

ELSA LANCOM™ Série I600 Office

© 2001 ELSA AG, Aachen (Germany)

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

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

Marques

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

Le logo ELSA est une marque déposée d'ELSA AG. Toutes les autres marques citées appartiennent à leurs propriétaires respectifs.

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

ELSA AG

Sonnenweg 11

52070 Aix-la-Chapelle

Allemagne

www.elsa.com

Aix-la-Chapelle, juin 2001

Avant-propos

Merci de votre confiance !

En acquérant le *ELSA LANCOM 1600 Office*, vous avez porté votre choix sur un routeur qui permet à des réseaux locaux ou différentes stations de travail d'accéder à Internet à grande vitesse.

Modèles

Cette documentation décrit différents modèles de la série *ELSA LANCOM 1600 Office* qui se différencient par leur équipement matériel et logiciel :

- *ELSA LANCOM DSL/1610 Office*
- *ELSA LANCOM DSL/I-1611 Office*

*Restrictions
selon les modèles*

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

Documentation

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

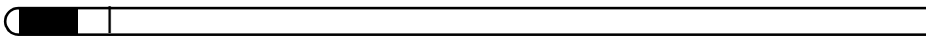
Si vous deviez trouver une erreur, ou désirez exprimer une critique ou une faire une suggestion concernant la documentation, envoyez-nous directement un courrier électronique à l'adresse suivante :



editorial@elsa.de



*Si vous aviez encore des questions sur les thèmes abordés dans ce manuel ou si vous aviez besoin d'assistance, nos services en ligne (www.elsa.com) sont à votre disposition 24 heures sur 24. Vous y trouverez sous 'Support' une FAQ (**F**oire **A**ux **Q**uestions – réponse aux questions fréquemment posées) concernant le produit que vous venez d'acquérir. De plus, notre banque de données (KnowledgeBase) vous fournit un grand nombre d'informations. Les pilotes les plus récents, les microprogrammes, des utilitaires et les manuels peuvent être téléchargés.*



FR

Contenu

1 Introduction	9
1.1 Champs d'application du routeur	9
1.2 Applications typiques	10
1.2.1 Internet dans le réseau local	10
1.2.2 Interconnexion de réseaux locaux	11
1.2.3 Télétravail avec l'accès à distance	11
1.2.4 Bureautique	12
1.3 Avantages d'un routeur <i>ELSA LANCOM 1600 Office</i>	12
1.3.1 Tous les périphériques de la série <i>ELSA LANCOM 1600 Office</i>	12
1.3.2 Fonctions supplémentaires <i>ELSA LANCOM DSL/I-1611 Office</i>	16
2 ELSA LANCOM 1600 Office se présente	21
2.1 La face avant de l'appareil	21
2.2 La face arrière de l'appareil	23
3 Installation	25
3.1 Contenu de l'emballage	25
3.2 Configuration système requise	25
3.3 Installation du matériel	26
3.4 Installation du logiciel	27
3.4.1 Lancer le programme d'installation ELSA	27
3.4.2 Quels logiciels installer ?	28
3.5 Le chapitre suivant...	29
4 Réglages de base	31
4.1 Démarrage de l'assistant d'installation	31
4.1.1 Réglages de base avec <i>ELSA LANconfig</i>	32
4.1.2 Réglages de base avec <i>ELSA WEBconfig</i>	34
4.2 Configuration de l'accès à Internet	37
4.2.1 Démarrage de l'assistant de configuration sous <i>ELSA LANconfig</i>	38
4.2.2 Démarrage de l'assistant de configuration sous <i>ELSA WEBconfig</i>	38
4.2.3 Saisie des données d'accès	38
4.3 Réglages des paramètres sur les postes de travail	38
4.4 Terminé !	39

5 Configuration et gestion	41
5.1 La configuration	41
5.2 Logiciels de configuration	42
5.2.1 Configuration par <i>ELSA LANconfig</i>	43
5.2.2 Configuration avec <i>ELSA WEBconfig</i>	44
5.2.3 Configuration par Telnet	46
5.2.4 Configuration par SNMP	47
5.3 La configuration à distance via l'accès réseau à distance	47
5.3.1 Ce dont vous avez besoin pour la configuration à distance	48
5.3.2 La première connexion à distance par l'accès réseau à distance	48
5.3.3 La première connexion à distance avec un client PPP et Telnet	49
5.3.4 Restriction de la configuration à distance	49
5.4 <i>ELSA LANmonitor</i> – garder une vue d'ensemble	51
5.4.1 Affichage des réglages disponibles	52
5.4.2 Contrôle de la connexion Internet	52
5.5 Editions des tracés – Informations pour les utilisateurs avancés	54
5.5.1 Lancement d'un tracé	54
5.6 Sauvegarde et restauration de la configuration	56
5.7 Nouveau microprogramme avec <i>ELSA FirmSafe</i>	57
5.7.1 Comment fonctionne <i>ELSA FirmSafe</i> ?	57
5.7.2 Comment charger le nouveau logiciel ?	58
6 Sécurité d'exploitation	61
6.1 Protection pour la configuration	61
6.1.1 Protection par mot de passe	61
6.1.2 Le verrouillage des accès	63
6.1.3 Contrôle des accès via TCP/IP	64
6.2 Protection pour le réseau local	65
6.2.1 La cachette – Masquering IP (NAT, PAT)	65
6.2.2 Filtrage de paquets de données – Pare-feu	69
6.3 Protection de l'accès RNIS	73
6.3.1 Le contrôle d'identification	74
6.3.2 Le rappel	76
6.4 La liste de contrôle sécurité	77
7 Services serveur pour le réseau local	81
7.1 Gestion d'adresses IP automatique via DHCP	81
7.1.1 Le serveur DHCP	81
7.1.2 DHCP – 'Actif', 'Inactif' ou 'Auto' ?	82
7.1.3 Attribution des adresses	83

7.2 DNS	87
7.2.1 Que fait un serveur DNS ?	87
7.2.2 Routage par DNS	89
7.2.3 Configuration du serveur DNS	90
7.3 Gestion des taxes téléphoniques	94
7.3.1 Limitation de la connexion pour modem DSL et modem-câble	95
7.3.2 Limitation des communications RNIS en fonction des unités de taxation... ..	96
7.3.3 Limitation des communications RNIS en fonction de la durée	97
7.3.4 Configuration dans le gestionnaire des coûts	98
7.4 Le module SYSLOG	98
7.4.1 Configuration du module SYSLOG	99
7.4.2 Exemple de configuration avec <i>ELSA LANconfig</i>	99
7.5 Bureautique avec <i>ELSA LANCAP</i>	101
7.5.1 Avantages de <i>ELSA LANCAP</i>	102
7.5.2 Installation du client <i>ELSA LANCAP</i>	102
7.5.3 Configuration des clients <i>ELSA LANCAP</i>	103
7.5.4 Configuration du serveur <i>ELSA LANCAP</i>	104
7.5.5 Utilisation de <i>ELSA LANCAP</i>	107
7.5.6 <i>ELSA CAPI Faxmodem</i>	108

8 Routage et connexions WAN 109

8.1 Connexions WAN - Généralités	109
8.1.1 Ponts pour protocoles standard	109
8.1.2 Que se passe-t-il lors d'une requête provenant du réseau local ?	110
8.2 Routage IP	111
8.2.1 Le tableau de routage IP	111
8.2.2 Routage local	114
8.2.3 Routage dynamique avec IP-RIP	115
8.2.4 Policy Based Routing	119
8.2.5 SYN/ACK-Speedup	119
8.3 Configuration des correspondants	120
8.3.1 Liste des noms	120
8.3.2 Liste des couches	122
8.4 Etablissement de la connexion via PPP	124
8.4.1 Le protocole	125
8.4.2 Tout est bon? Vérification de la ligne avec LCP	127
8.4.3 Attribution des adresses IP avec PPP	127
8.4.4 Paramètres dans la liste PPP	129
8.5 Etablissement de la connexion DSL avec PPTP	130
8.6 Liaison fixe pour flatrates – Keep-Alive	131

8.7 Fonctions de rappel automatique	132
8.7.1 Rappel automatique via le protocole CBCP de Microsoft	132
8.7.2 Rappel rapide selon la procédure ELSA	134
8.7.3 Rappel automatique selon RFC 1570 (extensions LCP PPP)	134
8.7.4 Vue d'ensemble de la configuration de la fonction de rappel	135
8.8 Regroupement des canaux avec MLPPP	136
9 Caractéristiques techniques	139
9.1 Puissance et spécifications	139
9.2 Brochage	141
9.2.1 Interfaces Ethernet 10/100Base-T (LAN) et 10Base-T (WAN)	141
9.2.2 Interface RNIS S_0	141
9.2.3 Interface de configuration (Outband)	142
10 Appendice	143
10.1 Conditions générales de garantie	143
10.2 Déclaration de conformité Union Européenne (CE)	145
11 Index	147

1

Introduction

Les développements rapides dans le domaine de la technique informatique ont entraîné, au cours des dernières années, une forte augmentation du volume de données transférées par voie électronique. De plus en plus d'utilisateurs souhaitent envoyer et recevoir de plus en plus de données. Une demande à laquelle ne peuvent plus répondre les technologies de transfert utilisées jusqu'alors (par l'intermédiaire de modems ou de périphériques RNIS).

Les nouvelles technologies permettent de dépasser ces barrières et offrent aux utilisateurs une réelle communication large bande, à des taux de transfert nettement plus élevés que ceux atteints jusqu'à aujourd'hui. L'un des principaux critères de propagation de ces nouvelles technologies d'accès est leur disponibilité dans un maximum de bureaux et de foyers. On compte parmi ces technologies la transmission par DSL qui permet de franchir la « dernière étape » par de simples conduites en cuivre. L'accès au réseau câblé de télédistribution permet également de réaliser un accès large bande à Internet.

Un *ELSA LANCOM 1600 Office* peut être utilisé avec pratiquement tous les accès ultrarapides à Internet, via DSL ou réseau câblé de télédistribution. L'accès réel à Internet s'effectue alors toujours par le biais d'un modem auquel le routeur est raccordé.

Ce chapitre...

...vous présente brièvement les fonctions et champs d'application des routeurs et vous donne ensuite une vue d'ensemble des possibilités que vous ouvre votre *ELSA LANCOM 1600 Office*. Vous trouverez dans les chapitres suivants une description détaillée des fonctions, du logiciel et de son utilisation ainsi qu'une introduction aux principes techniques de base.

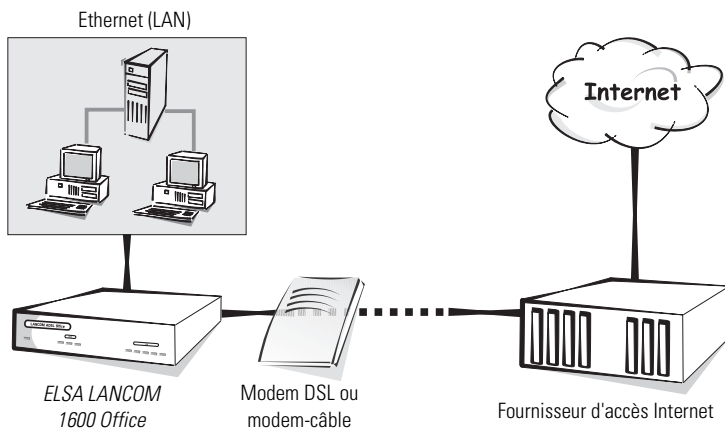
1.1

Champs d'application du routeur

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

Ce chemin se présente sous forme d'une connexion DSL réalisée par ex. sur une ligne téléphonique normale. Un *ELSA LANCOM DSL/I-1611 Office* met également à votre disposition une connexion RNIS avec un véritable routeur RNIS, les fonctions d'*ELSA LANCAP* et une fonction de sauvegarde pour la connexion Internet.

Ces performances font de l'un *ELSA LANCOM 1600 Office* le périphérique idéal pour l'utilisation de liaisons Internet ultrarapides. 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.



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 doivent, le cas échéant, lui être transmises.

1.2 Applications typiques

1.2.1 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, courrier électronique (e-mail) et le transfert de fichiers 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. Fonctions de sécurité comme masquering IP et filtres pare-feu protègent votre réseau contre tout accès extérieur.

1.2.2

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.

*Uniquement ELSA
LANCOM DSL/
I-1611 Office*

Un *ELSA LANCOM DSL/I-1611 Office* permet d'effectuer un couplage LAN-LAN direct via RNIS. En revanche, le couplage de réseaux est plus rapide, plus économique et plus flexible par l'intermédiaire d'Internet. C'est là que l'accès large bande (via DSL ou réseau câblé de télédistribution) à Internet entre en jeu. Les couplages LAN-LAN par Internet sont réalisés en tant que réseaux privés virtuels (VPN).

Tous les *ELSA LANCOM 1600 Office* peuvent être équipés de l'option *ELSA LANCOM VPN Option* et supportent la création de réseaux privés virtuels.

1.2.3

Télétravail avec l'accès à distance

*Uniquement ELSA
LANCOM DSL/
I-1611 Office*

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. Dans le cas de l'accès à distance, un *ELSA LANCOM 1600 Office* garantit bien entendu un degré de protection élevé pour 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.

Le *ELSA LANCOM DSL/I-1611 Office* autorise l'accès à distance par le biais de l'interface RNIS.

1.2.4

Bureautique

*Uniquement ELSA
LANCOM DSL/
I-1611 Office*

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 *ELSA LANCAPI*.

ELSA 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.

Le *ELSA LANCOM DSL/I-1611 Office* autorise les fonctions de bureautique par le biais de l'interface RNIS.

1.3

Avantages d'un routeur **ELSA LANCOM 1600 Office**

Pour vous donner un aperçu des fonctionnalités de votre périphérique, en voici les caractéristiques essentielles.

1.3.1

Tous les périphériques de la série **ELSA LANCOM 1600 Office**

Simplicité d'installation

- Connecter *ELSA LANCOM 1600 Office* à une source de tension
- Réaliser la connexion avec le réseau local
- Réaliser la connexion avec le modem DSL ou le modem-câble
- Raccorder le câble RNIS (uniquement *ELSA LANCOM DSL/I-1611 Office*)
- Allumer
- Installation des logiciels ELSA et de la configuration de base à l'aide d'assistants conviviaux
- A vous de jouer !

Connexion à un réseau local

Les routeurs DSL de ELSA sont connectés par port 10/100Base-T sur un (Fast-)Ethernet. Le port détecte automatiquement la vitesse de transmission dans le réseau local.

Connexion à un réseau étendu WAN

ELSA LANCOM 1600 Office sur l'interface Ethernet d'un modem DSL ou un modem-câble.

Un *ELSA LANCOM DSL/I-1611 Office* est également équipé d'une prise RNIS raccordée aux interfaces S_0 d'un connecteur multiple RNIS (configuration point-à-multipoint) ou d'un connecteur de standard (configuration point à point). Le routeur détecte automatiquement le type de l'accès RNIS et le protocole de canal D utilisé.

Routeur IP : Etablissement et gestion des liaisons

Dans un réseau, le routeur contrôle tous les paquets IP et vérifie s'ils doivent être envoyés dans un autre réseau ou non. Lorsque les données doivent être transmises, le routeur établit la liaison automatiquement et la termine à la fin de la transmission.

Fonctions de sécurité

Afin de protéger le réseau interne de l'entreprise contre tout accès non autorisé de l'extérieur, un *ELSA LANCOM 1600 Office* dispose de fonctions de sécurité très puissantes. La fonction Masquerading IP masque tous les postes de travail du réseau local derrière une seule et même adresse IP publique. Leur véritable identité reste cachée. Les filtres pare-feu permettent de bloquer de façon ciblée certaines adresses IP, certains protocoles et certains ports. Les filtres adresses MAC, quant à eux, permettent de contrôler de manière ciblée l'accès des postes de travail du réseau local à la fonction de routage IP du périphérique.

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. Cette mesure protège la configuration du routeur contre les attaques répétées.

DHCP

Votre *ELSA LANCOM 1600 Office* dispose des modes DHCP suivants :

- Serveur DHCP : attribue des adresses IP
- Relais DHCP : transmet les interrogations DHCP

Grâce au réglage réalisé en usine, le périphérique travaille en mode automatique intelligent, faisant ainsi de la mise en service d'un *ELSA LANCOM 1600 Office*, au sein d'un réseau existant tout comme dans un tout nouveau réseau, un véritable jeu d'enfant.

Serveur DNS

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

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

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

Virtual Private Network (VPN)

Votre *ELSA LANCOM 1600 Office* peut être équipé de l'option VPN et servir alors de véritable passerelle VPN (selon le standard IPSec). Il peut ainsi établir des couplages de réseaux sûrs vers d'autres passerelles VPN par l'intermédiaire d'Internet (ou d'autres réseaux IP). Le standard IPSec et les techniques de codage les plus modernes garantissent un niveau de sécurité élevé au niveau des liaisons VPN.

ELSA LANmonitor

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

- Etat de la liaison pour chaque canal de transmission (uniquement *ELSA LANCOM DSL/I-1611 Office*)
- Nom du correspondant en ligne
- Quel module de l'appareil est raccordé (routeur, *ELSA LANCAP*)
- Durée de communication et taux de transfert

- Extraits des statistiques du routeur (par ex. les informations de la négociation PPP)

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

Affichage de l'état

Des témoins lumineux sur la face avant du boîtier permettent de contrôler les accès LAN et WAN et facilitent le diagnostic en cas d'anomalie.

Configuration

Le réglage et l'adaptation des périphériques sur leur tâche spécifique s'effectue rapidement et confortablement à l'aide de l'outil de configuration pour Windows joint *ELSA LANconfig*.

Vous trouverez une version beta de xLANconfig pour Linux sur le CD-ROM ELSA LANCOM Office ou, pour sa dernière mise à jour, sur la page Internet d'ELSA, dans la rubrique Pilotes.

Les utilisateurs d'autres systèmes d'exploitation utilisent la configuration basée sur le HTML via *ELSA WEBconfig*, un système de gestion SNMP, Telnet ou un émulateur de terminal quelconque.

L'accès au périphérique est possible à partir du réseau local ou du réseau étendu, via la configuration à distance par RNIS (uniquement *ELSA LANCOM DSL/I-1611 Office*) ou directement par l'intermédiaire de l'interface de configuration intégrée. Dans les deux premiers cas, la configuration peut se faire avec SNMP ou le protocole de transfert TFTP.

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

Mise à jour des microprogrammes

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

La version la plus récente du microprogramme est toujours disponible sur la page d'accueil ELSA et peut être téléchargée via le réseau local, le réseau étendu (uniquement *ELSA LANCOM DSL/I-1611 Office*) ou l'interface de configuration.



ELSA FirmSafe

Vous ne courez aucun risque quand vous téléchargez le nouveau microprogramme : la fonction ELSA 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 périphérique réutilise automatiquement la version précédente en état de fonctionner.

Contrôle des coûts de communication

Les coûts pour l'utilisation d'Internet sont facturés, suivant le fournisseur d'accès, en fonction de la durée de connexion. Pour ne pas être surpris par une facture de téléphone démesurée à la fin du mois, vous pouvez fixer à l'avance combien de minutes vous souhaitez naviguer en ligne pendant une certaine période (par ex. : 600 minutes en 6 jours) en utilisant un *ELSA LANCOM 1600 Office*.

Statistiques

Grâce aux nombreuses fonctions de statistique, vous avez le routeur *ELSA LANCOM 1600 Office* dans votre poche. Vous trouverez ici par ex. toutes les informations concernant les paquets de données transmis et pourrez ainsi optimiser la configuration de votre appareil.

1.3.2

Fonctions supplémentaires *ELSA LANCOM DSL/I-1611 Office*

Le *ELSA LANCOM DSL/I-1611 Office* dispose d'une prise RNIS et met ainsi plusieurs fonctions supplémentaires à votre disposition.

Routeur multiprotocole

L'interface RNIS autorise non seulement le routage IP mais aussi le routage d'autres protocoles. Ainsi le protocole IPX permet le couplage de réseaux Novell.

Pour l'installation de réseau Microsoft Peer-to-Peer, les routeurs ELSA présentent une caractéristique spéciale : le routage intégré de paquets IP-Net-BIOS 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 proxy NetBIOS, le routeur répondra localement aux demandes concernant des ordinateurs connus et évitera donc l'établissement de connexions inutiles.

Compatibilité par PPP

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

Configuration à distance via PPP

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

Fonctions de sécurité pour l'interface RNIS

Pour la protection de l'interface RNIS intégrée, un *ELSA LANCOM DSL/I-1611 Office* utilise, en plus de la protection par mot de passe et de l'identification du numéro de l'appelant (CLIP), une fonction de rappel qui permet d'établir la liaison seulement avec des numéros d'appel RNIS déterminés au préalable. Les mécanismes d'authentification au sein du PPP viennent encore agrandir le concept de sécurité.

Option *ELSA Dynamic VPN*

Sur un *ELSA LANCOM DSL/I-1611 Office*, l'option *ELSA LANCOM VPN Option* vous permet également d'établir un tunnel VPN vers un site distant doté d'une adresse IP dynamique, grâce à la technologie *ELSA Dynamic VPN*, pour laquelle ELSA a d'ailleurs déposé une demande de brevet.

ELSA LANCAPI et *ELSA CAPI Faxmodem*

La mise en œuvre de l'interface *ELSA LANCAPI* apporte des avantages surtout économiques. *ELSA 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 *ELSA LANCAPI*, libre accès aux fonctions de bureautique telles que le télécopieur et EuroFileTransfer. Toutes les fonctions sont mises à disposition via le réseau sans que la station de travail ait besoin d'être dotée de matériel supplémentaire. Donc aucun achat d'adaptateurs de terminal RNIS ou de modems coûteux ne grève le budget informatique. Tout ce qu'il faut, ce sont les logiciels de communication et de bureautique à installer sur les stations de travail.

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

Interrogation automatique de l'heure

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

Regroupement des canaux et compression

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

Least Cost Routing

Même si le nombre d'opérateurs offrant les services de télécommunication est important, le rerouteur téléphonique permet d'obtenir toujours les lignes RNIS les plus avantageuses. Vous définissez pour commencer les opérateurs ayant les tarifs les plus avantageux pour vos besoins, et le routeur fait passer chaque appel (peu importe qu'il soit effectué par le routeur ou par l'interface *ELSA LANCAPI*) par l'opérateur le moins cher.

Option ligne permanente

Grâce à l'option ligne permanente, il est possible de coupler des réseaux via les lignes spécialisées RNIS.

2

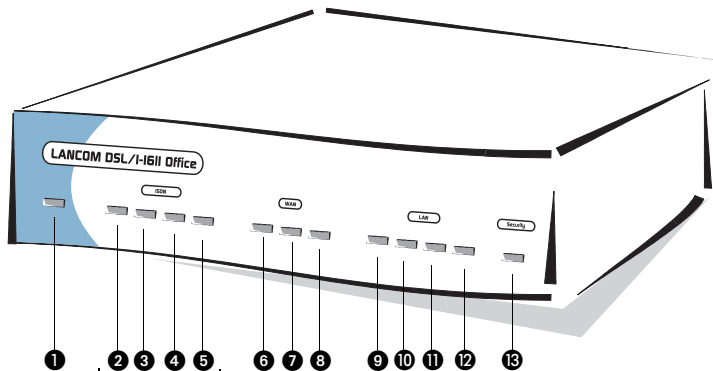
ELSA LANCOM 1600 Office se présente

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

2.1

La face avant de l'appareil

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



Ces LED sont uniquement présentes sur le *ELSA LANCOM DSL/I-1611 Office*

Signification des témoins lumineux (LED)

- ❶ **Power/Msg** – Cette LED sur le point d'accès s'allume brièvement lors de la mise sous tension. En cas d'erreur après l'auto-diagnostic, un code clignotant sera affiché, sinon, le périphérique sera en service et le témoin lumineux sera allumé constamment.

inactif		Périphérique hors circuit
rouge	1 x brièvement	Le lancement (test et chargement) a commencé
rouge	clignotant	Erreur lors du lancement (signalée par le code clignotant) ; clignote également lorsque le budget temps ou unités a été atteint
rouge		Périphérique prêt au service

Uniquement ELSA
LANCOM DSL/I/-
1611 Office

② ISDN S₀ Status – indique l'état de la connexion RNIS S₀ :

inactif		Non branché ou pas de tension S ₀ (sur les lignes RNIS, la tension S ₀ est souvent désactivée après une durée d'inactivité)
vert	clignotant	Initialisation (prise de contact avec le poste connecteur)
vert		Prêt au service (bus S ₀ activé, TEL présent et protocole canal D vérifié)
vert	alimentation arrêt	Témoin lumineux allumé bien que le témoin lumineux « Power » est éteint : appareil dans le moniteur de lancement

Uniquement ELSA
LANCOM DSL/I/-
1611 Office

③ ISDN Chan1 – état du premier canal B RNIS logique (aussi bien en mode routeur qu'en mode CAPI) :

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

Uniquement ELSA
LANCOM DSL/I/-
1611 Office

④ ISDN Chan2 – indique le deuxième état logique du canal RNIS B (signification identique à RNIS Chan1)

Uniquement ELSA
LANCOM DSL/I/-
1611 Office

⑤ ISDN-1+2 – indique si cette connexion RNIS est un regroupement statique ou dynamique de canaux.

inactif	Aucune connexion ou aucun regroupement actif de canaux
vert	Liaison par regroupement dynamique ou statique active

⑥ WAN Rx/Tx – cette LED jaune indique le transfert de données par l'intermédiaire de la connexion WAN (par modem DSL ou modem-câble).

⑦ WAN Link – cette LED verte indique que la connexion Ethernet entre ELSA LANCOM 1600 Office et le modem DSL ou modem-câble est correcte.

- ❸ **WAN Chan** – cette LED indique l'état de la connexion WAN (par modem DSL ou modem-câble) au fournisseur d'accès. La connexion au fournisseur d'accès nécessite normalement une ouverture de session avec nom d'utilisateur et mot de passe. Dans le cas de tarifs de connexion payants en fonction du temps, les unités sont comptabilisées durant cette période. Signification détaillée de la LED :

inactif	Aucune inscription n'a été demandée sur la ligne de jonction
rouge	Une inscription a été demandée auprès de la ligne de jonction et est actuellement effectuée
vert	L'inscription a été réalisée et la connexion est établie vers le fournisseur.

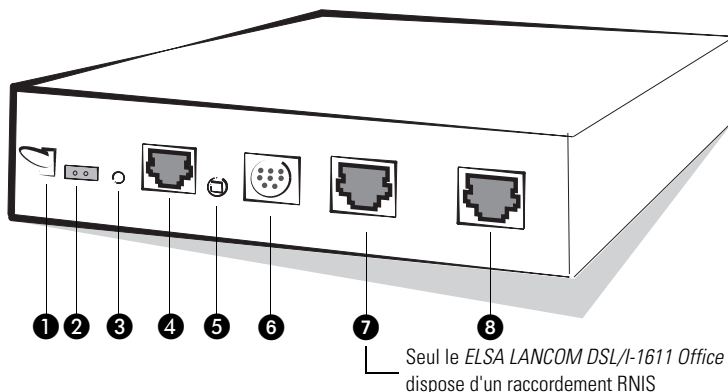
- ❹ **LAN Rx/Tx** – Un paquet de données est envoyé du périphérique vers le LAN ou du LAN vers le périphérique
- ❺ **LAN Coll** – Collision lors de l'envoi de données
- ❻ **LAN Link** – La connexion est établie vers le LAN et prête à fonctionner
- ❼ **LAN Fast** – Le périphérique fonctionne en LAN en mode 100 Mbits
- ❽ **Security VPN/Msg** – En mode passerelle VPN, cette LED fournit des informations sur le statut de toutes les activités VPN :

inactif	Aucune connexion active VPN établie
vert	Connexion(s) active(s) VPN établie(s)
rouge	Etablissement d'un tunnel VPN

2.2

La face arrière de l'appareil

Les ports et interrupteurs du périphérique se trouvent sur sa face arrière.



❶ Commutateur Marche/Arrêt

❷ Raccord bloc d'alimentation

Utilisez impérativement le bloc d'alimentation fourni. L'utilisation d'un bloc d'alimentation inapproprié peut entraîner des blessures ou dégâts matériels.

❸ Bouton de réinitialisation – pour remettre le périphérique à son état lors de la livraison, appuyer sur le bouton de réinitialisation pendant environ 5 secondes. Dès que le bouton est relâché, les LED situées sur la face avant du périphérique s'allument et l'appareil redémarre dans son état à la livraison.

❹ 10/100Base-Tx pour la connexion au réseau local. Supporte toutes les connexions 10 Mbits ou 100 Mbits. Le ELSA LANCOM 1600 Office reconnaît automatiquement la vitesse utilisée sur le réseau (Autosensing).

❺ Commutateur nœud/concentrateur – pour permettre le raccordement direct à un ordinateur, il est possible d'intervertir dans le périphérique les lignes d'envoi et de réception de la connexion au réseau local (❹), position 'Concentrateur'. En cas de raccordement à un concentrateur ou commutateur, ce contacteur devrait se trouver sur 'Nœud' (réglage par défaut).

❻ Interface de configuration V.24

❼ Raccordement RNIS/S₀ (uniquement ELSA LANCOM DSL/I-1611 Office)

❽ Raccordement 10Base-T pour modem DSL ou modem-câble

3 Installation

L'objectif de ce chapitre est de vous aider à installer le plus rapidement possible matériel et logiciels. Vérifier tout d'abord le contenu du coffret et la configuration système requise. Lorsque toutes les conditions sont remplies, le raccordement et la mise en route sont un véritable jeu d'enfant.

3.1 Contenu de l'emballage

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

- *ELSA LANCOM 1600 Office*
- Bloc d'alimentation
- Câble de connexion à un réseau local, fiche verte
- Câble de connexion à un réseau étendu pour modem DSL ou modem-câble, fiche bleu foncé
- Câble de connexion RNIS, fiche bleu clair (uniquement *ELSA LANCOM DSL/I-1611 Office*)
- Câble pour l'interface série de configuration
- CD-ROM *ELSA LANCOM Office* avec *ELSA LANtools* et autres logiciels
- Autocollant de licence d'utilisation avec les numéros de série des logiciels
- Documentation imprimée

Si l'un des composants devait manquer, veuillez vous adresser à l'adresse indiquée sur le bon de livraison de votre périphérique.

3.2 Configuration système requise

Les ordinateurs souhaitant établir une communication avec un *ELSA LANCOM 1600 Office* doivent au moins satisfaire aux exigences suivantes :

- Système d'exploitation de votre choix prenant en charge TCP/IP, par ex. Windows Millennium Edition (Me), Windows 2000, Windows 98, Windows 95, Windows NT, Linux, Apple Mac OS, OS/2, BeOS.
- Une carte Ethernet doit être installée.
- Le protocole TCP/IP doit être installé.
- Un navigateur Web doit être installé dans certains cas.



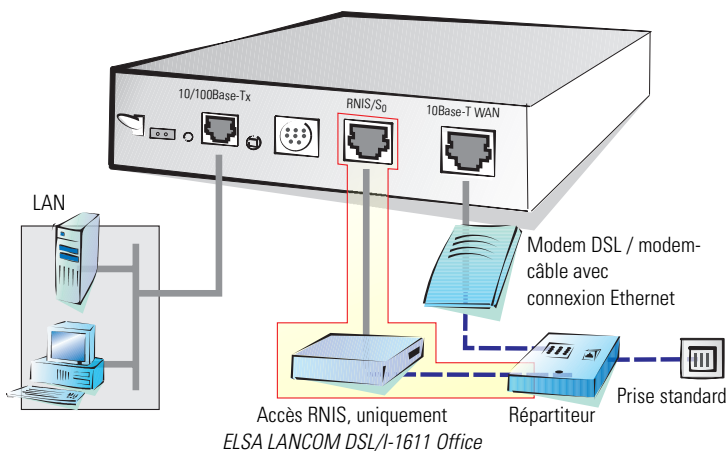
Les outils *ELSA LANtools* et les fonctions de l'interface *ELSA LANCAPI* (uniquement *ELSA LANCOM DSL/I-1611 Office*) requièrent un système d'exploitation Windows.

FR

3.3

Installation du matériel

- ① Connectez votre point d'accès *ELSA LANCOM 1600 Office* au réseau local LAN. Pour cela, relier une extrémité du câble réseau joint (fiche verte) à la connexion 10/100 Base-Tx du périphérique (④) et l'autre à une prise réseau libre de votre réseau local (ou bien une prise libre d'un concentrateur de votre LAN). Vous pouvez également choisir de raccorder un autre ordinateur. Dans ce cas, mettez le commutateur nœud/concentrateur (⑤) en position 'concentrateur'.



- ② Reliez votre *ELSA LANCOM 1600 Office* au réseau DSL ou câblé de télédistribution. Pour cela, branchez le câble de connexion WAN (fiche bleu foncé) dans la prise 10Base-T (⑧) du périphérique. Raccordez l'autre extrémité à votre modem DSL ou modem-câble.
- ③ Connectez votre *ELSA LANCOM DSL/I-1611 Office* au réseau RNIS. Pour cela, enfichez l'une des extrémités du câble de connexion RNIS (fiche bleu clair) fourni dans le connecteur RNIS/S₀ (⑦) de l'appareil et l'autre à un connecteur de standard ou multiple RNIS/S₀ (configuration point-à-point ou point-à-multipoint).

Uniquement *ELSA LANCOM DSL/I-1611 Office*



Attention, votre modem DSL ou modem-câble doit disposer d'une connexion Ethernet (10Base-T). Il n'est pas possible d'exploiter le ELSA LANCOM 1600 Office avec un modem disposant uniquement d'une interface USB ou ATM-F.

- ④ Alimentez l'appareil en tension nécessaire via le bloc d'alimentation et mettez-le en circuit. Après un autotest bref de l'appareil, le témoin lumineux 'Power/Msg' est allumé en permanence. Le témoin lumineux 'LAN-Link' indique qu'une liaison correcte est établie avec le réseau local.



Si cette LED ne s'allume pas, actionnez le commutateur nœud/concentrateur (⑤) situé sur le dos de l'appareil. Si la LED ne s'allume toujours pas, il est possible que la carte réseau ou les câbles soient défectueux.

3.4

Installation du logiciel

Cette section est consacrée à la description de l'installation du logiciel ELSA fourni pour Windows. Si vous utilisez votre *ELSA LANCOM 1600 Office* uniquement sur des ordinateurs fonctionnant avec des systèmes d'exploitation autres que Windows, vous pouvez passer à la section suivante. En effet, il n'est pas nécessaire, dans ce cas, d'installer le logiciel.



Certaines fonctions de votre routeur requièrent un système d'exploitation Windows. Parmi elles, la surveillance avec ELSA LANmonitor. Sur le ELSA LANCOM DSL/I-1611 Office, il est également nécessaire d'installer un système d'exploitation Windows sur les postes de travail afin de pouvoir utiliser les fonctions ELSA LANCAPI pour l'interface RNIS.

3.4.1

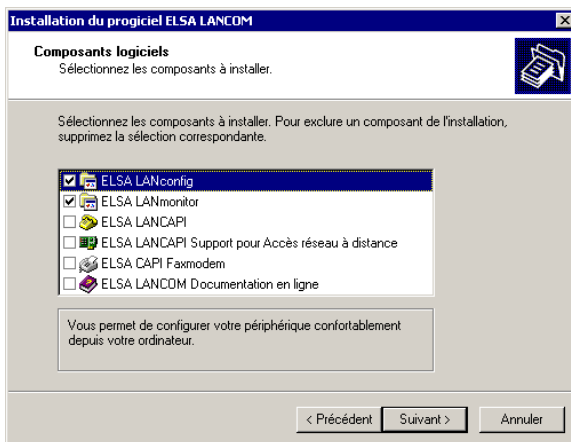
Lancer le programme d'installation ELSA

Introduisez le CD *ELSA LANCOM Office* dans le lecteur approprié. Le programme d'installation ELSA démarre automatiquement, sauf sous Windows NT : dans ce cas, vous devez lancer manuellement le fichier AUTO-RUN.EXE qui se trouve dans le répertoire principal du CD.



Vous devrez également lancer le fichier AUTORUN.EXE manuellement si la fonction AutoDémarrer n'est pas activée pour le lecteur de CD-ROM de votre ordinateur ou si le programme d'installation ELSA ne démarre pas automatiquement pour une autre raison.

Dans le menu ELSA Setup, cliquez sur **Installer le logiciel LANCOM**. Le menu de sélection suivant apparaît à l'écran :



3.4.2

Quels logiciels installer ?

Tous les logiciels proposés dans le menu ne sont pas nécessaires pour votre *ELSA LANCOM 1600 Office*.

- **ELSA LANconfig** constitue le programme d'installation pour tous les *ELSA LANCOM*. Il est également possible d'utiliser *ELSA WEBconfig* par l'intermédiaire d'un navigateur Web.
- **ELSA LANmonitor** vous permet de surveiller tous les *ELSA LANCOM* présents dans le réseau local.



Pour les trois programmes suivants, vous avez besoin d'un périphérique ELSA LANCOM avec interface RNIS. Parmi les périphériques de la série ELSA LANCOM 1600 Office, seul le ELSA LANCOM DSL/I-1611 Office en est équipé.

- L'interface **ELSA LANCAPI** vous permet à chaque ordinateur Windows du réseau local d'utiliser des applications RNIS comme s'il était équipé d'une carte RNIS. La connexion RNIS est réalisée de manière centralisée par le *ELSA LANCOM* avec interface RNIS.
- La **prise en charge de l'accès réseau à distance ELSA LANCAPI** vous permet d'utiliser l'interface logicielle CAPI sur votre ordinateur Windows comme une carte réseau, par ex. pour accéder à distance à *ELSA LANCOM*.

- **ELSA CAPI Faxmodem** installe un pilote Faxmodem sur votre ordinateur Windows, ce qui vous donne la possibilité d'envoyer des télécopies par l'intermédiaire de l'interface *ELSA LANCAPI*.

Sélectionnez les applications souhaitées et confirmez en cliquant sur **Suivant**. Les applications sont installées automatiquement.

FR

3.5

Le chapitre suivant...

...est consacré à la configuration de base du périphérique. Il vous suffira de quelques clics de souris pour configurer votre *ELSA LANCOM 1600 Office* de sorte que tous les ordinateurs du réseau local puissent accéder à Internet à grande vitesse.

4

Réglages de base

Dans ce chapitre, nous procéderons aux principaux réglages de base de votre *ELSA LANCOM 1600 Office* :

- Attribution d'une adresse IP
- Activation du serveur DHCP intégré (si désirée)
- Protection de l'accès à la configuration par mot de passe
- Configuration de l'interface RNIS (uniquement *ELSA LANCOM DSL/I-1611 Office*)
- Configuration de l'accès à Internet

4.1

Démarrage de l'assistant d'installation

Pour accéder à un appareil *ELSA LANCOM 1600 Office* non configuré, deux possibilités conviviales s'offrent à vous :

- *ELSA LANconfig* détecte automatiquement un *ELSA LANCOM* non configuré et lance l'assistant d'installation pour procéder aux réglages de base.
- Avec *ELSA WEBconfig* : indiquez l'adresse IP du périphérique *ELSA LANCOM 1600 Office* non configuré dans la ligne d'adresse du navigateur Web de l'un des ordinateurs du réseau. Certains environnements réseau permettent également d'accéder à votre *ELSA LANCOM 1600 Office* en tapant un nom de votre choix dans la ligne d'adresse (vous en apprendrez plus à ce sujet dans l'un des chapitres suivants).



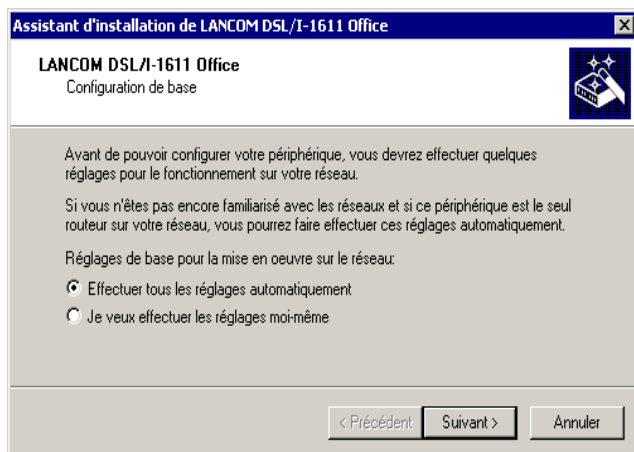
Dans un même réseau, il ne devrait jamais y avoir plusieurs ELSA LANCOM non configurés. En effet, tous les ELSA LANCOM non configurés s'inscrivent sous la même adresse IP (avec le suffixe 254), la présence de plusieurs périphériques entraîne des conflits d'adresse. Afin d'éviter ce genre de problème, il est préférable de configurer les différents appareils les uns après les autres en leur attribuant immédiatement une adresse IP univoque.

4.1.1

Réglages de base avec **ELSA LANconfig**

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

ELSA LANconfig reconnaît automatiquement le nouveau **ELSA LANCOM 1600 Office** dans le réseau TCP/IP. L'assistant d'installation démarre et vous aide à procéder au réglage de base du périphérique ; si l'environnement réseau le permet, il peut également faire tout le travail à votre place.



*Si l'assistant ne démarre pas automatiquement, vous devez rechercher manuellement les nouveaux périphériques présents dans le réseau (**Périphérique ► Rechercher**).*



Cette fenêtre apparaît uniquement lorsqu'aucun serveur DHCP n'est activé au sein du réseau et qu'aucune adresse IP n'a été attribuée, même manuellement, à votre ordinateur. Dans le cas contraire, l'assistant se comporte exactement comme décrit sous ② ('Je veux effectuer les réglages moi-même').

Avant de faire votre choix, tenez compte des points suivants :

Sélectionnez 'Effectuer tous les réglages automatiquement'...

...si vous **n'êtes pas** familiarisé avec les réseaux et les adresses IP et si jusqu'à présent vous n'avez pas utilisé d'adresses IP au sein de votre

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

Choisissez 'Je veux effectuer les réglages moi-même'...

...si vous êtes familiarisé avec les réseaux et les adresses IP et si l'une des hypothèses suivantes est juste :

- Jusque là, vous n'avez pas encore utilisé d'adresses IP dans votre réseau, mais vous aimeriez bien le faire dès maintenant. Vous voulez déterminer vous-même l'adresse IP de votre routeur et lui attribuer une adresse quelconque se trouvant dans une zone d'adresses personnelles, par ex. '10.0.0.1' avec le masque '255.255.255.0'. De cette manière, vous déterminez aussi la zone d'adresses qu'utilisera ensuite le serveur DHCP pour les appareils dans le réseau (si le serveur DHCP est mis en service).
 - Vous avez déjà utilisé des adresses IP avec les ordinateurs dans le réseau local.
- ② Si vous souhaitez procéder vous-même aux réglages IP, donnez au *ELSA LANCOM 1600 Office* une adresse libre se trouvant dans la zone d'adresses utilisée jusque là. Validez avec **Suivant**.
- ③ Parmi les réglages IP, vous devez également déterminer si le routeur doit servir ou non de serveur DHCP. Faites votre choix, puis confirmez avec **Suivant**.
- ④ Dans la fenêtre suivante, définissez le mot de passe pour l'accès à la configuration. Indiquez également si l'accès au périphérique doit être uniquement autorisé depuis le réseau local ou s'il doit être possible de le configurer à distance par l'intermédiaire d'une connexion au réseau étendu (via modem DSL/modem-câble et, pour le *ELSA LANCOM DSL/I-1611 Office*, via RNIS). Validez votre choix en cliquant sur **Suivant**.



Attention, en validant la configuration à distance, vous permettez également la téléconfiguration depuis Internet. Dans un tel cas, veuillez à protéger l'accès à la configuration de manière appropriée, par ex. par un mot de passe.

- ⑤ Avec un *ELSA LANCOM DSL/I-1611 Office*, vous pouvez alors configurer l'interface RNIS. Validez votre choix en cliquant sur **Suivant**.

- ⑥ Si vous souhaitez régler les paramètres RNIS sur votre *ELSA LANCOM DSL/I-1611 Office*, entrez un numéro d'appel (numéro MSN) sur lequel le périphérique devra prendre les appels. Vous pouvez également indiquer un préfixe d'accès à RNIS. Enfin, indiquez si les informations sur les unités de taxation doivent être transmises ou non à votre accès RNIS. Validez avec **Suivant**.
- ⑦ Pour clore l'installation, cliquez sur **Terminer**.

4.1.2

Réglages de base avec *ELSA WEBconfig*

ELSA WEBconfig vous permet de configurer votre *ELSA LANCOM 1600 Office* avec le navigateur Web de votre choix. Vous n'êtes donc pas lié au système d'exploitation Windows, comme c'est le cas avec *ELSA LANconfig*.

Seule condition pour l'accès : vous devez savoir comment communiquer avec le routeur non configuré au sein du réseau local. Un *ELSA LANCOM* non configuré réagit toujours à une adresse IP précise, voire, dans certaines configurations de réseau, à un nom.

Mon *ELSA LANCOM 1600 Office* réagit-il à un nom ?

S'il n'existe encore aucun serveur DHCP ou DNS dans votre réseau local, le routeur réagit à chaque nom (par ex. 'LANCOM' ou 'routeur') que vous saisissez dans le champ d'adresse URL d'un navigateur WEB.



Lorsque vous ne savez pas si des adresses IP ont déjà été utilisées dans votre réseau, faites afficher l'adresse IP de votre ordinateur (voir chapitre suivant). Si vous trouvez la valeur '0.0.0.0' dans la zone 'Adresse IP', votre carte de réseau n'a pas encore d'adresse IP.

Quelle est l'adresse IP du *ELSA LANCOM 1600 Office* ?

L'adresse IP d'un *ELSA LANCOM* non configuré correspond à l'adresse IP de l'ordinateur appelant dans laquelle vous remplacez le dernier nombre (situé derrière le troisième point) par 254.

Si, par exemple, l'adresse IP 10.0.0.17 a été attribuée à votre ordinateur, un *ELSA LANCOM* non configuré se trouvera à l'adresse 10.0.0.254. Pour connaître l'adresse IP de votre ordinateur, tapez (selon le système d'exploitation) l'une des instructions suivantes dans la ligne de commande (dans l'invite DOS sous Windows) :

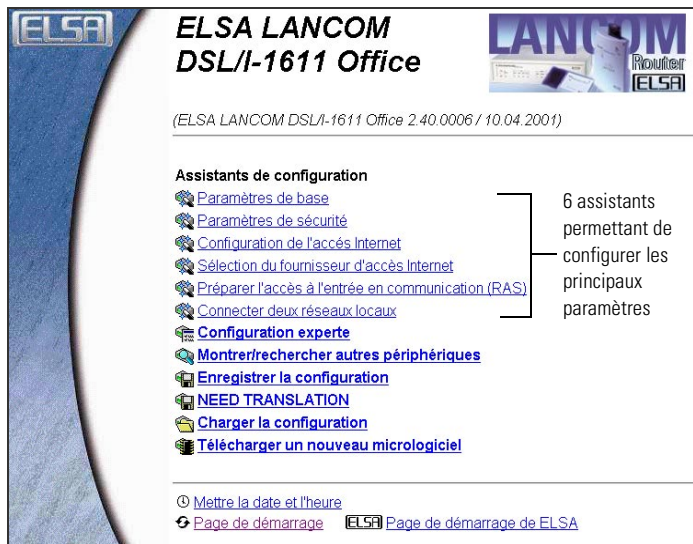
Système d'exploitation	Instruction dans la ligne de commande
Windows 95, Windows 98, Windows Me	winiptcg
Windows NT 4.0, Windows 2000	ipconfig
Linux, UNIX	ifconfig

Appel des assistants dans **WEBconfig**

- ① Lancez votre navigateur Web (Internet Explorer, Netscape Navigator) et appelez le *ELSA LANCOM 1600 Office* :

http://<Adresse IP du LANCOM> (ou un nom)

Vous voyez alors apparaître le menu suivant :



Les assistants dépendent du ELSA LANCOM concerné et diffèrent donc d'un périphérique à l'autre. Il est tout à fait possible que votre périphérique ne propose pas tous les assistants représentés dans cette section.

- ② Sélectionnez **Paramètres de base**. La fenêtre suivante vous donne le choix entre 'Déterminer automatiquement les paramètres IP' et 'Déterminer soi-même les paramètres IP'.

Cette alternative apparaît uniquement lorsqu'aucun serveur DHCP n'est activé au sein du réseau et qu'aucune adresse IP n'a été attribuée à votre

ordinateur. Dans le cas contraire, l'assistant se comporte exactement comme décrit à partir du point ④.

- ③ Avant de faire votre choix, tenez compte des points suivants :

Activez l'option 'Déterminer automatiquement les paramètres IP'...

...si vous **n'êtes pas** familiarisé avec les réseaux et les adresses IP et si jusqu'à présent vous n'avez pas utilisé d'adresses IP au sein de votre réseau. Le routeur déterminera et attribuera automatiquement alors, en tant que serveur DHCP, les adresses IP pour tous les appareils dans le réseau local.

Désactivez l'option 'Déterminer automatiquement les paramètres IP'...

...si vous êtes familiarisé avec les réseaux et les adresses IP et si l'une des hypothèses suivantes est juste :

- Jusque là, vous n'avez pas encore utilisé d'adresses IP dans votre réseau, mais vous aimeriez bien le faire dès maintenant. Vous voulez déterminer vous-même l'adresse IP pour le nouvel appareil et lui attribuer une adresse quelconque dans les zones d'adresse réservées à des fins personnelles comme p. ex. '10.0.0.x' avec le masque de réseau '255.255.255.0'. De cette manière, vous déterminez aussi la zone d'adresses qu'utilisera ensuite le serveur DHCP pour les appareils dans le réseau (si le serveur DHCP est mis en service).
 - Vous avez déjà utilisé des adresses IP avec les ordinateurs dans le réseau local. Attribuez au nouvel appareil une adresse libre se trouvant dans la zone d'adresses utilisée jusque là. Indiquez également si le périphérique doit servir ou non de serveur DHCP dans le réseau local.
- ④ Si vous souhaitez procéder vous-même aux réglages IP, donnez au *ELSA LANCOM 1600 Office* une adresse libre se trouvant dans la zone d'adresses utilisée jusque là. De plus, précisez si le périphérique doit servir ou non de serveur DHCP. Validez votre entrée en cliquant sur **Appliquer**.
- ⑤ Dans la fenêtre suivante 'Paramètres sécurité', définissez le mot de passe pour l'accès à la configuration. Indiquez également si l'accès au périphérique doit être uniquement autorisé depuis le réseau local ou s'il

doit être possible de le configurer à distance par l'intermédiaire d'une connexion au réseau étendu (via modem DSL/modem-câble et, pour le *ELSA LANCOM DSL/I-1611 Office*, via RNIS). Validez votre choix en cliquant sur **Appliquer**.



Attention, en validant la configuration à distance, vous permettez également la téléconfiguration depuis Internet. Dans un tel cas, veillez à protéger l'accès à la configuration de manière appropriée, par ex. par un mot de passe.

- ⑥ L'aide en ligne *ELSA WEBconfig* est disponible sur le site WEB d'ELSA. Vous pouvez aussi enregistrer le contenu de l'aide en ligne sous la forme de fichiers HTML sur un serveur de fichiers du réseau local ou localement sur l'ordinateur servant à la configuration. Indiquez alors l'emplacement de l'aide en ligne sous la forme d'un chemin d'accès URL.

Si vous reprenez le chemin prédéfini, le *ELSA LANCOM 1600 Office* charge les textes depuis le site d'ELSA lorsque vous en avez besoin. En revanche, si vous souhaitez être en mesure d'accéder à l'aide sans connexion Internet, vous devez modifier le chemin d'accès en conséquence. Vous trouverez de plus amples informations à ce sujet sous 'Les fichiers d'aide ELSA WEBconfig (module HTTP)' à la page 44.

Avec un *ELSA LANCOM DSL/I-1611 Office*, vous pouvez alors configurer l'interface RNIS. Validez votre choix en cliquant sur **Appliquer**.

- ⑦ Si vous avez demandé la configuration du raccordement RNIS, le programme vous demande ensuite si les informations de taxation doivent être transmises à votre accès RNIS. Faites votre choix et validez en cliquant sur **Suivant**.
- ⑧ Lorsque *ELSA WEBconfig* confirme la saisie des données, la configuration de base est terminée.

4.2

Configuration de l'accès à Internet

Un assistant spécifique vous permet de configurer l'accès à Internet. Pour le lancer, procédez comme suit :

4.2.1 Démarrage de l'assistant de configuration sous **ELSA LANconfig**

- ① Dans la fenêtre de sélection, choisissez votre *ELSA LANCOM 1600 Office*.
- ② Pour accéder au menu comportant les assistants disponibles, cliquez sur **Options ► Assistant d'installation**. Sélectionnez **Configuration de l'accès Internet**.

4.2.2 Démarrage de l'assistant de configuration sous **ELSA WEBconfig**

L'assistant de configuration de l'accès à Internet se trouve directement dans le menu principal d'*ELSA WEBconfig*.

4.2.3 Saisie des données d'accès

L'assistant de configuration de l'accès à Internet vous demande les unes après les autres toutes les données nécessaires pour accéder à Internet. Ces données vous ont été communiquées par votre fournisseur de service Internet.

4.3 Réglages des paramètres sur les postes de travail

Selon la méthode utilisée pour l'attribution des adresses IP au sein de votre réseau local, il est nécessaire de procéder aux réglages suivants sur les postes de travail pour leur permettre d'accéder à Internet :

- **Attribution DHCP via le *ELSA LANCOM 1600 Office* (cas normal)**
Le *ELSA LANCOM 1600 Office* transmet également aux ordinateurs sa propre adresse IP via DHCP en tant que passerelle standard et serveur DNS. Les postes de travail doivent être réglés de manière à recevoir automatiquement (via DHCP) leurs propres adresses IP, ainsi que celles de la passerelle standard et du serveur DNS.
- **Attribution DHCP par l'intermédiaire d'un serveur DHCP séparé**
Les postes de travail doivent être réglés de manière à recevoir automatiquement (via DHCP) leurs propres adresses IP, ainsi que celles de la passerelle standard et du serveur DNS. L'adresse IP du *ELSA*

LANCOM 1600 Office doit être inscrite sur le serveur DHCP de façon à ce qu'il la transmette aux ordinateurs du réseau local en tant que passerelle standard. De plus, le serveur DHCP doit indiquer le *ELSA LANCOM 1600 Office* en tant que serveur DNS.

● Attribution manuelle des adresses IP

Si les adresses IP sont attribuées de manière statique dans le réseau, il est nécessaire d'indiquer à chaque ordinateur du réseau local, dans la configuration TCP/IP, l'adresse IP du *ELSA LANCOM 1600 Office* en tant que passerelle standard et serveur DNS.

Pour plus de détails concernant les paramètres TCP/IP de votre ordinateur, veuillez vous référer à la documentation de votre système d'exploitation.



4.4

Terminé !

Avec ces quelques clics de souris vous avez entièrement configuré votre *ELSA LANCOM 1600 Office* pour un accès à Internet. Tous les ordinateurs reliés à votre réseau local (LAN) peuvent désormais surfer « à grande vitesse » sur Internet...

Au terme de la configuration de base, les principaux réglages nécessaires sur le *ELSA LANCOM 1600 Office* sont, en règle générale, déjà effectués pour la plupart des applications.

Bien entendu, vous pouvez encore définir de nombreux autres paramètres plus poussés. Vous trouverez une description détaillée de ces options dans les chapitres suivants.

5 Configuration et gestion

Dans ce chapitre, nous vous montrons avec quels moyens et par quels chemins vous pouvez accéder au périphérique pour effectuer les réglages avancés. Vous y trouverez la description des thèmes suivants :

- Outils de configuration
- Fonctions de contrôle et de diagnostic du périphérique et des logiciels
- Sauvegarde et restauration de configurations complètes
- Installation de nouveaux microprogrammes dans le périphérique

5.1 La configuration

Les *ELSA LANCOM 1600 Office* se caractérisent par leur flexibilité : ils supportent en effet pour leur configuration divers moyens (c'est-à-dire logiciels) et chemins (accès de communication). Nous vous donnons ici un aperçu des différents chemins.

Pour communiquer avec un *ELSA LANCOM 1600 Office*, vous disposez de trois accès différents :

- Par l'interface de configuration (interface config.) sur la face arrière du routeur (également nommée outband)
- Par le réseau (LAN et WAN – inband)
- Par la configuration à distance via l'accès RNIS (uniquement *ELSA LANCOM DSL/I-1611 Office*)

Quelle est donc la différence entre ces possibilités ?

D'une part la disponibilité : 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 de la connexion RNIS.

D'autre part les exigences envers le matériel ou les logiciels supplémentaires. La configuration Inband requière uniquement l'un des ordinateurs du réseau local ou étendu et un logiciel approprié, par ex. *ELSA LANconfig* (voir section suivante). La configuration Outband nécessite en plus du logiciel de configuration un ordinateur (avec interface série). C'est la configuration à distance qui pose le plus de conditions : outre le raccordement RNIS sur le *ELSA LANCOM 1600 Office* (uniquement *ELSA LANCOM DSL/I-1611 Office*), l'ordinateur servant à la configuration doit également être équipé d'une carte

RNIS, d'un adaptateur RNIS ou d'un accès par *ELSA LANCAPi* à un autre *ELSA LANCOM* avec interface RNIS.

5.2

Logiciels de configuration

Les accès de configuration ont montré que des logiciels spécifiques sont nécessaires pour configurer le périphérique.

Non seulement les situations de configuration diffèrent – mais également les exigences et préférences de la personne chargée de cette opération. Les routeurs *ELSA LANCOM 1600 Office* proposent donc de nombreux logiciels de configuration :

- **ELSA LANconfig** – guidé par menu, clair et simple, il permet de régler quasiment tous les paramètres d'un *ELSA LANCOM 1600 Office*. Il supporte les configurations Outband, Inband et à distance.
- **ELSA WEBconfig** – logiciel intégré dans le routeur. L'ordinateur utilisé pour la configuration a uniquement besoin d'un navigateur Web. *ELSA WEBconfig* peut ainsi être utilisé sous n'importe quel système d'exploitation. Il supporte les configurations Inband et à distance.
- **SNMP** – les programmes (indépendants du périphérique) de gestion des réseaux IP se basent en général sur le protocole SNMP. SNMP permet d'accéder à *ELSA LANCOM 1600 Office* par la configuration Inband ou à distance.
- **Programme de terminal, Telnet** – un *ELSA LANCOM 1600 Office* peut être configuré avec un programme de terminal par l'intermédiaire de l'interface de configuration (par ex. HyperTerminal) ou au sein d'un réseau IP (par ex. Telnet).
- **TFTP** – dans les réseaux IP (configuration Inband et à distance), il est également possible, dans une certaine mesure, d'utiliser le protocole de transfert de fichiers TFTP.



Attention, toutes ces procédures utilisent les mêmes données de configuration. Si, par ex., vous modifiez des paramètres dans ELSA LANconfig, ceci aura des répercussions directes sur les valeurs utilisées sous ELSA WEBconfig et Telnet.

5.2.1

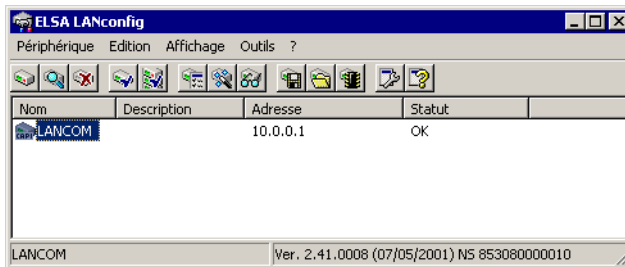
Configuration par *ELSA LANconfig*

Appelez *ELSA LANconfig* par ex. à partir de la barre de Windows avec **Démarrer ► Programmes ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* cherchera automatiquement des périphériques dans le réseau local. Si un périphérique non configuré est trouvé dans le réseau local, *ELSA LANconfig* lance automatiquement l'assistant de configuration. La configuration de base au moyen des assistants de configuration est décrite sous 'Réglages de base avec ELSA LANconfig' à la page 32.

Recherche de nouveaux périphériques

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

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



La recherche avancée pour les utilisateurs expérimentés

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

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

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



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

La fonction de recherche intégrée

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.

5.2.2

Configuration avec *ELSA WEBconfig*

Vous pouvez procéder à la configuration de votre appareil à partir de n'importe quel navigateur Web (également s'il supporte l'affichage de texte). Le *ELSA LANCOM 1600 Office* est équipé du logiciel de configuration *ELSA WEBconfig*. Vous avez juste besoin d'un navigateur Web pour accéder à *ELSA WEBconfig*.

Fonctionne avec tous les navigateurs Web

ELSA WEBconfig propose des assistants d'installation similaires à ceux de *ELSA LANconfig* et remplit ainsi les conditions idéales pour une configuration conviviale de *ELSA LANCOM 1600 Office* – et ce, contrairement à *ELSA LANconfig*, sous tous les systèmes d'exploitation pour lesquels un navigateur Web existe.

Afin de pouvoir utiliser *ELSA WEBconfig*, il est nécessaire d'établir une connexion au réseau local via TCP/IP (PPP pour la configuration à distance). L'accès à *ELSA WEBconfig* s'effectue par l'intermédiaire de l'adresse IP du *ELSA LANCOM 1600 Office* (ou, lorsque l'environnement réseau le permet, par l'intermédiaire d'un nom quelconque).

Vous trouverez sous 'Réglages de base avec *ELSA WEBconfig*' à la page 34 comment accéder pour la première fois à un périphérique non configuré avec *ELSA WEBconfig* et procéder à sa configuration de base.

Les fichiers d'aide *ELSA WEBconfig* (module HTTP)

Une documentation complète et contextuelle sur les diverses pages et champs de *ELSA WEBconfig* est disponible dans *ELSA WEBconfig* en sélectionnant le lien **Aide (manuel de référence)**.

Ce lien permet d'accéder à des fichiers d'aide en format HTML. Par défaut, le lien de l'aide renvoie aux pages Web d'ELSA.

Vous pouvez également télécharger les fichiers d'aide depuis le site Internet d'ELSA pour les sauvegarder à un emplacement de votre choix. Il est recommandé de sauvegarder les fichiers d'aide localement sur votre ordinateur ou sur un serveur auquel il est toujours possible d'accéder. Il peut s'agir soit d'un serveur de fichiers soit d'un serveur Web (HTTP).

La variante locale vous permet d'accéder à l'aide même lorsque la communication réseau est perturbée. En revanche, si vous enregistrez les données sur un serveur de votre réseau, vous pouvez accéder à la fonction d'aide depuis tous les ordinateurs sans devoir installer les fichiers d'aide au préalable sur chacun des ordinateurs. Dans ce cas, le serveur doit toutefois toujours être accessible depuis le réseau.

Lorsque vous avez choisi une solution et sauvegardé les fichiers d'aide à l'endroit souhaité, vous devez en indiquer le chemin d'accès dans *ELSA WEBconfig*. Pour cela, sélectionnez dans la **configuration avancée** d'*ELSA WEBconfig*, ► **Setup** ► **Module HTTP** ► **Racine documents**.

Deux remarques importantes concernant la syntaxe :

- Indiquez le chemin d'accès uniquement jusqu'au répertoire dans lequel se trouve la structure complète des fichiers d'aide.
Si vous avez, par ex., sauvegardé dans un répertoire local 'C:\ELSA\HTMLRef' la structure de fichiers d'aide '\500\2\1611\', indiquez seulement 'file://C:/ELSA/HTMLRef' en racine documents.
- Selon la variante choisie (sauvegarde locale, serveur de fichiers, serveur HTTP) et le système d'exploitation utilisé, le chemin d'accès diffère peu. Le tableau suivant vous en donne quelques exemples, les noms et chemins d'accès pouvant être choisis librement.

Variante	Systèmes d'exploitation	Exemple
Sauvegarde locale	Windows	file://C:/ELSA/HTMLRef
	Linux	file://usr/lib/ELSA/HTMLRef
Serveur de fichiers	Windows NT, Windows 2000, Novell, UNIX	file://Server1/ELSA/HTMLRef
Serveur HTTP	tous	http://<Adresse IP>/ELSA/HTMLRef

La balise <Adresse IP> représente soit l'adresse IP valide du serveur HTTP au format 'x.x.x.x', par exemple '128.7.9.155', soit un nom de serveur, par ex. 'www.elsa.com'.

La version à jour de l'aide HTML peut être téléchargée depuis le site Web d'ELSA.



5.2.3

Configuration par Telnet

Avec Telnet vous démarrez la configuration par ex. à partir de la ligne de commande Windows à l'aide de l'instruction :

```
C:\>telnet 10.0.0.1
```

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

Après l'introduction du mot de passe (si vous avez convenu un mot de passe pour protéger la configuration) vous disposez de toutes les commandes de configuration.

TFTP

Certaines fonctions ne peuvent pas être exécutées de manière satisfaisante via Telnet, voire pas du tout. Il s'agit, entre autres, de toutes les fonctions pour lesquelles des fichiers complets sont transférés, comme par exemple le téléchargement de microprogrammes ou la sauvegarde et la restauration de données de configuration. Dans un tel cas, c'est le protocole TFTP qui est utilisé.

TFTP est fourni en série avec les systèmes d'exploitation Windows 2000 et Windows NT. Il permet de transférer facilement des fichiers d'un périphérique à un autre en passant par le réseau.

La syntaxe des commandes TFTP dépend du système d'exploitation. Sous Windows 2000 et Windows NT, elle est la suivante :

```
tftp -i <Adresse IP d'hôte> [get|put] Source [Cible]
```

Le format ASCII est préétabli pour de nombreux clients TFTP. En cas de transfert de données binaires (par ex. les microprogrammes), il est donc la plupart du temps nécessaire de sélectionner explicitement la transmission binaire. Dans cet exemple pour Windows 2000 et Windows NT, vous y arrivez à l'aide du paramètre '-i'.



FR

5.2.4

Configuration par SNMP

Le simple protocole de management de réseau (SNMP V.1 après RFC 1157) permet la surveillance et la configuration des périphériques dans un réseau à partir d'une instance centrale.

De très nombreux programmes de configuration et de gestion sont basés sur le protocole SNMP. Parmi les applications commerciales, citons par exemple Tivoli, OpenView de Hewlett-Packard, SunNet Manager et CiscoWorks. Il existe également un grand nombre de logiciels Freeware et Shareware.

Si vous souhaitez utiliser des programmes SNMP, votre *ELSA LANCOM 1600 Office* vous permet d'exporter des fichiers MIB de périphérique (**M**anagement **I**nformation **B**ase).

Outil de configuration	Appel
<i>ELSA WEBconfig</i>	Appeler le fichier MIB de périphérique pour SNMP (menu principal)
TFTP	tftp 10.0.0.1 get readmib file1

5.3

La configuration à distance via l'accès réseau à distance



La section sur la configuration à distance concerne uniquement les ELSA LANCOM avec interface RNIS. Dans la série de périphériques ELSA LANCOM 1600 Office, seul le ELSA LANCOM DSL/I-1611 Office remplit cette exigence.

Le réglage de routeurs distants est particulièrement simple à l'aide de la configuration à distance par l'accès réseau à distance de Windows. L'administrateur peut établir la communication avec le périphérique immédiatement

après la mise sous tension et la connexion à l'accès du réseau étendu sans faire aucun 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.

5.3.1

Ce dont vous avez besoin pour la configuration à distance

- Un *ELSA LANCOM 1600 Office* avec interface RNIS
- Un ordinateur avec un client PPP, par ex. l'Accès réseau à distance de Windows
- Un logiciel pour la configuration Inband, par ex. *ELSA LANconfig* ou Telnet
- Un ordinateur pour la configuration avec carte RNIS, adaptateur RNIS ou un *ELSA LANCOM* avec interface RNIS et *ELSA LANCAPI*.

5.3.2

La première connexion à distance par l'accès réseau à distance

- 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 DSL/I-1611 Office* 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 *ELSA 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.

En effaçant l'inscription dans la liste des périphériques, vous supprimez également la connexion correspondante dans l'Accès réseau à distance de Windows.



- 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.

5.3.3

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 1600 Office* en utilisant les données suivantes :
- Nom d'utilisateur 'ADMIN'
 - Mot de passe comme sur le routeur *ELSA LANCOM DSL/I-1611 Office*, 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 DSL/I-1611 Office*. 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 DSL/I-1611 Office* 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 DSL/I-1611 Office* 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 DSL/I-1611 Office* comme tous les autres périphériques.

5.3.4

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 spé-

cifique pour accéder à la configuration. Si l'appareil reçoit un appel sur ce numéro, les réglages PPP seront utilisés, et ceci indépendamment des autres configurations du routeur. Durant cet échange PPP, il ne sera accepté que le nom d'utilisateur qui aura été enregistré automatiquement par *ELSA LANconfig* lors de l'établissement de la communication.

- ① Passez dans la zone de configuration 'Gestion' sur l'onglet 'Sécurité'.
- ② Sélectionnez dans la zone 'Accès à configuration' si l'accès à partir de réseaux distants est possible en totalité, en lecture seule ou pas du tout.

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

```
set /setup/config-module/wan-config [on] [read] [off]
```

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

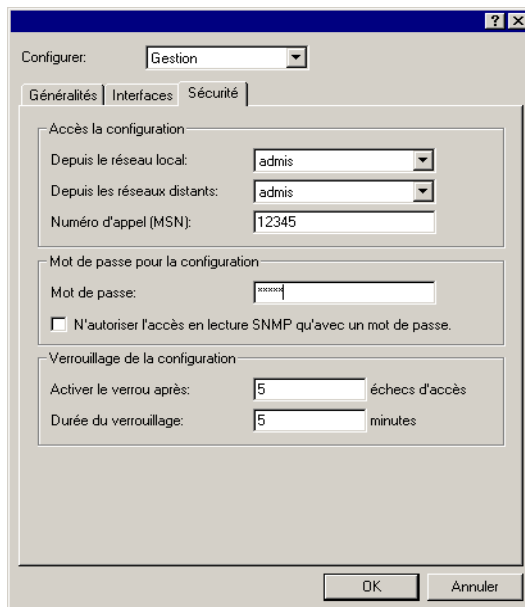
- ③ En guise de numéro d'appel dans la partie 'Accès à configuration', entrez un numéro d'appel de votre accès qui soit utilisé uniquement à cet effet.

Entrez alternativement l'instruction suivante :

```
set /setup/config-module/farconfig 123456
```

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





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

passwd

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

5.4

***ELSA LANmonitor* – garder une vue d'ensemble**

Avec l'outil de surveillance *ELSA LANmonitor* vous pouvez, sous les systèmes d'exploitation Windows, toujours afficher à l'écran les informations les plus importantes sur l'état de vos routeurs, et ce, pour tous les *ELSA LANCOM* présents sur le réseau.

Un grand nombre des messages internes des périphériques sont traduits en clair et vous indiquent l'état actuel du périphérique et vous assistent lors du dépannage.

ELSA LANmonitor vous permet également d'observer le trafic de données sur les différentes interfaces des routeurs et vous indique avec les paramètres susceptibles d'optimiser ce trafic.



En plus des statistiques sur l'appareil que vous pouvez, par exemple, lire durant une session Telnet ou terminal ou avec *ELSA WEBconfig*, *ELSA LANmonitor* met également d'autres possibilités à votre disposition, comme par exemple la mise en place d'une limite de coûts supplémentaire.

ELSA LANmonitor ne vous permet de surveiller que les périphériques auxquels vous accédez Inband par IP dans le réseau local. Avec ce logiciel, vous ne pouvez pas vous adresser à un routeur sur l'interface série. Il est également impossible d'accéder, avec ELSA LANmonitor, aux périphériques des réseaux distants accessibles uniquement par des routeurs intermédiaires.

5.4.1

Affichage des réglages disponibles

Les options d'affichage suivantes peuvent être activées ou désactivées sous **Affichage ► Options**:

- Messages d'erreur
- Messages des diagnostic
- informations système



De nombreux détails importants concernant le statut du ELSA LANCOM 1600 Office sont uniquement affichés lorsque l'affichage des informations système est activée. Les interfaces ainsi que la gestion des frais font notamment partie de ces détails. C'est pourquoi nous recommandons aux utilisateurs intéressés de mettre en œuvre l'affichage des informations système.

5.4.2

Contrôle de la connexion Internet

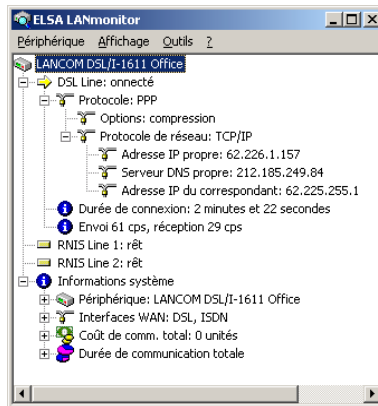
En tant qu'exemple des fonctions de *ELSA LANmonitor*, nous vous montrons d'abord les informations fournies par *ELSA LANmonitor* sur l'établissement de la liaison vers votre fournisseur d'accès Internet.

- ① Lancez *ELSA LANmonitor* avec **Démarrer ► Programmes ► 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 ► Surveillance d'appareil**.

- ② *ELSA LANmonitor* crée automatiquement un nouvel enregistrement dans la liste des appareils et indique tout d'abord l'état des canaux de trans-

mission. Lancez votre explorateur Internet et entrez un site quelconque. *ELSA LANmonitor* montre alors comment une connexion est établie sur un canal et quel correspondant est appelé. Dès que la communication est établie, un signe '+' devant l'inscription du canal de communication 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.

- ③ Un clic de la touche droite de la souris sur le canal actif vous permet de couper manuellement la communication. Il vous faut le cas échéant le numéro de passe de configuration.
- ④ Si vous souhaitez un protocole des sorties du *ELSA LANmonitor* sous forme de fichier, sélectionnez dans le menu 'Affichage' les 'Options' et passez à l'onglet 'Journal'. Activez la journalisation et choisissez si le *ELSA LANmonitor* doit établir un fichier protocole tous les jours, tous les mois ou continuellement.

5.5

Editions des tracés – Informations pour les utilisateurs avancés

Les éditions des tracés permettent de contrôler les processus internes du routeur pendant 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. Particulièrement positif : Les erreurs peuvent être détectées à la fois dans la configuration des propres routeurs et chez le correspondant.

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



5.5.1

Lancement d'un tracé

Vous pouvez, par exemple lancer l'édition de tracés lors d'une session Telnet. 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
Erreurs	messages d'erreurs des connexions
ELSA	négociation du protocole ELSA
routeur IPX	routing IPX

Ce paramètre affiche avec tracé :
PPP	négociation du protocole PPP
SAP	IPX Service Advertising Protocol
IPX-watchdog	IPX-Watchdog-Spoofing
SPX-watchdog	SPX-Watchdog-Spoofing
LCR	rerouteur téléphonique (Least-cost router)
Script	négociation de script
RIP	IPX Routing Information Protocol
Routeur IP	roulage IP
IP-RIP	IP Routing Information Protocol = protocole d'information de rou- tage IP
ARP	Address Resolution Protocol = protocole de résolution d'adresse
ICMP	Internet Control Message Protocol = protocole Internet de message de contrôle
Masquerading IP	processus dans le module Masquerading
DHCP	Dynamic Host Configuration Protocol
NetBIOS	gestion NetBIOS
DNS	Domain Name Service Protocol
Paket-Dump	affichage des premiers 64 octets d'un paquet en représentation hexadécimale
D-Kanal-Dump	tracé du canal D du bus RNIS branché

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

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

Exemples

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

5.6

Sauvegarde et restauration de la configuration

La configuration actuelle d'un *ELSA LANCOM 1600 Office* peut être sauvegardée en tant que fichier pour être rechargée en cas de besoin dans le périphérique (ou dans un autre périphérique de même type).

Copies de sécurité de la configuration

Cette fonction vous permet de réaliser des copies de sécurité de la configuration de votre *ELSA LANCOM 1600 Office*. Si votre *ELSA LANCOM 1600 Office* devait perdre ses données de configuration (par ex. suite à un défaut), il vous suffit alors de recharger la copie de sécurité.

Fonction conviviale de configuration en série

Lorsque vous devez configurer plusieurs *ELSA LANCOM 1600 Office* similaires, vous apprécierez rapidement la fonction de sauvegarde et de restauration des configurations. En effet, elle vous facilite la tâche en vous permettant de charger dans tous les périphériques l'ensemble des paramètres communs sous la forme d'une configuration de base. Il ne vous reste ensuite qu'à procéder aux réglages individuels sur chaque appareil.

Appel de la fonction

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Edition ► Sauvegarder la configuration dans un fichier Edition ► Restaurer la configuration à partir d'un fichier
<i>ELSA WEBconfig</i>	Sauvegarder / charger la configuration (menu principal)
TFTP	tftp 10.0.0.1 get readconfig file1 tftp 10.0.0.1 put file1 writeconfig

5.7

Nouveau microprogramme avec ELSA FirmSafe

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

5.7.1

Comment fonctionne ELSA FirmSafe ?

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

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

- 'Immédiatement' : La première possibilité consiste à charger et à activer le microprogramme immédiatement. Les situations suivantes peuvent s'en suivre :
 - Le nouveau microprogramme est chargé avec succès et fonctionne ensuite comme voulu. Donc tout est correct.
 - Le périphérique n'est plus accessible après le chargement du nouveau microprogramme. S'il survient une erreur déjà lors d'un téléchargement, le périphérique activera automatiquement l'ancien microprogramme et relancera le périphérique.

- 'Login' : Afin de remédier aux problèmes d'un téléchargement incorrect, vous avez la deuxième possibilité suivant laquelle le microprogramme sera chargé et également lancé immédiatement.
 - La différence avec l'autre variante réside dans le fait que le périphérique attendra ensuite durant cinq minutes un Login correct auprès du périphérique. Le nouveau microprogramme ne sera activé en permanence qu'après exécution correcte du login.
 - Si le périphérique n'est plus accessible, donc un login impossible, il activera automatiquement l'ancien microprogramme et relancera le périphérique.
- 'Manuel' : La troisième possibilité vous permet de déterminer auparavant vous-même un laps de temps durant lequel vous voulez tester le nouveau microprogramme. Le périphérique démarre avec le nouveau microprogramme et attend durant le laps de temps réglé que le microprogramme soit activé manuellement pour être actif en permanence.

5.7.2

Comment charger le nouveau logiciel ?

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

- *ELSA LANconfig*
- *ELSA WEBconfig*
- Emulateur de terminal
- TFTP



Certains réglages sont conservés lors du téléchargement du microprogramme ! Par souci de sécurité, vous devriez quand-même sauvegarder votre configuration (pour *ELSA LANconfig* 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 périphérique complètera les valeurs manquantes par des valeurs par défaut.

ELSA LANconfig



Dans l'outil de configuration *ELSA LANconfig* marquez l'appareil souhaité dans la liste de sélection et cliquez sur **Edition ► Gestion 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**.

ELSA WEBconfig

Lancez *ELSA WEBconfig* dans votre navigateur Web. Sur la page d'accueil, vous trouverez le lien **Charger nouveau microprogramme**. Dans la fenêtre suivante, recherchez le fichier du microprogramme dans l'arborescence, puis cliquez sur le bouton **Télécharger**.

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

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

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

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

TFTP

Vous pouvez installer un nouveau microprogramme sur *ELSA LANCOM 1600 Office* avec TFTP en tapant l'instruction (ou la cible) **writelflash**. Pour transmettre un nouveau microprogramme à un *ELSA LANCOM 1600 Office*

avec l'adresse IP 10.0.0.1, entrez par exemple sous Windows 2000 ou Windows NT l'instruction suivante :

```
tftp -i 10.0.0.1 put Lc_16xxu.240 writeflash
```

6

Sécurité d'exploitation

Ce chapitre est consacré à un sujet d'une importance toute particulière : la sécurité. Les paramètres de sécurité sont répartis dans différentes sections décrites ci-dessous :

- Protection pour la configuration
 - Protection par mot de passe
 - Verrouillage d'accès
 - Contrôle d'accès
- Protection pour le réseau local
 - IP masquerading
 - Filtrage des paquets de données
- Protection de l'accès RNIS (uniquement *ELSA LANCOM DSL/I-1611 Office*)

Vous trouverez en fin de chapitre une liste de contrôle reprenant les principaux paramètres de sécurité. Elle vous permettra de vérifier facilement si votre *ELSA LANCOM 1600 Office* bénéficie de la meilleure protection qui soit.

6.1

Protection pour la configuration

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

Les paramètres que vous avez saisis et fixés une fois pour toutes ne devraient évidemment pas être modifiés par des personnes non autorisées. C'est pourquoi *ELSA LANCOM 1600 Office* offre la possibilité de protéger la configuration par différents moyens.

6.1.1

Protection par mot de passe

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

Conseils pratiques pour l'utilisation de mots de passe

Lorsque vous définissez des mots de passe, veuillez tenir compte des conseils suivants :

- **Ne divulguez pas votre mot de passe.**

Ne notez jamais un mot de passe. Aussi prisée soit-elle, la solution des carnets, portefeuilles ou fichiers texte sur l'ordinateur n'en reste pas moins inappropriée. Cela peut paraître évident mais on ne le répètera jamais assez : ne donnez votre mot de passe à personne. Même les systèmes les plus sûrs capitulent devant les indiscretions.

- **Ne transmettez vos mots de passe que de manière sûre.**

Lorsque vous avez choisi un mot de passe, il vous faut le transmettre au site distant. Pour cela, choisissez la méthode la plus sûre possible et évitez plus particulièrement : courrier électronique non protégé, lettre ou télécopie. Préférez la transmission personnelle (« entre quatre yeux »). Le plus haut degré de sécurité est atteint si vous saisissez vous-même le mot de passe des deux côtés.

- **Choisissez un mot de passe sûr.**

Utilisez une suite aléatoire de lettres et de chiffres. Les mots de passe issus du vocabulaire courant ne peuvent pas être considérés comme sûrs. Vous rendrez la tâche des agresseurs encore plus difficile en utilisant des caractères spécifiques tels que '&"?#-*+_.,!°' et augmenterez par là même la sécurité du mot de passe.

- **N'utilisez jamais deux fois le même mot de passe.**

Si vous utilisez le même mot de passe pour plusieurs connexions, il perd de son efficacité. En effet, si un correspondant n'est plus sûr, vous mettez également en danger toutes les autres communications pour lesquelles vous utilisez ce mot de passe.

- **Changez régulièrement le mot de passe.**

Vous devriez modifier vos mots de passe le plus souvent possible. Ceci entraîne certes quelques désagréments mais augmente de manière non négligeable la sécurité du mot de passe.

- **Changez de mot de passe dès que vous avez un doute.**

Lorsqu'un collaborateur ayant accès à un mot de passe quitte l'entreprise, il est alors impératif de le modifier. Un mot de passe devrait toujours être changé dès qu'il existe le moindre doute sur des fuites éventuelles.

Si vous respectez ces quelques règles, vous obtiendrez un degré de sécurité relativement élevé.

Saisie du mot de passe

Le champ de saisie du mot de passe se trouve dans l'onglet 'Sécurité' du dossier de configuration 'Gestion' de *ELSA LANconfig*. Dans *ELSA WEBconfig*, lancez l'assistant **Paramètres de sécurité**. Pour une session de terminal ou Telnet, vous pouvez activer ou modifier la protection par mot de passe avec l'instruction `passwd`.

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Gestion ► Sécurité ► Mot de passe
<i>ELSA WEBconfig</i>	Paramètres de sécurité
Terminal/Telnet	<code>passwd</code>

Protection de l'accès SNMP

Vous pouvez également protéger l'accès SNMP en lecture seule à l'aide d'un mot de passe. Dans ce cas, c'est le mot de passe général de configuration qui est utilisé.

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Gestion ► Sécurité ► Autoriser accès SNMP en lecture seule avec mot de passe
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module SNMP ► Obligation mot de passe pour accès SNMP en lecture seule
Terminal/Telnet	<code>Setup/SNMP module/password prompt</code>

6.1.2

Le verrouillage des accès

La configuration du *ELSA LANCOM 1600 Office* est protégée contre les « attaques en force brute » par un verrouillage d'accès. Dans le cas d'une attaque en force brute, un utilisateur non autorisé cherche à trouver un mot de passe et à trouver un accès à un réseau, à un ordinateur ou à un autre périphérique. A cet effet, un ordinateur peut, par exemple, simuler automatiquement toutes les combinaisons possibles de lettres et de chiffres jusqu'à ce qu'il trouve le bon mot de passe.

Pour se protéger contre de telles manipulations, il est possible de prescrire un nombre maximum d'essais d'ouverture de séance infructueux. Dès que cette limite est atteinte, l'accès est verrouillé pendant une certaine période.

Le verrouillage d'un accès bloque automatiquement tous les autres accès.

Pour configurer le verrouillage des accès, les outils de configuration vous proposent les inscriptions suivantes :

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

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Gestion ► Sécurité
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module configuration
Terminal/Telnet	Setup/config-module

6.1.3

Contrôle des accès via TCP/IP

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

Au départ, ce tableau ne contient pas d'entrées afin de permettre à tout utilisateur d'accéder au routeur via TCP/IP 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.

Outil de configuration	Appel
<i>ELSA LANconfig</i>	TCP/IP ► Généralités ► Liste d'accès
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module TCP-IP ► Liste d'accès
Terminal/Telnet	/Setup/TCP-IP-module/access-list

6.2 Protection pour le réseau local

Vous n'apprécierez certainement pas qu'une personne externe puisse en toute liberté consulter ou modifier les données sur vos ordinateurs. *ELSA LANCOM 1600 Office* offre différentes possibilités pour limiter un accès de l'extérieur :

- Masquerading IP (NAT/PAT)
- Filtrage de paquets de données – Pare-feu

6.2.1 La cachette – Masquerading IP (NAT, PAT)

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

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

La cachette pour tous les ordinateurs sur Internet s'appelle masquerading IP. Seul le module routeur dans le périphérique ainsi que son adresse IP (fixe ou attribuée 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'une 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). Il existe une autre technique de pare-feu très utile : le filtrage ciblé de paquets de données entrants. Nous traiterons le filtrage de paquets de données dans la section suivante de ce chapitre.

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 de données 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 identificateurs.

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.

Configuration du masquerading IP

L'utilisation du masquerading IP est fixée séparément pour chaque route dans le tableau de routage. Pour accéder à ce tableau, procédez comme suit :

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Routeur IP ► Routage ► Tableau de routage
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module routeur IP ► Tableau de routage IP
Terminal/Telnet	/Setup/IP-router-module/IP-routing-tab

Deux adresses pour le routeur

Pour le masquerading, le routeur doit répondre à deux exigences 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.

- 'off' : pas de masquage.
- 'dyn.' : 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.' : votre fournisseur d'accès vous attribue une adresse fixe que vous utilisez ensuite pour la connexion et pour le masquage. Vous saisissez l'adresse IP souhaitée dans le champ suivant :

<i>ELSA LANconfig</i>	TCP/IP ► Généralités ► Adresse IP Internet
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module TCP/IP ► Adresse IP
Terminal/Telnet	/Setup/TCP-IP-module/IP-address

Accès à Internet non masqué pour certains périphériques

Si le fournisseur exige une adresse spécifique (option de masquage 'stat'), il existe deux possibilités pour l'attribution réelle de l'adresse :

- 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. Tout ordinateur est masqué derrière l'adresse fixe des routeurs.
 - Adresse IP avec masque de réseau non complet, par ex. 255.255.255.248 (pour 4 adresses IP) : vous disposez de plusieurs adresses IP enregistrées et en choisissez une que vous attribuez 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.

Un exemple : votre fournisseur vous donne l'adresse de réseau IP 123.45.67.0 avec masque de réseau 255.255.255.248. Vous pouvez alors répartir les adresses IP de la manière suivante :

Adresse IP	Signification / utilisation
123.45.67.0	Adresse réseau
123.45.67.1	Routeur <i>ELSA LANCOM 1600 Office</i> pour le réseau interne
123.45.67.2	Autre périphérique dans le LAN qui doit obtenir un accès non masqué à Internet, par exemple un serveur Web
123.45.67.3	Adresse de diffusion

Les autres ordinateurs et périphériques du réseau local ne disposent pas d'adresse IP publique et sont donc représentés sur Internet via l'adresse IP du *ELSA LANCOM 1600 Office* (123.45.67.1).

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. Grâce à l'inscription dans le tableau des services, le routeur lit l'adresse IP du serveur FTP dans le réseau local. 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 du réseau local à Internet en revanche, le routeur définit lui-même l'adresse IP et le port dans le tableau des services.

Ce tableau peut comprendre 2 048 entrées au maximum, c'est-à-dire qu'il permet 2 048 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 automatiquement dans le tableau.

Configuration du masquage inverse

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Routeur IP ► Masquerading ► Tableau des services
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module routeur IP ► Masquerading ► Tableau des services
Terminal/Telnet	/Setup/IP-router-module/masquerading/ service-table

Quels protocoles peuvent être utilisés avec le masquerading IP ?

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

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

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

6.2.2

Filtrage de paquets de données – Pare-feu

Les filtres pare-feu du *ELSA LANCOM 1600 Office* proposent des fonctions de filtrage pour les postes de travail individuels mais aussi pour des réseaux entiers. Ils garantissent une protection efficace contre tout intrus indésirable dans votre réseau.

Qu'est-ce qui peut être filtré ?

Il est important de pouvoir définir des filtres source et cible pour certains ports ou groupes de ports. En outre, il est possible de filtrer des protocoles ou des combinaisons de protocoles (TCP/UDP/ICMP). Les zones d'adresses IP ou les réseaux IP complets sont également des objets susceptibles d'être filtrés.

En plus de ces objets au niveau IP, il est également possible de sélectionner des stations du réseau local par l'intermédiaire de leur adresse MAC. L'abréviation « MAC » signifie **M**edia **A**ccess **C**ontrol et constitue le point central de la communication au sein d'un réseau local. Une adresse MAC est attribuée de manière permanente à chaque carte réseau. Les adresses MAC



sont univoques au niveau mondial, à l'image des numéros de série des périphériques, et permettent de s'adresser de manière sûre aux ordinateurs d'un réseau local afin de leur attribuer ou de leur refuser certains droits au niveau des paquets IP. Les adresses MAC sont souvent indiquées sur l'extérieur des périphériques réseau, sous forme hexadécimale (parex. 00:A0:57:01:02:03).

Le filtrage concerne uniquement le mode routeur IP. L'accès des ordinateurs du réseau local au ELSA LANCOM (par ex. aux données de configuration) ne peut pas être limité par l'intermédiaire des règles pare-feu.

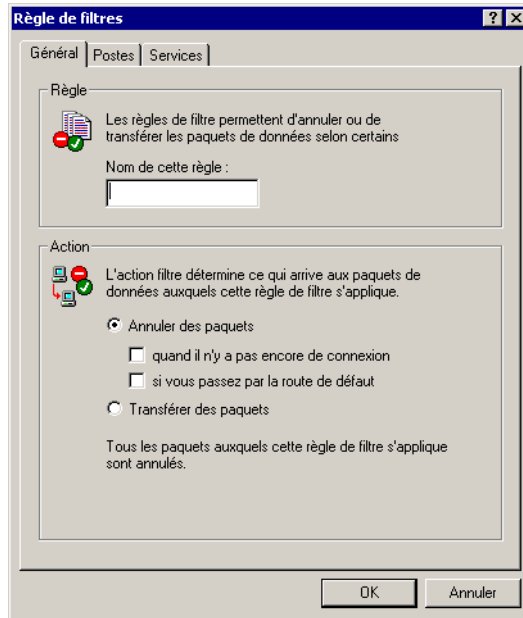
Configuration des filtres

Les filtres pare-feu sont configurés à l'aide des listes et menus suivants :

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Routeur IP ► Filtre ► Ajouter
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module routeur IP ► Pare-feu
Terminal/Telnet	/Setup/IP-router-module/firewall

Configuration des filtres dans *ELSA LANconfig*

La configuration des filtres à l'aide de *ELSA LANconfig* est particulièrement conviviale. Le menu 'Filtre' vous permet d'accéder aux onglets ci-dessous servant à définir les règles de filtrage.



- 'Général'
Le nom du service de filtrage est fixé ici, ainsi que l'action appliquée aux paquets de données.
- 'Postes'
Vous déterminez ici les stations pour lesquelles la règle de filtre doit servir – d'expéditeur ou de destinataire des paquets.
- 'Services'
Les protocoles IP ainsi que les ports source et cible auxquels la règle de filtrage doit s'appliquer sont fixés ici.

Configuration des filtres avec *ELSA WEBconfig* ou via Terminal/Telnet

La configuration via *ELSA WEBconfig* ou une connexion Terminal/Telnet est un peu plus compliquée qu'avec *ELSA LANconfig*.

Dans ce cas, la fonction du filtre est définie dans la liste des filtres qui, elle, se base sur les inscriptions de deux autres tableaux : d'une part, sur un tableau d'objets dans lequel les ordinateurs, réseaux, protocoles, etc., sont



définis en tant qu'objets et, d'autre part, d'un tableau de règles dans lequel source, cible et action sont décrites au moyen des différents objets.

La liste des filtres ne peut pas être créée directement. Elle est automatiquement formée à partir de la table des objets et de la table des règles.

La table des objets

Le tableau des objets contient les éléments ou objets qui doivent être utilisés dans le tableau des règles. Les objets peuvent être les suivants :

- Protocoles
- Postes individuels
- Réseaux entiers
- Services

Ces éléments peuvent aussi être combinés entre eux. De plus, il est possible de définir des objets de façon hiérarchique. Par exemple, on pourrait commencer par définir des objets pour les protocoles TCP et UDP. Plus tard, on pourrait ajouter des objets par exemple pour FTP (= TCP + Ports 20 et 21), HTTP (= TCP + Port 80) et DNS (= TCP, UDP + Port 53), ces derniers pouvant alors être réunis pour former un seul objet contenant les définitions de tous les objets individuels.

Vous trouverez plus de détails sur les descriptions directes que vous pouvez entrer ici dans la section suivante, consacrée au tableau des règles.

La table des règles

Le tableau des règles permet de combiner les différents objets pour constituer des règles de filtrage. Le tableau des règles comporte le protocole devant être filtré (défini dans la table des objets), les objets source, les objets cible et l'action de filtrage à exécuter.

Le protocole, les objets source et les objets cible peuvent aussi bien être formés par des objets confectionnés que contenir des descriptions directes (par exemple %P6 pour TCP) qui sont séparées par '+' ou des caractères d'espacement. Une description directe est caractérisée par le signe '%'. Les descriptions possibles sont les suivantes :

Description	Fonction
%A	Adresse IP
%M	Masque de réseau
%S	Service (port)

Description	Fonction
%L	Réseau local
%H	Nom d'hôte
%P	Protocole (TCP/UDP/ICMP etc.)

Des descriptions similaires peuvent être générées par des listes à séparateur virgule, par exemple des listes d'hôtes / listes d'adresses (%A10.0.0.1, 10.0.0.2) ou par des sélections séparées par un trait d'union telles que des listes de ports (%S20-25). Un '0' ou une chaîne vide désigne l'objet 'any' :

tous les ordinateurs : %A0.0.0.0

tous les services : %S0

tous les protocoles : %P0

Les noms d'hôtes ne peuvent être utilisés que si le *ELSA LANCOM 1600 Office* peut convertir les noms en adresses IP. A cet effet, les noms doivent avoir été déclarés au *ELSA LANCOM 1600 Office* via DHCP ou NetBIOS, ou les liens doivent être enregistrés de façon statique dans la table DNS ou de routage IP. Un enregistrement dans la table de routage IP peut affecter un réseau entier à un nom d'hôte.

Lors de la configuration via la console (Telnet ou émulateur de terminal) les paramètres combinés (port, destination, source) doivent chacun être entre guillemets (– ").

La liste des filtres

La liste des filtres est formée sur la base de la table des objets et de la table des règles. Elle est la conjonction de tous les filtres définis par les règles et les objets.



Nous attirons votre attention sur le fait que les filtres ne sont pas générés en cas de saisie incorrecte et qu'aucun message d'erreur ne vous en avertit. Si vous configurez les filtres manuellement, vérifiez ensuite si les filtres souhaités ont été générés.

6.3

Protection de l'accès RNIS

Chaque participant RNIS peut, en principe, accéder à votre *ELSA LANCOM* s'il s'agit d'un périphérique avec raccordement RNIS. Pour éviter l'intrusion de personnes non autorisées, vous devez donc protéger l'accès RNIS.



Parmi les périphériques de la série ELSA LANCOM 1600 Office, seul le ELSA LANCOM DSL/I-1611 Office en est équipé. Les explications données ci-dessous se réfèrent donc uniquement à ce périphérique précis.

Les fonctions de protection de l'accès RNIS peuvent être réparties en deux groupes :

- Contrôle d'identification
 - Protection de l'accès par un nom et un mot de passe
 - Protection de l'accès par l'identification de l'appelant
- Rappel automatique de numéros définis

6.3.1

Le contrôle d'identification

Le contrôle d'identification peut être effectué par l'intermédiaire du nom du site distant ou par l'identification de l'appelant. L'identification de l'appelant correspond au numéro de téléphone de l'appelant, généralement transmis au site distant lors d'un appel via RNIS.

L'« identificateur » devant être utilisé est défini dans la liste suivante :

Outil de configuration	Appel
ELSA LANconfig	Communication ► Prise d'appel
ELSA WEBconfig	Configuration expert ► Setup ► Module WAN ► Protection
Terminal/Telnet	/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.
- 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

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 d'utilisateur utilisé par le site distant (correspondant souvent au nom du périphérique) est enregistré dans la liste PPP.

Uniquement le nom, sans mot de passe ? Si, cette particularité est également proposée par PPP: ici on peut demander en supplément une protection spéciale pour ce protocole selon PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) ou MS-CHAP (variante Microsoft du CHAP).

Avec PPP, on entre d'abord un nom d'utilisateur (et, avec PAP, CHAP ou MS-CHAP, un mot de passe) lors de l'établissement de la communication avec le correspondant. Lorsqu'un ordinateur tente d'accéder au *ELSA LANCOM 1600 Office*, le logiciel de connexion, par exemple l'accès réseau à distance sous Windows, demande le nom d'utilisateur et le mot de passe dans une fenêtre de saisie.

Si le routeur établit une communication lui-même, par ex. vers un fournisseur d'accès à Internet, le nom du périphérique, le nom de l'utilisateur et le mot de passe seront repris de liste PPP. Si aucun nom d'utilisateur n'est inscrit dans la liste, c'est le nom du périphérique qui sera utilisé.

Pour accéder à la liste PPP, procéder comme suit :

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Communication ► Protocoles ► Liste PPP
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module WAN ► Liste PPP
Terminal/Telnet	Setup/WAN-module/PPP-list

Avec le protocole PPP, l'appelant peut également exiger une authentification du site distant. Il demande alors au site distant la transmission d'un nom d'utilisateur ou de périphérique et d'un mot de passe.



Il est évident que vous n'utiliserez pas les procédures de sécurité PAP, CHAP ou MS-CHAP si vous voulez accéder vous-même par ex. à un fournisseur d'accès Internet avec le ELSA LANCOM 1600 Office. Vous n'arriverez

probablement pas à convaincre le FAI à répondre à une requête du mot de passe...

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

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 – **C**alling **L**ine **I**dentifier).

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 1600 Office*, 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 (couches).

6.3.2

Le rappel

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

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Communication ► Sites distants ► Liste des noms (RNIS)
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module WAN ► Liste des noms RNIS
Terminal/Telnet	/Setup/WAN-module/ISDN-name list

Avec les réglages effectués dans la liste des noms et des numéros ainsi qu'avec le choix du protocole (ELSA ou PPP), vous pouvez contrôler le comportement au rappel de vos routeurs :

- Le routeur peut refuser le rappel.
- Il peut rappeler un numéro prédéfini.
- Il peut contrôler le nom, puis 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 'par nom', le routeur rappelant se charge de toutes les unités de taxation à une exception, celle qui est nécessaire pour la transmission du nom. L'appelant doit également prendre une unité à sa charge s'il n'est pas identifié par CLIP (**C**alling **L**ine **I**dentifier **P**rotocol). Si, par contre, une identification par le numéro d'appel de l'appelant est possible et permise, aucune taxe téléphonique ne sera facturée à l'appelant (rappel via le canal D).

Il existe une méthode très efficace pour le rappel, la procédure Fast-Call-Back (qui fait d'ailleurs l'objet d'une demande de brevet). Celle-ci accélère considérablement la procédure de rappel. Elle ne peut être utilisée que lorsque les deux sites distants la prennent en charge. Tous les routeurs *ELSA LANCOM* actuels supportent la procédure Fast-Call-Back.

Les détails supplémentaires sont décrits dans le chapitre 'Fonctions de rappel automatique' à la page 132.



6.4

La liste de contrôle sécurité

La liste de contrôle suivante vous donne une vue d'ensemble des principales fonctions de sécurité. Ainsi, vous pouvez être sûr de ne rien avoir oublié d'important lors de la configuration des paramètres de sécurité de votre *ELSA LANCOM 1600 Office*.

○ Avez-vous défini un mot de passe pour la configuration ?

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*. Il est particulièrement recommandé de définir un mot de passe pour la configuration lorsque vous souhaitez autoriser la configuration à distance.

○ Avez-vous autorisé la configuration à distance ?

Si vous n'avez pas besoin de la configuration à distance, vous devez désactiver la fonction. Si vous en avez besoin, vous devez absolument définir ici une protection par mot de passe (cf. ci-dessus). Vous trouverez également le champ de désactivation de la configuration à distance pour *ELSA LANconfig* dans l'onglet 'Sécurité' du dossier de configuration 'Gestion'.

Uniquement ELSA
LANCOM DSL/-
1611 Office

Uniquement ELSA
LANCOM DSL/-
1611 Office

○ **Avez-vous défini un mot de passe pour la configuration SNMP ?**

La configuration SNMP devrait également être protégée par mot de passe. Vous trouverez également le champ de protection par mot de passe de la configuration SNMP pour *ELSA LANconfig* dans l'onglet 'Sécurité' du dossier de configuration 'Gestion'.

○ **Avez-vous autorisé l'accès à distance ?**

Si vous n'avez pas besoin de l'accès à distance, désactivez la prise d'appels en choisissant une prise d'appel selon le numéro et laissez vide la liste des numéros dans l'onglet 'Prise d'appel' du dossier de configuration 'Communication' de *ELSA LANconfig*.

○ **Avez-vous activé les options de rappel pour l'accès à distance et le CLI ?**

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 – **C**alling **L**ine **I**dentifier). 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 (ce rappel via le canal D n' est pas supporté par l'accès réseau à distance Windows). Si une protection de l'accès par numéro d'appel a été convenue dans le routeur *ELSA LANCOM 1600 Office*, tous les appels de correspondants dont les numéros sont inconnus seront refusés.

○ **Avez-vous activé le Masquerading IP ?**

La cachette pour tous les ordinateurs du réseau local accédant à Internet s'appelle masquerading IP. Seul le module routeur dans le périphérique ainsi que son adresse IP (fixe ou attribuée 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'une passerelle et ne peuvent pas être reconnus eux-mêmes. Le routeur sépare Internet et Intranet comme par un mur. 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*.

○ **Avez-vous bloqué l'accès aux ports critiques par l'intermédiaire de filtres ?**

Les filtres pare-feu du *ELSA LANCOM 1600 Office* proposent des fonctions de filtrage pour les postes de travail individuels mais aussi pour

des réseaux entiers. Les filtres source ou cible peuvent être appliqués à un port choisi ou à une série de ports. En outre, il est possible de filtrer des protocoles ou des combinaisons de protocoles (TCP/UDP/ICMP). La configuration des filtres à l'aide de *ELSA LANconfig* est particulièrement conviviale. 'Routeur IP' vous permet d'accéder à l'onglet 'Filtre' servant à définir les règles de filtrage.

○ **Avez-vous bloqué l'accès de certaines stations au routeur ?**

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

○ **La sauvegarde de votre configuration LANCOM se trouve-t-elle à un endroit sûr, protégé contre tout accès non autorisé ?**

Votre configuration LANCOM doit être sauvegardée à un endroit sûr, protégé contre tout accès non désiré. Si tel n'est pas le cas, une personne non autorisée pourrait la charger dans un autre périphérique et, par ex. utiliser vos accès Internet à vos frais.

7

Services serveur pour le réseau local

Un *ELSA LANCOM 1600 Office* propose toute une gamme de services aux ordinateurs du réseau local. Ces services représentent des fonctions centrales qui peuvent être utilisées par les différents ordinateurs de poste de travail et, en particulier :

- Gestion d'adresses automatique via DHCP
- Gestion des noms des ordinateurs et réseaux via DNS
- Journalisation du trafic réseau via SYSLOG
- Calcul des unités de taxation
- Fonctions de bureautique avec *ELSA LANCAPI* (uniquement *ELSA LANCOM DSL/I-1611 Office*)

7.1

Gestion d'adresses IP automatique via DHCP

Pour une exploitation sans accroc dans un réseau TCP/IP, tous les périphériques d'un réseau local requièrent des adresses IP bien définies.

De plus, ils ont besoin des adresses des serveurs DNS et NBNS ainsi que d'une passerelle par défaut, qui permet de router les paquets de données des adresses inaccessibles localement.

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

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

7.1.1

Le serveur DHCP

ELSA LANCOM 1600 Office peut gérer les adresses IP en tant que serveur DHCP dans son réseau TCP/IP. Pour ce, il communique aux ordinateurs de postes de travail les paramètres suivants :

- Adresse IP
- Masque de réseau
- Adresse de diffusion

- Passerelle standard
- Serveur DNS
- Serveur NBNS
- Durée de validité des paramètres attribués

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

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

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

7.1.2

DHCP – 'Actif', 'Inactif' ou 'Auto' ?

Le serveur DHCP peut prendre trois états différents :

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

- Si aucun autre serveur DHCP n'est détecté, le périphérique active son propre serveur DHCP.

Enfin, les statistiques DHCP permettent d'établir si le serveur DHCP est connecté ou déconnecté.

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

7.1.3

Attribution des adresses

Attribution d'adresses IP

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

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

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

- Si le routeur n'a ni une propre adresse IP ni une adresse Intranet, le périphérique se trouve dans un état de service particulier. Il utilise alors lui-même l'adresse IP '10.0.0.254' et le pool d'adresses '10.x.x.x' pour l'attribution des adresses IP dans le réseau.

Si un ordinateur est à présent démarré dans le réseau réclamant une adresse IP à l'aide de ses paramètres réseau via DHCP, un périphérique avec module DHCP activé lui proposera l'attribution d'une adresse. Une adresse valable issue du pool est choisie comme adresse IP. Si une adresse IP a déjà été

attribuée par le passé à cet ordinateur, il réclame également cette adresse et le serveur DHCP tente de lui attribuer cette adresse à nouveau, si elle n'a pas été déjà attribuée à un autre ordinateur.

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

Attribution du masque de réseau

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

Attribution de l'adresse de diffusion

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

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

Affectation de la passerelle standard

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

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

Affectation du serveur DNS et du serveur NBNS

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

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.

Durée de validité d'une attribution

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

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

- Période de validité maximale en minutes

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

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

La valeur par défaut de 6 000 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 de poste de travail – Ecraser l'attribution

Si un ordinateur utilise d'autres paramètres que ceux qui lui sont attribués, (une autre passerelle par défaut p. ex.), ces paramètres doivent être réglés directement sur l'ordinateur du poste de travail. Celui-ci ne tient alors pas compte des paramètres correspondants provenant de l'attribution par le serveur DHCP.

Sous Windows 98, cela se fait parex. 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.

Contrôler les adresse IP au sein du réseau local

Outil de configuration	Appel / tableau
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module DHCP ► Tableau DHCP
Terminal/Telnet	Setup/DHCP-module/table-DHCP

Le tableau DHCP suivant fournit une vue d'ensemble des adresses IP du réseau local. Il indique l'adresse IP attribuée / utilisée, l'adresse MAC, la période de validité, le nom de l'ordinateur du 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 de poste de travail a fait une première demande. Le serveur DHCP vérifie si l'adresse devant être attribuée à l'ordinateur est sans ambiguïté.
- 'unkn.'
Lors de ce contrôle, il s'est avéré que l'adresse avait déjà été attribuée à

un autre ordinateur. Le serveur DHCP n'a malheureusement pas la possibilité d'obtenir des informations supplémentaires concernant cet ordinateur.

- 'stat.'

Un ordinateur a communiqué au serveur DHCP qu'il possédait une adresse IP définie. Cette adresse ne peut plus être utilisée.

- 'dyn.'

Le serveur DHCP a attribué une adresse à l'ordinateur.

7.2

DNS

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

7.2.1

Que fait un serveur DNS ?

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

Sans serveur DNS dans le réseau local, chaque nom inconnu au niveau local est recherché via la route par défaut. 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 1600 Office* :

- Un routeur *ELSA LANCOM 1600 Office* faisant fonction de serveur DHCP est en mesure d'affecter les adresses IP aux ordinateurs au sein du réseau local de façon autonome. Le serveur DHCP connaît donc déjà tous les ordinateurs de son propre réseau, qui reçoivent leur adresse IP via DHCP, par leur nom d'ordinateur et par leur adresse IP. Lors de l'attribution dynamique de l'adresse via le serveur DHCP, un serveur DNS externe

Uniquement ELSA
LANCOM
DSL/I-1611 Office

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 1600 Office* connaît les noms d'ordinateur et les adresses IP au sein des autres réseaux NetBIOS connectés. Les ordinateurs avec adresse IP fixe, en outre, du fait qu'ils s'identifient sur le tableau NetBIOS, sont connus par leurs noms et leurs adresses.
- Le serveur DNS dans le routeur *ELSA LANCOM 1600 Office* peut être utilisé en même temps comme mécanisme filtrant très confortable. Les requêtes concernant certains domaines auxquels l'accès n'est pas permis, peuvent être verrouillées pour tout le réseau local, ou seulement pour des sous-réseaux voire des ordinateurs isolés ; pour cela, il suffit d'indiquer le nom des domaines concernés.

Comment le serveur DNS réagit-il à une requête ?

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.
- Enfin, le serveur DNS vérifie si la requête doit être transmise à un autre serveur DNS via une interface WAN (acheminement DNS spécifique par l'intermédiaire du tableau de destinations DNS).

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

7.2.2

Routage par DNS

Si le serveur DNS ne peut résoudre une requête à partir de ses propres tableaux DNS, il la retransmet à d'autres serveurs DNS. On parle alors de routage par DNS (acheminement DNS).

La distinction est faite entre :

- **Routage par DNS spécifique**
Les requêtes relatives à certaines zones de noms sont renvoyées à des serveurs DNS spécifiques.
- **Routage par DNS général**
Toutes les autres requêtes relatives à des noms non spécifiés sont renvoyées au serveur DNS « supérieur ».

Routage par DNS spécifique

Dans ce cas, il est possible de définir des zones de noms dont certains serveurs DNS sont responsables.

Un cas typique pour l'utilisation de l'acheminement DNS spécifique serait le poste de télétravail : l'utilisateur souhaite avoir simultanément accès au réseau interne de l'entreprise (Intranet) et à Internet. Les requêtes concernant l'Intranet doivent être transmises au serveur DNS de la société, tandis que les autres requêtes doivent être renvoyées au serveur DNS du fournisseur d'accès à Internet.

Routage par DNS général

Toutes les requêtes DNS qui ne peuvent être résolues sont transmises à un serveur DNS défini selon les règles suivantes :

- Le routeur recherche d'abord dans sa propre configuration si un serveur DNS a été défini. S'il trouve cette indication, il établit une connexion avec ce serveur et récupère l'information souhaitée. Il est possible de définir jusqu'à deux serveurs 'supérieurs'.

<i>ELSA LANconfig</i>	TCP/IP ► Adresses ► Premier serveur DNS / Deuxième serveur DNS
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module TCP/IP ► DNS par défaut / Sauvegarde DNS
Terminal/Telnet	/Setup/TCP-IP-module/DNS-default /Setup/TCP-IP-module/DNS-backup

- 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 de 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 exemple, 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.

7.2.3

Configuration du serveur DNS

Les paramètres pour le serveur DNS se trouvent dans le menu ou liste ci-dessous :

Outil de configuration	Appel / tableau
<i>ELSA LANconfig</i>	TCP/IP ► Serveur DNS
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module DNS
Terminal/Telnet	cd /Setup/DNS-module

Pour configurer le serveur DNS, procédez de la manière suivante :

- ① Activez le serveur DNS.

<i>ELSA WEBconfig</i>	... ► Etat
Terminal/Telnet	set operating on

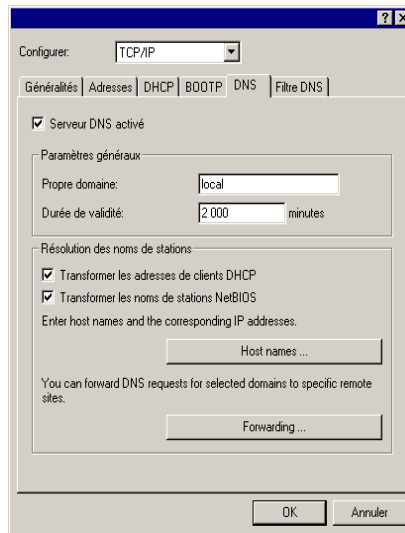
- ② Entrez le domaine auquel appartient le serveur DNS. C'est sur la base de ce domaine que le serveur DNS reconnaît si le nom recherché dans une

requête fait partie du réseau local ou non. L'indication du domaine est facultative.

ELSA WEBconfig	... ► Domaine
Terminal/Telnet	set domain yourdomain.com

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

ELSA WEBconfig	... ► Utiliser DHCP ... ► Utiliser NetBIOS
Terminal/Telnet	set DHCP-usage yes set NetBIOS-usage yes



Serveur DNS actif dans la configuration de TCP-IP

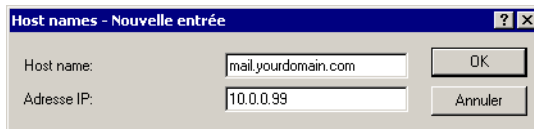
- ④ Le serveur DNS sert avant tout à séparer les requêtes relatives à des noms sur Internet d'avec les requêtes relatives à des noms chez d'autres correspondants. Inscrivez tous les ordinateurs dans le tableau des noms de station
- dont vous connaissez le nom et l'adresse IP,
 - qui ne font pas partie de votre réseau local,
 - qui ne se trouvent pas sur Internet et

○ qui sont joignables via le routeur.

Pour ajouter des stations dans le tableau, utilisez les instructions suivantes :

<i>ELSA LANconfig</i>	TCP/IP ► DNS ► Noms de station ► Ajouter
<i>ELSA WEBconfig</i>	... ► Tableau DNS ► Ajouter
Terminal/Telnet	cd setup/DNS-module/DNS-table set mail.yourdomain.com 10.0.0.99

Si, par ex., vous travaillez dans un bureau extérieur et souhaitez accéder au serveur de messagerie électronique de la centrale via le routeur (nom : mail.yourdomain.com, IP: 10.0.0.99), inscrivez les informations suivantes :



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

Si vous exécutez le logiciel de messagerie électronique, il recherchera probablement automatiquement le serveur 'mail.yourdomain.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 dans la liste des noms, etc., la connexion au réseau du bureau central est établie automatiquement vers le serveur de messagerie électronique enfin trouvé.

- ⑤ Pour qu'un autre serveur DNS se charge de zones de noms entières, ajoutez une inscription d'acheminement composée de la zone de noms et du site distant :

ELSA LANconfig	TCP/IP ► DNS ► Acheminement ► Ajouter
ELSA WEBconfig	... ► Tableau des destinations DNS ► Ajouter
Terminal/Telnet	cd setup/DNS-module/destination table set *.internal COMPANY

Lors de la saisie des zones de noms, vous pouvez utiliser les caractères joker '?' pour des caractères individuels et '*' pour une suite de caractères.

Pour renvoyer tous les domaines se terminant par '.intern' à un même serveur DNS du réseau local du site distant 'COMPAGNIE', tapez l'inscription suivante :



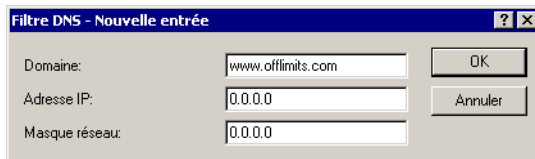
L'adresse IP du serveur DNS doit être transmise automatiquement par le site distant via PPP. Il n'est pas possible de saisir manuellement l'adresse IP de ce serveur DNS.



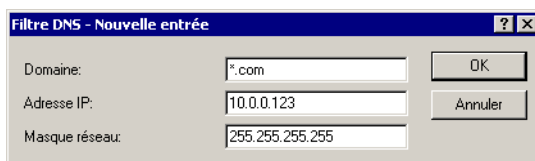
- ⑥ La liste des filtres vous permet de décider qui a le droit d'accéder à quel nom ou à quel domaine.

Pour bloquer l'accès de tous les ordinateurs du réseau local au domaine (dans ce cas le serveur Web) 'www.gesperrt.de', utilisez les instructions et saisies suivantes :

ELSA LANconfig	TCP/IP ► Filtre DNS ► Filtre DNS ► Ajouter
ELSA WEBconfig	... ► Liste-filtre ► Ajouter
Terminal/Telnet	cd setup/DNS-module/filter-list set 001 www.offlimits.com 0.0.0.0 0.0.0.0



L'index '001' de l'instruction console 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 un seul ordinateur (parex. IP 10.0.0.123) ne doit pas pouvoir accéder aux domaines COM, entrez :



En mode console :

```
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' renvoie à tous les réseaux.

7.3

Gestion des taxes téléphoniques

La caractéristique du routeur (établir de façon autonome la connexion avec tous les correspondants souhaités, puis la terminer automatiquement une fois la transmission finie) permet à l'utilisateur d'accéder de façon très conviviale à Internet ou à des ordinateurs et réseaux à distance. Cependant, lors de la transmission de données via les lignes commutées RNIS, une mauvaise configuration du routeur (parex. 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.

Pour limiter ces coûts, le logiciel offre différentes possibilités :

- Les minutes en ligne disponibles peuvent être limitées pour une période déterminée.
- Les coûts ou la durée des connexions RNIS peuvent être limités pour une période déterminée.

Uniquement ELSA
LANCOM
DSL/I-1611 Office

7.3.1

Limitation de la connexion pour modem DSL et modem-câble

Même si une connexion par modem DSL ou modem-câble se comporte comme une connexion fixe pour laquelle un établissement de la connexion n'est pas nécessaire (le début et la fin de la connexion ne pouvant ainsi pas être reconnus), les frais sont tout de même calculés, selon le fournisseur d'accès, en fonction du temps.



Dans la suite de cette section, nous parlerons uniquement des connexions DSL. Les explications s'appliquent toutefois à toutes les autres connexions, établies via la prise 10Base-T-WAN au ELSA LANCOM 1600 Office, par ex. pour les connexions par modem-câble.

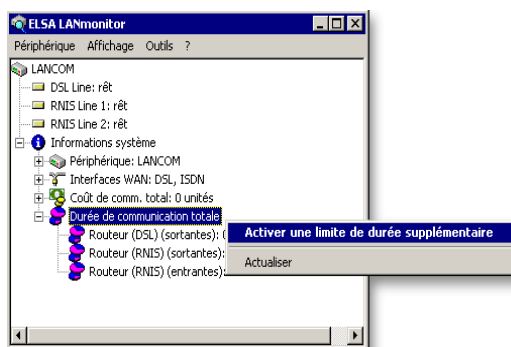
Pour pouvoir néanmoins limiter les frais de téléphone, la durée de connexion maximale peut être fixée en fonction du temps. Pour ce faire, on fixe un budget en fonction du temps pour une période déterminée. Les connexions DSL par défaut par ex. permettent d'établir des connexions actives pendant 600 minutes au maximum en l'espace de six jours.



Une fois l'un des deux plafonds atteint, toutes les connexions DSL ouvertes sont terminées automatiquement. Ce n'est qu'au terme de la période actuelle que les budgets sont à nouveau libérés et les connexions autorisées. L'administrateur peut bien entendu débloquer les budgets également avant terme !

Si vous souhaitez rallonger le budget 'Temps en ligne' pour des actions uniques, par ex. pour télécharger un fichier énorme d'Internet, vous ne devez pas obligatoirement modifier la limite temps. En effet, vous pouvez définir une limite supplémentaire pouvant être activée séparément.

Dans *ELSA LANmonitor*, vous activez cette limite supplémentaire par l'intermédiaire du menu contextuel du temps global de connexion (cliquer avec le bouton droit de la souris sur 'Temps total de connexion') :



Si vous ne voyez pas les informations système dans *ELSA LANmonitor*, activez l'affichage correspondant en passant par **Affichage ► Afficher ► Informations système**.

Les instructions de libération de la limite temps supplémentaire dans *ELSA WEBconfig* et dans la console sont les suivantes :

Outil de configuration	Appel
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Gestionnaire des coûts ► Activation de la réserve
Terminal/Telnet	<code>cd /setup/charges module</code> <code>do activate reserve</code>

L'activation de la limite temps supplémentaire s'applique à la période actuelle. La période suivante est ensuite à nouveau soumise à la limite temps normale.

7.3.2

Limitation des communications RNIS en fonction des unités de taxation

Si les informations de taxation sont transmises à un accès RNIS, les coûts de connexion peuvent être limités de façon très simple. La configuration par défaut permet, par ex., d'utiliser au maximum 830 unités de taxation en six

jours. Dès que cette limite est atteinte, le routeur interdit tout établissement actif d'une connexion.



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



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

7.3.3

Limitation des communications RNIS en fonction de la durée

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

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



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

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



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

7.3.4

Configuration dans le gestionnaire des coûts

Outil de configuration	Appel / tableau
ELSA LANconfig	Management ► Coûts
ELSA WEBconfig	Configuration expert ► Setup ► Gestionnaire des coûts
Terminal/Telnet	cd /setup/charges module

Ce gestionnaire des coûts de communication vous permet d'effectuer tous les paramétrages nécessaires portant sur les durées de connexion et la protection de l'établissement de connexions.

- Période

Durée d'une période de surveillance spécifiée en jours

- Unités de budget, budget de minutes DSL / RNIS

Nombre maximal d'unités RNIS ou de minutes DSL / RNIS en ligne pour une période de surveillance



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

7.4

Le module SYSLOG

Le module SYSLOG permet de consigner les accès au ELSA LANCOM 1600 Office dans un fichier-journal. Cette fonction est en particulier intéressante pour les administrateurs du système puisqu'elle offre la possibilité d'enregistrer un historique sans lacune de toutes les activités.

Pour pouvoir recevoir les messages SYSLOG, il vous faut un client ou démon SYSLOG adéquat. Sous UNIX/Linux, la journalisation est effectuée par le démon SYSLOG qui est en général installé automatiquement. Ce démon s'annonce soit directement via la console ou enregistre le journal dans un fichier SYSLOG correspondant.

Sous Linux, le fichier `/etc/syslog.conf` indique quelles ressources (cf. plus bas) sont déclarées dans quel fichier-journal. Vérifiez dans la configuration du démon si les connexions réseau sont explicitement surveillées.

Windows ne fournit pas de fonction système correspondante. Vous devrez installer des logiciels spécifiques qui se chargent de la fonction de démon SYSLOG.

7.4.1

Configuration du module SYSLOG

Outil de configuration	Appel / tableau
<i>ELSA LANconfig</i>	Management ► Messages
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module SYSLOG
Terminal/Telnet	<code>cd /Setup/SYSLOG-module</code>

7.4.2

Exemple de configuration avec *ELSA LANconfig*

Création d'un client SYSLOG

- ① Démarrez *ELSA LANconfig*. Sélectionnez 'Gestion', puis l'onglet 'Messages'.
- ② Activez le module et cliquez sur **Clients SYSLOG**.
- ③ Dans la fenêtre suivante, cliquez sur **Ajouter...**
- ④ Entrez d'abord l'adresse IP du client SYSLOG, puis définissez les sources et les priorités.

Clients SYSLOG - Nouvelle entrée

Adresse IP:

Source:

☒ Système
☒ Temps système
☒ Connexions
☐ Gestion

☒ Ouvertures de session
☐ Ouverture de session
☐ Comptabilisation
☐ Routeur

Priorité:

☒ Alarme
☒ Avertissement
☐ Débogage

☒ Erreur
☒ Information

SYSLOG provient de la plate-forme UNIX dans laquelle certaines sources sont prédéfinies. *ELSA LANCOM 1600 Office* attribue ses propres sources internes aux sources SYSLOG prédéfinies (les "lignes").

Le tableau suivant fournit une liste des sources de messages disponibles que vous pouvez paramétrer dans le *ELSA LANCOM 1600 Office*, ainsi que leur signification. En plus, la dernière colonne indique l'attribution des sources internes du *ELSA LANCOM 1600 Office* aux lignes SYSLOG dans la configuration au départ usine.

Source	Signification	Ligne
Système	Messages système (procédures d'amorçage, système d'estampillage etc.)	KERNEL
Ouvertures de session	Messages concernant les tentatives d'accès et les déconnexions d'un utilisateur pendant la négociation PPP ainsi que les erreurs survenues.	AUTH
Temps système	Messages concernant les modifications de l'heure système	CRON
Ouverture de session	Messages concernant les accès via consoles (Telnet, outband, etc.), les déconnexions et les erreurs survenues	AUTHPRIV
Connexions	Messages concernant l'établissement et la terminaison d'une connexion ainsi que les erreurs survenues (display trace)	LOCAL0
Comptabilisation	Informations sur le compte après la terminaison d'une connexion (utilisateur, temps en ligne, volume transféré)	LOCAL1
Gestion	Messages concernant les modifications de la configuration, les commandes exécutées à distance, etc.	LOCAL2
Routeur	Statistiques régulières sur les services les plus utilisés (triés par numéro de port) ainsi que messages concernant les paquets filtrés, les erreurs de routage etc.	LOCAL3

Les huit niveaux de priorité définis dans SYSLOG ont été réduits à cinq niveaux dans le *ELSA LANCOM 1600 Office*. Le tableau suivant montre les liens entre le niveau d'alarme, la signification et les priorités SYSLOG.

Priorité	Signification	Priorité SYSLOG
Alarme	Ce niveau regroupe tous les messages qui requièrent l'attention particulière de l'administrateur.	PANIC, ALERT, CRIT

Priorité	Signification	Priorité SYSLOG
Erreur	Ce niveau transmet tous les messages d'erreur qui peuvent être générés même en mode de fonctionnement normal sans qu'une intervention de l'administrateur soit nécessaire (par exemple des erreurs de connexion).	ERROR
Avertissement	Ce niveau véhicule les messages d'erreur qui ne détériorent pas le fonctionnement correct du périphérique.	WARNING
Information	Ce niveau transmet tous les messages ayant un caractère purement informatif (par exemple les informations sur le compte).	NOTICE, INFORM
Débogage	Surveillance des messages de débogage. Les messages de débogage génèrent un volume de données important et entravent le bon fonctionnement du périphérique. Il devraient donc être désactivés en mode de fonctionnement normal et utilisés uniquement pour la recherche d'erreurs.	DEBUG

- ⑤ Quand vous avez terminé de définir tous les paramètres, confirmez les données saisies avec **OK**. Le client SYSLOG est ajouté dans le tableau SYSLOG avec ses paramètres.

Lignes

Le bouton **Attribution de ligne** permet d'attribuer tous les messages de *ELSA LANCOM 1600 Office* à une ligne ; le client SYSLOG peut ensuite les enregistrer dans un fichier-journal spécial.

Exemple

Toutes les lignes sont mises à 'local7'. Sous Linux, la commande

```
local7.* /var/log/lancom.log
```

sert à enregistrer tous les messages du fichier '/etc/syslog.conf' générés par le *ELSA LANCOM 1600 Office* dans le fichier '/var/log/lancom.log'.

7.5

Bureautique avec *ELSA LANCAPI*



Parmi les périphériques de la série *ELSA LANCOM 1600 Office*, seul le *ELSA LANCOM DSL/I-1611 Office* est équipé d'une prise RNIS. Les explications données ci-dessous se réfèrent donc uniquement à ce périphérique précis.

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.

Cette section a pour objectif de vous présenter brièvement l'interface *ELSA LANCAPI* et son utilisation pour les tâches de bureautique.

7.5.1

Avantages de *ELSA LANCAPI*

La mise en œuvre de l'interface *ELSA LANCAPI* apporte des avantages surtout économiques. Tous les postes de travail Windows reliés au réseau local (LAN) ont, via *ELSA LANCAPI*, libre accès aux fonctions de bureautique telles que le télécopieur, le répondeur téléphonique, la gestion de comptes en ligne et le transfert de fichiers (Transfert EuroFile). Toutes les fonctions sont mises à disposition via le réseau sans que les ordinateurs de 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 stations de travail.

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



Nota : toutes les applications que vous exploitez via ELSA 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 !

7.5.2

Installation du client *ELSA LANCAPI*

L'interface *ELSA LANCAPI* est formée par deux composants, un serveur (dans le *ELSA LANCOM DSL/I-1611 Office*) et un client (sur les PC). Le client *ELSA LANCAPI* est installé sur tous les ordinateurs du réseau local qui souhaitent utiliser les fonctions de l'interface *ELSA LANCAPI*.

- ① Introduisez le CD-ROM *ELSA LANCOM Office* 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 Office*.
- 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 éventuel de l'ordinateur, l'interface *ELSA 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*.

7.5.3

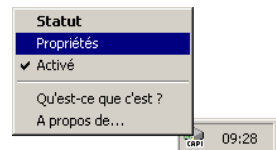
Configuration des clients *ELSA LANCAPI*

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

- ④ Démarrez le client *ELSA LANCAPI* dans le dossier 'ELSAIlan'. Vous trouverez les informations sur le pilote du service mis à disposition dans l'onglet 'Généralités'.



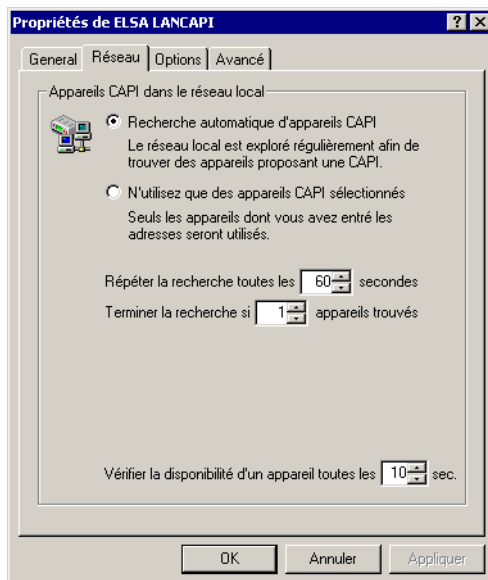
*Vous pouvez également lancer le client ELSA LANCAPI à partir de la barre des tâches de Windows. Pour cela, cliquez avec le bouton droit de la souris sur le symbole ELSA LANCAPI de la barre des tâches de Windows, à côté de l'horloge et sélectionnez **Propriétés**.*



- ⑤ Dans le client *ELSA LANCAPI*, passez à l'onglet **Réseau**. Indiquez si le PC doit rechercher son serveur *ELSA 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* en tant que serveurs

ELSA 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.



7.5.4

Configuration du serveur *ELSA LANCAPI*

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

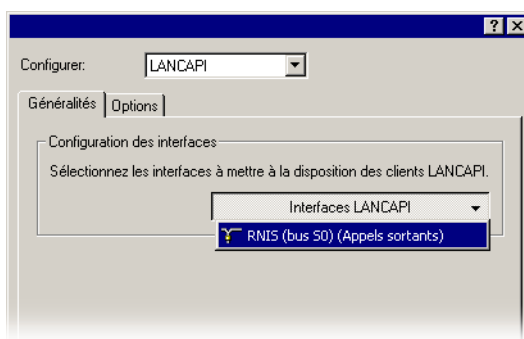
- A quels numéros d'appel l'interface *ELSA LANCAPI* doit-elle réagir ?
- Lequel des ordinateurs du réseau local doit-il avoir accès au réseau RNIS via *ELSA LANCAPI* ?

Le serveur *ELSA LANCAPI* est configuré au moyen des menus suivants :

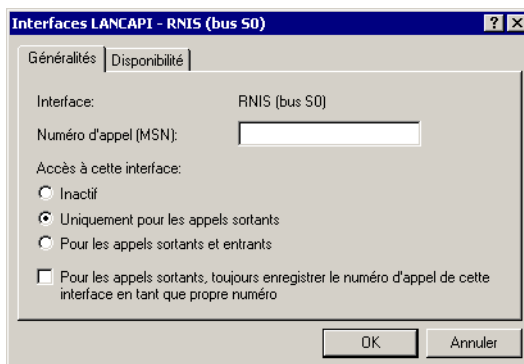
Outil de configuration	Appel / menu
<i>ELSA LANconfig</i>	LANCAPI
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module LANCAPI
Terminal/Telnet	cd /setup/LANCAPI-module

Exemple de configuration avec *ELSA LANconfig*

- ① Ouvrez la configuration du routeur en double-cliquant sur le nom souhaité dans la liste et sélectionnez la zone de configuration **LANCAPI**.
- ② Sélectionnez l'interface RNIS que vous souhaitez configurer.



- ③ Activez le serveur *ELSA LANCAPI* pour les appels sortants et entrants ou autorisez uniquement les appels sortants.

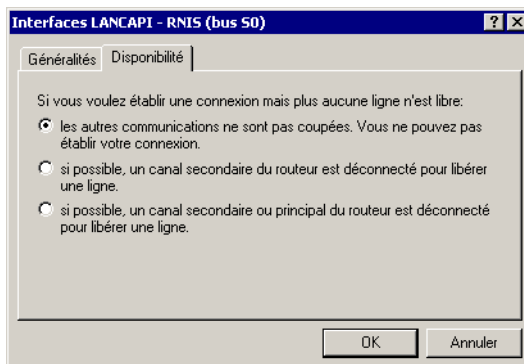


- ④ Dans le deuxième cas, l'interface *ELSA LANCAPI* ne réagit pas aux appels entrants et ne peut pas être mise en œuvre par ex. pour la réception de télécopies. Par ex., autorisez uniquement les appels sortants lorsque vous avez déjà attribué tous les numéros d'appel disponibles aux autres appareils de télécommunication.
- ⑤ Quand le serveur *ELSA LANCAPI* est actif, entrez dans le champ 'Numéro d'appel (MSN)' les numéros de téléphone auxquels *ELSA LANCAPI* doit réagir. Séparez les numéros par un point-virgule. Pour que *ELSA LANCAPI* accepte tous les appels entrants, laissez ce champ vierge.
- ⑥ Par défaut, le port IP utilisé par *ELSA 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.
- ⑦ Lorsque certains ordinateurs du réseau local ne doivent pas accéder aux fonctions de *ELSA LANCAPI*, spécifiez dans la liste d'accès l'adresse IP des participants autorisés.



Si vous indiquez plusieurs numéros d'appel pour ELSA LANCAPI, vous pouvez mettre à la disposition des divers ordinateurs de 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.

- ⑧ Sélectionnez l'onglet 'Disponibilité'. Indiquez comment un *ELSA LANCOM DSL/I-1611 Office* se comporte lorsqu'une connexion doit être établie via *ELSA LANCAPI* (appel entrant ou sortant) mais que les deux canaux B sont occupés (gestion des priorités).



Signification des options proposées :

- 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 *ELSA 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. Lorsque le routeur établit deux connexions distinctes avec deux correspondants (deux canaux principaux sont occupés), l'interface *ELSA LANCAP* doit attendre.
- La connexion via *ELSA LANCAP* peut toujours être établie, une connexion du routeur sera coupée le cas échéant pour la durée de la communication. Ainsi, la fonction télécopie est toujours accessible.

7.5.5

Utilisation de *ELSA LANCAP*

Vous avez deux possibilités pour utiliser *ELSA LANCAP* :

- Vous utilisez un logiciel qui accède directement à une interface CAPI (dans ce cas : *ELSA 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 commu-

nication installés vous souhaitez utiliser. Pour *ELSA LANCAPI*, sélectionnez 'ISDN WAN Line 1'.

7.5.6

ELSA CAPI Faxmodem

Avec *ELSA CAPI Faxmodem*, vous disposez sous Windows d'un pilote de télécopie (fax class 1) qui, en tant qu'interface entre *ELSA LANCAPI* et l'application, permet d'utiliser des programmes de télécopie standard en liaison avec un routeur *ELSA LANCOM 1600 Office*.

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, parex. sous 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 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 parex. au petit symbole CAPI en bas à droite sur l'écran. Veuillez observer également les réglages du pilote ELSA LANCAPI lui-même.

8

Routage et connexions WAN

Ce chapitre est consacré à la description des principaux protocoles et inscriptions de configuration qui entrent en jeu dans les connexions WAN. Il vous indiquera également comment optimiser ces connexions via DSL, modem-câble ou RNIS.

FR

8.1

Connexions WAN - Généralités

Les connexions WAN sont utilisées pour les applications suivantes :

- Accès à Internet via DSL, modem-câble ou RNIS
- Couplage LAN-LAN via RNIS
- Accès à distance via RNIS

8.1.1

Ponts pour protocoles standard

Les connexions WAN se distinguent des connexions directes (par exemple avec l'interface *ELSA LANCAP*) par le fait qu'elles font appel, pour le transfert de données au sein du réseau étendu, à des protocoles réseau standardisés également utilisés dans le réseau local. Les connexions directes, quant à elles, utilisent des procédures spécifiques développées spécialement pour les connexions point à point.

Les connexions WAN permettent d'étendre un réseau local tandis que les connexions directes autorisent uniquement l'accès d'un ordinateur à un autre. Les premières constituent donc une sorte de pont permettant la communication entre plusieurs réseaux (par exemple pour relier différents ordinateurs individuels à un réseau local).

Protocoles utilisés pour les connexions WAN

Les connexions WAN utilisent l'accès grande vitesse (pour les connexions via DSL et modem-câble) lors du transfert de paquets selon le standard IP. Outre le standard IP, le *ELSA LANCOM DSL/I-1611 Office* supporte également le standard IPX grâce à son interface RNIS.

Etroite collaboration avec les modules routeur

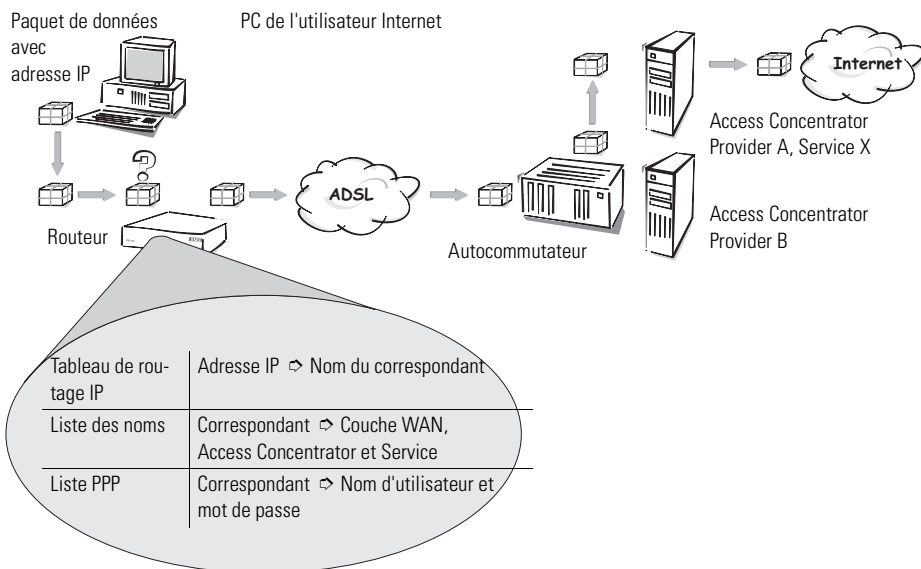
Les connexions WAN se caractérisent par l'étroite collaboration avec les modules routeur au sein du *ELSA LANCOM*. Ces modules (IP et, pour le *ELSA LANCOM DSL/I-1611 Office*, IPX) permettent de relier le réseau local au

8.1.2

Que se passe-t-il lors d'une requête provenant du réseau local ?

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 nécessaires doivent être déclarés. Ces paramètres sont définis dans plusieurs listes qui permettent d'établir les connexions requises.

Nous allons expliquer cette procédure à l'aide d'un exemple simplifié (via ADSL). Pour cela, nous partons du principe que l'adresse IP de l'ordinateur recherché sur Internet est connue.



① Sélection de la bonne route

Un paquet de données en provenance d'un ordinateur trouve en premier lieu sa voie vers Internet via l'adresse IP du destinataire. Avec cette adresse, l'ordinateur envoie le paquet au routeur via le réseau local. Le

routeur recherche dans son tableau de routage IP le correspondant par lequel il est possible d'accéder à l'adresse IP cible, par ex. 'Provider_A'.

② **Données d'authentification du site distant**

Grâce à ce nom, le routeur trouve dans la liste des noms celui de l'Access Concentrator correspondant et du service qu'il doit utiliser dans ce AC. Par ailleurs le routeur obtient à partir de la liste PPP le nom d'utilisateur et le mot de passe qui sont nécessaires pour établir la communication avec le fournisseur d'accès A.

③ **Etablissement de la connexion WAN**

Le routeur peut ensuite établir une liaison sur la ligne ADSL et indiquer qu'il souhaite une connexion à l'Access Concentrator du fournisseur d'accès A et utiliser son service X. Il transmet son nom d'utilisateur et son mot de passe pour l'authentification.

④ **Transfert du paquet de données**

Dès que la connexion est établie, le routeur peut transmettre le paquet de données sur Internet via la ligne ADSL.

8.2

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 paragraphe vous montre comment le tableau de routage IP est organisé dans un routeur ELSA, ainsi que les fonctions de routage IP supplémentaires.

8.2.1

Le tableau de routage IP

Dans le tableau de routage IP, vous déclarez au routeur les correspondants (donc les autres routeurs ou ordinateurs) auxquels doivent être envoyées 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 supprimez, 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 256 entrées, le

tableau dynamique 128. Lorsque IP-RIP est actif, le routeur IP tient compte des deux tableaux.

En outre, le tableau de routage IP 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 de 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 » doivent être utilisées uniquement lorsqu'aucune autre route vers le correspondant n'est trouvée.

Configuration du tableau de routage

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Routeur IP ► Routage ► Tableau de routage
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module routeur IP ► Tableau de routage IP
Terminal/Telnet	<code>cd /Setup/IP-router/IP-routing-tab.</code>

Un tableau de routage IP peut prendre la forme suivante :

Adresse IP	Masque de réseau IP	Routeur	Distance	Masquage
192.168.120.0	255.255.255.0	MAIN	2	On
192.168.125.0	255.255.255.0	NODE1	3	Off
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

Il s'agit de l'adresse du réseau de destination des paquets de données 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.

L'adresse IP '255.255.255.255' avec le masque de réseau '0.0.0.0' correspond à la route par défaut. Tous les paquets ne pouvant pas être

acheminés sur la base des autres entrées de routage sont transmis au correspondant indiqué ici.

- **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 situé dans un autre réseau ou un ordinateur de 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 connaissant le chemin vers le réseau de destination.

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

Les routes ayant le nom de routeur '0.0.0.0' désignent des routes d'exclusion. Les paquets destinés à ces « routes zéro » sont rejetés et ne sont donc pas transmis. Ceci permet, par exemple, d'exclure les routes interdites sur Internet (zones d'adresses privées, parex. '10.0.0.0').

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

- **Distance**

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

- Masquage

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

Les détails supplémentaires sont décrits dans le chapitre 'La cachette – Masquerading IP (NAT, PAT)' à la page 65.

8.2.2

Routage local

Vous connaissez déjà le comportement des ordinateurs de 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 standard. Lorsque plusieurs routeurs coexistent dans un réseau, on n'aura souvent qu'un seul routeur par défaut qui doit pouvoir joindre toutes les adresses IP inconnues pour l'ordinateur au poste de travail. Or, ce routeur par défaut est lui-même parfois incapable d'atteindre le réseau de destination mais il connaît un autre routeur qui trouvera le chemin.

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

En standard, le routeur envoie à l'ordinateur une réponse comportant l'adresse du routeur connaissant la route vers le réseau de destination (cette réponse est appelée redirection ICMP). Sur ce, l'ordinateur de 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. Vous donnez ainsi au routeur dans votre appareil l'instruction d'envoyer le paquet automatiquement à l'autre routeur correspondant. En outre, le routeur n'émet plus de redirection ICMP. Paramétrage :

Outil de configuration	Appel
<i>ELSA LANconfig</i>	Routeur IP ► Général ► Transmettre les paquets dans le réseau local
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module routeur IP ► Routage local
Terminal/Telnet	<code>set /setup/IP-router/loc.-routing on</code>

Parfois, le routage local peut s'avérer très utile mais son utilisation devrait rester une exception. En effet, le routage local entraîne un volume de transfert deux fois plus important vers le réseau de destination. Les données sont d'abord envoyées au routeur par défaut qui les envoie ensuite au routeur compétent du réseau local.



8.2.3

Routage dynamique avec IP-RIP

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

Quelles sont les informations propagées avec IP-RIP ?

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

- Routes rejetées dans le cas de la configuration avec '0.0.0.0'.
- Routes qui renvoient à d'autres routeurs dans le réseau local.
- Routes qui relient les ordinateurs de postes de travail 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 dans ce cas que la route considérée n'est pas accessible actuellement. L'impossibilité pour le routeur d'établir une connexion supplémentaire s'explique par l'une des causes suivantes :

- Une autre connexion a déjà été établie dans tous les autres canaux (également via *ELSA LANCAP*).
- Les connexions en Y pour l'accès S_0 sont expressément interdites dans le tableau des interfaces.
- La connexion en cours utilise tous les canaux B (regroupement des canaux).
- La connexion en cours se fait via une liaison permanente. Très peu de fournisseurs RNIS offrent la possibilité d'établir une communication sur le second canal B alors que le premier canal B fait l'objet d'une liaison permanente.

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	Routeur
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

Signification de ces entrées

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

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

- La route n'existe pas dans le tableau et, dans ce cas, elle est ajoutée (s'il y a de la place).
- La route figure dans le tableau avec un temps '5' ou '6'. La nouvelle route est insérée dans le tableau si la valeur de la distance est inférieure ou égale à l'ancienne.
- La route figure dans le tableau avec un temps de '7' à '10', donc avec la distance '16'. La nouvelle route est insérée dans le tableau dans tous les cas.
- La route figure dans le tableau. Une nouvelle route vient du même routeur qui avait déjà communiqué la première route, mais celle-ci a une distance plus avantageuse que la nouvelle route. Lorsqu'un périphérique communique ainsi la détérioration de son propre tableau de routage statique (par ex. quand la distance passe de 1 à 2 après la coupure de la connexion, voir plus loin), le routeur le croit et ajoute l'enregistrement plus mauvais 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 ne prenant pas en charge le protocole RIP. Ces routeurs ne peuvent pas détecter les paquets RIP et les traitent comme des paquets normalement diffusés 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 enregistrer 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.

Configuration de la fonction IP-RIP

Outil de configuration	Menu/Table
<i>ELSA LANconfig</i>	Routeur IP ► Général ► Options RIP
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module routeur IP ► Paramétrage RIP
Terminal/Telnet	<code>cd /setup/IP-router-module/RIP setting</code>

- Le champ 'Prise en charge RIP' (ou 'Type RIP') propose les sélections suivantes :
 - ☐ 'off' : IP-RIP n'est pas utilisé (standard).
 - ☐ 'RIP-1' : les paquets RIP-1 et RIP-2 sont reçus mais seuls les paquets RIP-1 sont envoyés.
 - ☐ 'compatible RIP-1' : les paquets RIP-1 et RIP-2 sont également reçus. Les paquets RIP-2 sont envoyés en tant que diffusion IP.
 - ☐ 'RIP-2' : similaire à 'compatible RIP-1'. En revanche, tous les paquets RIP sont envoyés à l'adresse de diffusion restreinte IP 224.0.0.9.
- L'inscription sous 'Masque RIP-1' (ou 'Masque R1') peut prendre les valeurs suivantes :
 - ☐ 'Classe' (standard) : le masque de réseau utilisé dans le paquet RIP est constitué de la classe d'adresse IP, ce qui signifie que les masques suivants sont utilisés pour les classes de réseau :

Classe A	255.0.0.0
Classe B	255.255.0.0
Classe C	255.255.255.0

- ☐ 'Adresse' : le masque de réseau se compose du premier bit défini dans l'adresse IP saisie. Ce bit et tous les bits supérieurs au sein du

masque de réseau sont définis. Pour une adresse IP '127.128.128.64', on obtient donc le masque de réseau IP '255.255.255.192'.

- 'Classe+Adresse' : le masque de réseau est constitué à partir de la classe d'adresse IP et d'un supplément selon la procédure d'adressage utilisée. L'adresse indiquée ci-dessus et le masque de réseau 255.255.0.0 donnent donc le masque de réseau IP 255.128.0.0.



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.

8.2.4

Policy Based Routing

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

Pour activer ou désactiver la procédure Policy Based Routing, procédez comme suit :

Outil de configuration	Menu/Table
ELSA LANconfig	Routeur IP ► Général ► Tenir compte du champ TOS
ELSA WEBconfig	Configuration expert ► Setup ► Module routeur IP ► Méthode de routage ► Méthode de routage
Terminal/Telnet	cd /setup/IP-router-module/routing method set routing method TOS (on) set routing method NORMAL (off)

8.2.5

SYN/ACK-Speedup

La procédure SYN/ACK-Speedup permet d'accélérer le trafic de données IP. Lorsqu'elle est activée, les signaux de contrôle IP (SYN pour synchronisation et ACK pour acknowledge) sont traités en priorité dans la mémoire tampon 'Envoi' par rapport aux paquets de données simples. Ceci évite que les signaux de contrôle restent bloqués dans la file d'attente pour les envois, ce qui pourrait entraîner un arrêt de la transmission depuis le site distant.

La procédure SYN/ACK-Speedup est particulièrement utile lors de connexions rapides au cours desquelles des données sont transmises à grande vitesse dans les deux sens.

La procédure SYN/ACK-Speedup est activée par défaut.

Désactivation dans les cas critiques

Certains paquets étant traités en priorité, l'ordre original des paquets est modifié. Bien que TCP/IP ne garantit pas une suite spécifique des paquets, cela peut entraver le fonctionnement de certaines applications, et pas seulement des applications qui exigent un ordre spécifique, différent du protocole standard. Dans un tel cas, il est possible de désactiver la procédure SYN/ACK-Speedup :

Outil de configuration	Menu/Table
<i>ELSA LANconfig</i>	Routeur IP ► Général ► Transmission prioritaire des paquets TCP SYN et ACK
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module routeur IP ► Méthode de routage ► SYN/ACK-Speedup
Terminal/Telnet	<code>cd /Setup/IP-router-module/routing method</code> <code>set SYN/ACK-Speedup OFF</code>

8.3

Configuration des correspondants

Les correspondants sont configurés dans deux tableaux :

- La liste des noms permet de configurer toutes les informations concernant un seul correspondant.
- Les paramètres appliqués aux niveaux de protocole inférieurs (en dessous de IP / IPX) sont définis dans la liste des couches communication.

Ce chapitre ne traite pas de la configuration de l'authentification (protocole, nom d'utilisateur, mot de passe). Vous trouverez de plus amples informations concernant l'authentification sous 'Etablissement de la connexion via PPP' à la page 124.



8.3.1

Liste des noms

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

Les périphériques de type *ELSA LANCOM DSL/I-1611 Office* disposent de deux listes de noms, l'une pour les correspondants DSL (ou modem-câble) et l'autre pour les correspondants RNIS. Les *ELSA LANCOM 1600 Office* sans prise RNIS comportent uniquement la liste des noms DSL.

Outil de configuration	Menu/Table
<i>ELSA LANconfig</i>	Communication ► Correspondants ► Liste des noms (DSL) Communication ► Correspondants ► Liste des noms (RNIS)
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module WAN ► Liste des noms DSL ou Liste des noms RNIS
Terminal/Telnet	cd /setup/WAN-module set DSL name list [...] set ISDN name list [...]

- Les paramètres suivants sont nécessaires pour un correspondant DSL :

Liste des noms	Paramètres	Signification
DSL	Nom	Ce nom permet aux modules de routage d'identifier le correspondant. Dès que le routeur a déterminé au moyen de l'adresse IP chez quel correspondant la destination souhaitée peut être jointe, les paramètres de connexion correspondants peuvent être trouvés dans la liste des noms.
	Time-out	Ce délai indique la durée pendant laquelle la connexion reste active quand plus aucune donnée n'est transmise. Lorsque le time-out indiqué est zéro, la connexion n'est pas terminée automatiquement. Lorsque le time-out indiqué est 9999 secondes, les connexions interrompues sont relancées automatiquement (cf. 'Liaison fixe pour flatrates – Keep-Alive' à la page 131).
	Access Concentrator	L'Access Concentrator (AC, concentrateur d'accès) est le serveur qui peut être joint via le correspondant considéré. Lorsqu'on a le choix entre plusieurs fournisseurs d'accès qui sont joignables via votre accès DSL, sélectionnez le fournisseur d'accès compétent pour la zone d'adresses IP de ce correspondant en indiquant le nom de l'AC. La valeur de l'AC vous est communiquée par votre fournisseur d'accès. Lorsque la valeur de l'AC n'est pas indiquée, chaque AC qui propose le service demandé est accepté.

Liste des noms	Paramètres	Signification
	Service	Indiquez ici le service que vous souhaitez utiliser chez votre fournisseur d'accès. Il peut s'agir de la navigation simple sur Internet mais aussi du téléchargement de vidéos. La valeur du service vous est communiquée par votre fournisseur d'accès. Lorsque la valeur du service n'est pas indiquée, chaque service que l'AC demandé propose est accepté.
	Nom de la couche	Choisissez la couche communication devant être utilisée pour la connexion considérée. La configuration de cette couche est décrite dans la section suivante.
RNIS	Nom	Comme pour la liste des noms DSL.
	Numéro d'appel	Un numéro d'appel est uniquement nécessaire si le correspondant doit être appelé. Ce champ peut rester vide s'il est seulement prévu de prendre les appels entrants. Il est possible d'entrer plusieurs numéros d'appel pour un même correspondant dans la liste RoundRobin.
	Time-out	Comme pour la liste des noms DSL.
	Time-out pour le regroupement	Le second canal B d'un regroupement est libéré lorsqu'il n'a pas été utilisé pendant la durée définie.
	Nom de la couche	Comme pour la liste des noms DSL.
	Rappel automatique	Le rappel automatique permet une connexion sûre et réduit les coûts pour l'appelant. Vous trouverez de plus amples informations sous 'Fonctions de rappel automatique' à la page 132.



Lorsque ni l'Access Concentrator ni le service ne sont indiqués dans la liste des noms DSL, le routeur établit une connexion avec le premier AC qui répond à la requête via l'autocommutateur.

8.3.2

Liste des couches

Dans une couche, vous combinez les paramètres du protocole de transmission à utiliser pour la connexion vers certains correspondants. Vous trouverez la liste des couches communication sous :

Outil de configuration	Liste
<i>ELSA LANconfig</i>	Communication ► Général ► Couche communication
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module WAN ► Liste des couches
Terminal/Telnet	<code>cd /setup/WAN-module</code> <code>set layer-list [...]</code>

Les combinaisons courantes de protocoles sont déjà prédéfinies dans la liste des couches communication. Elles ne devraient être modifiées que si les correspondants ne sont pas compatibles avec les couches existantes. Le tableau suivant vous donne une vue d'ensemble des différentes possibilités :

Paramètres	Signification
Nom de la couche	Ce nom permet de sélectionner la couche dans la liste des noms.
Encapsulation	Au-delà de la troisième couche du modèle de référence OSI, les paquets de données peuvent également être agrégés en tant que paquets Ethernet. Ce paramètre est indispensable pour permettre la communication avec les anciens périphériques <i>ELSA LANCOM</i> . Si la valeur est 'Transparent', les paquets ne font pas l'objet d'une encapsulation.
Couche 3	Les options suivantes sont disponibles pour la couche transmission (ou couche réseau) :
	'Transparent' Aucun en-tête supplémentaire n'est ajouté.
	'PPP' L'établissement de la connexion est effectué selon le protocole PPP (en mode synchrone, c'est-à-dire dans les deux sens). Les données de configuration sont reprises du tableau PPP.
	'AsyncPPP' Comme pour 'PPP' mais en mode asynchrone. PPP s'oriente donc sur les signaux.
	'... avec script' Toutes les options peuvent également être exécutées au moyen d'un script particulier, indiqué dans la liste des scripts.
	'ELSA' Procédure propre à ELSA pour la négociation des connexions.
	'DHCP' Attribution des paramètres réseau via DHCP.

Paramètres	Signification	
Couche 2	Ce champ permet de configurer la partie supérieure de la couche sécurité (Data Link Layer). Les options possibles sont les suivantes :	
	'Transparent'	Aucun en-tête supplémentaire n'est ajouté.
	'X.75LAPB'	Etablissement de la connexion selon X.75 et LAPM (Link Access Procedure Balanced).
	'PPPoE'	La négociation PPP passe par Ethernet. Pour cela, les paquets PPP sont agrégés en trames Ethernet. Cette procédure est souvent utilisée lors de connexions DSL.
Options	Vous pouvez activer ici la compressions des données transférées et le regroupement de canaux. Cette option n'est efficace que si elle est prise en charge aussi bien par les interfaces utilisées que par les protocoles couche 2 et couche 3 sélectionnés. Les détails supplémentaires sont décrits dans le chapitre 'Regroupement des canaux avec MLPPP' à la page 136.	
Couche 1	Ce champ permet de configurer la partie inférieure de la couche sécurité (Data Link Layer). Les options possibles sont les suivantes :	
	'ETH-10'	Ethernet 10 Mbits transparent selon IEEE 802.3.
	'HDLC'	Sauvegarde et synchronisation de la transmission de données selon HDLC (en mode 7 ou 8 bits).
	'V.110'	Transmission selon V.110 à un taux maximum de 38 400 bits/seconde.

8.4

Etablissement de la connexion via 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.

8.4.1

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 selon PAP, CHAP ou MS-CHAP
- Fonctions de rappel (uniquement *ELSA LANCOM DSL/I-1611 Office*)
- 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 emploie le protocole IPCP (IP Control Protocol).
- Vérification de la connexion avec LCP (Link Control Protocol)
- Regroupement de plusieurs canaux RNIS (multilink PPP – uniquement *ELSA LANCOM DSL/I-1611 Office*)

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 de poste de travail distants (uniquement *ELSA LANCOM DSL/I-1611 Office*)
- 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, MS-CHAP ou aucun). LCP passe ensuite en état Opened.

- Authenticate phase (phase d'authentification)

Au besoin, les mots de passe sont échangés. Pour l'authentification selon PAP, le mot de passe n'est transmis qu'une seule fois. Dans le cas de CHAP ou de MS-CHAP, un mot de passe crypté est transmis périodiquement en 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 (ce dernier uniquement dans le *ELSA LANCOM DSL/I-1611 Office*) sont implémentés dans le *ELSA LANCOM 1600 Office*.

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 tracés PPP offrent une autre possibilité d'analyse. La commande

```
trace + ppp
```

Uniquement ELSA
LANCOM
DSL/I-1611 Office

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.

8.4.2

Tout est bon? Vérification de la ligne avec LCP

Pendant l'établissement de la connexion avec PPP, les périphériques en présence négocient une procédure commune pour la transmission des données. Ils décident, 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. Si, par exemple, la connexion grande vitesse ne fonctionne pas, une interface RNIS existante peut prendre le relais pour assurer l'accès à Internet.



Dans le cas de l'accès à distance d'ordinateurs de poste de travail sous Windows, 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 'Temps' et 'Rép.' vous servent à fixer l'intervalle entre les requêtes LCP ainsi que le nombre de tentatives quand il n'y a pas de réponse. Dès que ces valeurs sont atteintes, la ligne peut être considérée comme en dérangement. Pour désactiver totalement les requêtes LCP, le temps et les répétitions sont mis tous les deux à 0.

8.4.3

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 1600 Office* peut lui attribuer 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 (en règle générale) au sein d'un réseau local.

Une adresse IP peut être attribuée uniquement lorsque le ELSA LANCOM 1600 Office peut identifier le correspondant au moyen de son numéro d'appel ou de son nom, c'est-à-dire si l'authentification a abouti.

Exemples

● Accès à distance

L'attribution de l'adresse est possible grâce à une entrée spéciale dans le tableau de routage IP. En plus de l'adresse IP dans le champ 'Nom du routeur' devant 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 1600 Office*.

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 1600 Office* lui fournisse automatiquement l'adresse IP et les serveurs de noms. 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.

● Accès à Internet

Lorsqu'on réalise un accès Internet pour un réseau local via *ELSA LANCOM 1600 Office*, l'attribution des adresses IP peut prendre le chemin inverse. Dans ce contexte, on peut réaliser des configurations dans lesquelles *ELSA LANCOM 1600 Office* 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 1600 Office* obtient

également des informations sur les serveurs DNS pendant la négociation PPP.

Dans le réseau local, *ELSA LANCOM 1600 Office* 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 *ELSA 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 connexion sont affichées.

8.4.4

Paramètres dans la liste PPP

A l'aide de cette liste, vous pouvez créer une définition individuelle de la négociation PPP pour chaque correspondant prenant contact avec votre réseau.

Outil de configuration	Liste
<i>ELSA LANconfig</i>	Communication ► Protocoles ► Liste PPP
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module WAN ► Liste PPP
Terminal/Telnet	<code>cd /setup/WAN-module</code> <code>set PPP-list [...]</code>

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 de périphérique)	Nom que le correspondant utilise pour s'annoncer sur votre routeur
Nom d'utilisateur	Nom que votre routeur utilise pour s'annoncer chez le correspondant. Si ce champ reste vide, c'est le nom de périphérique de votre routeur qui est utilisé.
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 :
Vérification du correspondant (authentification)	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', '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.
Temps	Délai entre deux vérifications de la connexion selon LCP (cf. chapitre suivant). Vous exprimez ce temps par un multiplicateur de 10 secondes (par ex. : 2 pour indiquer 20 secondes). Correspond également au délai entre deux vérifications de la connexion selon CHAP. Indiquez ce délai en minutes. Ce temps doit être '0' pour les correspondants utilisant Windows !
Répétitions (Rép)	Nombre de tentatives de vérification. En choisissant plusieurs tentatives, vous contournez l'effet des perturbations sporadiques de la ligne. C'est uniquement lorsque toutes les tentatives échouent que la connexion est coupée. Le délai entre deux tentatives s'élève à 1/10e du délai séparant deux vérifications. En même temps le nombre maximal de requêtes de configuration (configure requests) que le routeur émet avant qu'il ne suppose une perturbation de la ligne et raccroche lui-même.
Conf, Fail, Term	Ces paramètres permettent d'influencer le mode de fonctionnement de PPP. Ils sont définis dans la recommandation RFC 1661 et ne seront pas décrits ici. Si vous ne pouvez pas établir de connexion PPP, vous trouverez dans cette recommandation et dans les statistiques PPP du routeur des informations sur le dépannage. En général, les paramètres par défaut suffisent. Ces paramètres ne peuvent être modifiés que par <i>ELSA LANconfig</i> , SNMP ou TFTP !

8.5

Etablissement de la connexion DSL avec PPTP

De plus en plus de fournisseurs d'accès DSL autorisent l'établissement de connexions non seulement via PPPoE mais aussi via PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol). PPTP est une extension du protocole PPP, principalement développée par Microsoft.

PPTP permet de créer des « tunnels » pour joindre un correspondant via les réseaux IP. Un tunnel représente une connexion logique blindée qui protège

les données transmises contre tout accès non autorisé en utilisant l'algorithme de cryptage RC4.

Configuration de PPTP

Dans *ELSA LANCOM 1600 Office*, tous les paramètres PPTP requis sont passés en revue par l'assistant d'accès à Internet dès que l'accès via PPTP est sélectionné. Outre les informations nécessaires pour l'accès normal via PPPoE, il suffit d'entrer ici l'adresse IP de la passerelle PPTP. La passerelle PPTP est souvent le modem DSL. Pour plus de renseignements, contactez votre fournisseur d'accès DSL.

Les modifications de la configuration sont apportées dans la liste PPTP :

Outil de configuration	Liste
<i>ELSA LANconfig</i>	Communication ► Protocoles ► Liste PPTP
<i>ELSA WEBconfig</i>	Configuration expert ► Setup ► Module WAN ► Liste PPTP
Terminal/Telnet	cd /Setup/WAN-module set PPTP-list [...]

La configuration PPTP comporte trois paramètres :

- 'Correspondant' – Désignation reprise de la liste des noms DSL.
- 'Adresse IP' – Adresse IP de la passerelle PPTP, correspondant généralement à l'adresse du modem DSL
- 'Port' – Port IP utilisé par le protocole PPTP. Selon le standard de protocole, il devrait toujours s'agir du port '1.723'.

8.6

Liaison fixe pour flatrates – Keep-Alive

Les 'flatrates' désignent des tarifs de connexion forfaitaires facturés non pas selon le temps de connexion mais selon une période définie. Dans ce cas, il n'est plus nécessaire ni avantageux de procéder à un établissement de connexion au cas par cas. Au contraire : l'arrivée de nouveaux courriers électroniques peut ainsi être signalée directement sur l'ordinateur, le poste de télétravail continuellement relié au réseau d'entreprise et les utilisateurs joignables en permanence grâce aux services de messagerie Internet (ICQ ou autres). Dans ce cas, il est préférable de toujours rester en connexion.

Dans le *ELSA LANCOM 1600 Office*, la procédure Keep relance les connexions dès qu'elles sont interrompues par le correspondant.

Configuration de la procédure Keep-Alive

Cette procédure est configurée dans les listes de noms (DSL et, pour le *ELSA LANCOM DSL/I-1611 Office*, RNIS).

Si le time-out est 0 seconde, la connexion n'est pas terminée activement par le *ELSA LANCOM 1600 Office*. Un time-out de 0 seconde désactive la terminaison automatique de connexions sur lesquelles aucune donnée n'a été transmise pendant une période prolongée. En revanche, les connexions interrompues ne sont, dans ce cas, pas relancées automatiquement.

Si le time-out est 9999 secondes, la connexion sera toujours relancée si elle a été établie à l'origine par ce périphérique et terminée par le correspondant.

8.7

Fonctions de rappel automatique

Grâce à sa prise RNIS, le *ELSA LANCOM DSL/I-1611 Office* supporte également la fonction de rappel.



Parmi les périphériques de la série ELSA LANCOM 1600 Office, seul le ELSA LANCOM DSL/I-1611 Office est équipé d'une prise RNIS. Les explications données ci-dessous se réfèrent donc uniquement à ce périphérique précis.

Outre le rappel via le canal D et le protocole CBCP (**C**allback **C**ontrol **P**rotocol) de Microsoft, il prend aussi en charge 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 ordinateurs avec système d'exploitation Windows peuvent uniquement être rappelés via CBCP.

8.7.1

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, à partir d'un ordinateur fonctionnant sous Windows, d'établir une connexion vers *ELSA LANCOM DSL/I-1611 Office* 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 RNIS.

Dialogue box titled "Liste des noms (RNIS) - Nouvelle entrée".

Fields:

- Nom: MAIN
- Numéro d'appel: (empty)
- Time-out: 20 secondes
- Time-out pour regroupement: 20 secondes
- Nom de la couche: PPPHDLC

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 *ELSA WEBconfig* ou une console.

Numéro de rappel défini par l'appelant

Il faut, pour activer cette option, sélectionner l'option 'Rappeler le correspondant après vérification du nom' (ou, dans *ELSA WEBconfig* ou dans la console, la valeur 'Nom'). La liste de noms ne doit contenir **aucun** numéro d'appel.

Après l'authentification, l'appelant voit apparaître une fenêtre de saisie dans Windows, dans laquelle il doit inscrire le numéro d'appel RNIS de l'ordinateur.

Numéro de rappel défini dans *ELSA LANCOM DSL/I-1611 Office*

Il faut, pour activer cette option, sélectionner l'option 'Rappeler le correspondant après vérification du nom' (ou, dans *ELSA WEBconfig* ou dans la console, la valeur 'Nom'). La liste de noms doit contenir **un** numéro d'appel.

Certaines versions de Windows (en particulier Windows 98) demandent à l'utilisateur de confirmer le rappel automatique du numéro d'appel ('Administrator Specified') inscrit dans le *ELSA LANCOM DSL/I-1611 Office*.

D'autres versions de Windows lui indiquent juste que l'ordinateur attend le rappel du *ELSA LANCOM DSL/I-1611 Office*.

Le rappel d'un ordinateur Windows s'effectue environ 15 secondes après la terminaison de la première connexion. Ce délai est prescrit par Windows et ne peut pas être réduit.

8.7.2

Rappel rapide selon la procédure 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 *ELSA WEBconfig*, un émulateur de terminal ou via Telnet).
- L'appelant sélectionne dans la liste des noms 'Rappeler le correspondant (procédure rapide)' et inscrit le numéro d'appel ('ELSA' pour la configuration via *ELSA WEBconfig*, programme de terminal ou Telnet).

Pour permettre le rappel rapide selon la procédure ELSA, la liste des numéros pour la prise d'appel doit être à jour des deux côtés.



8.7.3

Rappel automatique selon RFC 1570 (extensions LCP PPP)

Le rappel selon 1570 constitue la procédure standard pour le rappel de routeurs d'autres constructeurs. Cette extension de protocole décrit cinq possibilités pour demander un rappel. Toutes les cinq sont acceptées par *ELSA LANCOM DSL/I-1611 Office*. La procédure est la même pour chacune des variantes :

Après authentification du correspondant, *ELSA LANCOM DSL/I-1611 Office* coupe la connexion et rappelle ce dernier quelques secondes plus tard.

Configuration

Pour un rappel selon PPP, sélectionnez dans *ELSA LANconfig* l'option 'Rappeler le correspondant' ou 'Auto' en cas de configuration via *ELSA WEBconfig*, programme de terminal ou Telnet.

Pour permettre le rappel selon PPP, la liste des numéros pour la prise d'appel doit être à jour dans le ELSA LANCOM DSL/I-1611 Office.



8.7.4

Vue d'ensemble de la configuration de la fonction de rappel

Pour le rappel, les options suivantes sont proposées dans la liste des noms RNIS de *ELSA WEBconfig* et du programme de terminal/Telnet :

Avec l'option...	...vous réglez le rappel comme suit :
'inactif'	Il n'y a pas de rappel.
'Auto' (pas sous Windows, cf. ci-dessous)	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.
'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 se connectant sur le périphérique). Des unités de taxation sont facturées.
'ELSA'	Un rappel rapide est réalisé si le correspondant a été trouvé dans la liste des numéros : <i>ELSA LANCOM 1600 Office</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 résélectionnée 2 secondes plus tard (durée env. 8 secondes). Ce mode est uniquement disponible au niveau des ports DSS1.
'Looser'	Utilisez l'option 'Looser' lorsque le correspondant attend un rappel. Cette option 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'option 'Nom' offre une sécurité maximum lorsqu'un numéro figure à la fois dans la liste des numéros et dans la liste PPP. L'option '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'.*

8.8

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 comprimer vos données et/ou utiliser plusieurs canaux B pour la transmission (Regroupement des canaux).



Parmi les périphériques de la série ELSA LANCOM 1600 Office, seul le ELSA LANCOM DSL/I-1611 Office est équipé d'une prise RNIS. Les explications données ci-dessous se réfèrent donc uniquement à ce périphérique précis.

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 (**M**ultilink **P**PP). 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.

Il existe deux méthodes pour le regroupement de canaux

- Regroupement statique des canaux

Lors de l'établissement d'une connexion avec regroupement statique des canaux, le *ELSA LANCOM DSL/I-1611 Office* essaie, une fois le premier canal B connecté, d'établir une connexion avec le second canal B. Si cela ne réussit pas, du fait par ex. que ce canal est déjà occupé par un autre périphérique ou par une autre connexion au sein du routeur *ELSA LANCOM DSL/I-1611 Office*, le routeur réessaye automatiquement et périodiquement jusqu'à ce que le second canal B soit lui aussi disponible.

- Regroupement dynamique des canaux

Dans le cas d'une connexion avec regroupement dynamique des canaux, le *ELSA LANCOM DSL/I-1611 Office* établit dans un premier temps une connexion uniquement avec un seul canal B et commence aussitôt le transfert des données. Si au cours du transfert il détecte que le débit dépasse pendant un certain laps de temps un seuil déterminé, il essaie d'utiliser en plus le second canal.

Une fois le second canal connecté et le débit redescendu en deçà du seuil, le *ELSA LANCOM DSL/I-1611 Office* attend la fin du timeout B2 Timeout réglé avant de libérer à nouveau le second canal. Ce faisant, les

unités de facturation entamées sont consommées jusqu'à la fin lorsque les informations de facturation sont transmises pendant le transfert. Le *ELSA LANCOM DSL/I-1611 Office* utilise donc le second canal B uniquement et tant qu'il en a vraiment besoin.

Procédure de configuration pour le regroupement de canaux

Le regroupement des canaux se configure en trois temps :

- ① Dans la liste des couches, sélectionner pour le correspondant une couche communication pour laquelle le regroupement est activé dans les options couche 2. Faites votre choix parmi les options couche 2 suivantes :
 - **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** fait intervenir deux canaux B pour une connexion.
 - **Compr.+regroupement** utilise les deux (compression et regroupement des canaux) et permet donc de disposer du plus grand débit de transmission possible.
- ② Procédez à une nouvelle inscription dans la liste des noms RNIS en tenant compte des valeurs de time-out 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 précise si le regroupement est de type statique ou de type dynamique (voir plus haut). Quand le timeout est réglé à '0' ou '9999' le regroupement est statique. Les valeurs intermédiaires rendent possible un regroupement dynamique de canaux. Le timeout B2 définit combien de temps le taux de transmission peut se trouver en dessous du seuil limite pour le regroupement dynamique de canaux avant que le second canal B ne soit automatiquement terminé.
- ③ 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

ELSA WEBconfig	Configuration expert ► Setup ► Module WAN ► Liste des interfaces routeur
Terminal/Telnet	cd setup/WAN-module set router-interface-list [...]

- Connexion en Y **active** : le routeur supprime le regroupement des canaux afin d'établir la seconde connexion avec l'autre correspondant. Une fois le second 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 telle qu'elle est, l'autre correspondant doit attendre.



Attention : en cas de regroupement de canaux, l'utilisateur doit payer le prix de deux communications et aucune autre connexion n'est possible par l'intermédiaire de l'interface ELSA LANCAP1 ! Recourez par conséquent au regroupement de canaux uniquement lorsqu'il est réellement possible de tirer profit du débit de transfert deux fois plus important.

9

Caractéristiques techniques

9.1

Puissance et spécifications



	<i>ELSA LANCOM 1600 Office</i>
Modes de fonctionnement	<p>tous les périphériques : Routeur IP, serveur DNS, serveur DHCP ; possibilité d'utilisation simultanée de tous les modes de fonctionnement</p> <p>uniquement <i>ELSA LANCOM DSL/I-1611 Office</i>: Routeur IPX, serveur CAPI, Least Cost Router pour liaisons routeur et CAPI</p>
Raccordement WAN 10Base-T	Ethernet IEEE 802.3, 10Base-T (RJ45) avec protocole de communication PPP-over-Ethernet (PPPoE) ou PPTP
Interface RNIS (uniquement <i>ELSA LANCOM DSL/I-1611 Office</i>)	<p>connexion : Bus RNIS-S₀, configuration point à point et point à multipoint, I.430 ; canal D : 1TR6, Euro-RNIS (DSS1), auto-sense, en option : prise en charge liaisons fixes groupe 0 (D64S, D64S2, D64SY) ; canal B : PPP (asynch./synch.), MLPPP, X.75, HDLC, V.110, CAPI 2.0 par <i>ELSA LANCOM CAPI</i>, compression de données Stac</p>
Connexion LAN	Ethernet IEEE 802.3, 10/100Base-TX (RJ45, nœud/concentrateur, commutateur), auto-sense, Full-Duplex
Protocoles de réseau	<p>tous les périphériques : Routeur IP : ARP, Proxy ARP, serveur DHCP, IP, ICMP, UDP, TCP, RIP-1, RIP-2, Proxy DNS</p> <p>uniquement <i>ELSA LANCOM DSL/I-1611 Office</i>: Proxy NetBIOS/IP Routeur IPX : IPX, SPX, RIP, SAP, Novell NetBIOS, mode Novell-Burst</p>
Fonctions Security	<p>tous les périphériques : PAP, CHAP et MS-CHAP pour authentification sous PPP ; possibilités de filtrage en mode routeur, protection de la configuration par listes d'accès et mot de passe, enregistrement des dernières informations de connexion, masquerading IP</p> <p>uniquement <i>ELSA LANCOM DSL/I-1611 Office</i>: Analyse du numéro d'appel du correspondant (CLIP) ; rappel automatique via RNIS ;</p>
Possibilités de filtrage (pare-feu)	<p>tous les périphériques : Routeur IP : filtres source et cible pour réseaux, protocoles et ports ; filtres d'adresses MAC</p> <p>uniquement <i>ELSA LANCOM DSL/I-1611 Office</i> – Routeur IPX : RIP, SAP, chien de garde IPX et SPX, Sockets, routes, Propagated Pakkets</p>
IP masquerading	conversion d'adresses IP et de port via une adresse IP externe ; affectation statique/dynamique de l'adresse IP via PPP ; masquage de TCP, UDP, ICMP et FTP ; routage par DNS ; masquage inverse pour services issus de l'Intranet comme par ex. le serveur Web (DMZ)
Spoofing (seulement <i>ELSA LANCOM DSL/I-1611 Office</i>)	routeur IPX : RIP- et SAP-Packets ; Chiens de garde IPX et SPX, Novell NetBIOS, Keep-alive-Packets

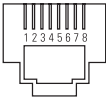
	ELSA LANCOM 1600 Office
Serveur CAPI (seulement <i>ELSA LANCOM DSL/I-1611 Office</i>)	CAPI 2.0 virtuelle pour systèmes d'exploitation Windows, gestionnaire NDIS-WAN, Fax-classe 1
Gestion des lignes, optimisation de la transmission	tous les périphériques : Keep-Alive sur connexions WAN, Policy Based Routing, SYN/ACK-Speedup uniquement <i>ELSA LANCOM DSL/I-1611 Office</i> – Rappel automatique via RNIS avec ou sans établissement de la connexion ; Line-on-Demand (regroupement dynamique de canaux), mode Short-Hold, sélection Round-Robin, Fast Call Back, sauvegarde de numérotation (Dial-Backup) pour lignes spécialisées
Contrôle des coûts de communication :	temps maximal en ligne ou unités de taxation par période
Management	tous les périphériques : Via LAN ou V.24, logiciel de management <i>ELSA LANconfig</i> et <i>ELSA LANmonitor</i> pour Windows, configuration possible par SNMP v.1, TFTP, Telnet ou terminal uniquement <i>ELSA LANCOM DSL/I-1611 Office</i> – Via ISDN (télémaintenance)
Sécurité d'exploitation	chiens de garde matériel, autotests permanents, concept <i>ELSA Firm-Safe</i> pour mise à jour à distance du logiciel
Statistiques	compteurs séparés LAN / WAN, paquets, erreurs, connexions et temps en ligne ; ouverture de session de la gestion des connexions et temps en ligne avec <i>ELSA LANmonitor</i> et SYSLOG ; informations sur les connexions, temps en ligne, volume par IP avec <i>ELSA LANmonitor</i> ; tracé de protocoles pour diagnostic
Affichages/ Manipulation	DEL : marche/arrêt, statut WAN / LAN, Sécurité / VPN ; touche de réinitialisation, commutateur nœud / concentrateur
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 dimen- sions	boîtier métallique robuste, raccordements sur l'arrière ; dimensions 230 x 38 x 228 mm (l x h x p)
Contenu du coffret :	bloc d'alimentation, câble pour interface Outband, câble de raccordement RNIS (uniquement <i>ELSA LANCOM DSL/I-1611 Office</i>), deux câbles à paires torsadées LAN, documentation détaillée et CD-ROM <i>ELSA LANCOM Office</i> ; <i>ELSA LANconfig</i> , <i>ELSA LANmonitor</i> , <i>ELSA LANCAPI</i> , ELSA CAPI Faxmodem, logiciel de bureautique ELSA-RVS-COM, LapLink Pro
Homologations	pour l'Allemagne, la Suisse et tous les pays de l'UE
S.A.V. et garantie	garantie de 6 ans
Support technique	par hotline et Internet

9.2 Brochage

9.2.1 Interfaces Ethernet 10/100Base-T (LAN) et 10Base-T (WAN)

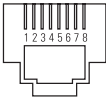


Broche RJ45 8 pôles selon ISO 8877, EN 60603-7

Raccordement enfichable	Broche RJ45	Ligne
	1	T+
	2	T-
	3	R+
	4	—
	5	—
	6	R-
	7	—
	8	—

9.2.2 Interface RNIS S₀

Broche RJ45 8 pôles selon ISO 8877, EN 60603-7

Raccordement enfichable	Broche RJ45	Ligne	IAE
	1	—	—
	2	—	—
	3	T+	2a
	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	—	—
	8	—	—

9.2.3 Interface de configuration (Outband)

Broche Mini-Din 8 pôles



Raccordement enfichable	Mini-DIN 8 pôles	Ligne
	1	CTS
	2	RTS
	3	RxD
	4	RI
	5	TxD
	6	DSR
	7	DCD
	8	DTR
	U	GND

10 Appendice

10.1 Conditions générales de garantie



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

1 Objet de la garantie

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

2 Durée de la garantie

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

3 Modalités

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

4 Application de la garantie

La garantie est exclue dans les cas suivants :

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

5 Erreurs de manipulation

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

6 Conditions complémentaires

- a) En dehors des conditions mentionnées, l'acquéreur n'aura aucun recours envers ELSA AG.
- b) Cette garantie n'établit aucun droit supplémentaire, en particulier le droit à réhabilitation ou la prétention à diminution. Toute réclamation de dommages-intérêts, quelle qu'en soit la raison, est exclue. Cette garantie ne limite pas les droits de l'acquéreur conformément aux lois sur la responsabilité produit, par exemple dans les cas de dommages corporels ou d'endommagement des objets personnels ou dans les cas de préméditation ou de négligence grossière, dans lesquels ELSA AG engage impérativement sa responsabilité.
- c) En particulier, le remboursement d'un manque à gagner ou de dommages directs ou indirects sont exclus.
- d) Nous n'engageons aucune responsabilité pour la perte de données ou la récupération de ces données en cas de faute légère ou moyenne.
- e) Dans les cas où nous provoquons la destruction de données avec préméditation ou par négligence grossière, nous engageons notre responsabilité pour le rétablissement typique tel qu'il serait à réaliser en cas de création régulière de copies de sauvegarde selon les mesures de sécurité adéquates.
- f) La garantie s'applique uniquement au premier acheteur et ne peut être transférée à un tiers.
- g) Pour toute contestation le tribunal d'Aix-la-Chapelle (Aachen) est seul compétent, si l'acquéreur a la qualité de commerçant et en 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.

10.2

Déclaration de conformité Union Européenne (CE)

Vous trouverez les déclarations de conformité CE pour l'*ELSA LANCOM 1600 Office* dans la zone de téléchargement de la page d'accueil de ELSA (www.elsa.com/download).

11 Index

- **Numerique**
 - 10/100Base-TX24
- **A**
 - Accès à distance11, 47, 128
 - Accès à Internet 128
 - Accès réseau à distance 47, 75
 - Adresse d'arrivée83
 - Adresse de départ83
 - Adresse Internet66
 - Adresse Intranet66
 - Adresse IP53, 65, 127
 - Adresse MAC69
 - Affichage de l'état15
 - AOCD97
 - Authentification 17, 133
 - Autosensing24
- **B**
 - BACP18
 - Banque de données3
 - Bloc d'alimentation 24, 25
 - Bouton de réinitialisation24
 - Brochage141
 - interface de configuration142
 - interface Ethernet141
 - interface LAN141
 - interface RNIS S₀141
 - interface WAN141
 - Outband142
 - Budget en fonction du temps95, 97
 - Bureautique102
- **C**
 - Câble de connexion à un réseau étendu
25
 - Câble de connexion à un réseau local 25
 - Câble RNIS12
 - Calling Line Identifier Protocol77
 - Canal B
 - état de la liaison14
 - Protocole76
 - Canal D76
 - CAPI Faxmodem108
 - Caractères joker94
 - Caractéristiques techniques139
 - CBCP132
 - Challenge Handshake
Authentication Protocol75
 - CHAP75
 - Charger le logiciel57
 - Client PPP41, 48
 - CLIP17, 76, 77
 - Common ISDN Application Programming
Interface101
 - Commutateur nœud/concentrateur24
 - Compression18
 - Compression de données LZS137
 - Compression de données Stac18
 - Conditions de garantie143
 - Conf130
 - Configuration15
 - procédure41
 - SNMP47
 - Configuration à distance17, 41
 - Configuration de l'accès à Internet37
 - Configuration Inband41
 - Configuration Outband41
 - Configuration point à point13
 - Configuration point-à-multipoint13
 - Configuration WINS86
 - connecteur de standard13
 - Connecteur multiple13
 - Connexion à distance48

Connexion à un réseau étendu WAN	13
Connexion à un réseau local	13
Connexion DSL	24
Connexion en Y	137
Connexion modem-câble	24
Connexion PPP	49
Contenu de l'emballage	25
Contrôle d'identification	74
Contrôle des accès	64
Contrôle des coûts de communication	16,
	102
Correspondant	129
Coupe-feu	65, 102
Couplage LAN-LAN	11
Courrier électronique	10

D

Débit de transfert	136
Dépannage	51
Déterminer soi-même les paramètres IP	35
DHCP	55, 81
DHCP pour résolution WINS	86
Diffusion IP	118
Diffusion restreinte IP	118
Disponibilité	106
Distance d'une route	113
D-Kanal	55
DNS	55, 87
Domain Name Service	87
Domaine	93, 94
Domaines	87
Durée de communication	14
Durée de validité	82, 85
Dynamic Host Configuration Protocol	81

E

ELSA CAPI Faxmodem	17
ELSA Dynamic VPN	17
ELSA FirmSafe	16, 57

ELSA LANCAPI	14
ELSA LANCAPI	48
ELSA LANconfig	43, 48, 58
ELSA LANmonitor	51
Affichage des réglages disponibles	52
Contrôle de la connexion Internet	52
informations système	52
ELSA WEBconfig	58
ELSA-RVS-COM	12
ELSA-ZOC	12
Emulateur de terminal	15, 58
Envoi de télécopies	108
Essais d'ouverture de séance	63
Etablissement d'une liaison	13
Ethernet	
10/100Base-T	13
Fast-Ethernet	13
EuroFileTransfer	18

F

Fail	130
FAQ	3
Fast Call Back	77
Fast-Ethernet	13
10/100Base-T	13
Fax Class 1	108
Faxmodem	17
Filtres	11, 65
Filtres adresses MAC	13
Filtres pare-feu	11
Flatrate	131
Foire Aux Questions	3
Fonction de rappel	17
Fonctions de sécurité	11
Force brute	13, 63
Fournisseur d'accès Internet	10
Frais de téléphone élevés	95

G

Gestion d'adresses	81
--------------------	----

Gestion d'adresses IP	81
Gestion des communications	97
Gestion des liaisons	13
Gestion des lignes	11
Gestion des priorités	106
Gestion des taxes téléphoniques	94

H

Heure du RNIS	18
Hôte	87

I

Identification de l'appelant	74
Identification du numéro de l'appelant 17	
Inband	41
avec Telnet	46
Information de facturation	137
Installation	12
Interconnexion de réseaux locaux	11
Interface ATM	13
Interface CAPI	101
Interface de configuration	25
Interface de configuration V.24	24
Interface de configurations	41
Interface S ₀	13
Interface sériele	41
Interfaces	24
Internet	10, 65
Interrogation de l'heure	18
IP masquerading	
Masquage simple	68
protocoles pris en charge	69

K

Keep-Alive	131
KnowledgeBase	3

L

LANCAPI	17
LCR	18, 97

le regroupement statique des canaux 18	
Least Cost Routing	18
Least-cost routing	97
Liaison commutée	11
Lignes spécialisées	11
Limitation des communications en	
fonction de la durée	97
Limitation des communications RNIS 96	
Limitation des taxes téléphoniques ...	94
Limite supplémentaire	95
Limiter les coûts	95
Liste de contrôle sécurité	77
Liste des filtres	73
Liste PPP	75
Listes des interfaces routeur	137
Login	58

M

Masquage inverse	68
Masquerading IP	11, 13, 55, 65
Mécanisme d'acheminement DNS	88
Media Access Control	69
Mémoire flash	15, 57
Microprogramme	16
Microprogrammes	3
Minutes en ligne	95
Mise à jour des microprogrammes	15
MLPPP	18, 136
Mode automatique	82
Mode DHCP automatique	82
Modem DSL	10, 12
Modem-câble	10, 12
Mot de passe	50, 52, 74, 75, 129
MS-CHAP	125, 126
Multilink PPP	125, 136

N

NAT	65
NetBIOS	55, 88
Nom d'utilisateur	50, 75, 129

Nom de périphérique	129
Nom du routeur	113
Noms d'ordinateur	87
Noms de réseau	87

● O

Option ligne permanente	19
Outband	41

● P

Paket-Dump	55
PAP	75
Paramètres de sécurité	63
Pare-feu	13, 65
pas d'informations de taxation	97
Passerelle	65, 81, 84
passwd	63
Password Authentication Protocol	75
PAT	65
Période	95
Période déterminée	95
Phase d'échange PPP	50
Pilote de télécopie	108
Pilotes	3
Point-to-Point Tunneling Protocol	130
Policy Based Routing	119, 140
Pool d'adresses	83
Port	68, 106
Port IP	106
Power	21
PPP	17, 53, 75, 136
Attribution des adresses IP	127
Extensions LCP	134
Fonctions de rappel automatique	132
Vérification de la ligne avec LCP	127
PPTP	130
Procédé de compression de données	
LZS	137
Procédés de sécurisation	75
Programmes de télécopie standard	108

Protection d'accès	74
Protection de l'accès	
Par nom	74
Par nom ou numéro	74
Par numéro	74
Protection de la configuration	61
Protection par mot de passe	17, 61
Protection pour la configuration	61
Protection pour le réseau local	65
Protocole ELSA	76
Proxy NetBIOS	17

● R

Raccordement 10Base-T	24
Raccordement RNIS/S ₀	24
Raccordements	24
Rappel	76
Fast callback	77
Rappel automatique	11, 74
Recherches en ligne	10
Regroupement des canaux	18, 136
Dynamique	136
Statique	136
regroupement des canaux	18
dynamique	18
statique	18
Regroupement dynamique des canaux	136
regroupement dynamique des canaux	18
Regroupement statique des canaux	136
Rép	130
Répétitions	130
Répondeur téléphonique	12
Réponse sur écho LCP	127
Requête d'écho LCP	127
Réseau 100 Mbits	24
Réseau Peer-to-Peer	16
Réseau Windows	86
Réseaux NetBIOS	88
Réseaux privés virtuels	11

Réseaux TCP/IP	87
Réseaux Windows	16
RIP	55
RNIS	
canal B	76
Canal D	13, 77
Routeage dynamique	111
Routeage IP	13
Passerelle standard	114
Routeur par défaut	114
Routeage par DNS	89
Routeage statique	111
Routes d'exclusion	113

S

Sécurité	61, 65, 130
Serveur de messagerie électronique ..	92
Serveur DHCP	81, 87
Serveur DNS	14, 81, 84, 87
information disponible	88
liste-filtre	93
mécanisme filtrant	88
Serveur NBNS	81, 84, 86
Service	87
Single User Access	65
SNMP	47
Stac	137
Statistiques	16
Support	3
Surveillance	51
SYN/ACK-Speedup	119, 140

T

Table des objets	72
Table des règles	72
Tableau de routage IP	111
Tableau des noms de station	91
Tableau DNS	92, 93
Taux de transfert	14, 53
TCP/IP	111

Téléchargement	16, 57
Téléchargement de microprogramme	
Avec <i>ELSA LANconfig</i>	58
Avec <i>ELSA WEBconfig</i>	59
Téléchargement du microprogramme	
avec émulateur de terminal	59
avec TFTP	59
Télécopie	12, 18, 108
Telnet	15, 48
Témoins lumineux	15, 21
Temps	130
Term	130
TFTP	46
Timeout	136, 137
Tracé	
Code et paramètres	54
Exemples	56
Lancement	54
Tracés	
Editions	54
Transfert de fichiers	10
Transfert des données	136
Travail à domicile	11
Type-of-Service	119

U

Unités de facturation	137
Unités de taxation	96, 97
Unités pour la connexion RNIS	95

V

Verrouillage	64
Verrouillage d'accès	63
Verrouiller domaines	94
Virtual Private Network	14
VPN	11, 14

Z

Zone d'adresses IP	69
--------------------------	----

