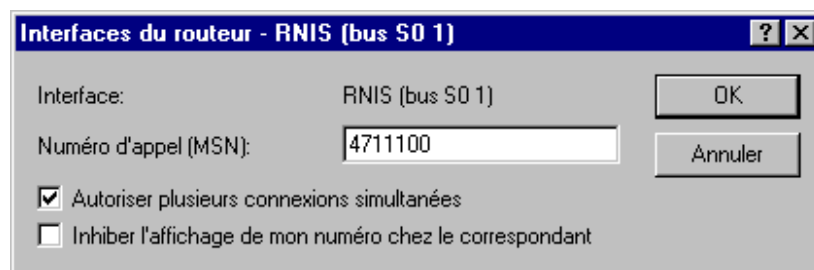


Pour des configurations avec d'autres ressources, spécifiez le nom du périphérique directement dans le menu 'Setup' :

```
cd Setup
set Name Exemple_SA
```

Les routeurs dans les filiales reçoivent en conséquence les noms 'Bordeaux', 'Metz' et 'Lyon'.

- ② Puis inscrivez le **propre** numéro d'appel du premier routeur de la centrale (zone de configuration 'Communication', onglet 'Généralités') :



```
cd /Setup/WAN-module/Router-interface-list
S0-1 4711100
S0-2 4711200
S0-3 4711300
S0-4 4711400
```

Les autres périphériques reçoivent en conséquence leurs propres numéros d'appel (1234561, 1234562, 1234563 et 1234564).

- ③ De nouvelles entrées dans la liste des noms (zone de configuration 'Communication', onglet 'Correspondants') avec désignation des correspondants et des numéros d'appel associés ainsi que la sélection d'une couche existante pour tous les routeurs (ici par ex. la couche prédéfinie DEFAULT) permet au routeur dans la centrale d'appeler les routeurs dans les autres réseaux d'entreprise. Chaque

réseau doit supporter lui-même les coûts téléphoniques, c'est pourquoi l'option de rappel reste désactivée :

```
cd Setup/WAN-module/Name-list
set Bordeaux 1234561 * * DEFAULT OFF
set Paris 1234562 * * DEFAULT OFF
set Metz 1234563 * * DEFAULT OFF
set Lyon 1234564 * * DEFAULT OFF
```

Les routeurs dans les filiales n'inscrivent que le routeur 'Exemple\_SA' et en plus le numéro d'appel de l'une des interfaces du routeur de la centrale.

- ④ Il ne manque maintenant plus que des adresses. Afin que le routeur puisse différencier le propre LAN des autres LAN et du WAN, enregistrez l'adresse du réseau et la liaison pour le réseau de Exemple SA (zone de configuration 'IPX', onglet 'Généralités').

```
Setup/IPX-module/LAN-config
set Network 00000009
set Binding 802.3
```



*Le réseau de la centrale a un serveur. Si vous ne connaissez pas le numéro du réseau, vous pouvez le rechercher automatiquement à l'aide du paramètre '00000000' comme numéro de réseau. Vous pouvez aussi faire rechercher automatiquement la liaison. Étant donné que le routeur contacte toujours le réseau, dans lequel la plupart des informations RIP/SAP sont échangées, ce procédé est indiqué lorsqu'un seul réseau logique est utilisé sur la cordée Ethernet.*

Pour les appareils dans les filiales de Metz et de Lyon, entrez également l'adresse de réseau correspondante avec le Binding 'Auto'.

```
cd /Setup/IPX-module/LAN-config
set network 00000003 and 00000004
set Binding auto
```

Pour les réseaux des filiales de Bordeaux et de Paris il faut entrer explicitement le Binding, par ex. 'SNAP' ainsi que le numéro du réseau parce qu'il n'y a pas de serveur dans ces réseaux :

```
cd /Setup/IPX-module/LAN-config
set network 00000001 and 00000002
set Binding SNAP
```

- ⑤ Vers où les appareils doivent-ils router ? Dans le tableau de routage (zone de configuration 'IPX', onglet 'Routeur'), indiquez les correspondants avec une adresse de réseau **propre** pour le WAN (pas celle de l'autre LAN !). Pour le routeur dans le réseau de la centrale, les entrées de tableau apparaissent comme ci :

```
cd /Setup/IPX-module/WAN-config/Routing-table
set Bordeaux 00000101 802.3 Route Off
set Paris 00000102 802.3 Route Off
set Metz 00000103 802.3 Route ON
set Lyon 00000104 802.3 Route ON
```

Outre le nom du périphérique du routeur dans le réseau du correspondant, chaque entrée dans le tableau de routage reçoit une adresse WAN propre. Adresse réseau du WAN sur lequel la liaison '802.3' est utilisée. Puisque, pour les réseaux des filiales de Metz et de Lyon un serveur existe, le mécanisme 'Exponential Backoff' est activé.



*Pour de plus amples informations concernant la fonction du mécanisme 'Exponential Backoff', reportez-vous au 'Exponential Backoff'.*

Pour le réseau dans la filiale à Bordeaux, l'entrée apparaît par ex. comme ci :

```
cd /Setup/IPX-module/WAN-config/Routing-table
set Exemple_SA 00000101 802.3 Route On
```

L'adresse du réseau WAN correspond respectivement à l'entrée pour le réseau de la filiale dans le routeur de la centrale. Comme liaison, '802.3' est toujours utilisé sur le WAN. Puisque, pour les réseaux des filiales, un serveur existe toujours chez le correspondant, le mécanisme 'Exponential Backoff' est activé.

## 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 personnels 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, le routeur fait naturellement tout pour protéger les données internes de l'entreprise : la fonction de rappel automatique via les noms enregistrés et les numéros d'appel ne donne qu'à certaines personnes la clé Sésame ouvre-toi. En plus, les coûts de communication sont alors saisis centralement pour faciliter la facturation.

## **Accès à distance avec TCP/IP**

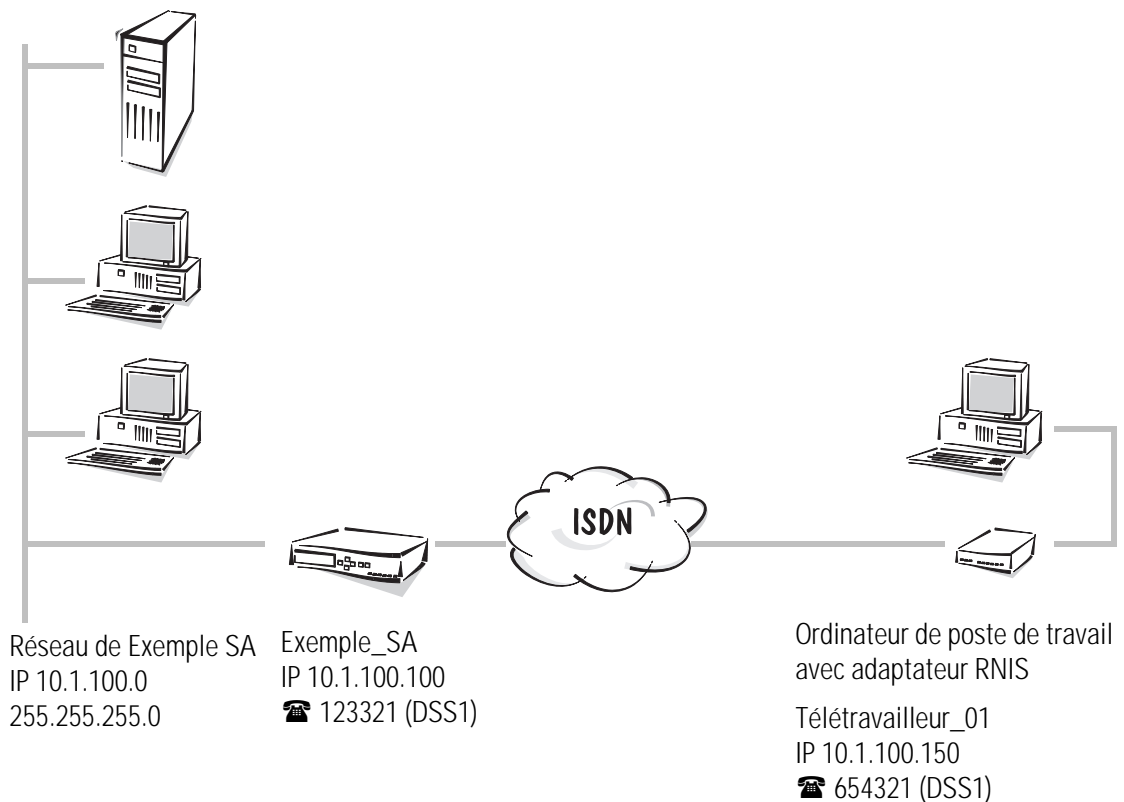
### **Motivation**

Une entreprise emploie quelques collaborateurs, qui en tant que personnels en déplacement ou télétravailleurs ne sont pas tous les jours à l'entreprise. Pourtant, ils doivent avoir accès au réseau local (Intranet) de l'entreprise depuis leur PC pour échanger des données et des informations (par ex. le courrier électronique). PPP est le protocole utilisé pour la transmission de données, parce que tous les périphériques et les systèmes d'exploitation habituels le maîtrisent. Les adresses IP sont affectées par Pooling IP afin de réduire les frais d'entretien des accès.

### **Illustration à l'aide d'un exemple**

Les collaborateurs qui recourent à l'accès à distance ont chez eux un ordinateur à leur poste de travail avec un adaptateur terminal RNIS ou une carte RNIS. Certains collaborateurs nomades se connectent de l'extérieur au réseau de l'entreprise à l'aide de leur ordinateur de poche et de leur téléphone mobile GSM.

Sur les ordinateurs distants, un client PPP est installé, dans notre exemple l'accès réseau à distance de Windows avec TCP/IP comme protocole. Le routage de paquets NetBIOS doit également être prise en charge afin que les personnels en déplacement puissent accéder aux réseaux Windows par la validation des fichiers et des imprimantes. Le LAN de l'entreprise dispose d'un *ELSA LANCOM Business* qui rappelle les ordinateurs aux postes de travail si besoin est.



### Accès à distance en toute simplicité avec *ELSA LANconfig* et les assistants

Pour la configuration des accès, un assistant effectuant tous les paramétrages nécessaires à votre place dans le logiciel et recoupant en même temps les particularités des réseaux TCP/IP est disponible dans *ELSA LANconfig*. Après démarrage de l'assistant, choisissez (automatiquement ou à l'aide d' **Outils ► Assistant de configuration**) l'option 'Mise à disposition de l'accès (RAS)'. L'assistant demande alors brièvement les données requises, entre autres aussi le protocole de réseau utilisé.



### Pas à pas : à quels paramétrages devez-vous procéder dans le routeur ?

- ① Entrez d'abord votre **propre** numéro d'appel pour les appels entrants et sortants dans le tableau de l'interface du routeur (zone de configuration 'Communication', onglet 'Généralités') :

```
cd /Setup/WAN-module/Router-interface-list
set S0-1 123321 ON
```

Si vous avez entré plusieurs numéros d'appels, le premier numéro est utilisé pour les appels sortants.



*L'option 'Connexion en Y' doit être en tout cas activée pour que des connexions soient aussi possibles simultanément à deux télétravailleurs différents.*

- ② L'accès à distance doit être possible sans pour autant contrôler les numéros d'appel entrants, puisque les personnels en déplacement doivent pouvoir accéder au réseau

de l'entreprise depuis divers endroits. L'assignation d'une couche utilisant PPP n'est alors pas réalisable à l'aide de la reconnaissance du numéro d'appel. Vérifiez les valeurs de la couche 'DEFAULT' et réglez le cas échéant les valeurs nécessaires de cette couche :

```
cd /Setup/WAN-module/Layer-list
set DEFAULT trans PPP trans none HDLC64K
```

Chaque appelant ne pouvant pas être identifié par la liste des numéros sera accueilli immédiatement par une négociation PPP.

Si le routeur constate que le correspondant appelle par GSM, il réglera automatiquement le protocole sur `Trans APPP Trans no V.110 9600` afin de permettre l'établissement de la communication.

- ③ Pour le rappel des téléphones GSM on aura besoin plus tard d'une couche réglée sur la connexion via le protocole V.110 :

```
cd /Setup/WAN-module/Layer-list
set RAS_GSM Trans APPP Trans none Of comp. V.110 9600
```

- ④ L'entrée dans la liste des noms pour chaque correspondant RAS avec la désignation du correspondant, de la couche ('DEFAULT' ou 'RAS\_GSM') et de l'option de rappel 'Nom' permet au *ELSA LANCOM* de rappeler l'ordinateur au poste de travail du personnel en déplacement. Ici, une négociation du protocole est entamée via PPP, le numéro d'appel pour le rappel reste libre dans la liste des noms et peut être défini par le personnel en déplacement lui-même. Si un personnel en déplacement appelle alternativement par RNIS et par GSM, il faut entrer deux inscriptions dans la liste des noms pour ce collaborateur.

```
cd /Setup/WAN-module/Name-list
set Tele_01_ISDN * * * DEFAULT Name
set Tele_01_GSM * * * RAS_GSM Name
set Tele_02 * * * DEFAULT Name
```

- ⑤ Dans la liste des canaux vous pouvez déterminer combien de canaux doivent être utilisés pour un accès, et définir en option quels canaux peuvent être utilisés. Un regroupement de deux canaux doit être permis sur un accès par RNIS. Pour un accès GSM on ne disposera que d'un canal sur une autre interface :

```
cd /Setup/WAN-module/Channel-list
set Tele_01_ISDN 1 2 1-1;1-2 0
set Tele_01_GSM 1 1 2-1 0
set Tele_02 1 2 1-1;1-2 0
```



- ⑥ Étant donné que vous utilisez PPP pour accéder à l'ordinateur distant, vous pouvez définir dans la liste PPP le nom de l'utilisateur (par ex. Monsieur Toutlemonde) et le mot de passe (par ex. Distance) pour le correspondant 'Télétravailleur\_01'. Utilisez PAP comme procédure de sécurité et autorisez le routage de paquets IP et NetBIOS sur cette connexion :

```
cd /Setup/WAN-module/PPP-list
Tele_01_ISDN PAP Remote 0 0 Tele_01 IP+NTB
Tele_01_GSM PAP Remote 0 0 Tele_01 IP+NTB
```

Ici vous pouvez de nouveau affecter la même valeur aux deux inscriptions RNIS et GSM comme nom d'utilisateur. Le collaborateur correspondant pourra alors toujours s'inscrire avec le même nom. Le mot de passe 'Distance' est remplacé lors de la saisie par un \* !



*Veillez à respecter l'écriture en majuscules et en minuscules pour le nom de l'utilisateur et le mot de passe.*

- ⑦ Une inscription dans le tableau NetBIOS est également nécessaire pour le routage des paquets NetBIOS. De cette manière vous faites comprendre au routeur que des informations NetBIOS peuvent être échangées avec ce correspondant et qu'il s'agit là d'un poste de travail unique qui ne doit pas être appelé directement :

```
cd /Setup/NetBIOS-module/Remote-table
Tele_01_ISDN Workstation
Tele_01_GSM Workstation
```

- ⑧ Il ne manque maintenant plus que des adresses. Le routeur a besoin d'une adresse libre issue du réseau d'entreprise afin d'être trouvé dans son propre réseau TCP/IP. Vous l'obtenez en entrant l'adresse Intranet avec le masque de réseau associé :

```
cd /Setup/TCP-IP-module
set Intranet address 10.1.100.100
set Intranet netmask 255.255.255.0
```

- ⑨ Et l'adresse IP pour l'ordinateur appelant ? L'affectation se fait d'une manière dynamique pour la durée de la connexion à partir d'un pool d'adresses IP. Pour cela il ne sera défini que le début et la fin de la zone d'adresse. Il est donc inutile de porter une inscription dans le tableau de routage IP :

```
cd /Setup/IP-router-module
set Start-WAN-pool 10.1.100.110
set End-WAN-pool 10.1.100.120
```

- ⑩ Afin que le routeur puisse router les données pour un ordinateur distant avec une adresse issue du propre réseau logique, la fonction Proxy-ARP doit être activée.

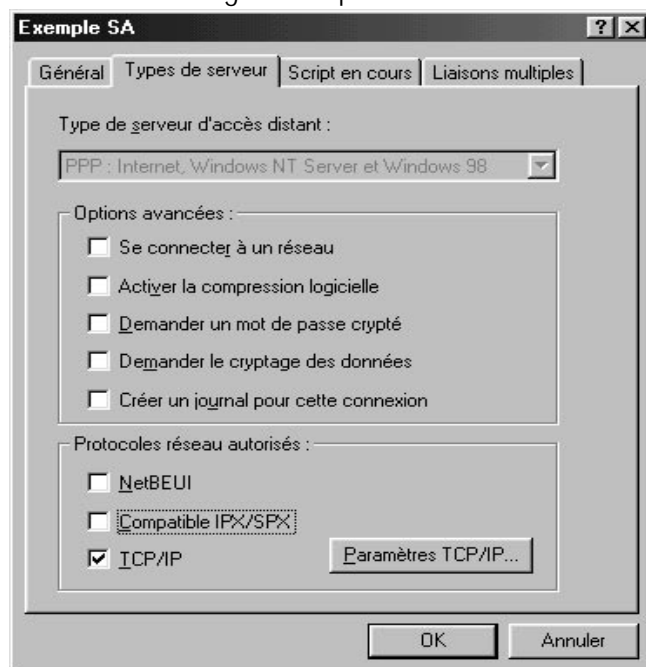
```
cd /Setup/IP-router-module  
set Proxy-ARP ON
```

- ⑪ Activez maintenant le routeur IP, et le routeur sera prêt pour l'accès par les personnels en déplacement.

```
cd /Setup/IP-router-module  
set operating on
```

- ⑫ Que reste-t-il à faire ? L'ordinateur du poste de travail du personnel en déplacement doit être configuré de manière à ce que de son côté aussi l'accès au réseau de l'entreprise soit également possible. A ces fins, les configurations suivantes sont nécessaires. Elles sont brièvement énumérées ci-après :

- Accès réseau à distance configuré correctement
- TCP/IP installé et lié à la carte d'accès réseau à distance
- Nouvelle connexion dans l'Accès réseau à distance avec le numéro d'appel du routeur
- Adaptateur terminal ou carte RNIS configurée sur PPPHDLC
- PPP choisi en guise de type de serveur d'accès à distance, 'Activer la compression logiciel' et 'Demander un mot de passe crypté' désactivés
- TCP/IP choisi en guise de protocole réseau



- Affectation de l'adresse IP et de l'adresse du nom du serveur activées, 'Utiliser la compression d'en-tête IP' désactivée



### Qu'avez-vous obtenu ?

Le collaborateur sur l'ordinateur du poste de travail à distance peut maintenant établir la connexion au réseau de l'entreprise via l'accès réseau à distance. Il entre ici le nom d'utilisateur convenu dans la liste PPP et le mot de passe correspondant.



Puis, il peut accéder aux serveurs libérés et aux réseaux Windows dans le réseau TCP/IP. Il trouvera ces serveurs avec trois clics sur **Démarrer** ► **Rechercher** ► **Ordinateur** dans la barre de Windows.

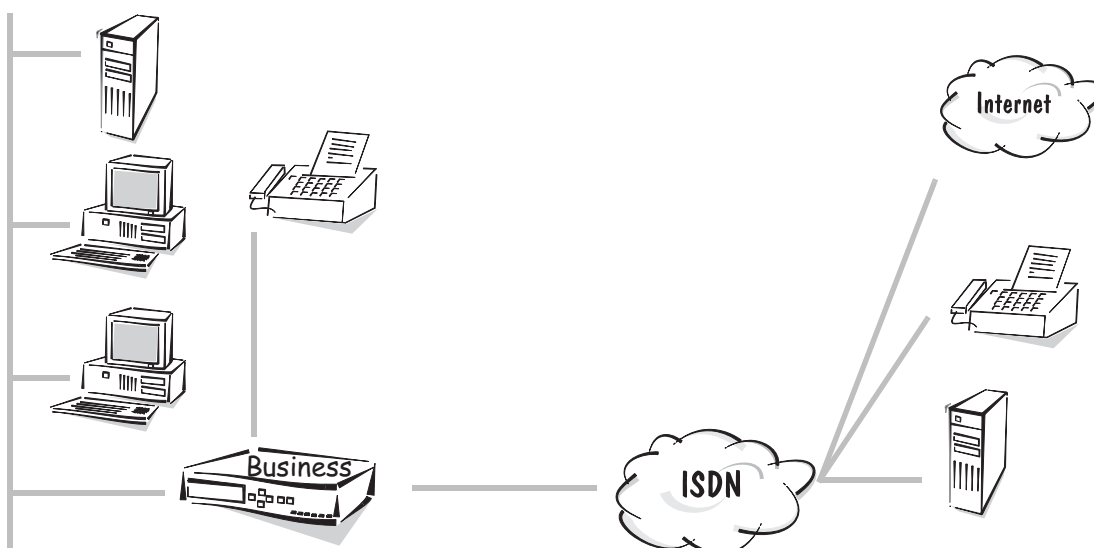
## Least Cost Router

Dans ce chapitre, nous vous montrons à l'aide d'un exemple comment à l'aide de Least Cost Router économiser une somme non négligeable sur vos factures de téléphone.

Après son réglage, le Least Cost Router recherchera automatiquement après chaque établissement d'une connexion le fournisseur d'accès le plus avantageux et essaiera d'établir la communication par son réseau.

### Exemple :

Nous prenons comme exemple un petit bureau d'ingénieurs (une agence externe d'un bureau d'études plus important) doté de deux ordinateurs aux postes de travail. Les deux ordinateurs aux postes de travail sont équipés d'un téléphone, d'un télécopieur et d'un répondeur.



Les deux collaborateurs de ce bureau utilisent aussi les fonctions suivantes d'*ELSA LANCOM Business* :

- *ELSA LANconfig* et ses assistants, vous ont permis de configurer en un rien de temps l'accès à Internet à l'aide d'un fournisseur d'accès. Le routeur IP est utilisé dans ce cas.
- L'échange de données avec la centrale se fait à l'aide d'une interconnexion LAN-LAN avec les fonctions du routeur IPX.
- Pour envoyer les messages télécopie directement depuis le PC, utilisez *ELSA-RVS-COM* à l'aide de *LANCAPI*.

Le bureau nous servant d'exemple dans ce chapitre désire naturellement effectuer de manière aussi avantageuse que possible ses connexions télécopie, Internet et comparaison de données par la centrale. Le Least Cost Router est la solution par excellence, il recherche automatiquement à chaque sélection l'opérateur le plus

avantageux. Vous trouverez des informations sur les tarifs utilisés par ex. dans les magazines, brochures ou dans Internet.

Le bureau nous servant d'exemple dispose d'un accès téléphonique du grand opérateur national. Les entrées qui suivent pour le Least Cost Router sont établies sur la base des particularités locales et à l'aide d'informations tirées d'Internet sur les zones et les tarifs.

*Veillez à ne pas appliquer obligatoirement ces entrées à d'autres situations, elles ne servent que d'exemple.*



### Configuration du Least Cost Router via *ELSA LANconfig*

Avec les étapes suivantes, vous faites de *ELSA LANCOM Business* le roi des petits prix :

- ① Dans *ELSA LANconfig*, ouvrez la configuration du périphérique en double-cliquant sur l'entrée dans la liste des périphériques et passez à la zone de configuration 'Least Cost Router'.
- ② Sous l'onglet 'Généralités', activez la fonction du LCR pour tous les modes de service offerts. Étant donné que le bureau n'a pas besoin de surveillance des coûts de communication, l'utilisation du LCR pour les modules du routeur n'est pas critique.
- ③ Traitez alors le tableau des jours fériés en choisissant l'onglet 'Plages horaires et jours fériés'.
  - Entrez d'abord les jours fériés revenant chaque année avec indication du jour et du mois mais sans l'année. Ces entrées sont positionnées automatiquement pour chaque année.
  - Entrez ensuite les jours fériés variables avec indication du jour, du mois et de l'année si possible pour les deux, trois années à venir.
- ④ Nous arrivons alors au cœur du sujet : les entrées dans le tableau LCR. Pour certaines entrées, on peut trouver plusieurs préfixes de réseau. Celles-ci sont parcourues une rangée après l'autre lorsque les numéros précédents sont occupés. Pour qu'une connexion soit établie en une fraction de seconde, le repli automatique sur le propre opérateur est activé.
- ⑤ Tout d'abord les liaisons à distance. Cette entrée vous permet de dévier toutes les liaisons à distance à l'intérieur du pays, en fonction de l'heure via un autre fournisseur d'accès :

Indicatif	Indicatif sans abonnement	Jours	Heure	Repli
0	01015	Lun – Ven	0:00 – 1:59	Oui
0	01033	Lun – Ven	2:00 – 4:59	Oui
0	01015	Lun – Ven	5:00 – 7:59	Oui
0	01050	Lun – Ven	8:00 – 8:59	Oui

Indicatif	Indicatif sans abonnement	Jours	Heure	Repli
0	01028	Lun-Ven	9:00 – 17:59	Oui
0	01015	Lun – Ven	18:00 – 23:59	Oui
0	01015	Sam, Dim, jours fériés	0:00 – 7:59	Oui
0	01050	Sam, Dim, jours fériés	8:00 – 8:59	Oui
0	01013 ; 01090	Sam, Dim, jours fériés	8:00 – 20:59	Oui
0	01015	Sam, Dim, jours fériés	21:00 – 23:59	Oui

- ⑥ Les connexions hors-circonscription vers l'étranger sont relativement rares. C'est pourquoi seule une entrée doit être valable pour toutes les connexions à l'étranger :

Indicatif	Indicatif sans abonnement	Jours	Heure	Repli
00	01015 ; 01028	tous les jours	0:00 – 23:59	Oui

- ⑦ Certains réseaux urbains à proximité de là où vous vous trouvez sont sûrement accessibles avec indicatif préalable mais au tarif urbain. Ils ne doivent pas être affectés par le reroutage des appels interurbains, c'est pourquoi ils sont à nouveau « récupérés » en laissant de côté l'indicatif de réseau. Le bureau de notre exemple est implanté dans une grande métropole. Les collaborateurs savent par Internet quels réseaux urbains font encore partie de la zone proche c'est la raison pour laquelle les entrées suivantes sont effectuées en sus :

Indicatif	Indicatif sans abonnement	Jours	Heure	Repli
02408		tous les jours	0:00 – 23:59	Oui
02464		tous les jours	0:00 – 23:59	Oui
02404		tous les jours	0:00 – 23:59	Oui
02401		tous les jours	0:00 – 23:59	Oui
02403		tous les jours	0:00 – 23:59	Oui
02454		tous les jours	0:00 – 23:59	Oui
02451		tous les jours	0:00 – 23:59	Oui
02406		tous les jours	0:00 – 23:59	Oui
02407		tous les jours	0:00 – 23:59	Oui
02429		tous les jours	0:00 – 23:59	Oui
02465		tous les jours	0:00 – 23:59	Oui

Indicatif	Indicatif sans abonnement	Jours	Heure	Repli
02423		tous les jours	0:00 – 23:59	Oui
02471		tous les jours	0:00 – 23:59	Oui
02456		tous les jours	0:00 – 23:59	Oui
02473		tous les jours	0:00 – 23:59	Oui
02409		tous les jours	0:00 – 23:59	Oui
02402		tous les jours	0:00 – 23:59	Oui
02405		tous les jours	0:00 – 23:59	Oui

Une fois la première entrée saisie, il ne vous reste plus qu'à la copier et à changer à chaque fois l'indicatif.

- ⑧ Quelques autres numéros spéciaux ne sont pas non plus affectés par le reroutage, ceci concerne entre autres les '0130', '0180', '0190' et '0800' :

Indicatif	Indicatif sans abonnement	Jours	Heure	Repli
01		tous les jours	0:00 – 23:59	Oui
0800		tous les jours	0:00 – 23:59	Oui

- ⑨ Terminé ! Votre Least Cost Router est déjà bien configuré. Au début, contrôlez le fonctionnement du LCR à l'aide d'*ELSA LANmonitor* et jetez un coup d'œil à la fin du mois sur votre facture de téléphone. Vous trouverez éventuellement à l'aide de la vue d'ensemble des connexions personnalisées quelques indicatifs que vous pourrez entrer dans le tableau LCR.



### Least Cost Router Pas à pas

Au cas où vous n'utiliseriez pas l'outil de configuration *ELSA LANconfig*, vous arrivez au même but en recourant à la configuration via Telnet (ou programme d'émulation terminal). Pour ce, effectuez les commandes suivantes :

Menu	Paramètres	Remarque ou valeur
Setup/LCR-module	Routeur-usage	Activation du module LCR pour les différents modes d'exploitation.
	LANCAPI-usage	
	Exemple	'set router on' 'set lancapi on' 'set ab-port on'
Setup/LCR-module/ Timetable	Index	Index défilant pour les entrées dans le tableau.
	Prefix	Indicatif à rerouter.

Menu	Paramètres	Remarque ou valeur
	Jours	Validité de l'entrée pour les jours de la semaine et les jours fériés par représentation d'un masque à 8 bits : le Bit 0 symbolise le lundi, le bit 7 symbolise les jours fériés. L'entrée '31' désigne quant à elle tous les jours fériés, '192' les dimanches et les jours fériés.
	Start	Début de la validité de l'entrée aux jours définis.
	Stop	Fin de validité de l'entrée pendant les jours définis.
	number-list	Indicatif de réseau du fournisseur d'accès sans abonnement.
	Fallback	Repli automatique sur le propre opérateur Télécom au cas où tous les numéros sans abonnement seraient occupés.
	Exemple	'set 1 02 31 1:00 11:59 01030;01090;01070 on' dévie tous les appels lointains dans la région '02' entre une heure et midi sur le fournisseur d'accès avec le préfixe de réseau '01030'. Si lui aussi est occupé, les préfixes de réseau '01090' et '01070' sont contactés. S'ils ne sont pas disponibles, la connexion via la société de téléphone normale est établie.

Suivez ce modèle pour toutes les entrées requises et reportez-vous aux tableaux pour la configuration via *ELSA LANconfig*.



# Appendice

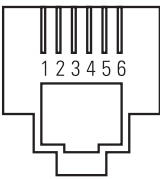
Cet appendice contient en plus des données techniques, l'affectation des connecteurs ainsi que les conditions générales de garantie.

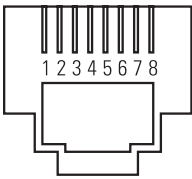
## Caractéristiques techniques

Modes de fonctionnement :	Routeur IP, routeur IPX, serveur CAPI, Serveur DHCP ; Least Cost Router pour liaisons routeur et CAPI, possibilité d'utilisation simultanée de tous les modes de fonctionnement
Connexion LAN :	Ethernet IEEE 802.3, 10/100Base-TX (RJ45, Node/Hub, Switch), auto-sense, mode Full-Duplex
Protocoles de réseau :	IP-router : IP, TCP, ICMP, ARP, RIP-1, RIP-2, PROXY ARP, DHCP routeur IPX : RIP, SAP, Novell NetBIOS, mode Novell-Burst
Possibilités de filtrage :	IP-router : Filtrage de port TCP, UDP, filtres de réseaux source et destination IPX-Router : RIP, SAP, chiens de garde IPX et SPX, Sockets, Propagated Packets
Spoofing :	IPX-router : RIP- et SAP-Packets ; chiens de garde IPX et SPX, Novell NetBIOS, Keep-alive-Packets
Interface RNIS :	Connexion : Bus RNIS-S0, configuration point à point et point à multipoint, I.430 Canal D : 1TR6, Euro-RNIS (DSS1), auto-sense, liaisons fixes groupe 0 (D64S, D64S2, D64SY) Canal B : PPP (asynch./synch.), MLPPP, X.75, HDLC, V.110, CAPI 2.0 par ELSA LANCAPI, compression de données Stac
Serveur I-CAPI :	CAPI 2.0 virtuelle pour systèmes d'exploitation Windows, gestionnaire NDIS-WAN, Fax-classe 1
Commande de ligne :	Rappel automatique avec ou sans établissement de communication ; Line-on-Demand (regroupement dynamique des canaux), mode Short-Hold, sélection RoundRobin, Fast Call Back, Dial-Backup pour liaisons fixes
Contrôle des coûts de communication :	Détermination du nombre maximum d'unités de tarification dans une certaine durée
Fonctions Security et Firewall :	Evaluation du numéro d'appel du correspondant ; PAP et CHAP, mécanismes d'authentification dans PPP ; rappel Firewall automatique par protocole CLIP, PPP ou ELSA ; possibilités de filtrage en mode IP, IPX Bridge ; protection de la configuration par listes d'accès et mot de passe, entrée des dernières informations de communication, Masquerading IP, chiffrement en préparation.
IP-masquerading :	(NAT/PAT) Conversion d'adresse et de port IP par une adresse IP, affectation statique/dynamique de l'adresse IP par PPP, masquage de TCP, UDP, ICMP, FTP ; DNS-Forwarding ; masquerading inverse pour services IP dans l'Intranet
Management :	Via LAN, ISDN (télémaintenance) ou V.24, logiciel de management ELSA LANconfig et ELSA LANmonitor pour Windows, configuration possible par SNMP v.1, TFTP, Telnet ou terminal
Sécurité d'exploitation :	Chiens de garde matériel, autotests permanents, concept FirmSafe pour mise à jour à distance du logiciel

Statistiques :	Compteur de paquets LAN et WAN, compteurs d'erreurs, de connexions, de durée et d'unités
Affichages/ Manipulation :	Affichage LCD et clavier, LED affichant l'état LAN et WAN
Alimentation :	12 V AC avec alimentation secteur enfichable pour 230 V, 12 VA
Conditions ambiantes :	Température : 5..40°C, humidité relative : 0..80%, sans condensation
Boîtier et dimensions :	Boîtier métallique robuste, raccordements sur l'arrière ; dimensions 230 x 38 x 228 mm (l x h x p)
Contenu du coffret :	Accessoires : Alimentation secteur, câble de raccordement RNIS, câble pour interface Outband, câble Twisted-Pair (CAT-5), documentation détaillée et CD ROM ELSA LANCOM logiciel : ELSA LANconfig, ELSA LANmonitor, ELSA LANCAPI, TFTP-Client, Logiciel de communication bureautique ELSA RVS-COM, programme de terminal ELSA-ZOC, logiciel de télémaintenance LapLink pour Windows, T-Online, CompuServe
Homologations :	pour l'Allemagne, la Suisse et en préparation pour tous les pays de l'UE
S.A.V. et garantie :	Garantie de 6 ans, ELSAcare (remplacement dans les 100 premiers jours)
Support :	par Hotline, ELSA LocalWeb et Internet

## Affectation des connecteurs :

Raccordement enfichable	Broche RJ11	Ligne
 Ports a/b – RJ11	1	libre
	2	libre
	3	a
	4	b
	5	libre
	6	libre

Raccordement enfichable	Broche RJ45	Ligne	Conjoncteur RNIS
 RNIS – RJ45	1	libre	libre
	2	libre	libre
	3	T+	2a
	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	libre	libre
	8	libre	libre

## Conditions générales de garantie du 01.06.1998

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

### 1 Objet de la garantie

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

### 2 Durée de la garantie

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

### 3 Modalités

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

### 4 Application de la garantie

La garantie est exclue dans les cas suivants :

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

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

## **5 Erreurs de manipulation**

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

## **6 Conditions complémentaires**

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

# Déclaration de conformité



## KONFORMITÄTSERKLÄRUNG

### DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

<b>Geräteart:</b>	<b>ISDN Router</b>
Type of Device:	
<b>Typenbezeichnung:</b>	<b>ELSA Lancom Business</b>
Product Name:	
<b>EG-Baumusterprüfbescheinigungs Nr.:</b>	<b>D801080L</b>
Registration No.:	
<b>Benannte Stelle:</b>	<b>CETECOM ICT Services GmbH</b>
Notified Body:	<b>CE 0682 X</b>

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/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: 1992 Teil 2: 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, 8<sup>th</sup> February 1999

i.V. Peter Wieninger  
Bereichsleiter Entwicklung  
VP Engineering



# Glossaire

- **100BaseTX.** Paire torsadée ; variante de connecteurs Fast-Ethernet 100 Mbits ; raccordement au réseau avec connecteur RJ45
- **10Base2.** Thin Ethernet ; Cheapernet ; variante de connecteurs Ethernet 10 Mbits ; raccordement au réseau avec connecteur BNC
- **10Base5.** Thick Ethernet ; variante de connecteurs Ethernet 10 Mbits ; raccordement au réseau avec connecteur AUI ou SUB-D 15 points
- **10BaseT.** Paire torsadée ; variante de connecteurs Ethernet 10 Mbits ; raccordement au réseau avec connecteur RJ45
- **1TR6.** Version allemande du RNIS ; protocole du canal D anciennement répandu dans le RNIS allemand ; ce protocole n'est plus installé que sur demande spéciale auprès de Deutsche Telekom.
- **Accès de base.** Raccordement élémentaire au RNIS avec deux →canaux de base (de 64.000 bit/s chacun) et un canal de signalisation (16.000 bit/s). Le point de référence de l'accès de base côté abonné est l'interface →S<sub>0</sub>.
- **Adresse IP.** 1ère partie de l'adresse par laquelle un composant réseau se fait connaître dans un réseau TCP/IP.
- **Adresse IPX.** Formée par → l'ID de noeud, l'adresse de réseau IPX et le Socket ; sert à identifier un composant réseau au sein d'un réseau IPX.
- **ARP.** Address Resolution Protocol est un protocole de la →famille de protocoles TCP/IP.
- IP. ARP mappe les adresses IP sur les adresses MAC correspondantes.
- **AUI.** Attachment Unit Interface = interface pour les connexions réseau générales.
- **BNC.** Technique de connectique courante pour Cheapernet (Thin-Ethernet). Ce raccordement est aussi appelé T-BASE2. Pour raccorder des périphériques ayant une douille BNC, il faut utiliser des joncteurs en T.
- **Canal B.** Canal de transmission de données dans le RNIS (64 Kbits) ; un accès de base du RNIS a 1 canal D et 2 canaux B.
- **Canal D.** Canal de signalisation dans le RNIS (numérotation, transmission du numéro d'appel, informations sur les coûts de communication, raccrochage) ; un accès de base a un canal D et 2 canaux B.
- **Canal de signalisation.** Le canal de signalisation permet de transmettre des informations de service, telles que l'identification de l'appelant etc., entre l'accès RNIS et l'autocommutateur avec un débit de 16.000 bit/s pour les →accès de base ou de 64.000 bit/s pour les accès →primaires multiplexés. Le canal de signalisation est également appelé canal D.
- **CEPT.** Conférence Européenne des Postes et des Télécommunications. Comité établissant des normes de télécommunication.
- **Chien de garde IPX.** IPX-Watchdog. Paquets envoyés périodiquement par le serveur pour surveiller une station de travail. Si la station de travail ne répond pas, elle est déconnectée automatiquement.

- **Chien de garde SPX.** SPX-Watchdog. Paquets envoyés périodiquement par le serveur pour surveiller une connexion SPX.
- **Client.** Client = poste de travail. Un client est un utilisateur d'un service proposé par un →serveur.
- **CLIP.** Caller Line Identification Parameter = numéro d'appel de l'appelant, pouvant être transmis en même temps que la voix ou les données dans le RNIS.
- **Compression de données.** Méthode de réduction du volume de données à transmettre. La compression des données permet d'augmenter le débit dans les voies de télécommunication (procédés courants : V.42bis, STAC, MPPC)
- **Compression STAC.** Méthode de compression des données
- **Configuration hors bande.** Dans le cas de la configuration hors bande (Outband, Out-of-Band), l'échange de données avec le périphérique à configurer se fait via une interface série V.24. La connexion pendant la configuration est maintenue même en cas de perturbation d'un accès réseau.
- **Connexion en Y.** Connexions simultanées avec deux correspondants différents dans un canal B chacune du même accès  $S_0$ .
- **Couche.** (Voir le modèle de référence OSI). Couche d'une connexion à structure modulaire entre deux systèmes communicants.
- **Coupe-feu.** Mécanisme de protection dans un Intranet permettant de se protéger contre les accès de l'extérieur ; le *ELSA LANCOM* prend en charge les mécanismes de coupe-feu suivants : IP-Masquerading, filtrage des ports, liste d'accès.
- **Diffusion.** Configuration dans laquelle les paquets de données sont envoyés simultanément à plusieurs stations. Dans les réseaux Ethernet, ces paquets de données sont caractérisés par l'adresse de destination FFh FFh FFh FFh FFh FFh (c'est-à-dire à tous).
- **Diffusion restreinte.** Les paquets à diffusion restreinte (multicast) sont des paquets envoyés simultanément à toutes les stations faisant partie d'un groupe.
- **DNS.** Domain Name Server. Désigne un serveur mettant à disposition un service de noms pour chaque ordinateur d'un →domaine. Suite à une requête auprès de ce serveur, un autre ordinateur ne connaissant que le nom symbolique de sa destination peut apprendre l'adresse IP correspondante.
- **Domaine.** (angl. : Domain) Un domaine désigne un réseau logique limité, par ex. un réseau d'entreprise ou un fournisseur d'accès Internet.
- **DSS1.** Euro-ISDN ; protocole de canal D qui s'est établi actuellement dans le RNIS.
- **EAZ.** Utilisé par le protocole 1TR6, l'EAZ, le chiffre de sélection du terminal, permet de distinguer des terminaux différents raccordés au même →accès de base. Ce chiffre est collé au dernier chiffre du numéro d'appel.
- **Ethernet.** Un réseau Ethernet est un →système de bus avec →accès CSMA/CD et →transfert dans la bande de base. Ce réseau local a été développé en 1979 par les sociétés DEC, Intel et Xerox. Etant l'un des premiers réseaux locaux →LAN, il est devenu un standard de facto, et a été adopté par l'IEEE (Institute of Electrical and Electronics Engineers) qui en a fait une norme (norme 802.3). La transmission des données utilise des câbles coaxiaux, des paires torsadées,



des fibres optiques ou d'autres supports avec 10 Mbits par seconde.

- **ETSI.** European Telecommunications Standards Institute = Institut européen pour les normes de télécommunication. Cet organisme de normalisation a créé une norme européenne pour le protocole du canal D (DSS1).
- **Flash-ROM.** Le flash-ROM est une mémoire morte effaçable et reprogrammable. Les flash-ROM sont souvent employés dans les appareils dont le microprogramme peut être amélioré par des mises à jour.
- **HDLC.** High Level Data Link Control. Format d'un paquet de données sécurisé par un calcul de redondance cyclique CRC.
- **HOPS.** Nombre de routeurs via lesquels une connexion réseau est établie.
- **Hub.** Composant réseau encore appelé concentrateur, permet de répartir une entrée réseau sur plusieurs sorties pour réaliser une topologie en étoile.
- **Identificateur de noeud.** Adresse MAC
- **Interface S<sub>0</sub>.** Interface de l'accès de base côté abonné. Il s'agit d'un bus auquel on peut relier jusqu'à huit terminaux RNIS. On peut installer sur ce bus jusqu'à douze prises.
- **Interface V.24.** Interface série, servant par ex. à connecter un modem. Le *ELSA LANCOM* possède une interface V.24 afin de pouvoir effectuer des transferts de données sur une ligne analogique au moyen d'un modem.
- **INTERNET.** L'Internet est le maillage de tous les réseaux interconnectés via →TCP/IP.
- **Intranet.** Domaine ; réseau limité par ex. à une seule entreprise et où les accès de

l'extérieur ou vers l'extérieur sont strictement réglementés.

- **IP.** IP = Internet Protocol. Famille de protocoles développée au début des années 70 par le Ministère de la défense américain (DoD, Department of Defence) servant à interconnecter des réseaux étendus (WAN) hétérogènes.
- **IP-masquerading.** Single IP-Address ; Port Address Translation. Procédure utilisée pour relier un Intranet (plusieurs stations de travail) à l'Internet via une seule adresse IP ; le *ELSA LANCOM* maîtrise cette technique.
- **IPX.** Internet Packet eXchange = protocole de transmission défini par Novell pour la transmission de données dans un autre réseau. Sur un PC, ce protocole est réalisé par le pilote IPX.COM ou la shell →VLM.
- **ISDN.** Integrated Services Digital Network = Traduction anglaise de RNIS.
- **ISO.** International Standardization Organization. L'ISO est une organisation internationale qui coordonne le développement de normes internationales – pour tous les champs d'application – et se charge de leur publication. Leurs membres sont les comités de normalisation nationaux tels que l'AFNOR (France), le DIN (Allemagne), l'ANSI (Etats-Unis), le BSI (Grande-Bretagne).
- **ITU-T.** Le secteur de normalisation Télécommunication de l'Union Internationale des Télécommunications (UIT - en anglais ITU : International Telecommunications Union) se charge du développement de normes internationales en matière de transmission de la voix et de transmission de données. Les recommandations de la série V. de l'ITU-T portent sur la transmission de données dans les réseaux téléphoniques.

L'ITU-T succède au CCITT (Comité Consultatif International Télégraphique et Téléphonique).

- **LAN.** Local Area Network = réseau local. Selon l'→ISO, un réseau local est un réseau se trouvant dans l'enceinte d'un terrain sous contrôle juridique de l'utilisateur et servant à la transmission de bits d'information entre ses éléments indépendants et connectés entre eux. Un réseau local est donc un réseau géographiquement très restreint qui est installé la plupart du temps dans un immeuble ou au siège d'une société.
- **Liaison spécialisée.** Une liaison spécialisée est une connexion (active) permanente entre deux participants. Cette liaison ne peut être utilisée que par ces deux participants.
- **Line-on-Demand.** Etablissement d'une connexion à la demande. Dans le cas du *ELSA LANCOM*, le contenu de paquets de données reçus en provenance du réseau local décide de l'établissement d'une connexion.
- **MAC.** Media Access Control. Sous-couche de la couche 2 du modèle de référence OSI défini par l'→ISO. Dans les réseaux Ethernet, l'adresse source et l'adresse de destination ainsi que le type de protocole font partie des données de la couche MAC.
- **Masque de réseau IP.** 2ème partie de l'adresse par laquelle un composant réseau se fait connaître dans un réseau TCP/IP.
- **Mode rafale.** Le mode rafale est un type spécial du transport des paquets dans les réseaux Novell. Plusieurs paquets sont envoyés l'un à la suite de l'autre sans acquittement de réception.
- **MPPC.** Microsoft Point to Point Compression. Méthode de compression de données (n'est pas pris en charge actuellement par le *ELSA LANCOM*).
- **MPR.** Multi-Protocol-Router. Routeur capable de router divers protocoles (comme le *ELSA LANCOM Business 4100*).
- **MSN.** Multiple Subscriber Number = numéro d'abonné multiple. Le protocole DSS1 permet d'attribuer plusieurs numéros d'appel RNIS à un abonné. En règle générale, il s'agit de trois numéros, huit au maximum. Grâce à eux, les terminaux reliés à l'interface S<sub>0</sub> peuvent être adressés de manière ciblée. Alors que l'EAZ (1TR6) est un chiffre attaché au numéro d'abonné, le MSN peut se composer de seize chiffres au maximum.
- **Multilink-PPP.** MLPPP ; procédure de regroupement des canaux sous PPP ; (actuellement, le *ELSA LANCOM* ne prend pas en charge cette procédure).
- **NBNS.** NetBIOS Name Server = serveur de noms NetBIOS. Désigne un serveur mettant à disposition un service de noms pour chaque ordinateur d'un →domaine. Suite à une requête auprès de ce serveur, un autre ordinateur ne connaissant que le nom symbolique de sa destination peut apprendre l'adresse correspondante.
- **NETX.** NETX = shell NetWare. Ce programme représente une interface entre les logiciels d'application et le système d'exploitation d'un réseau Novell.
- **Noeud.** Angl. = Node. Un noeud est un périphérique, raccordé au réseau, pouvant envoyer et recevoir des données. Il peut s'agir de *ELSA LANCOM*, d'ordinateurs, de serveurs ou d'imprimantes adressés par plusieurs utilisateurs du réseau.
- **Novell.** Constructeur du système d'exploitation de réseau Novell NetWare

- **OSI.** Open System Interconnection = interconnexion de systèmes ouverts. Modèle de référence développé pour les réseaux par l'→ISO (International Standardization Organization) établissant les normes des interfaces assurant les échanges entre systèmes hétérogènes.
- **Paquet.** Un paquet comprend un certain nombre de caractères (caractères de commande) imposé par le réseau de données pour véhiculer les données.
- **Passerelle.** Composant réseau permettant d'accéder au niveau d'une couche du → modèle OSI à d'autres composants réseau (par ex. à la couche 3 dans Windows).
- **Ping.** Commande via ICMP. Comparable au ping (écho-sonde) des sous-marins, cette commande permet de mesurer la distance des composants réseau dans un réseau TCP/IP.
- **Pont.** Un pont (Bridge) est une jonction entre deux réseaux ayant la même structure de la couche 2 selon le → modèle OSI. Un tel pont peut être composé de deux périphériques reliés entre eux par un segment de transmission de données. Cette topologie est appelée pont distant.
- **PPP.** Point to Point Protocol = protocole point-à-point ; famille de protocoles (LCP, IPCP, IPXCP, CBCP, ECP, CCP etc.). Le protocole PPP permet de négocier les paramètres de communication des connexions point-à-point entre les composants réseau (par ex. le rappel automatique, les protocoles réseau, la compression).
- **Protocole.** Les protocoles servent à établir et à maintenir des connexions (réseau, RNIS, modes de transmission analogiques). Il s'agit d'un dialogue entre les composants connectés.
- **Proxy-ARP.** Avec Proxy-ARP, les stations qui sont normalement connectées directement à un réseau local TCP/IP et qui possèdent donc une adresse IP locale peuvent aussi être jointes via un routeur (donc via un réseau étendu). Pour une requête ARP dans le réseau local, le routeur se fait passer pour le périphérique distant, il dévoile donc sa propre adresse MAC. Il peut ensuite recevoir les paquets de données et les envoyer vers le correspondant distant.
- **Regroupement des canaux.** Regroupement des deux canaux B du RNIS formant une connexion logique pour doubler la vitesse de transmission.
- **Regroupement dynamique des canaux.** Band-with-on-Demand ; suivant les besoins, la bande passante est augmentée en ajoutant automatiquement le deuxième canal B (ou davantage).
- **Réseau.** Un réseau est un système multi-utilisateurs et multifonctions formé par un groupe d'ordinateurs et de terminaux reliés entre eux par un câblage, permettant l'utilisation commune des informations et des ressources.
- **RIP.** Routing Information Protocol. Dans les réseaux (dans ce cas Netware-IPX), sert à propager les informations pour les routeurs.
- **RoundRobin.** Procédure servant à accéder à un correspondant logique (par ex. la centrale d'un groupe industriel) au moyen de divers numéros d'appel de périphériques différents. Lorsque le correspondant par défaut est occupé, les autres correspondants libres sont appelés automatiquement.
- **Routeurs.** Un routeur est un boîtier permettant de connecter deux réseaux ayant la même structure de la couche 3 selon le → modèle OSI. Un tel routeur peut être

composé de deux périphériques reliés entre eux par un segment de transmission de données. Cette topologie est appelée routeur distant.

- **RTS.** Request to Send = requête pour émettre. Active le composant chargé de l'envoi des données.
- **SAP.** Service Advertising Protocol. Dans les réseaux NetWare, est utilisé pour diffuser les services.
- **Serveur.** Un serveur met des services à la disposition d'un →client. De nombreux systèmes d'exploitation réseau ont une architecture client-serveur, c'est-à-dire qu'un ordinateur très performant et à grosse capacité de stockage fonctionnant comme serveur fournit à un grand nombre de clients (ordinateurs individuels, stations de travail) les données et les programmes.
- **Short Hold.** Au bout d'une durée définie à l'avance, une connexion est coupée si des données ne sont plus transmises. Une connexion peut donc être maintenue pendant un certain délai jusqu'à ce qu'on soit sûr que plus aucune information ne doit être transmise.
- **SNMP.** Simple Network Management Protocol. Protocole normalisé servant à gérer les composants réseau. Avantage : contrôle de plusieurs composants réseau au moyen de la même interface utilisateur (par ex. HP-Openview ou Cabletron-Spectrum) ; indépendant d'un constructeur ; le *ELSA LANCOM* prend en charge SNMP Version 1.
- **Socket.** Numéro d'identification désignant le service sous lequel un paquet de données est envoyé.
- **Solution autonome.** Le *ELSA LANCOM Business 4100* est une solution autonome,

aucun ordinateur supplémentaire ni logiciel sur un serveur n'étant requis pour l'intégrer dans un réseau (comme c'était le cas pour les routeurs ordinaires), c'est-à-dire qu'il est un composant réseau à part entière.

- **Spoofing.** Le spoofing est une méthode permettant d'éviter des coûts de communication inutiles. Le routeur répond directement aux requêtes venant du réseau local, sans qu'une connexion soit établie pour l'envoi de données au correspondant.
- **SPV (1TR6).** SPV = liaison semi-permanente. Ligne commutée permanente commandée à l'avance. Une liaison semi-permanente est proposée pour le protocole →1TR6. Elle peut être mise en place entre deux accès RNIS, séparément pour chaque canal B. Dès que la liaison semi-permanente est active, la communication n'est plus facturée selon la consommation, mais selon un forfait mensuel. Cette procédure permet d'économiser des coûts de communication.
- **SPX.** Sequenced Packet eXchange = protocole défini par Novell pour la transmission sécurisée de données dans le réseau. Sur un PC, ce protocole est réalisé par le pilote NETX.COM (ou similaire).
- **TCP/IP.** Transmission Control Protocol/Internet Protocol. Famille de protocoles développée au début des années 70 par le Ministère de la défense américain (DoD, Department of Defence) servant à interconnecter des réseaux étendus (WAN) hétérogènes. Les deux fondements de cette famille de protocole sont IP qui implémente la couche 3 du →modèle OSI, ainsi que TCP, son pendant pour la couche 4.
- **Telnet .** Telnet est un protocole de la famille de protocoles →TCP/IP. Il permet l'accès à distance d'une station de travail à un autre

ordinateur se trouvant dans le réseau. Le protocole Telnet utilise pour la transmission de données le protocole →TCP, car il requiert une communication bidirectionnelle sécurisée. Ceci permet de mettre à la disposition d'un client Telnet un terminal virtuel sur l'hôte Telnet.

- **TFTP.** Trivial File Transfer Protocol. Protocole simple pour le transfert d'un fichier (par ex. le téléchargement d'un microprogramme, sauvegarder/restaurer un fichier).

- **TICS.** Unité de temps système du *ELSA LANCOM*

- **Transceiver.** Récepteur-émetteur = convertisseur de signaux. Un transceiver ou récepteur-émetteur est un appareil qui transforme un format de signal d'entrée en un format de sortie différent.

- **Transmission asynchrone.** Dans une transmission de données sérielle, il faut une procédure de synchronisation entre émetteur et récepteur qui permet au récepteur de détecter le début et la fin d'un caractère transmis. A cet effet, chaque octet à émettre dans une transmission asynchrone est caractérisé par un bit de départ et un ou deux bits d'arrêt. Ce procédé départ-arrêt (Start-Stop) est l'un des plus utilisés en matière de transmission, en particulier en micro-informatique, dans la mesure où, contrairement à la transmission synchrone, il est techniquement assez simple à réaliser.

- **Transmission synchrone.** La transmission synchrone est, comme la transmission →asynchrone, une procédure destinée à mettre le récepteur et l'émetteur en phase. A l'inverse de la transmission asynchrone, la synchronisation n'est pas réalisée par des bits Start et Stop, mais par des impulsions d'horloge constantes pour chaque bit. Le fait

de ne pas transmettre de bits Start et Stop rend la transmission synchrone plus rapide, mais techniquement ce mode est nettement plus contraignant à réaliser.

- **UDP.** User Datagram Protocol. Contribue à la transmission des données de certains services dans les réseaux IP, mais n'est, à l'inverse de TCP, pas sécurisé.

- **UNIX.** UNIX est un système d'exploitation pour micro-ordinateurs, ordinateurs moyens et supercalculateurs développé par AT&T.

- **V.110.** Recommandation de l'→ITU-T servant à adapter les flux de données asynchrones et synchrones au taux de transfert de 64 Kbits/s du RNIS pour pouvoir acheminer les données dans le →canal B du RNIS (également appelé I.463).

- **V.42bis.** Recommandation de l'→ITU-T servant à comprimer les données envoyées par un modem.

- **VLM.** Virtual Loadable Module. Ce programme représente l'interface entre les logiciels d'application et le système d'exploitation d'un réseau Novell.

- **WAN.** Wide Area Network. Réseau étendu longue distance, incluant par ex. les connexions avec des terminaux RNIS.

- **Workstation.** Traduction anglaise de station de travail, donc d'un ordinateur installé au poste de travail de l'utilisateur.

- **X.75.** Recommandation de l'→ITU-T portant sur la transmission sécurisée de données dans le →canal B du RNIS selon la procédure HDLC.

- **XModem.** XModem est un →protocole de transmission avec détection et correction automatiques des erreurs. La transmission s'effectue par blocs de 128 octets. Si une erreur de transmission est détectée, le bloc défectueux est envoyé une nouvelle fois. XModem fait partie des protocoles les plus utilisés. Il est implémenté dans de nombreux émulateurs de terminal courants. Il a été dépassé entre-temps par des protocoles plus évolués et plus efficaces tels que ZModem.

# Index

## ■ Numerics

10/100Base-TX .....	10
100BASE-T .....	R-48
1TR6 .....	3, R-40
802.2 .....	R-50
802.3 .....	R-50

## ■ A

Accès à configuration .....	19
Accès à distance .....	2, 17, 56, 92, 132
Accès à distance avec TCP/IP .....	132
Accès commuté .....	98
Accès Internet .....	57
Accès réseau à distance .....	13, 17, 38
Access-list .....	R-59
Adaptateur .....	14
Address pool .....	R-70
Address ranges .....	R-62
Adressage .....	91
Adressage IPX .....	62
Adresse d'arrivée .....	81
Adresse de départ .....	81
Adresse Internet .....	77
Adresse Intranet .....	77
Adresse IP .....	16, 33, 39, 56
Adresse IP fixe .....	115
Adresses IP .....	7, 98
Adresses IP enregistrées .....	111
Affectation des adresses .....	16
Affichage de l'état .....	4
Affichage des canaux .....	33
Afficheur .....	4
Aging-minute(s) .....	R-54, R-56
AOCD .....	4, 40
Appels internationaux .....	103
Appels longue distance .....	104
Applications Internet .....	110
APPP .....	R-44
ARP cache .....	R-60
ARP-aging-minute(s) .....	R-60

Assistant de configuration .....	14
Asynchronous PPP .....	R-44
Attaques en force brute .....	5, 36
Auth. ....	R-45
Authentification .....	59
Automode .....	80, R-70

## ■ B

Backoff .....	R-53
BACP .....	3
Bancatque .....	1
B-channel protocols .....	R-43
Binding .....	R-50
Boot system .....	R-82
Budget en fonction de la durée .....	40
Buffers .....	R-48
Bureautique .....	98

## ■ C

Câble RNIS .....	3
Cache .....	R-60
Call numbers .....	R-46
Callback .....	R-41, R-46, R-48
Callback options .....	R-42
Call-by-Call .....	104, R-77
Calling Line Identification Restriction ....	R-40
Canal B .....	33
Etat de la liaison .....	4
Canal D .....	38
CAPI Faxmodem .....	102
Caractères joker .....	90
Caractéristiques techniques .....	143
CBCP .....	58
CE .....	10
Challenge Handshake Authentication Protocol .....	38, R-45
Channel bundling .....	R-44
CHAP .....	38, R-45
Charge .....	R-42
Charger le logiciel .....	22
Charges .....	R-50, R-55

- Charging information ..... R-41
  - Charging unit ..... R-41
  - Chiens de garde (Watchdogs) IPX ..... 68
  - Chiens de garde (Watchdogs) SPX ..... 68
  - CLI ..... 38, R-46
  - Client LANCAPi ..... 99
  - Client pour réseaux Windows ..... 93
  - Client PPP ..... 18
  - CLIP ..... 5
  - CLIR ..... R-40
  - Common ISDN Application Programming Interface ..... 98
  - Communautés ..... 26
  - Communication urbaine ..... 105
  - Commutateur Node/Hub ..... 10
  - Compatibility ..... R-43
  - Compression ..... 3
  - Compression de données LZS ..... 61
  - Compression de données Stac ..... 3
  - Compte Internet ..... 110
  - Compuserve ..... 91
  - Compuserve select ..... 92
  - Conditions Inband ..... 16
  - Conditions Outband ..... 14
  - Config-aging-minute(s) ..... R-75
  - Configuration ..... 5
    - Instructions ..... 21
    - Procédés ..... 13
    - SNMP ..... 26
  - Configuration à distance ..... 6, 13
  - Configuration de l'accès à Internet ..... 111
  - Configuration de la liaison permanente ..... 49
  - Configuration Inband ..... 13
  - configuration options ..... R-74
  - Configuration Outband ..... 13, 14
  - Configuration point-à-multipoint ..... 3
  - Configuration point-à-point ..... 3
  - Configuration WINS ..... 84
  - Connect ..... R-47
  - Connection time-outs ..... R-41
  - Connector ..... R-48
  - Connexion à distance ..... 18
  - Connexion à un réseau étendu WAN ..... 3
  - Connexion à un réseau local ..... 3
  - Connexion en Y ..... 61
  - Connexion par réseau ..... 1
  - Connexion PPP ..... 13, 19
  - Control outputs ..... 93
  - Contrôle des accès ..... 36
  - Contrôle des coûts de communication .. 4, 99
  - Correspondants NetBIOS ..... 92
  - Couche de communication ..... 50
  - Coupe-feu ..... 5, 99, 110, 111
  - Couplage LAN-LAN ..... 2
  - Courrier électronique ..... 2
  - Coûts de communication ..... 91
- D**
- D64S ..... 49
  - D64S2 ..... 49
  - D64SY ..... 49
  - Data compression ..... R-44
  - DDI numbers ..... R-43
  - Débit ..... 60
  - Default Layer ..... 19
  - Default route ..... R-63
  - Dépannage ..... 32
  - Destination network ..... R-61
  - Destination port ..... R-63, R-64
  - Device names ..... R-41
  - DHCP ..... 7, 80, R-70
  - DHCP pour résolution WINS ..... 84
  - DHCP server ..... R-70
  - DHCP-Automode ..... 80
  - Dial prefix ..... R-42
  - Dialup-remote ..... R-41
  - Disconnect ..... R-47
  - Disponibilité ..... 101
  - Distance ..... 69
  - DNS ..... 79, 87, R-59
  - DNS forwarding ..... R-60
  - DNS queries ..... R-64
  - DNS-backup-IP-address ..... R-60
  - Domain Name Service ..... 79, 87
  - Domaines ..... 87
  - DSS1 ..... 3, R-40



Dst-address ..... R-64  
 Dst-netmask ..... R-64  
 Durée de communication ..... 4  
 Durée de validité ..... 80, 83  
 Dynamic assignment of the IP address .. R-61  
 Dynamic bundling ..... R-41  
 Dynamic Host Configuration Protocol ..... 80  
 Dynamic IP routing table ..... R-67  
 Dynamic short-hold ..... R-41

## E

Echange PPP ..... 19  
 Economies sur la facture de téléphone .... 105  
 Ecran ..... 8  
 Éditions des tracés ..... 30  
 ELSA CAPI Faxmodem ..... 6  
 ELSA-RVS-COM ..... 3  
 ELSA-ZOC ..... 3  
 Émulateur de terminal ..... 14  
 Encaps ..... R-43  
 End-address-pool ..... R-70  
 Envoi de télécopies ..... 103  
 Espace d'adressage ..... 91  
 Etablissement d'une connexion ..... 91  
 Etats de service ..... 8  
 Ethernet ..... 3, R-43  
   10/100Base-T ..... 3  
   Fast Ethernet ..... 3  
 Ethernet packet format ..... R-50  
 Exponential backoff ..... R-53  
 Extensions LCP PPP ..... 60

## F

Fast callback ..... 39  
 Fast callback procedure ..... R-42  
 Fast Ethernet  
   10/100Base-T ..... 3  
 Fast-Ethernet ..... 3  
 Fax Class 1 ..... 7, 102  
 Fax-modem  
   LANCAPI ..... 103  
 Faxmodem ..... 6  
 Filtre ..... 37  
 Filtre de Socket ..... 67

Filtre IP ..... 92  
 Filtres ..... 2, 121  
 Firewall function ..... R-64  
 Firmsafe ..... 6, 22, R-81  
 Firmware ..... R-80  
 Firmware upload ..... R-80  
 Fonction de coupe-feu ..... 39  
 Fonctions de sécurité ..... 2  
 Fournisseur d'accès Internet ..... 1  
 Frais de téléphone élevés ..... 40

## G

Gestion d'adresses ..... 80  
 Gestion des communications ..... 40  
 Gestion des lignes ..... 2, 121  
 Gestion des priorités ..... 102  
 Gestion multicanaux ..... 4  
 Gestionnaire ..... 28  
 Group table ..... R-73  
 Groupes ..... 91  
 GSM ..... 7

## H

HDLC packets ..... R-44  
 HDLC56K ..... R-44  
 HDLC64K ..... R-44  
 Heure ..... 104  
 Heure du réseau RNIS ..... 107  
 Heure du RNIS ..... 5  
 Horloge ..... 107  
 Horloge interne ..... 107  
 Host table ..... R-73  
 Hôte ..... 87  
 Hyperterminal ..... 14

## I

ICMP ..... R-64, R-66, R-68  
 Identification ..... 93, R-38  
 Identification de l'appelant ..... 37  
 Identification du numéro de l'appelant ..... 5  
 Inband ..... 13, 16  
   Avec Telnet ..... 17  
 Indicatif ..... 104  
 Informations de facturation ..... 61

Informations sur le nom ..... 91  
 Installation ..... 3  
 Installation du serveur Web dans Internet ....  
 115  
 Interception ..... 28  
 Interconnexion de réseaux locaux ..... 2  
 Interconnexions LAN-LAN ..... 121  
 Interface CAPI ..... 98  
 Interface de configuration ..... 13, 14  
 Interface de configuration V.24 ..... 10  
 Interface list ..... R-39  
 Interface S0 ..... 3  
 Interface sériele ..... 13, 24  
 Interfaces ..... 9  
 Internet ..... 2, 39  
 Interrogation de l'heure ..... 5  
 Intranet ..... R-58  
 Intranet-mask ..... R-58  
 Inverse masquerading ..... R-67  
 IP ..... R-66  
 IP address ..... R-58  
 IP broadcast ..... R-66  
 IP header ..... R-65  
 IP masquerading ..... R-61, R-67  
 IP multicast ..... R-66  
 IP-Masquerading ..... 5, 77  
   Masquage simple ..... 78  
   Protocoles ..... 79  
 IP-netmask ..... R-58  
 IP-Pooling ..... 3  
 IP-routing-table ..... R-61  
 IPX-router ..... R-49  
 IPX-watchdog ..... R-50  
 ISDN layers ..... R-43  
 ISDN time ..... R-5

■ **J**

Jours de semaine ..... 104  
 Jours fériés ..... 104

■ **K**

Key ..... R-45

■ **L**

LANCAPI ..... 1, 3, 6, 18, 98, R-76  
 LAN-Coll ..... 9  
 LANconfig ..... 5, 13, 16, 18, 23, 32  
   Assistants ..... 16  
 LAN-configuration ..... R-75  
 LAN-filter-table ..... R-54, R-56, R-63  
 Language ..... R-75  
 LAN-Link ..... 9  
 LANmonitor ..... 4, 28, 32, 107  
 LAN-Rx ..... 9  
 LAN-Tx ..... 9  
 Layer-name ..... R-41, R-43  
 LCP echo reply ..... 55  
 LCP echo request ..... 55  
 LCR ..... 5, 40, 103, R-77  
 Leased-line connection ..... R-43  
 Least Cost Router ..... 103, 106  
   Contrôle des coûts de communication ... 106  
   Modes de fonctionnement ..... 106  
   Repli automatique ..... 107  
 Least Cost Routing ..... 5, 40  
 LED état du Link ..... 10  
 Liaison commutée ..... 2  
 Liaison permanente ..... 110, 116  
 Liaisons commutées ..... 121  
 Lignes commutées RNIS ..... 39  
 Lignes spécialisées ..... 2, 121  
 Limitation des communications ..... 40  
 Limitation des communications en fonction de  
   la durée ..... 40  
 Limiter les frais ..... 40  
 Liste d'accès IP ..... 16  
 Liste PPP ..... 37  
 Local-routing ..... R-51, R-65  
 Location ..... R-38  
 Lock-minutes ..... R-75  
 Logiciel de terminal ..... 5  
 Login ..... 22  
 Log-in block ..... R-75  
 Login-errors ..... R-75  
 LOOP-propagate ..... R-52  
 Looser ..... R-42

■ **M**

MAC address .....	R-48
Management Information Base .....	28
Manual connection .....	R-47
Masquerading .....	R-58, R-61, R-67
Masquerading IP .....	2, 37, 39, 111
Masquerading IP inverse .....	116
Masquerading table .....	R-68
Maximum number of simultaneous connections .....	R-75
Mécanisme d'acheminement DNS .....	88
Médias en ligne .....	16
Mémoire flash-ROM .....	6, 22
Messages .....	8
MIB .....	26
Microprogramme .....	6
Mise à jour des logiciels .....	6
MLPPP .....	3, 60
Modem operation .....	R-44
Modes d'exploitation .....	35
Mot de passe .....	20, 33, 37, 38, 54
Mots de passe .....	94
Multilink PPP .....	52, 60

■ **N**

Name .....	R-38
Name server .....	R-59
Name verification .....	R-46
Name-list .....	R-41
NAT .....	37, 39, 77
NBNS .....	91, R-60
NBNS-backup .....	R-60
NetBIOS .....	7, 88, R-51
Accès à distance .....	96
Correspondant .....	95
Filtre IP .....	95
Interconnexion entre deux réseaux locaux ... 95	
Protocole réseau .....	92
TCP/IP .....	92
NetBIOS name server .....	R-60
NetBIOS propagated frames .....	R-52
NetWare server .....	R-50

Network .....	R-50
Network address .....	R-52
Network connection .....	R-48
Network Information Center .....	77
Networking dans un réseau Windows .....	96
NIC .....	77
Node .....	10
Node-ID .....	R-49
Noeud d'accès .....	3
Nom d'ordinateur .....	91
Nom d'utilisateur .....	19, 38, 55
Noms d'ordinateur .....	87
Noms de réseau .....	87
Noms et désignation des groupes .....	93
Novell .....	R-52
NT domain .....	R-72
Number .....	R-41
Number list .....	R-46
Numéro de configuration .....	20
Numéro vert .....	105

■ **O**

Objets .....	27
Opérateurs .....	103, 105
Operating .....	R-49, R-58, R-61
Ordinateurs accessibles .....	97
Other .....	R-82
Outband .....	13, 14

■ **P**

PAP .....	38, R-45
Partage .....	94
Partage de fichiers et d'imprimantes .....	93
Pas d'informations relatives aux frais .....	40
Passerelle .....	39, 80, 83
Password .....	R-59
Password Authentication Protocol ...	38, R-45
Password-required .....	R-75
PAT .....	37, 39, 77
Période .....	40
Pictogrammes .....	110
Pilote de télécopie .....	7
Pilote de télécopieur .....	102
Plage horaire .....	104

- Point-to-point protocol ..... R-44
  - Policy Based Routing ..... 105
  - Pool d'adresses ..... 81, 86
  - Pool d'adresses IP ..... 98
  - Pooling IP ..... 98
  - Port ..... 78, 101
  - Ports NetBIOS ..... 92
  - Power ..... 8
  - PPP ..... 5, 6, 33, 38, 60, R-44, R-46
    - Attribution des adresses IP ..... 56
    - Fonctions de rappel automatique ..... 57
    - Vérification de la ligne avec LCP ..... 55
  - PPP negotiation ..... R-58
  - PPP-Client ..... 13
  - Préfixe ..... 103
  - Présélection ..... 103
  - Procédé de compression de données
    - LZS ..... 61
  - Procédés de sécurisation ..... 38
  - Programmes de télécopie standard ..... 103
  - Prohibited address ranges ..... R-62
  - Propagated ..... 66
  - Propagated Frames ..... R-52
  - Protect ..... R-46
  - Protection ..... 35, 37
  - Protection contre les accès ..... 5
  - Protection d'accès ..... 37
  - Protection de l'accès
    - Par nom ..... 37
    - Par nom ou numéro ..... 37
    - Par numéro ..... 37
    - Tous ..... 37
  - Protection par mot de passe ..... 5, 36
  - Protocole de canal B ..... 38
  - Protocole V.110I ..... 7
  - Proxy ..... 7
  - Proxy ARP ..... R-61, R-62
  - Proxy NetBIOS ..... 90
  - Proxy-ARP ..... R-65
- **R**
- R1-mask ..... R-67
  - Raccordements ..... 9
  - Rappel ..... 38
    - Fast Call Back ..... 39
  - Rappel automatique ..... 2, 5, 37
  - Recherche en ligne ..... 2
  - Registered IP address ..... R-58
  - Réglage automatique de l'heure ..... 107
  - Regroupement des canaux ..... 3, 60
    - Dynamique ..... 3, 60
    - Statique ..... 3, 60
  - Regroupement dynamique des canaux .. 3, 60
  - Regroupement statique des canaux ..... 3, 60
  - Remote Access ..... R-53, R-65
  - Remote station verifications ..... R-45
  - Remote-table ..... R-72
  - Répondeur téléphonique ..... 1, 2
  - Reroutage direct ..... 104
  - Réseau 100-Mbit ..... 10
  - Réseau Windows ..... 84, 91
  - Réseaux NetBIOS ..... 88
  - Réseaux Peer-to-Peer ..... 7
  - Réseaux TCP/IP ..... 87
  - Réseaux Windows ..... 7
  - Reset system ..... R-82
  - Ressources partagées ..... 94
  - RIP ..... 64, R-66
  - RIP-SAP-scaling ..... R-51
  - RIP-type ..... R-66
  - Round robin list ..... R-42
  - Round-Robin ..... R-43
  - Routage ..... 91
  - Routage dynamique ..... 69
  - Routage IP
    - Filtrage ..... 72
    - FTP ..... 72
    - Telnet ..... 72
  - Routage IPX
    - Backoff ..... 64
    - Correspondant ..... 63
    - Exponential Backoff ..... 66
    - Filtre ..... 66
    - Hops ..... 65
    - Liaison ..... 63
    - Loop Propagated ..... 65

Propagated ..... 63  
Réseau ..... 63  
Tables RIP et SAP ..... 64  
Tics ..... 65  
Routage par DNS ..... 79  
Routage statique ..... 68  
Routage téléphonique à la demande ..... 103  
Router des réseaux Windows ..... 90  
Routes exclues ..... 71  
Routes/FRM ..... R-54  
Routeur ..... 69  
Routing Information Protocol ..... 64  
Routing-table ..... R-52

## S

SAP ..... 64, R-55  
SAP numbers ..... 83  
SAP services ..... R-56  
Scaling ..... R-51  
Scope ID ..... R-72  
Scopes ..... 91  
Script List ..... 92  
Script list ..... R-46  
Script processing ..... 91  
Script processing ..... R-44, R-46  
Sécurité ..... 35, 37, 39, 111  
Security procedure ..... R-45  
Semipermanent leased-line connection R-42  
Server information ..... R-55  
Server list ..... R-74  
Server/FRM ..... R-56  
Serveur de messagerie électronique ..... 90  
Serveur de noms NetBIOS ..... 91  
Serveur DHCP ..... 7, 16, 80, 87  
    Configuration ..... 85  
Serveur DNS ..... 7, 80, 82, 87  
    Information disponible ..... 88  
    Liste des filtres ..... 90  
    Mécanisme filtrant ..... 88  
Serveur LANCAPI ..... 100  
Serveur NBNS ..... 80, 82, 84  
Serveur Web ..... 110, 115  
Serveur WINS ..... 91

Service ..... 87  
Service Advertising Protocol ..... 64  
Service information ..... R-56  
Service table ..... R-67  
Setup  
    DHCP-module ..... R-70  
    IP-router-module ..... R-61  
    IPX-module ..... R-49  
    LAN-module ..... R-48  
    TCP-IP-module ..... R-57  
    WAN-module ..... R-38  
Short-hold ..... R-41  
Single User Access ..... 39  
SNAP ..... R-50  
SNMP ..... 26, R-69  
    Agents ..... 26  
    Gestionnaire ..... 26  
    MIB ..... 26  
Socket-Filter ..... R-51, R-53  
Source port ..... R-64  
Spare-heap-blocks ..... R-49  
Special dialing characters ..... R-41, R-42  
Speed ..... R-44  
Split Horizon ..... 65  
Spoofing ..... R-55, R-57  
SPX-watchdog ..... R-51  
Stac ..... 61, R-44  
Start-address-pool ..... R-70  
Static bundling ..... R-41  
Static IP address ..... R-61  
Statistiques ..... 4  
Status ..... R-3  
    Call-info-table ..... R-33, R-34, R-36, R-37  
    Config-statistics ..... R-30  
    Connection-state ..... R-5  
    Connection-statistics ..... R-31  
    Delete values ..... R-37  
    Info-connection ..... R-32  
    IP-router-statistics ..... R-28  
    IPX-statistics ..... R-17  
    LAN-statistics ..... R-8  
    Layer-connection ..... R-33  
    operating time ..... R-5

PPP-statistics ..... R-9  
 Queue-statistics ..... R-30  
 SO-bus ..... R-35  
 TCP-IP-statistics ..... R-22  
 WAN-statistics ..... R-6  
 Supported Protocols and Functions ..... 95  
 Suppresses the outgoing MSN ..... R-40  
 Surveillance ..... 32  
 System-administrator ..... R-69  
 System-location ..... R-69

■ **T**

Table-ARP ..... R-60  
 Tableau de reroutage ..... 104  
 Tableau de routage  
   Entrées particulières ..... 71  
   IP-Masquerading ..... 71  
 Tableau de routage IP ..... 68  
 Tableau de routage IPX ..... 63  
 Tableau des interfaces ..... 49  
 Tableaux RIP ..... 65  
 Tableaux SAP ..... 65  
 Table-RIP ..... R-53, R-67  
 Table-SAP ..... R-55  
 Tarif local ..... 105  
 Tarifs ..... 103, 105  
 Taux de transfert ..... 4, 33  
 TCP ..... R-64, R-68  
 TCP max. connections ..... R-60  
 TCP/IP ..... 16, 68  
 TCP-aging-minute(s) ..... R-60  
 Téléchargement ..... 6, 22  
 Téléchargement de microprogramme  
   Avec LANconfig ..... 23  
 Téléchargement du microprogramme ..... 23  
   Avec émulateur de terminal ..... 24  
   Avec TFTP ..... 24  
 Téléconfiguration ..... 13  
 Télécopie ..... 1, 6, 103  
 Télécopier ..... 2  
 Telephone company ..... R-77  
 Télétravail ..... 2, 132  
 Teleworkers ..... R-65

Telnet ..... 14  
 Telnet ..... 5, 18  
 Telnet server ..... R-59  
 Témoin lumineux ..... 4, 8  
 Tentatives d'accès ..... 36  
 TFTP ..... 16  
 TFTP server ..... R-59  
 Time ..... R-5, R-45, R-79  
 Timeout ..... 61, R-71  
 TOS ..... R-66, 105  
 Touches ..... 8  
 Tracé  
   Code et paramètre ..... 30  
   Exemples ..... 32  
   Lancement ..... 30  
 Trace editions  
   SCRPT ..... 105  
 Trace Outputs ..... 93  
 Trace outputs  
   ARP ..... 103  
   control ..... 94  
   DHCP ..... 104  
   Error ..... 97  
   examples ..... 95  
   ICMP ..... 103  
   IP-RIP ..... 102  
   IP-Rt. .... 101  
   IPX watchdogs ..... 100  
   IPX-NetBIOS ..... 101  
   IPX-Rt. .... 98  
   PPP ..... 97  
   RIP ..... 99  
   SAP ..... 99  
   SCRPT ..... 104  
   Source ..... 97  
   SPX watchdogs ..... 101  
   Time ..... 96  
 Transfert de données ..... 60  
 Transfert de fichiers ..... 2, 6  
 Transmission de données dans le réseau IPX  
   64  
 Trap-IP ..... R-69  
 Traps-active ..... R-69

Travail à domicile ..... 2, 131  
trunk seizure ..... R-42  
Type d'accès ..... 94  
Type-of-Service ..... 80, R-65

## ■ U

UDP ..... R-64, R-68  
Unités ..... 40  
Unités de taxation ..... 4, 40, 61  
Upload-system ..... R-82  
Username ..... R-45

## ■ V

Vérification ..... 54  
Verification attempt ..... R-45  
Verrouillage ..... 36  
Verrouillage d'accès ..... 36  
Verrouiller les domaines ..... 90  
Version-table ..... R-80  
Voisinage réseau ..... 96

## ■ W

WAN-configuration ..... R-75  
WAN-filter-table ..... R-54, R-56, R-64  
WAN-update-minute(s) ..... R-55, R-57  
Watchdog ..... R-50  
Windows Internet Name Service-Server ... 91  
WWW ..... 39

## ■ X

X.75 data protection ..... R-44  
X.75 secured format ..... R-44  
XModem ..... 24

## ■ Y

Y connections ..... R-40

## ■ Z

Zone tarifaire ..... 105





# 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


	<b>Setup</b>		<b>Status</b>
	Name		Connection
	WAN-module		Current-time
	Charges-module		Operating-time
	LAN-module		WAN-statistics
	IPX-module		LAN-statistics
	TCP-IP-module		PPP-statistics
	IP-router-module		IPX-statistics
	SNMP-module		TCP-IP-statistics
	DHCP-module		IP-router-statistics
	NetBIOS-module		Config-statistics
	Config-module		Queue-statistics
	LANCAPI-module		Conn.-statistics
	LCR-module		Info-connection
	DNS module		Layer-connection
	Time-module		Call-info-table
	<b>Firmware</b>		Remote-statistics
	Version-table		S <sub>0</sub> -bus
	Table-firmsafe		Channel-statistics
	Mode-firmsafe		Time-statistics
	Timeout-firmsafe		LCR-statistics
	Test-firmware		Delete-values
	Firmware-upload		<b>Other</b>
			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 <sub>0</sub> -bus		Status of the S <sub>0</sub> 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 S<sub>0</sub> 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:

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

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

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

*Error-statistics*

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

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

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

Ifc	Designates the associated channel.
Rx-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:













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

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











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

## Status/LAN-statistics

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










/LAN-statistics	Running status displays	
LAN-rx-packets		Number of data packets received
LAN-tx-packets		Number of data packets sent
LAN-rx-errors		Number of data packets incorrectly received
LAN-tx-errors		Number of data packets incorrectly sent
LAN-stack-errors		Number of packets without a suitable receive module (bridge/router)
LAN-NIC-errors		Number of data packets discarded by the NIC
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
LAN-collisions		Number of collisions during a send procedure
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 <b>AUTHENTICAT</b> , <b>NETWORK</b> and <b>TERMINATE</b> .
LCP	Status of the 'Link Control Protocol' subprotocol. The possible values are: <b>Initial</b> , <b>Starting</b> , <b>Stopping</b> , <b>Stopped</b> , <b>Closing</b> , <b>Closed</b> , <b>ReqSent</b> , <b>AckRcvd</b> , <b>AckSent</b> and <b>Opened</b> .
IPCP	Similarly to 'LCP', displays the status of the 'IP Control Protocol' subprotocol.
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	<b>M</b> aximum <b>R</b> eceive <b>U</b> nit designates the maximum packet size that the remote station can receive
ACCM	<b>A</b> synchronous <b>C</b> ontrol <b>C</b> haracter <b>M</b> ap designates the character in the asynchronous data flow that is interpreted as the control character
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 'ffffffff' 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
Refreshes		Number of name renewals performed
Timeouts		Number of names dropped due to aging
B-Nodes		Number of currently active B nodes (broadcast) in the network
P-Nodes		Number of currently active P nodes (peer-to-peer) in the network
M-Nodes		Number of currently active M nodes (mixed-mode) in the network
W-Nodes		Number of currently active W nodes (hybrid) in the network

*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: <b>Init</b> , <b>Setup WAN</b> , <b>Ready</b> , <b>Dial</b> , <b>Incoming call</b> , <b>Protocol</b> , <b>Connection</b> , <b>Callback</b> , <b>Bundle</b> and <b>Reserved</b> . The <b>Bundle</b> status is indicated in the display <i>ELSA LANCOM Business 4100</i> by the addition of a "I2" in columns 15 and 16 of the associated display line. <b>Bundle</b> is displayed for the second interface either when a bundle connection has been activated via the first interface or when a leased-line connection with two B channels has been set. <b>Reserved</b> is displayed for the second interface when a connection exists to the first B channel and the Y connection has been deactivated.
Mode	Reflects the type of establishment. The following are possible: <b>Active</b> (active call establishment = dialing) <b>Passive</b> (passive call establishment = call acceptance) <b>CB</b> (call establishment via callback)



Dialup-remote	Indicates the call number of the remote station from the name list.
Device-name	Indicates the logical name of the remote station (if it can be detected). The device name is also displayed on the appropriate display line as soon as a logical connection is established.
B1-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 <sub>0</sub>	5678	1234	HDLC64K	2
OT; 00:20:46	S <sub>0</sub>	4321	1234	HDLC64K	1
OT; 00:19:47	S <sub>0</sub>	4321	1234	HDLC64K	1
OT; 00:11:33	S <sub>0</sub>	5678	1234	HDLC64K	1
OT; 00:01:13	S <sub>0</sub>	4321	1234	HDLC64K	2
OT; 00:01:02	S <sub>0</sub>	4321	1234	HDLC64K	1
OT; 00:00:06	S <sub>0</sub>	5678	1234	HDLC64K	1

The different entries have the following meaning:

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
0T; 00:20:57	LONDON	Active	Ch01	50	5
0T; 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/S<sub>0</sub>-bus

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

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

### D-info

This table shows general information related to the D channel:

Channel	B-channel identification.
Protocol	D-channel protocol. Either the protocol fixed in the interface table or the protocol detected in the 'Auto' settings at the ISDN terminal.
Layer-2	Activation of layer 2 of the D channel ('Yes' or 'No')
TEI	TEI assigned ('Yes' or 'No')
S <sub>0</sub> -activation	Displays activation status ('Yes' or 'No')

### D2-statistics

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

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

## Status/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 <sub>0</sub> -1-ERR	00000000	Router	active	0000	0241123456	00000000	3	0		
S <sub>0</sub> -1-B1	00000000	a/b	active	0000	0241123457	00000000	2	20		
S <sub>0</sub> -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 Business* 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 Business* 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		ELSA LANCAPI 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 <sub>0</sub> 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: <b>Auto</b> : automatic detection of the D-channel protocol <b>DSS1</b> : Euro-ISDN <b>1TR6</b> : National ISDN <b>GRP0</b> : Leased-line connection group 0 <b>P2P-DSS1</b> : Point-to-point connection
LL-B-chan.	B-channel settings for a leased-line connection. The possible values are: <b>none</b> : Leased-line connection not assigned to a specific channel. <b>1</b> or <b>2</b> : Leased-line connection operates over the assigned B channel. Please refer to the information on setting these parameters in the fixed connection description.
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><b>On:</b> Y connection is supported; a number of connections can be established simultaneously (default). A channel bundling connection is broken off when a second connection to another remote station has to be established.</p> <p>Refer also to the settings for the availability of the <i>LANCAPI</i>.</p> <p><b>Off:</b> Y connection not supported; only one connection can be established. The second connection is blocked. If a connection to an additional remote station is to be established, this establishment is rejected. A channel bundling connection is not affected.</p>
CLIP	<p>Calling Line Identification Protocol: Suppresses the outgoing MSNs.</p> <p>Possible values:</p> <p><b>Yes:</b> Activate CLIR, do not send MSN.</p> <p><b>No:</b> 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 <sub>0</sub> 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 <b>Device Name</b> column, you can enter an original remote station name, which you must then assign to the relevant remote station via the <b>Name</b> option in the <b>Setup</b> menu.
Dialup-remote	In this column, you can store the number to be called and, if applicable, supplement it with special dialing characters (see above, default: None).
B1-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 <b>Head</b> column, the following entries are possible: <b>Last:</b> The next connection to be established will begin with the DDI that was successfully used for establishing the last connection (default). <b>First:</b> The next connection to be established will always begin with the first DDI. For a logical remote station, this field can be modified only by means of its <b>first</b> entry in the table. The field is automatically updated when other entries are made for this remote station.

#### Layer-list

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

The following table below is provided as an example and also shows the default settings for an *ELSA LANCOM Business*:

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
RAWHDLC	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 <b>DEFAULT</b> is defined in this column, the settings stored there are always used when no layer name can be assigned (e.g. a caller does not transmit his or her call number). This entry is also used when a group 0 leased-line connection is established. If the <b>DEFAULT</b> entry is not present, a B channel protocol developed by ELSA is used as the default. The user may delete or change any of the layers predefined here.				
Encaps.	Additional information regarding the data to be transmitted may be specified in the <b>Encaps</b> column. The following entries are possible:				
	ETHER	The data is provided with an Ethernet header. This setting is required for communication with older <i>ELSA LANCOM</i> devices.			
	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.
	SCTrans	Following completion of script processing, a connection exists to the remote station. No further protocol negotiation is performed.
Lay-2	In this column, you can select the protocol for ISDN layer 2:	
	TRANS	The data is packed directly in HDLC packets. Always select this setting if communication is to take place via transparent HDLC.
	X.75LAPB	The data is exchanged in X.75 secured format. Always select this setting if the remote station is to work with X.75 data protection.
L2-Opt.	The L2-opt. enables the setting of an option for the data transfer setting under Lay-2 with an additional <i>ELSA LANCOM</i> .	
	none	No data compression or channel bundling is performed.
	compr.	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
CSEVERE	<>[Host]<CIS>[User]\$U[Password]\$P[PPP]\$C

The entries in the script list have the following meaning:

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

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

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

/Manual-dialing	Settings for manual connection control	
Connect		Establishes a connection.
Disconnect		Termination of connections
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-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 DCHP module, the 'Table-DCHP' 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



*Type*

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.

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, <b>On</b> or <b>Off</b>
Lancapi-usage		Activate LCR for the <i>LANCAPI</i> , <b>On</b> or <b>Off</b>
Timetable		Call forwarding table
Celebration-day-table		List of holidays affecting the timetable.

### Timetable

The table has 256 entries and the following structure:

Index	Prefix	Days	Start	Stop	Number-list	Fallback
1	0171	192	0:00	23:59	01013;01070	On

The individual entries have the following meaning:

Index	Continuing index of entries in the table.
Prefix	Area code to be diverted.
Days	Validity of the entry for week days and holidays shown in an 8-bit mask: Bit 0 represents Monday, bit 7 holidays. The entry '31' therefore designates all business days, '192' Sundays and holidays.
Start	Beginning time for the validity of the entry on the defined days.
Stop	Termination time for the validity of the entry on the defined days.
Number-list	Network identification number of the call-by-call providers.
Fallback	Automatic fallback to your own telephone company if all call-by-call numbers are busy.

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: <b>On, Off</b>
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.

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



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

Position	Status	Version	Date	Size	Index
1	Inactive	1.60	23061999	690	6
2	Active	1.60	30061999	692	7
3	<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.

# Novell SAP Numbers

Decimal	Hexa-decimal	SAP description
1	0001	User
2	0002	User Group
3	0003	Print Queue or Print Group
4	0004	File Server (SLIST source)
5	0005	Job Server
6	0006	Gateway
7	0007	Print Server or Silent Print Server
8	0008	Archive Queue
9	0009	Archive Server
10	000a	Job Queue
11	000b	Administration
15	000F	Novell TI-RPC
23	0017	Diagnostics
32	0020	NetBIOS
33	0021	NAS SNA Gateway
35	0023	NACS Async Gateway or Asynchronous Gateway
36	0024	Remote Bridge or Routing Service
38	0026	Bridge Server or Asynchronous Bridge Server
39	0027	TCP/IP Gateway Server
40	0028	Point to Point (Eicon) X.25 Bridge Server
41	0029	Eicon 3270 Gateway
42	002a	CHI Corp
44	002c	PC Chalkboard
45	002d	Time Synchronization Server or Asynchronous Timer
46	002e	ARCserve 5.0 / Palindrome Backup Director 4.x (PDB4)
69	0045	DI3270 Gateway
71	0047	Advertising Print Server
74	004a	NetBlazer Modems

Decimal	Hexa-decimal	SAP description
75	004b	Btrieve VAP/NLM 5.0
76	004c	Netware SQL VAP/NLM Server
77	004d	Xtree Network Version Netware XTree
80	0050	Btrieve VAP 4.11
82	0052	QuickLink (Cubix)
83	0053	Print Queue User
88	0058	Multipoint X.25 Eicon Router
96	0060	STLB/NLM
100	0064	ARCserve
102	0066	ARCserve 3.0
114	0072	WAN Copy Utility
122	007a	TES-Netware for VMS
146	0092	WATCOM Debugger or Emerald Tape Backup Server
149	0095	DDA OBGYN
152	0098	Netware Access Server (Asynchronous gateway)
154	009a	Netware for VMS II or Named Pipe Server
155	009b	Netware Access Server
158	009e	Portable Netware Server or SunLink NVT161
161	00a1	Powerchute APC UPS NLM
170	00aa	LAWserve
172	00ac	Compaq IDA Status Monitor
256	0100	PIPE STAIL
258	0102	LAN Protect Bindery
259	0103	Oracle DataBase Server
263	0107	Netware 386 or RSPX Remote Console
271	010f	Novell SNA Gateway
273	0111	Test Server
274	0112	Print Server (HP)
276	0114	CSA MUX (f/Communications Executive)

Decimal	Hexa-decimal	SAP description
277	0115	CSA LCA (f/Communications Executive)
278	0116	CSA CM (f/Communications Executive)
279	0117	CSA SMA (f/Communications Executive)
280	0118	CSA DBA (f/Communications Executive)
281	0119	CSA NMA (f/Communications Executive)
282	011a	CSA SSA (f/Communications Executive)
283	011b	CSA STATUS (f/Communications Executive)
286	011e	CSA APPC (f/Communications Executive)
294	0126	SNA TEST SSA Profile
298	012a	CSA TRACE(f/Communications Executive)
299	012b	Netware for SAA
301	012e	IKARUS virus scan utility
304	0130	Communications Executive
307	0133	NNS Domain Server or Netware Naming Services Domain
309	0135	Netware Naming Services Profile
311	0137	Netware 386 Print Queue or NNS Print Queue
321	0141	LAN Spool Server (Vap, Intel)
338	0152	IRMLAN Gateway
340	0154	Named Pipe Server
358	0166	NetWare Management
360	0168	Intel PICKIT Comm Server or Intel CAS Talk Server
371	0173	Compaq
372	0174	Compaq SNMP Agent
373	0175	Compaq
384	0180	XTree Server or XTree Tools
394	018A	NASI services broadcast server (Novell)
432	01b0	GARP Gateway (net research)

Decimal	Hexa-decimal	SAP description
433	01b1	Binview (Lan Support Group)
447	01bf	Intel LanDesk Manager
458	01ca	AXTEC
459	01cb	Shiva NetModem/E
460	01cc	Shiva LanRover/E
461	01cd	Shiva LanRover/T
462	01ce	Shiva Universal
472	01d8	Castelle FAXPress Server
474	01da	Castelle LANPress Print Server
476	01dc	Castille FAX/Xerox 7033 Fax Server/Excel Lan Fax
496	01f0	LEGATO
501	01f5	LEGATO
563	0233	NMS Agent or Netware Management Agent
567	0237	NMS IPX Discovery or LANtern Read/Write Channel
568	0238	NMS IP Discovery or LANtern Trap/Alarm Channel
570	023a	LABtern
572	023c	MAVERICK
575	023f	Used by eleven various Novell Servers / Novell SMDR
590	024e	Netware Connect
591	024f	NASI server broadcast (Cisco)
618	026a	Network Management (NMS) Service Console
619	026b	Time Synchronization Server (Netware 4.x)
632	0278	Directory Server (Netware 4.x)
640	0280	Novell File and Printer Sharing Service for PC
989	03dd	Banyan ENS for Netware Client NLM
772	0304	Novell SAA Gateway
776	0308	COM or VERMED 1
778	030a	Galacticomm's Worldgroup Server

Decimal	Hexadecimal	SAP description
780	030c	Intel Netport 2 or HP JetDirect or HP Quicksilver
800	0320	Attachmate Gateway
807	0327	Microsoft Diagnostics
808	0328	WATCOM SQL server
821	0335	MultiTech Systems Multi-synch Comm Server
835	0343	Xylogics Remote Access Server or LAN Modem
853	0355	Arcada Backup Exec
858	0358	MSLCD1
865	0361	NETINELO
894	037e	Twelve Novell file servers in the PC3M family
895	037f	VirusSafe Notify
902	0386	HP Bridge
903	0387	HP Hub
916	0394	NetWare SAA Gateway
923	039b	Lotus Notes
951	03b7	Certus Anti Virus NLM
964	03c4	ARCserve 4.0 (Cheyenne)
967	03c7	LANspool 3.5 (Intel)
983	03d7	Lexmark printer server (type 4033-011)
984	03d8	Lexmark XLE printer server (type 4033-301)
990	03de	Gupta Sequel Base Server or NetWare SQL
993	03e1	Univel Unixware
996	03e4	Univel Unixware
1020	03fc	Intel Netport
1021	03fd	Print SErver Queue
1196	04ac	On-Time Scheduler NLM
1034	040A	IpServer Running on a Novell Server
1037	040D	LVERRMAN Running on a Novell Server
1038	040E	LVLIC Running on a Novell Server
1044	0414	Kyocera

Decimal	Hexadecimal	SAP description
1065	0429	Site Lock Virus (Brightworks)
1074	0432	UFHELP R
1075	0433	Synoptics 281x Advanced SNMP Agent
1092	0444	Microsoft NT SNA Server
1096	0448	Oracle
1100	044c	ARCserve 5.01
1111	0457	Canon GP55 Running on a Canon GP55 network printer
1114	045a	QMS Printers
1115	045b	Dell SCSI Array (DSA) Monitor
1169	0491	NetBlazer Modems
1200	04b0	CD-Net (Meridian)
1299	0513	Emulux NQA Something from Emulux
1312	0520	Site Lock Checks
1321	0529	Site Lock Checks (Brightworks)
1325	052d	Citrix OS/2 App Server
1343	0535	Tektronix
1344	0536	Milan
1387	056b	IBM 8235 modem server
1388	056c	Shiva LanRover/E PLUS
1389	056d	Shiva LanRover/T PLUS
1408	0580	McAfee's NetShield anti-virus
1466	05BA	Compatible Systems Routers
	05B8	NLM to workstation communication (Revelation Software)
	0606	JCWatermark Imaging
1569	0621	IBM AntiVirus NLM
1600	0640	Microsoft Gateway Services for NetWare
1614	064e	Microsoft Internet Information Server
1900	076C	Xerox
1947	079b	Shiva LanRover/E 115
1958	079c	Shiva LanRover/T 115

Deci- mal	Hexa- decimal	SAP description
1972	07B4	Cubix WorldDesk
	07c2	Quarterdeck IWare Connect V2.x NLM
	07c1	Quarterdeck IWare Connect V3.x NLM
2084	0824	Shiva LanRover Access Switch/E
2154	086a	ISSC collector NLMs
2175	087f	ISSC DAS agent for AIX
2857	0b29	Site Lock
3113	0c29	Site Lock Applications
3116	0c2c	Licensing Server
9088	2380	LAI Site Lock
9100	238c	Meeting Maker
18440	4808	Site Lock Server or Site Lock Metering VAP/NLM
21845	5555	Site Lock User
25362	6312	Tapeware
28416	6f00	Rabbit Gateway (3270)
30467	7703	MODEM??
32770	8002	NetPort Printers (Intel) or LANport
32776	8008	WordPerfect Network Version
34238	85BE	Cisco Enhanced Interior Rou- ting Protocol (EIGRP)
34952	8888	WordPerfect Network Version or Quick Network Manage- ment
36864	9000	McAfee's NetShield anti- virus
38404	9604	?? CSA-NT_MON
46760	b6a8	Ocean Isle Reachout Remote Control
61727	f11f	Site Lock Metering VAP/NLM
61951	f1ff	Site Lock
62723	f503	Microsoft SQL Server
63749	f905	IBM Time and Place/2 appli- cation
64507	fbfb	TopCall III fax server
65535	ffff	Any Service or Wildcard

# TCP/IP Ports

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

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

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

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



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



# ELSA LANCOM Business Internal

This chapter provides information on the internal functions of the router. It is not always necessary in day-to-day work with the ISDN routers but can be very useful to specialists in specific situations.

## Script Processing

### General

Some Internet service providers (e.g. CompuServe) run a script-controlled login procedure before a PPP negotiation. To enable the establishment of such a connection, a simple script process is implemented in the *ELSA LANCOM*.

A script can include the following elements:

Element	Description
<>	Send the included text with a carriage return at the end.
[]	Wait until the included text has been received. The text may be upper or lower case. It is sufficient to enter an unambiguous subtext.
\$U	Send the user name (from the PPP table) with a carriage return at the end.
\$P	Send the password (from the PPP table) with a carriage return at the end.
\$C	End of the script.

As previously noted in the overview, the user name and password are taken from the PPP table if there is an appropriate entry there. If there is no user name in the PPP table, the device name of the *ELSA LANCOM* is forwarded as the user name.

Once the script is complete, a PPP negotiation is started or the login procedure is concluded.

The layer 3 entry in the layer list is used to define whether a PPP negotiation is started after the script has been processed. There are three possible entries:

SCPPP	A synchronous PPP negotiation is started once the script has been processed.
SCAPPP	An asynchronous PPP negotiation is started once the script has been processed.
SCTTRANS	The logical connection to the remote station exists once the script has been processed. There is no more protocol negotiation.

## The Script List

Scripts are entered in a script list table provided for that purpose. This table is in the /Setup/WAN-module and has the following structure:

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, another entry similar to the RoundRobin list for the logical remote station may be added. The syntax for this is: Device name followed by '#' and a number. The entries are processed from top to bottom.

Example:

Device name	Script
CSERVE#1	<>[Host]<CIS>[User]
CSERVE#2	\$U[Password]\$P[PPP]\$C

In the *ELSA LANconfig* the script list is on the 'Communication' tab.

## CompuServe Select

The settings required for selection on the CompuServe network via X.75, asynchronous PPP and script control with an example.

Layer list:

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
CSERVE	TRANS	SCAPPP	X.75LAPB	none	HDLC64K

Name list:

Device name	Dialup-remote	B1-DT	B2-DT	WAN-layer	Callback
CSERVE	0021194260	60	60	CSERVE	Off

PPP list:

Device name	Authent.	Key	Time	Rep.	User-name
CSERVE	none	*	0	0	xxxxxx,xxxx/PPP:CISPPP

The CompuServe account is to be entered for xxxxxx,xxxx.

Script list:

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

The script elements have the following meaning:

Element	Meaning
<>	Start script on the remote station by sending a carriage return.
[Host]	Wait for the answer from the CompuServe node. At some point the 'Host Name' will appear in the answer.
<CIS>	Send 'CIS' followed by a carriage return.
[User]	Wait for the answer. CompuServe requests the 'User ID'.
\$U	Send the user name. For CompuServe this consists of the CompuServe User ID with attached '/PPP:CISPPP'. The user name is taken from the PPP table and sent to the remote station with a final carriage return.
[Password]	Wait for the password query.
\$P	Send the password followed by a carriage return. The password will be taken from the PPP table.
[PPP]	Wait for the connect message from the remote station.
\$C	The script is fully processed. The asynchronous PPP negotiation (SCAPPP) in the layer list is started.

## Online Trace Outputs

### General

With so-called 'online trace outputs' (control outputs) the user can receive information on internal processes of a working *ELSA LANCOM*. Such information can aid in finding erroneous configurations easily and securely, both from *ELSA LANCOM* and from other devices connected with an *ELSA LANCOM*.

The online trace outputs can be flexibly administered for individual protocols and functions in the firmware and individual configuration sessions. With session-based "Trace Profiles" only the trace information activated within a session is displayed.

The online trace outputs are controlled by a newly implemented command in the remote configuration, which is evaluated by the command interpreter and gives a direct acknowledgment of the settings that have been made to the user. Changes to these settings are effective immediately and generate or suppress the corresponding outputs directly.

The online trace outputs are displayed by the remote configuration with a time delay with respect to the actual event. The time stamp that is optionally displayed reflects the time of the output, but not the time of the actual event. There is usually not a substantial difference between these times; however, this point should always be considered when analyzing the outputs.

All displays within the online trace outputs are shown in plain text so far as possible. Because analysis of network protocols cannot completely avoid showing numerical parameters and a trace system only makes sense when the information displayed is also understood, exact descriptions of the trace information will be given below for all protocols and functions.

If displays are activated for a protocol, the next output will overwrite the current system prompt; every additional output will be preceded by a <Return> <LineFeed>. If the user presses a key, the entire buffered input will be shown again with the current system prompt. The user therefore receives visual feedback and inputs need not to be entered "blind".

## Control of Trace Outputs

Trace outputs are controlled by command line in the usual way. For this purpose, the remote configuration has the command `trace` added; this has the following command syntax:

<code>trace [key] [parameter] ...[parameter]</code>	Shows or influences the status of the trace outputs of individual protocols or functions.
Key	<code>'?'</code> display a help page <code>'+'</code> activate the trace outputs <code>'-'</code> deactivate the trace outputs <code>'#'</code> toggle the trace outputs (toggle) <code>(no)</code> status display
Parameter	Symbolic protocol or function name.

Keys and parameters must be separated by spaces. The keys are recognized by the command interpreter only if they are unambiguous, i.e. they consist of one of the characters listed above with no prefix or suffix. For the input of the symbolic protocol or function name the input of an unambiguous prefix is sufficient, as usual.

Any number of keys and parameters may be entered in a command line, limited only by the size of the line input buffer. The parameters are processed corresponding to the last

preceding key. If a key is not entered prior to the parameters, the status of that trace function (ON or OFF) is output.

It should also be noted that the command line is processed from left to right. Therefore, the trace output of a parameter can be activated and deactivated several times in one line, because it is toggled from the input buffer while the token is being read (see also examples).

In addition to activating online trace outputs, the preset output of the system time and the protocol names may be activated or deactivated via the key words "Time" and "Source". Without these two displays every trace output is shortened to 21 characters.

## Examples for Control of Trace Outputs

The table below is intended to show some practical examples of how the command for the trace outputs can be used:

Input	Effect
trace	Output of all protocols that can be generated in the trace outputs configuration session, and the status of the outputs (ON, OFF).
trace + all	Activates all trace outputs in the current session.
trace + protocol display	Activates all connection structural protocols and the display outputs.
trace + all - icmp	Activates all trace outputs, but deactivates outputs from the ICMP protocol.
trace ppp elsa	Shows the status of the PPP and ELSA trace outputs.
trace # ipx-rt display	Toggles the trace outputs of the IPX router and the display outputs.
trace - time	Deactivates the operating time display before the actual output.

## Supported Protocols and Functions

The following symbolic names for protocol stacks are supported:

Status	Display status messages via connections
Error	Display error messages via connections
PPP	Display PPP protocol negotiation
SCRPT	Display script negotiation
IPX-Rt.	Display IPX routing
RIP	Display IPX routing information protocol
SAP	Display IPX service advertising protocol
IPX-Wd.	Display IPX watchdog spoofing
SPX-Wd.	Display SPX watchdog spoofing

NetBIOS	Display IPX NetBIOS administration
IP-Rt.	Display IP routing
IP-RIP	Display IP routing information protocol
ICMP	Display Internet control message protocol
IP-MASQ	Display procedures in masquerading module
ARP	Display address resolution protocol
DHCP	Display Dynamic Host Configuration Protocols (only <i>LANCOM Office-Router</i> )
Packet dump	Display of the 64 bytes of a packet in hexadecimal format (only <i>LANCOM Office-Router</i> )

In addition to these parameters there are also the following "group parameters" (parameters for a specific type of protocol), with whose aid the online trace outputs for a complete, logically connected protocol family can be activated or deactivated:

All	Display all online trace outputs
Display	Display 'status' and 'error'
Protocol	Display 'ELSA', 'PPP' and 'SCRPT'
TCP-IP	Display 'IP-Rt.', 'IP-RIP', 'ICMP', 'ARP' and 'IP-MASQ'
IPX-SPX	Display 'IPX-Rt.', 'RIP', 'SAP', 'IPX-Wd.', 'SPX-Wd.' and 'NetBIOS'

Finally, still more parameters are recognized with which the display format of the trace outputs can be influenced:

Time	Display the system time as a prefix
Source	Display the generating protocol as a prefix

Every trace output is shortened to 21 characters by switching off the prefix outputs 'time' and 'source'. The output of the prefixes is activated by default.

### Prefix Output 'Time'

By activating the prefix output 'time' every trace output has the system time (at the time the output is generated) in the following form as a prefix:

- Format: [days]d; \_[hours]:[Minutes]:[Seconds]\_
- Example:  
12t; 07:23:15

corresponds to the system time of twelve days, seven hours, twenty-three minutes and fifteen seconds.



### Prefix Output 'Source'

Activation of the prefix output 'source' shows a trace output of the symbolic name of the protocol that caused this trace output. The display is always 9 characters (if necessary by filling spaces).

- Example: ICMP

ie the following trace output was caused by the ICMP protocol.

### Online Trace 'Status'

The outputs under 'status' describe status changes on a WAN interface (at present only the internal  $S_0$  terminal). They are displayed in the following format:

- Format: [Interface] [Status]

- Example:

Ch01: Dial 8700

On the first B channel of the internal  $S_0$  terminal the call number 8700 is dialed.

### Online Trace 'Error'

The outputs under 'error' describe errors that have occurred on a WAN interface. They are displayed in the following format:

- Format: [Interface] [Error]

- Example:

Ch01: No response

The remote station dialed did not react to the call.

### Online Trace'PPP'

The point-to-point protocol consists of a collection of subprotocols, of which *ELSA LANCOM* detects and manages the following:

LCP	The link control protocol
PAP	The password authentication protocol
CHAP	The challenge-handshake protocol
IPXCP	The IPX control protocol
IPCP	The IP protocol

These PPP subprotocols are addressed directly in specific phases during a protocol negotiation. The link control protocol is negotiated within the ESTABLISH phase; at this time only LCP packets are permitted within the PPP. If an authentication is negotiated by the LCP, PPP switches into the AUTHENTICATE phase; LCP, PAP and CHAP packets may be transmitted from this point. After the end of the (optional) authentication PPP

switches to the NETWORK phase; LCP, authentication and network control protocol packets (such as IPXCP and IPCP) may be transmitted in any combination from now on. To terminate a PPP connection it switches into the TERMINATE phase where once again only LCP packets are permitted. Once the connection has been terminated, PPP is in the DEAD phase. It will switch into the ESTABLISH phase only when a new connection is established. Every PPP phase change is displayed in the form

Change Phase to [New phase]

approximately as below

Change Phase to AUTHENTICAT

Received and sent packets, important parameters and options with completed actions are displayed for all PPP subprotocols listed above. A received frame is always displayed in the following format:

- Format: [Interface] Rx [Protocol] [Packet type] [Packet type] [Length of packet]

- Example:

Ch01: Rx IPXCP ConfReq ID=00 Length=22

In the above example a configure request for the IPX control protocol with the ID 00 and a length of 22 bytes has been received on the first B channel. If a packet cannot be assigned to any of the five subprotocols, this message appears:

- Format: [Interface] Rx Unknown Protocol [Protocol ID]

- Example:

Ch01: Rx Unknown Protocol 8029

A Packet with the protocol ID 8029 (= Appletalk control protocol) has been received.

### Online Trace 'IPX-Rt.'

The outputs under 'IPX-Rt.' describe the processing of IPX frames by the IPX router. They are displayed in the following format:

- Format: [Source interface] [IPX target address] [IPX source address] [Target / Action]

- Example:

Internal Rx

DstAddr: 00000002 ffffffff 0453

SrcAddr: 00000002 00a057123456 0453

WAN-Tx Peer: ELSA.SUP.TEST

The IPX router has received a frame from an internal process (in this case from the entity of the routing information protocol) whose target address is assigned to a logical remote station (ELSA.SUP.TEST) and therefore is sent to a WAN interface.

LAN RX

DstAddr: 00000001 ffffffff 0455

SrcAddr: 00000001 0123456789ab 0455

Filter

The IPX router has received a NetBIOS frame (IPX-socket 455) from the local network, which is to be forwarded as broadcast ffffffff to all stations in network 00000001. Because a filter has been set on the socket, the frame is rejected by the router.

### Online Trace'RIP'

The outputs under 'RIP' describe the processing of IPX routing information protocol frames by the RIP process of the IPX router. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit/Action] [Source node address] [Frame type] [Para.] [Network address] [Hops] [Tics] [Action] ... [Network address] [Hops] [Tics] [Action]

- Example:

LAN-Rx node: 0000c0123456 Req: 00000002

An RIP request for the IPX network 00000002 is received from the local network. The RIP request was sent from the IPX node 0000c0123456.

- Example:

LAN-Rx node: 00a057123456 Resp

Route: 00000002 Hops: 0001 Tics: 0002 Up

An RIP response (routing information protocol response) was received from the local network (generated by the IPX node 00a057123456). With this response route 00000002, with a hop distance (number of interim stations) of 1 and a tic distance of 2, is entered as available again in the RIP table.

LAN update

The RIP process sends all required routing information to the local network.

### Online Trace'SAP'

The outputs under 'SAP' describe the processing of IPX service advertising protocol frames by the SAP process of the IPX router. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit/Action] [Source node address] [Frame type] [Para.] [Service type] [Server name] [Action] ... [Service type] [Server name] [Action]

- Example:

LAN-Rx node: 00a057123456 response

0004 FS\_development up

```
0107 FS_development up
023f FS_development up
0511 FS_development up change
030c 08000912345678CGNP-development filtered
```

An SAP response was received (sent by the IPX node 00a057123456) by the local network. With this response the servers 'FS\_development' (file server), 'FS\_development' (NetWare 386 server), 'FS\_development' (DNS server) and 'FS\_development' (time sync server) are recorded as available again in the SAP table. In this case the status of the time sync server 'FS\_development' has changed in the SAP table (i.e. the server was previously not available). The last displayed server is a print server; because this server type is set with a SAP filter, it is not recorded in the SAP table but is rejected.

#### LAN trigger

Because of a received SAP response a status change in the SAP table has occurred, which is immediately reported in the local network by the SAP process; the change can therefore only have occurred because of the WAN's evaluation of a SAP response.

#### LAN age

The SAP process of the router "ages" all server/services forwarded from the local network minute by minute. After a period that can be adjusted a SAP entry is deleted (Setup/IPX-module/SAP-configuration/Aging-minutes)

### Online Trace 'IPX watchdogs'

The outputs under 'IPX-Wd.' describe the processing of so-called 'IPX watchdog' packets. These are packets that are sent at regular intervals from a Novell server to a workstation to verify the connection to this workstation. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit] [Source address] [Target address] [Action]
- Example:

```
LAN RX
```

```
DstAddr: 12345678 00a057654321 0451
```

```
SrcAddr: 00000002 00a057123456 0451
```

```
SpooF
```

The *ELSA LANCOM* has received an IPX watchdog from the node 00a057123456, which was intended for checking a remote workstation. Because the remote network with the workstation is active, the IPX watchdog is answered locally by *ELSA LANCOM* to avoid establishing a connection unnecessarily. Alternatively the following displays for actions will appear:

- **Route:** The IPX watchdog is forwarded (establishes a connection)
- **Filter:** The IPX watchdog is rejected and not answered
- **Dst Net DOWN Error:** The IPX watchdog target network is not available.

### Online Trace 'SPX watchdogs'

The processing of 'SPX watchdog' packets by the outputs under SPX-Wd. is described analogous to the trace outputs for IPX watchdogs. These are packets sent by a Novell server at regular intervals to the workstation to check an SPX connection (e.g. R-console). The trace outputs are displayed as follows:

- Format: [Source interface] [Receive/Transmit] [Source address] [Target address] [Action]

therefore completely analogous to the displays of the IPX watchdog packets.

### Online Trace 'IPX-NetBIOS'

The outputs under NetBIOS describe the processing of IPX NetBIOS and IPX propagated packets. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit] [Source address] [Target address] [Action]
- Example:  

```

LAN RX
DstAddr: 12345678 00a057654321 0455
SrcAddr: 00000002 00a057123456 0455
Route
```

### Online Trace 'IP-Rt.'

The outputs under 'IP-Rt.' describe the processing of IP frames by the IP router. They are displayed in the following format:

- Format: [Source interface] [IP target address] [IP source address] [Protocol] [Target port] [Source port] [Type of service] [Action] [Target]
- Example:  

```

LAN RX
DstIP: 195.162.38.161, SrcIP: 194.162.38.162
Prot.: TCP, DstPort: 23, SrcPort: 1197, TOS: ----
Route: WAN-Tx peer: R1
```

The IP router has received a TCP packet from the computer with the IP address 194.162.38.162, which is to be sent to the computer 195.162.38.161.

The source port is 1197, the target port 23 (telnet), a bit is not set in the TOS. The field TOS may accept the following values (or a combination of them):

D---	Low delay
-T--	High throughput
--R-	High reliability
---C	Low costs

The packet is routed and the target computer can be reached under the logical remote station **R1**. Therefore, the packet is sent on a WAN interface.

LAN RX

DstIP: 195.162.38.161, SrcIP: 194.162.38.162

Prot.: ICMP, DstPort: ---, SrcPort: ---, TOS: --R-

Route: WAN-Tx peer: R1

The IP router has received an ICMP packet from the computer with the IP address 194.162.38.162, which is to be sent to the computer 195.162.38.161.

Because ICMP does not know any ports, --- is output as target or source port. The field **High Reliability** is set in the TOS.

### Online Trace 'IP-RIP'

The outputs under 'IP-RIP' describe the processing of IP routing information protocol frames by the RIP process of the IP router. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/transmit/Action] [Source address] [RIP version] [Routing domain] [Network address] [Network mask] [Best route] [Distance] [Action] ... [Network address] [Network mask] [Best route] [Distance] [Action]

- Example:

LAN-Rx Src: 194.162.38.252

Vers.: RIP-1 Routg.Dom.: 0000

190.254.0.0255.255.0.0194.162.38.1623Store

195.126.38.0255.255.255.0194.162.38.1623update

255.255.255.2550.0.0.0194.162.38.1622Discard

194.162.38.0255.255.255.0194.162.38.1622Discard

An RIP-1 frame has been received from the local network. This frame contains the route to the networks 190.254.0.0, 195.126.38.0, 255.255.255.255 (DEFAULT route) and 194.162.38.0. The procedure with these routes was as follows:

Route 190.254.0.0 is saved because it is either better than the prior one or is still unknown.

Route 195.126.38.0 is processed, ie the route is unchanged, only the distance may have changed. In every case the aging timer is reset.

The DEFAULT route has been rejected because a better route is known.

The route to network 194.162.38.0 is rejected because it is a route to the local network (split horizon).

The trace outputs of received RIP frames are always done after they have been evaluated by the RIP process and network masks (RIP-1) and best route have been determined. With RIP frames that have been sent the packets are displayed as they were sent. For example, with RIP-1 frames this means that the network masks are always output as 0.0.0.0.

### Online Trace 'ARP'

The outputs under 'ARP' describe the processing of address resolution protocol frames by the TCP-IP module. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit/Action] [Source address] [Target address] [Target/Action]

- Example:

LAN-Rx request

SrcIP: 194.162.38.162, DstIP: 194.162.38.171

Cache update: 194.162.38.162 : 0000c0717860

Response LAN-Tx

An ARP request for the IP address 194.162.38.171 has been received from computer 194.162.38.162. The MAC address of the source computer is saved in the ARP table. In addition, the queried computer is the *ELSA LANCOM*. Then an ARP response is sent back on the LAN interface.

### Online Trace 'ICMP'

The outputs under 'ICMP' describe the processing of Internet control message protocol frames by the TCP-IP module. The trace outputs are displayed in the following format:

- Format [Source/Target interface] [Receive/Transmit] [Source/Target address] [Message] [Action]

- Example:

LAN RX

SrcIP: 194.162.38.162: Echo request

LAN TX

DstIP: 194.162.38.162: Echo reply

An ICMP echo request (**ping**) from computer 194.162.38.162 has been received on the LAN interface. The *ELSA LANCOM* answers this with an ICMP echo reply.

### Online Trace 'IP-MASQ'

The outputs under 'IP-MASQ' describe the procedures in the masquerading module. The opening and the closing of a masked connection is output. The display is in the following format:

- Format: [Open/close]: [Protocol] [IP source address] [Source port] [Mapped port] [Reason]

TCP, UDP or ICMP are possible protocols. If the protocol is ICMP, the source port gives the identifier of the request packet. The mapped port field shows how the source port has been set. The cause of a close is given in the reason field. Possible reasons are:

Timeout	The set protocol timeout is expired
TCP finish	A TCP connection was terminated normally
TCP reset	A TCP connection was interrupted because of an error in one of the machines involved
Port assigned	A 'passive' TCP connection was assigned to source port. Example: FTP in passive mode

- Examples:

Open: TCP SrcIP: 10.0.0.44, 1121 -> 64107

Open: TCP SrcIP: 10.0.0.44, 1122 -> 64104

Open: TCP SrcIP: 10.0.0.44, 1123 -> 64105

Close: TCP SrcIP: 10.0.0.44, 1121 -> 64107 TCP reset

### Online Trace "SCRIPT"

The outputs under 'SCRIPT' describe the progress of a script negotiation. The display is in the following format:

- Format: [Source interface] [Receive/transmit/Error] [Text] [Action]

- Example:

CH01: Rx: Password -> Tx: \* \r

In the above example, the password is requested by the remote station. It is returned to the remote station (hidden under a '\*').

### Online Trace 'DHCP'

The outputs under 'DHCP' describe the procedures in the Dynamic Host Configuration Protocol. The queries from DHCP clients and the answer from the DHCP servers are then displayed in the *ELSA LANCOM*. The display is in the following format:

- Format: [DHCP Client Message] [DHCP Server Message]



## Online Trace 'Packet dump'

The 'packet dump' online trace supplements the trace outputs, which are generated by the IP router. The first 64 bytes of a packet is output in hexadecimal format.

# Policy Based Routing

## General

The term 'policy based routing' describes the option of using additional routing methods to the standard routing procedure for IP packets (these "policies").

To make the in-band configuration easier on wide-area networks with heavy data traffic and to improve the cooperation of *ELSA LANCOM* with 'ping' and 'traceroute' mechanisms, two methods for the IP routing have been introduced. Both methods are based on the evaluation of the 'Type of Service' field in the IP header.

The 'Type of Service' field (for short TOS) describes how IP packets should preferably be treated (but need not be), i.e. it reflects the preferred processing procedure intended by the generator of this IP packet. TOS has the following structure in this context:

Bit 7, 6	Bit 5	Bit 4	Bit 3	Bit 2, 1, 0
Unused	Reliable transmission	High Throughput	Low delay	Precedence

The **R** and the **D** bit are evaluated and the behavior adapted to its circumstances by the routing methods.

A set **R** bit requires secured transmission of the associated IP packet. Packets identified as such are always transmitted over a "secured" queue corresponding to their reception sequence. In an extreme case this can result in a "normal" packet that is already in a transmission queue being removed and placed back into the heap to make room for the packet to be sent. This occurs if the maximum number of buffers for the associated connection has already been used. However, the transmission sequence between packets with a set **R** bit and 'normal' bits is not changed by this mechanism.

The secured transmission can be activated for all ICMP packets independently of the entry in the 'Type of Service' field. Because an ICMP packet identified as such is sent without changing the transmission sequence, the throughput delays of a *ELSA LANCOM* can be determined by 'ping' or 'traceroute'.

With a set **D** bit the generator requests the fastest possible forwarding of an IP packet. IP packets identified as such are transmitted over an 'urgent' queue before the send queue packets corresponding to their reception sequence. On one hand, this results in changes in the transmission sequence, because an IP packet identified as last received

is sent first. On the other hand, there is the possibility that a packet already in the send queue will be removed from it again to make room for the IP packet that is to be sent (see above).

Packets that are already in the secured or urgent queue are not rejected. If there is no longer a packet in the normal send, secured or urgent queue, no more packets can be sent. Received IP packets are therefore rejected even with the **D** or **R** bit set.

## Examples

With the setting

`Setup/IP-router-module/Routing-method/IP TOS`

the 'Type of Service' field of the IP header of a received packet is evaluated as described above, ie IP packets with set **D** bit are placed in the urgent queue and packets with set **R** bit in the secured queue. All other packets are placed in the normal send queue.

This means simultaneously that any "normal" IP packets from "secured" or "urgent" packets can be removed (with maximum filling of the send queue of this connection) or changes in the packet sequence can be made.

In the 'normal' setting all IP packets are treated equally, in accordance with the routing regulations of the Internet protocol.

With the setting

`Setup/IP-router-module/Routing-method/ICMP-routing-method`  
all received ICMP packets are transmitted as if they had the **R** bit in the 'Type of Service' field of the IP header. (see above)

This means that the secured transmission of ICMP packet may result in errors in other data flows. The latency period of the router is however not influenced, because the ICMP packet is taken into the send queue as the last in spite of this.

With the 'normal' setting ICMP packets are treated like all other IP packets in accordance with the routing regulations of the Internet protocol.