Cours, exercices corrigés et QCM

1er cycle/Licence • DUT • BTS • Écoles d'ingénieurs

INTERNET : SERVICES ET RÉSEAUX

Stéphane Lohier
Dominique Présent

DUNOD

INTERNET : SERVICES ET RÉSEAUX

INTERNET : SERVICES ET RÉSEAUX

Cours, exercices corrigés et QCM

Stéphane Lohier
Professeur à l'IUT de Marne-la-Vallée

Dominique Présent
Directeur de l'IUT de Marne-la-Vallée

DUNOD

Illustration de couverture : Digital Vision

ISBN 2 10 006492 4

Table des matières

Chapitre **1**

Internet : un réseau d'opérateurs

1.1 INTERNET : LA PARTIE INVISIBLE

Nous connaissons, utilisons, « surfons » régulièrement sur Internet. Nous maîtrisons plus ou moins le navigateur, connaissons les adresses de nos sites préférés. Nous savons chercher, trouver le « meilleur » abonnement au prestataire de service. Ce qui est moins connu, moins visible, ce sont les métiers et techniques qui permettent à nos messages d'arriver à leur destinataire, et nous permettent d'interroger et naviguer sur les serveurs web.

1.2 OPÉRATEURS INTERNET : TROIS MÉTIERS

Pour que des données transitent d'un ordinateur « source » jusqu'à un ordinateur « destinataire », il faut un réseau de câbles, fibres optiques ou faisceaux hertziens, des équipements pour diriger les données jusqu'à leur destinataire et connecter les ordinateurs et matériels traversés. Qui investit dans ces matériels et équipements, qui les entretient et qui finance tout ce réseau ?

Tout le fonctionnement d'Internet repose sur trois types d'opérateurs (figure 1.1) : le prestataire de service, le fournisseur d'accès, l'opérateur de transport. Mais tout repose sur un réseau de câbles utilisés pour Internet ou d'autres types de données installés et gérés par des opérateurs de câblage.

Au plus proche de l'internaute se trouve le **prestataire de service** (*Internet Services Provider*). Il propose des services de connexions aux internautes. En échange d'un abonnement, le client dispose au minimum d'une connexion au réseau Internet et d'une adresse électronique (*dupont@wanadoo.fr*) correspondant à une boîte aux

lettres électronique. Des services complémentaires sont souvent proposés avec ou en plus de l'abonnement tels qu'hébergement de pages web, interface minitel, WAP, informations thématiques personnalisées et actualisées.

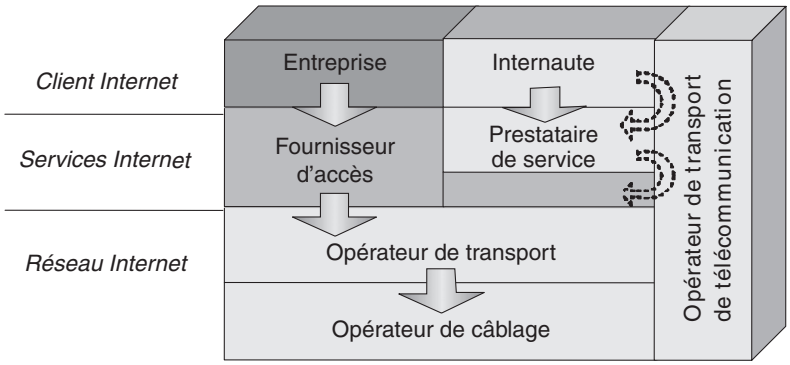

Figure 1.1 Les opérateurs Internet.

Si d'un côté, le prestataire de service propose une connexion à ses clients, il doit, de l'autre, être lui-même connecté à un réseau Internet (figure 1.2). Pour cela, il loue une connexion Internet à un Fournisseur d'Accès Internet (FAI est la traduction de *Internet Access Provider*) et achète un nom de domaine auprès d'un organisme habilité par une autorité d'administration Internet. Trois organismes regroupés au sein de l'ICANN (*www.icann.org*) couvrent l'ensemble des régions : l'APNIC (*www.apnic.net*) pour l'Asie et le Pacifique, l'ARIN (*www.arin.net*) pour l'Amérique nord et sud et le sud de l'Afrique et le RIPE (*www.ripe.net*) pour les réseaux européens, y compris le nord de l'Afrique, le bassin méditerranéen et la Russie. L'AFNIC (Association Française pour le Nommage Internet en Coopération – *www.afnic.fr*) est chargée d'attribuer les noms de domaine en « fr ».

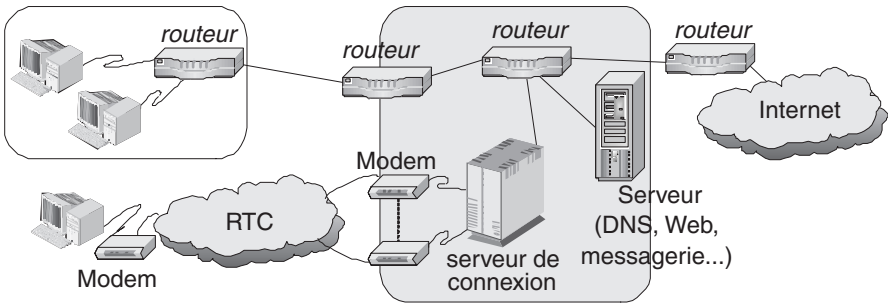

Figure 1.2 Le prestataire de service.

L'internaute ou l'entreprise utilise généralement un opérateur de télécommunications pour raccorder ses équipements à ceux du prestataire de services. Il peut utiliser

le Réseau Téléphonique Commuté (RTC) à l'aide d'un modem standard ou haut débit ADSL, une liaison par câble ou hertzienne. Ces types de raccordement sont détaillés au chapitre 2, *Se connecter à Internet*.

Le **Fournisseur d'Accès Internet** (FAI) dispose des équipements permettant de connecter les équipements du prestataire de service. C'est un point d'accès à un réseau Internet. Certains fournisseurs d'accès connectent directement les équipements des entreprises, sans que celles-ci ne passent par un prestataire de service. S'ils fournissent ainsi l'accès à Internet, ils ne proposent pas à leurs clients les autres services (messagerie, hébergement de pages web…). Le fournisseur d'accès choisit un opérateur de transport pour prendre en charge les données de ses clients.

L'opérateur de transport Internet est chargé d'acheminer les données prises en charge à l'un de ses points d'accès vers à un autre point de son réseau. Si le destinataire n'est pas l'un de ses clients, les données seront dirigées vers le réseau d'un autre opérateur de transport, jusqu'à atteindre le réseau de transport dont le destinataire est client.

La plupart des opérateurs actuels assurent deux voir trois métiers décrits. On trouve des opérateurs de dimension européenne tels que Eunet ou Oléane, nationale comme Renater, mais aussi régionale tel que ICX Networks intervenant dans le Bassin méditerranéen. Les réseaux de tous ces opérateurs de transport sont interconnectés entre eux.

Tableau 1.1 Exemples d'opérateurs Internet

Prestataire	Fournisseur d'accès	Opérateur de transport
AOL	AOL	
Wanadoo	Wanadoo	
	Oléane	Oléane
	Eunet	Eunet
	Renater	Renater
	Netissimo	
	ICX Network	ICX Networks

1.3 LES OPÉRATEURS DE CÂBLAGE

Les réseaux de transport sont soit des réseaux câblés, le plus souvent en fibre optique, ou des réseaux hertziens utilisant des satellites comme relais.

Les réseaux câblés sont de type maillé, c'est-à-dire qu'ils proposent plusieurs chemins pour aller d'un point à un autre (figure 1.3). Ils sont donc constitués d'un ensemble de liaisons point à point. Chacune de ces liaisons présente un débit maximum de transmission, appelé également capacité du support ou bande passante.

Ces liaisons point à point sont installées par un opérateur de câblage ou câblo-opérateur. Elles peuvent être gérées et maintenues en état soit par l'opérateur de transport, soit par l'opérateur de câblage.

Un segment ou équipement du réseau d'un opérateur de transport peut s'avérer insuffisant pour assurer la transmission des données (bande passante des liaisons ou du routeur insuffisante). L'opérateur peut augmenter la capacité de son équipement ou du segment, mettre en place des liaisons permettant de proposer un autre chemin au trafic excédent. Il peut également louer à un opérateur de câblage ou de transport tiers une liaison pour ce trafic excédentaire comme le montre la figure 1.3.

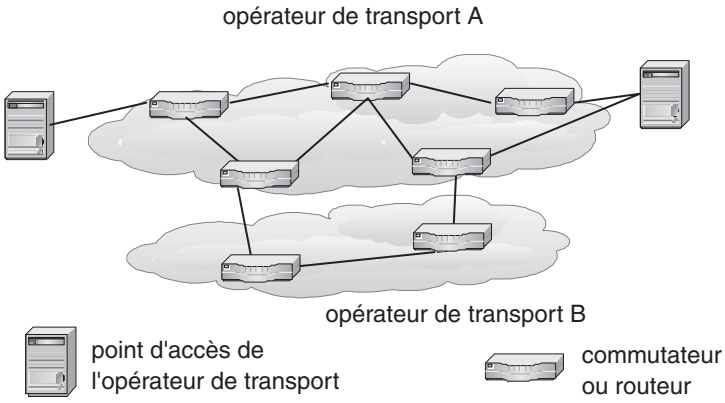

Figure 1.3 Topologie d'un réseau d'opérateur.

Comme pour les opérateurs de transport, les câblo-opérateurs peuvent être de dimension européenne, nationale ou régionale. Le tableau 1.2 répertorie quelques opérateurs de câblage opérant sur le territoire français, ainsi que les fournisseurs d'accès qui leur sont associés.

Tableau 1.2 Exemples d'opérateurs de câblage.

Câblo-opérateur	Région	Fournisseur d'accès
France Telecom	Europe	Wanadoo
British Telecom	Europe	
Cable & Wireless	Grande Bretagne	
Sprint	USA	Sprint
AT&T	USA	
Mediaréseaux	est de Paris	UPC
NTL	Paris - Toulon	Noos
est vidéocommunication	Strasbourg	

1.4 TOPOLOGIE DES RÉSEAUX DE TRANSPORT INTERNET

La France est donc couverte par plusieurs réseaux de transport de tailles très différentes. La figure 1.4 montre le réseau de l'opérateur ICX Network.

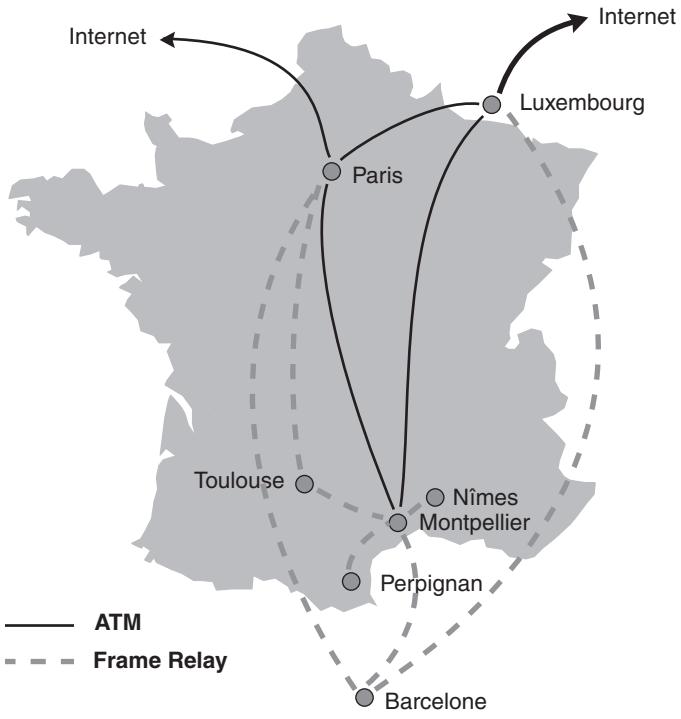

Figure 1.4 Topologie du réseau de l'opérateur ICX Network (*www.icx.fr*).

Son réseau interconnecte quatre villes du Languedoc-Roussillon, ainsi que la ville de Barcelone, où se trouvent des points d'accès Internet pour les abonnés. Le réseau est relié directement à Paris et au Luxembourg pour accéder au réseau Ebone (figure 1.6) interconnectant les réseaux de tous les opérateurs de transport.

Le réseau national Oléane de l'opérateur GlobalOne est représentatif d'une topologie en pétale (figure 1.5). L'architecture est centrée sur Paris où se trouve l'interconnexion avec les réseaux des autres opérateurs et avec le réseau d'interconnexion Ebone. De là partent des segments radiaux, par exemple vers Toulouse, puis un segment circulaire, ici Montpellier et Marseille, et un retour par un segment radial, Lyon Paris.

Les prestataires de service et les entreprises doivent prévoir une liaison jusqu'au point d'accès de l'opérateur de transport. Si cela représente un faible coût en région parisienne, cela peut être différent en province. C'est un point à prendre en compte dans le choix de l'implantation d'une entreprise. Une ligne louée à 2 Mb/s coûtait au

1er juillet 2003 environ 2 000 €/mois pour 50 km (tarif Transfix – *www.francetelecom.com/fr/entreprises/*).

Les temps de transmission sont le plus souvent inférieurs à 150 ms. Depuis l'installation des fibres optiques, les capacités des liaisons sont utilisées à environ 10 %.

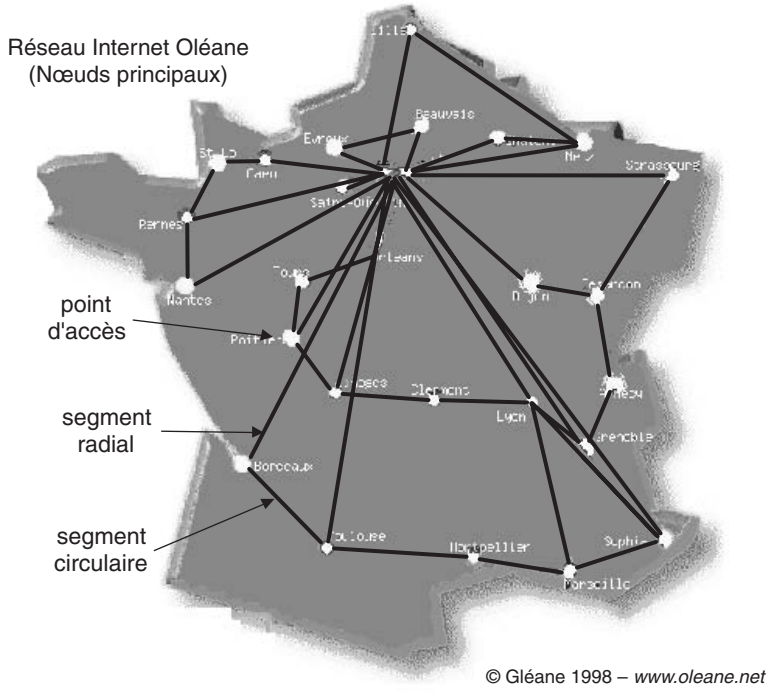

Figure 1.5 Topologie du réseau de l'opérateur Oléane (*www.oleane.net* ou *www.transpac.fr*).

1.5 LE RÉSEAU D'INTERCONNEXION EUROPÉEN EBONE

Les réseaux des opérateurs de transport doivent être interconnectés pour permettre à leurs clients de pouvoir joindre tout destinataire abonné à un autre opérateur. C'est le rôle du réseau européen Ebone (figure 1.6).

Il est constitué de plaques reliées par des liaisons à haut débit (155 Mb/s à 2,5 Gb/s). l'interconnexion avec le continent américain est assurée par un ensemble de liens (câbles transatlantiques) totalisant plusieurs gigabits par seconde, au départ des villes d'Amsterdam et de Rotterdam.

Pour bénéficier de ce réseau, les opérateurs de transport doivent se raccorder au niveau des points de présence (figure 1.6, PoP). Cela explique la topologie en pétale adoptée par la majorité des opérateurs de transport. Le réseau Ebone est ouvert à tout type de trafic, qu'il soit gouvernemental (administration, recherche, enseignement…) industriel ou commercial.

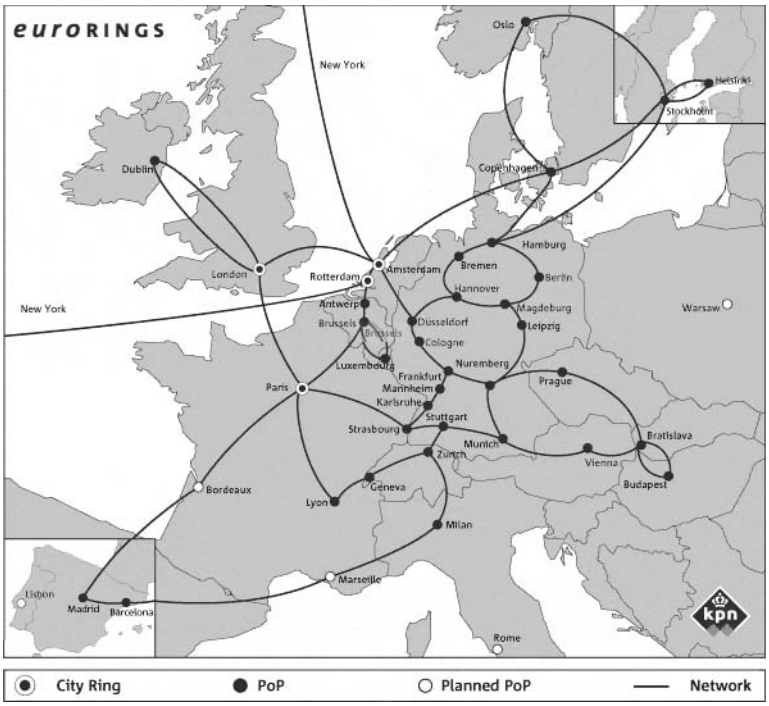

Figure 1.6 Réseau d'interconnexion Ebone (*www.eurorings.kpn.com*).

Ce réseau, a été racheté en mars 2002 par KPNQwest (*www.eurorings.kpn.com*) et intégré au réseau EuroRing qui interconnecte 50 villes européennes.

1.6 LES OPÉRATEURS DE TRANSPORT INTERNATIONAUX

Beaucoup d'opérateurs européens sont des filiales d'opérateurs de transport internationaux. L'exemple du réseau mondial (figure 1.7) de l'opérateur mci (*www.global.mci.com/fr/)* montre la place centrale occupée par le continent nord américain dans la topologie des réseaux mondiaux. Cette architecture amène deux remarques :

– une perturbation du trafic sur le réseau Internet américain conduira à des perturbations sur les trafics intercontinentaux entre l'Europe, le continent asiatique et l'Australie ;
– toutes les données entre l'Europe et l'Asie transitent par le continent américain, induisant la possibilité d'une « surveillance ».

L'utilisation de liaisons satellites est une réponse à cette situation.

Aujourd'hui, avec l'utilisation généralisée de la fibre optique, les débits des liaisons transatlantiques sont suffisants pour faire face au trafic actuel. Les difficultés de connexion à des sites américains après 15 heures sont devenues assez rares.

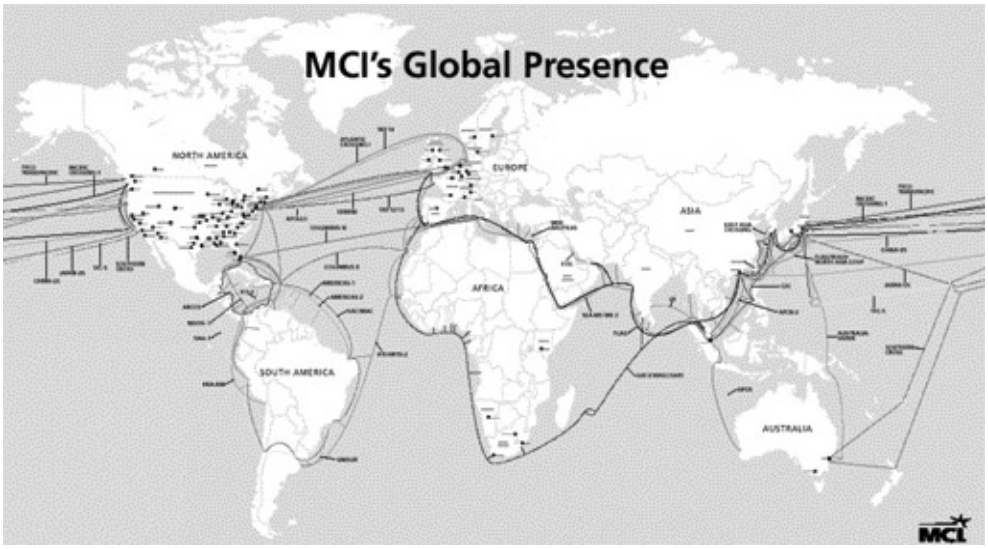

Figure 1.7 Réseau international de l'opérateur WorldCom (*www.global.mci.com/fr/*).

1.7 TRAFIC ET ROUTAGE

La topologie des réseaux des opérateurs Internet est telle que :

– les données traversent le plus souvent plusieurs réseaux d'opérateurs (figure 1.8) ;
– si l'on peut choisir l'opérateur de transport auquel sont raccordés nos équipements et maîtriser ainsi localement la qualité de la transmission, il n'est pas possible de garantir cette qualité à travers les réseaux traversés ;

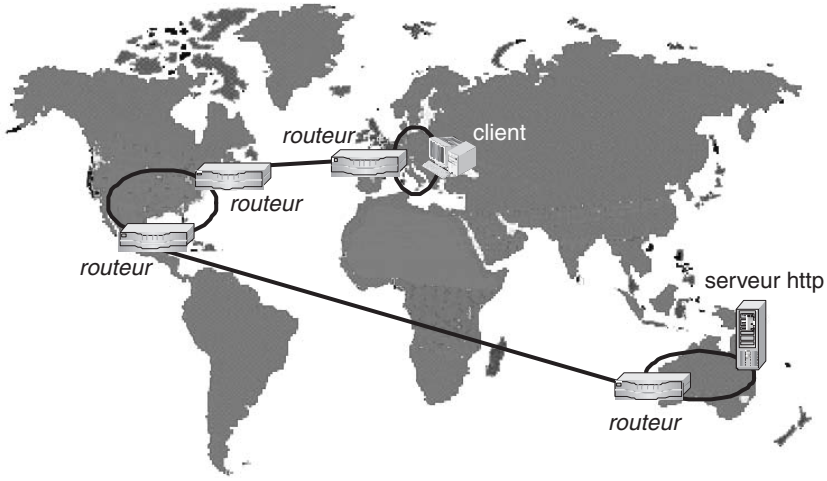

Figure 1.8 Les données traversent plusieurs réseaux d'opérateurs.

– pour assurer la transmission des données nécessaires à certaines applications telles la vidéo, l'ensemble des opérateurs devra dans les années à venir assurer une qualité de service (QoS) sur leur réseau ;
– le routage (choix d'un chemin entre ordinateurs source et destination à partir des adresses) emprunte rarement le plus court chemin, rallongeant le délai de transmission. Les temps de traversée d'un réseau d'opérateur sont de quelques centaines de millisecondes ;
– si les capacités actuelles des liaisons engendrent peu d'encombrement des réseaux (environ 10 % de la capacité est utilisée), les opérateurs ne peuvent garantir les délais de transmission. Les graphiques de la figure 1.9 montrent une anomalie apparaissant dans les temps de réponse des réseaux d'opérateurs, simultanément en Europe, aux États-Unis et sur le continent sud-américain.

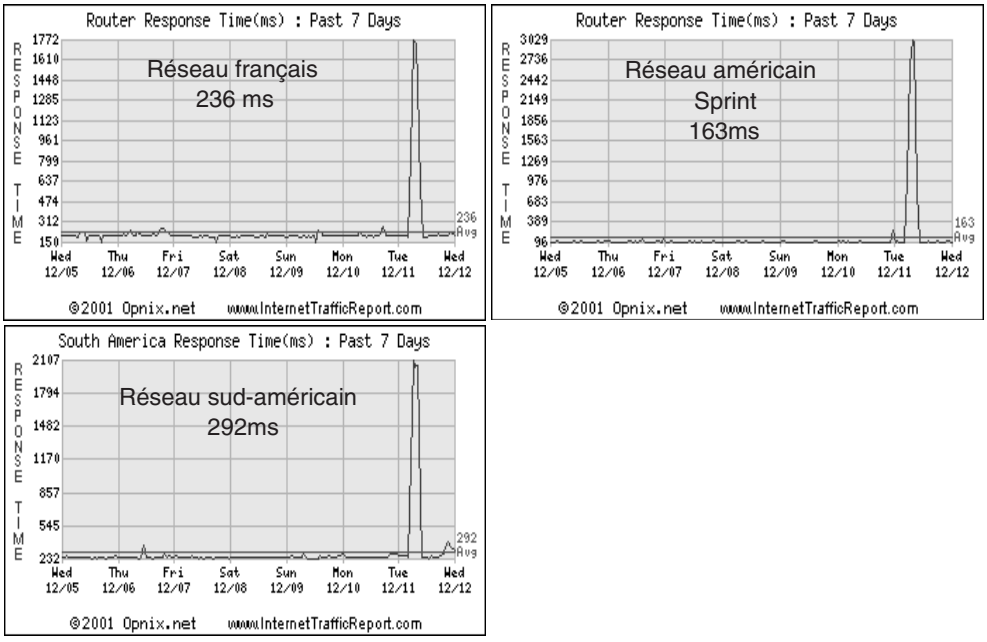

Figure 1.9 Performances de réseaux d'opérateurs (*www.internettrafficreport.com*).

1.8 LES RÉSEAUX SATELLITES

Les opérateurs de transport utilisant les satellites se multiplient. Si le coût est encore plus élevé que les liaisons câblées, ils sont une solution appropriée pour les zones géographiques où les liaisons câblées sont de qualité limitant les débits à quelques dizaines de Kb/s ou lorsqu'il n'existe pas d'infrastructure câblée. Deux exemples illustrent ces propos :

– ISF Télécom (*www.valsat.7p.com*), opérateur de transport canadien offre des liaisons satellites dans les deux sens (émission-réception), pour les régions ou les techniques DSL ne sont pas utilisables ;
– le réseau Eutelsat (*www.eutelsat.com*) couvre en plus de l'Europe, l'Europe de l'est et l'Afrique, territoires où l'infrastructure câblée est faible (figure 1.10).

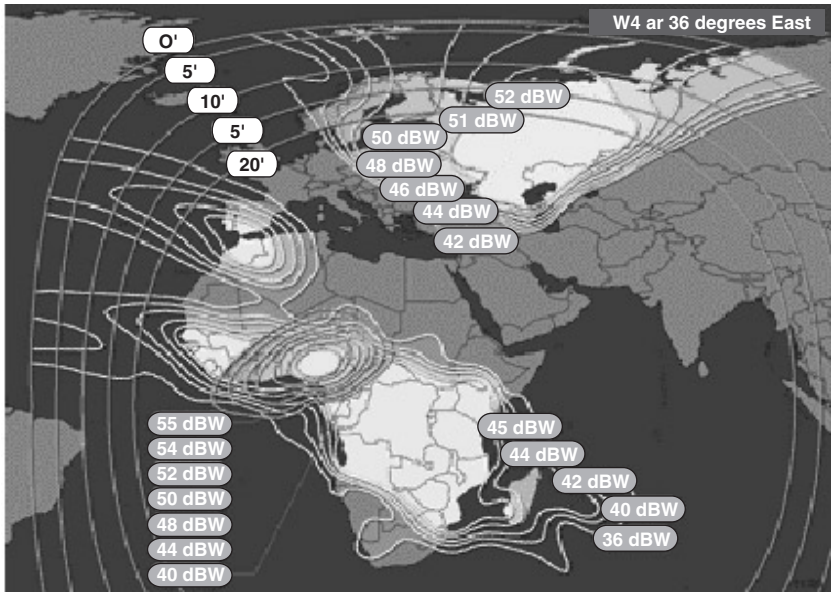

Figure 1.10 Couverture du satellite W4 d'Eutelsat (*www.eutelsat.com*).

Grâce à leurs capacités de liaison point-multipoint (*broadcasting*), les réseaux satellites offrent à leurs clients un ensemble très complet de services :

– TV et radio numériques et analogiques ;
– la téléphonie mobile ;
– des liaisons point à point voix-données pour réaliser un réseau étendu d'entreprises ;
– la localisation de véhicules ou bateaux et des liaisons voix-données pour les entreprises de logistique.

Outre l'opérateur EutelSat, citons Intelsat (*www.intelsat.com*) et Hughes Network systems (*www.hns.com*) en Amérique du nord, Europe et Asie ; Gilat (*www.gilat.com*) intervient en plus en Amérique latine et en Chine.

Ces opérateurs de transport ont la spécificité d'être également fournisseur d'accès Internet pour les entreprises et les particuliers, comme pour les prestataires de services.

Pour le client, deux cas se présentent (figure 1.11) :

– la liaison hertzienne est à double voie (émission-réception), l'équipement satellitaire (antenne + modulateur/démodulateur) est suffisant ;
– la liaison hertzienne est à simple voie (réception uniquement). Il doit alors se connecter à un prestataire de service par une infrastructure câblée (câble ou réseau de télécommunication) pour envoyer des données.

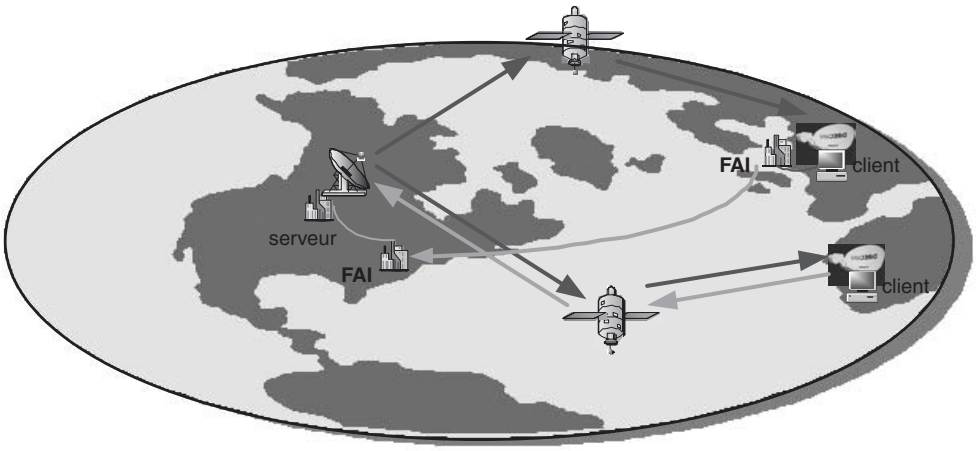

Figure 1.11 Les deux cas de liaison par satellite.

Résumé

1. Opérateurs Internet : trois métiers

➢ le prestataire de services propose des services d'accès, messagerie, hébergement de pages ;
➢ le fournisseur d'accès dispose des équipements permettant la connexion des équipements de l'abonné d'une part, la connexion de ses équipements à un réseau Internet d'autre part ;
➢ l'opérateur de transport Internet assure le transport des données à travers son réseau.

La plupart des opérateurs assurent au moins 2 des 3 métiers.

2. Les opérateurs de câblage

➢ un réseau Internet est de type maillé ;
➢ un réseau maillé est un ensemble de liaisons point à point ;
➢ les opérateurs de câblage disposent de liaisons point à point ;
➢ un opérateur de transport Internet peut louer des liaisons à un opérateur de câblage.

3. Topologie des réseaux de transport Internet

➢ les réseaux peuvent être de taille régionale, nationale ou européenne ;
➢ les réseaux nationaux ont le plus souvent une topologie en pétale ;
➢ pour se connecter au réseau, les clients doivent faire appel à un opérateur de télécommunication.

4. Le réseau d'interconnexion européen Ebone

➢ Ebone est constitué :
- de Points de Présence européens reliés par des liaisons à haut débit (155 Mbit/s à 2,5 Gb/s) ;
- de liaisons transatlantiques totalisant plusieurs gigabits par seconde.

➢ les réseaux nationaux, privés ou autres qui veulent bénéficier de Ebone viennent se raccorder au Point de Présence le plus proche ;
➢ Ebone admet tous types de trafic : enseignement, recherche, industrie...

5. Les opérateurs de transport internationaux

➢ le continent nord américain occupe une place centrale dans la topologie des réseaux Internet mondiaux ;
➢ les liaisons satellites permettent des échanges directs entre l'Europe et l'Asie.

6. Trafic et routage

➢ les données traversent le plus souvent plusieurs réseaux d'opérateurs ;
➢ il n'est pas possible de garantir la qualité de la transmission tout au long des réseaux traversés ;
➢ les temps de traversée d'un réseau d'opérateur sont de quelques centaines de millisecondes ;
➢ les opérateurs ne peuvent garantir, pour l'instant, les délais de transmission.

7. Les réseaux satellites

➢ ils permettent de desservir des zones géographiques non câblées ;
➢ ils sont adaptés à une diffusion multipoint (*broacasting*) ;
➢ ils nécessitent des équipements plus coûteux, notamment pour un particulier souhaitant émettre.

QCM

Une version électronique et interactive est disponible sur le site *www.dunod.com*.

1. Opérateurs Internet : trois métiers

Q1. L'opérateur de transport fournit un service direct :
a) à l'opérateur de câblage *b) au fournisseur d'accès*
c) au prestataire de service *d) à l'internaute*

Q2. Le fournisseur d'accès Internet travaille directement avec :
a) l'opérateur de câblage *b) le prestataire de service*
c) l'opérateur de transport *d) l'internaute*

Q3. Le réseau Internet est de type maillé parce que :
a) l'internaute a le choix du prestataire de service
b) il est constitué d'un ensemble relié d'opérateurs de transport
c) les données peuvent emprunter plusieurs chemins pour aller d'un point à un autre
d) les données peuvent emprunter plusieurs réseaux d'opérateurs de transport

2. Les opérateurs de câblage

Q4. La topologie des réseaux Internet des opérateurs de transport de dimension nationale est de type :
a) en étoile *b) en anneau* *c) maillé* *d) en pétale*

Q5. Un opérateur de câblage gère :
a) des routeurs *b) des liaisons point à point*
c) des serveurs d'accès distant

3. Topologie des réseaux de transport Internet

Q6. Le réseau d'un opérateur de transport couvre au moins :
a) une ville *b) un pays* *c) une région* *d) un continent*

4. Le réseau d'interconnexion européen Ebone

Q7. Le réseau Ebone interconnecte les équipements :
a) des opérateurs de transport *b) des prestataires de service*
c) des fournisseurs d'accès *d) des opérateurs de câblage*

5. Trafic et routage

Q8. Indiquer le temps moyen pour accéder à un site américain :
a) 50 ms *b) 250 ms* *c) 540 ms* *d) 930 ms*

Chapitre **2**

Se connecter à Internet

2.1 QUEL TYPE DE CONNEXION CHOISIR ?

2.1.1 Mode « connecté » ou « non connecté »

Que le client soit une grande entreprise, une PME/PMI ou un particulier, l'objectif est le même : maîtriser les coûts de communication. Le choix va dépendre du type de service envisagé (fournir et/ou recevoir de l'information), du volume d'informations à traiter et du temps imparti.

Deux modes de connexion existent : le mode connecté et le mode permanent (non connecté).

Le mode connecté nécessite, préalablement à l'accès à Internet, l'établissement d'une liaison avec l'opérateur de raccordement à Internet (prestataire de service ou fournisseur d'accès) à travers un réseau commuté (réseau téléphonique commuté par exemple). Dans ce mode, le client ne paie que le temps d'utilisation effectif de la connexion à Internet. Par contre, il ne pourra accéder à Internet que si son opérateur dispose d'une ligne libre pour la connexion. Aux heures de pointe, il faudra patienter et attendre qu'une ligne se libère. Le temps d'attente est souvent inversement proportionnel au prix de l'abonnement. Plus le rapport du nombre d'abonnés au nombre de lignes d'un prestataire est grand (*over-booking*), plus la probabilité de disposer d'une ligne est faible. Le mode connecté est utilisé pour les liaisons par le RTC, les GSM et GPRS (figure 2.1).

Le mode non connecté utilise une liaison permanente entre le client et l'opérateur, que le client se connecte à Internet ou non. Le coût est le plus souvent forfaitaire (abonnement mensuel) et/ou au volume de données échangées (en méga-octets ou Mo). Certains prestataires incluent dans l'abonnement un volume forfaitaire au-delà duquel les données supplémentaires échangées sont facturées au Mo.

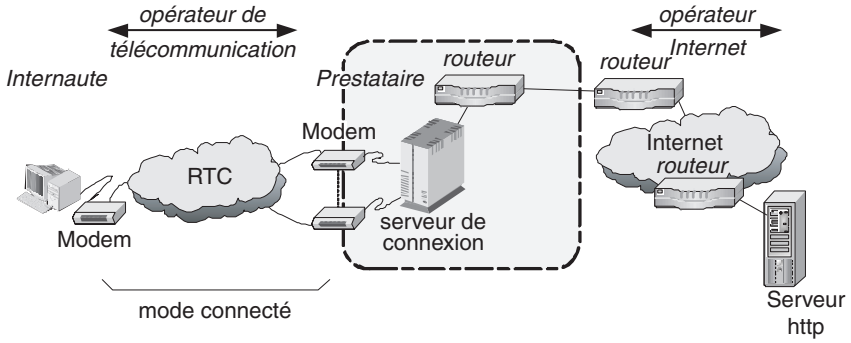

Figure 2.1 Raccordement à Internet par un réseau en mode connecté.

Dans ce mode, le client est sûr de pouvoir accéder à Internet au moment de son choix. C'est un mode de connexion quasiment indispensable pour les clients souhaitant installer dans leurs locaux un serveur web. Celui-ci doit en effet être accessible en permanence par les internautes. L'alternative consiste à faire héberger son serveur chez un prestataire. Cette solution peut s'avérer plus économique, mais moins souple quant à la mise à jour du site.

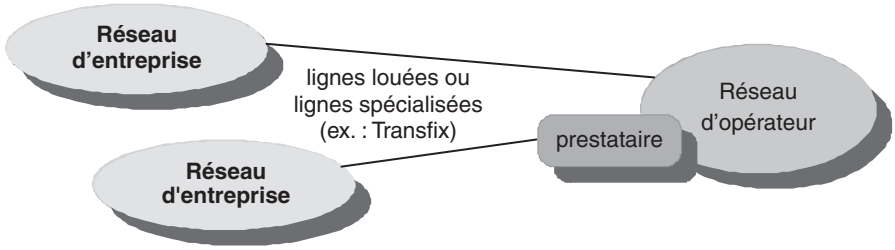

Figure 2.2 Raccordement à Internet par un réseau en mode non connecté.

2.1.2 Professionnel ou particulier : deux problématiques différentes

Vous l'avez deviné, il n'y a pas de solution évidente dans le choix d'un type de connexion à Internet et d'un prestataire. Par contre il y a les bonnes questions à se poser. En plus des paramètres classiques tels le débit, le coût de l'abonnement et de la liaison, d'autres paramètres sont utiles pour guider le choix. Parmi ceux-ci :

– le taux de disponibilité des lignes du prestataire ;
– le débit disponible entre le prestataire et Internet ;
– le taux d'indisponibilité des services du prestataire (pannes et maintenance) ;
– le temps de remise en service en cas de panne (le taux de panne zéro n'existe pas).

Si ces informations sont accessibles assez facilement par les responsables des grandes entreprises, elles sont plus difficiles à obtenir des prestataires pour les PME/PMI, voir le particulier. Par contre l'obtention de ces informations est un gage

de sérieux du prestataire. Il montre une surveillance de la qualité des services fournis et un engagement qualité vis-à-vis du client. Cet engagement a forcément un coût pour le prestataire, qu'il répercute sur l'abonnement.

Un autre élément à considérer concerne le débit. Il faut garder en mémoire le fait que le débit garanti par le prestataire est celui de la liaison entre ses équipements et ceux de l'abonné, en aucune manière le débit sur Internet. Or sur Internet, le débit n'est pas garanti (voir paragraphe 3.4, *Les protocoles de niveau transport : UDP et TCP*). Disposer d'un débit supérieur au débit réel entre le prestataire et Internet ou sur Internet conduit à une sous-utilisation de la liaison avec le prestataire.

Pour un usage professionnel, le moins cher n'est pas toujours le plus économique. Pour établir un budget prévisionnel fiable, le professionnel a besoin de maîtriser le coût de sa connexion et de disposer d'un service conforme à ses besoins. Le coût de la connexion comporte l'amortissement de l'équipement nécessaire, l'abonnement et le coût des communications. Le service prend en compte les débits disponibles, dont dépend la durée de la communication, et la facilité d'établir une connexion (capacité de connexion du prestataire et taux d'indisponibilité). C'est donc le rapport (amortissement équipement + abonnement + communication)/(services) qu'il faudra prendre en compte. L'évaluation des services est bien sûr subjective. Toutefois, il ne faut pas oublier que pour un professionnel, le temps passé en connexion sur Internet coûte non seulement la communication, mais également le salaire de la personne connectée.

2.1.3 Les protocoles utilisés

Quel que soit le mode choisi, le raccordement avec le prestataire de service ou le fournisseur d'accès Internet se fait par une liaison point à point :

– point de raccordement du client (modem ou routeur) ;
– point de raccordement du prestataire ou fournisseur d'accès (même équipement que le client).

Il est nécessaire que client et prestataire ou fournisseur utilisent les mêmes protocoles :

– protocole d'établissement de la liaison pour un réseau en mode connecté ;
– protocole de transmission des données sur la liaison ;
– protocole d'établissement de la connexion entre l'application du client (navigateur par exemple) et le serveur de connexion du prestataire ou fournisseur ;
– protocole d'identification du client.

Dans le cas d'un raccordement par le RTC, l'ouverture par le client du navigateur paramétré sur l'adresse du prestataire nécessite la mise en œuvre des protocoles présentés sur la figure 2.3 :

1. Demande d'établissement de connexion TCP avec le service TCP du prestataire.
2. Demande (initiée par TCP/IP) d'établissement de connexion au protocole PPP (demande traitée par le protocole LCP, voir paragraphe 3.6, *Le protocole PPP*).
3. Établissement de la liaison par le modem, à la demande du protocole LCP.

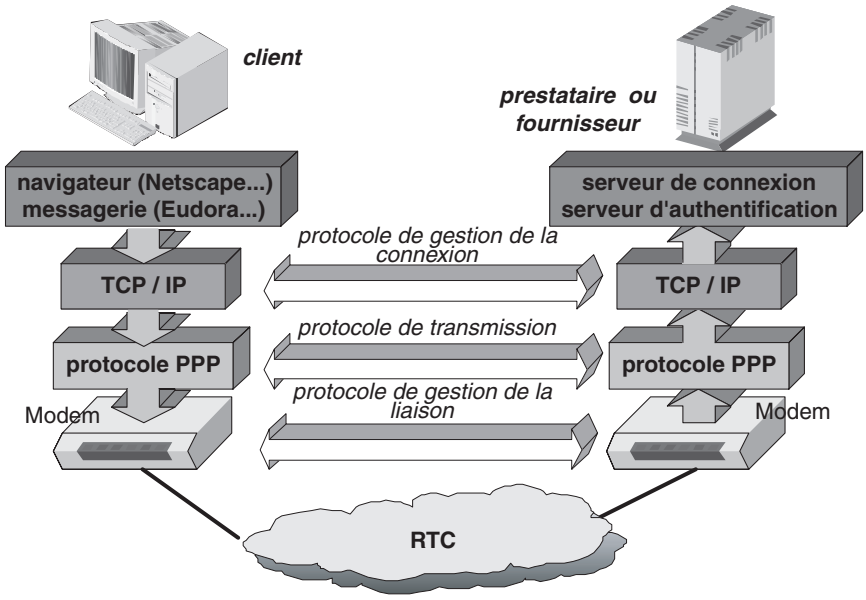

Figure 2.3 Protocoles utilisés dans un raccordement par le RTC.

Une fois la liaison établie entre les modems, les protocoles PPP se mettent d'accord sur les paramètres d'échange des données, puis c'est au tour des protocoles TCP d'établir le dialogue. Enfin le serveur d'authentification demandera le nom d'utilisateur et le mot de passe du client.

Chaque établissement de dialogue par les protocoles peut être visualisé par des messages ou des icônes s'affichant sur l'écran de l'ordinateur client. Ces informations sont importantes pour suivre les phases de connexion et localiser les causes possibles d'un dysfonctionnement lors de l'établissement d'une connexion avec le prestataire.

2.2. SE CONNECTER PAR LE RTC

2.2.1 Introduction

Le raccordement par le RTC nécessite :

– un modem chargé de la gestion de la liaison avec le modem du prestataire, du codage des données à transmettre et de leur mise en forme (trame asynchrone orientée caractère). Les fonctions et modes de transmission des modems sont détaillés au paragraphe 4.3 de l'ouvrage *Transmissions et Réseaux*[1] ;
– le protocole PPP (*Point to Point Protocol*) ;
– le protocole TCP/IP.

1. Lohier S. et Présent D., *Transmissions et Réseaux*, 3e édition, Dunod, 2003.

Pour que l'ensemble fonctionne, il faut paramétrer tous les protocoles et établir un lien entre chacun des protocoles contigus. Ce paramétrage et ces liens (par exemple entre IP et PPP) sont généralement assurés par le système d'exploitation de manière transparente pour l'utilisateur.

2.2.2 Installation et paramétrage d'un modem

L'installation d'un modem est de plus en plus simplifiée par les fonctions « plug & play » d'installation de périphérique fournies par les systèmes d'exploitation. Sous Windows, beaucoup de modems sont détectés et installés automatiquement, y compris le choix du port série et de l'IRQ (n° d'interruption utilisée) associés. Sous Unix ou Linux, suivant les distributions, l'installation peut être automatique ou nécessiter la modification de fichiers de configuration.

Le paramétrage du modem peut par contre introduire des dysfonctionnements. Il faut se rappeler que le dialogue entre modem est un dialogue « point à point » nécessitant un paramétrage identique des deux modems[1]. Le pilote (*driver*) installé utilise des paramètres « *par défaut* ». Comme peu d'utilisateurs modifient ce paramétrage, les modems peuvent dialoguer entre eux. Les paramètres par défaut sont le plus souvent :

– un débit maximum de 56 Kb/s sur la ligne pour les modems récents V.90 ou V.92 ;
– 8 bits de données ;
– aucune parité ;
– 1 bit d'arrêt ;
– contrôle de flux matériel (RTS/CTS).

Si par contre, le paramétrage « par défaut » est spécifique, ou si une application a modifié ce dernier, le dialogue avec le modem du prestataire peut s'avérer impossible.

La figure 2.4 montre les fenêtres de paramétrage des modems sous Windows.

2.2.3 Le protocole PPP avec le RTC

Dans une connexion point à point le protocole PPP s'interpose entre le protocole IP et le protocole de transmission (dans le cas du RTC, la transmission asynchrone du modem) (figure 2.5). Le premier protocole conçu dans ce but est SLIP (*Serial Line Internet Protocol*). PPP (*Point to Point Protocol*) ajoute la détection d'erreurs et s'interface avec plusieurs protocoles de niveau 2 et 3 (IP, IPX) et de niveau 1 et 2 (ATM, Ethernet).

Le protocole PPP regroupe en fait trois protocoles :

– le protocole PPP met les données dans des trames. Le format de la trame PPP permet la détection des erreurs, le marquage de la fin d'une trame et du début de la suivante ;
– le protocole LCP (*Link Control Protocol*) active et teste la ligne, négocie les options et désactive la ligne en fin de connexion ;

1. Cf. l'étude de cas du chapitre 3 de l'ouvrage *Transmissions et Réseaux*.

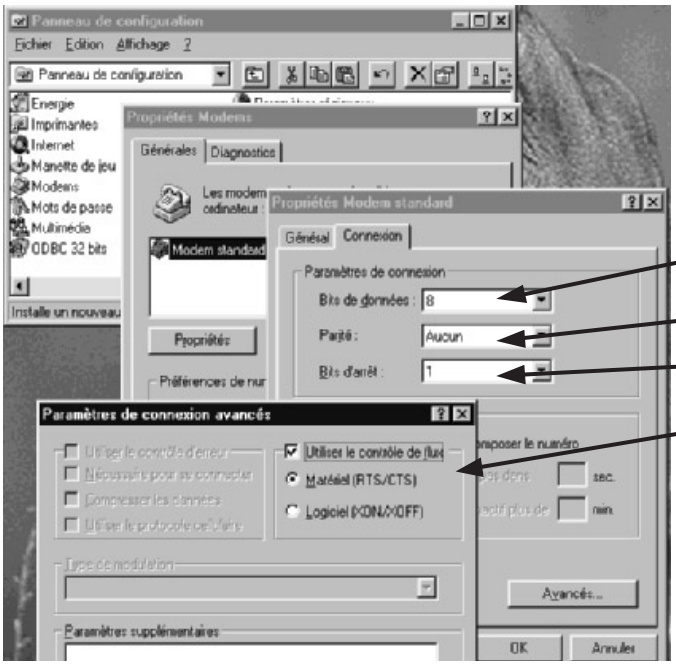

Figure 2.4 Paramétrage d'un modem sous Windows.

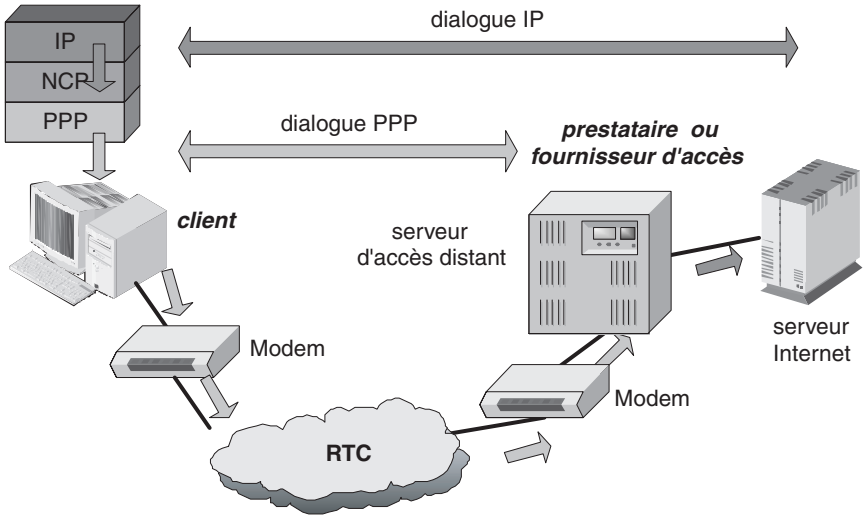

Figure 2.5 Dialogues PPP et IP entre le client et le prestataire de service.

– le protocole NCP (*Network Control Protocol*) différent pour chaque protocole réseau supporté.

Pour permettre la transmission à travers le RTC, les paquets IP subissent une succession de fragmentation/réassemblage destinées à passer de blocs de 64 Ko maximum au niveau IP à 1 octet au niveau modem. La figure 2.6 donne une idée des traitements et fragmentations nécessaires :

– sur le RTC, les modems transmettent les données octet par octet ;
– le datagramme IP peut contenir jusqu'à 64 Ko de données ;
– NCP doit fragmenter les datagrammes et contrôler la transmission correcte des trames PPP.

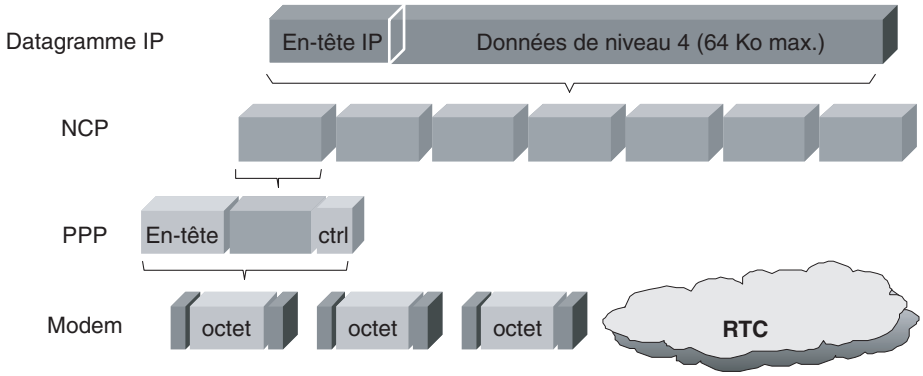

Figure 2.6 Fragmentation des blocs de données pour une transmission asynchrone sur le RTC.

2.3 SE CONNECTER PAR NUMÉRIS

2.3.1 Introduction

Le Réseau Numérique à Intégration de Services (RNIS) dont l'appellation commerciale en France est Numéris utilise un mode de transmission unique pour la voix et les données numériques[1]. L'architecture d'une connexion par Numéris est identique à celle utilisant le RTC, seul le réseau de l'opérateur est différent. Quelques différences toutefois :

– le protocole de niveau 2 utilisé par Numéris définit un format de trame, l'utilisation de PPP est donc inutile ;
– pour un accès de base, Numéris offre un débit vers Internet de 64 Kb/s ou de 128 Kb/s ;
– un accès de base autorise deux connexions simultanées à 64 Kb/s (ex. : deux connexions simultanées à Internet ou une connexion à Internet et une connexion voix ou fax).

1. Cf. paragraphe 8.5 de l'ouvrage *Transmissions et Réseaux*.

Le raccordement par Numéris nécessite :

– un boîtier ou une carte de connexion, parfois appelé modem par analogie avec le RTC bien que le signal reste numérique ;
– le protocole TCP/IP.

2.3.2 Installation et paramétrage d'un modem Numéris

La procédure d'installation d'un modem (ou pseudo-modem) RNIS est identique à celle d'un modem analogique. Sous Windows, utiliser l'ajout/suppression de matériel pour un modem sur carte. Le paramétrage est par contre spécifique.

2.4 SE CONNECTER PAR ADSL

2.4.1 Introduction

L'ADSL est un mode de transmission analogique de données numériques autorisant des débits de 2 Mb/s sur les paires téléphoniques du RTC. Comme pour Numéris, les liaisons ADSL autorisent une connexion simultanée au RTC et à Internet *via* un réseau de collecte ATM. Les signaux de chaque source (voix et Internet) sont séparés par un filtre à chaque extrémité de la liaison de l'abonné au réseau de l'opérateur (figure 2.7).

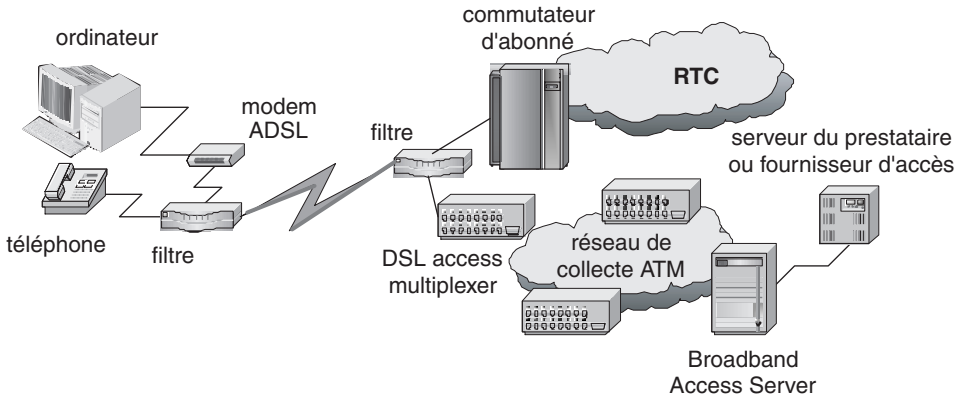

Figure 2.7 Architecture d'une connexion ADSL au prestataire ou fournisseur d'accès.

Le raccordement par ADSL utilise :

– un modem associé à un filtre ;
– une connexion VPN (*Virtual Private Network*) en accès distant ;
– le protocole PPTP (*Point to Point Tunneling Protocol*) ;
– le protocole TCP/IP.

Le protocole PPTP met en œuvre les mécanismes de base du protocole PPP (incluant LCP et NCP). De plus, intégrant l'encapsulation et le cryptage, il permet de créer de manière sécurisée des réseaux privés virtuels sur Internet.

2.4.2 Installation et paramétrage d'une connexion VPN

L'établissement d'une connexion VPN (*Virtual Private Network*) s'appuie sur un serveur VPN et un serveur d'authentification (souvent de type *Radius*) :

– à l'établissement de la connexion VPN, le serveur VPN alloue une adresse IP qui peut être publique ou privée ;
– à l'établissement de la connexion le serveur d'accès (*Network Access Server*) du fournisseur d'accès (FAI) alloue à la station une adresse IP publique ;
– l'adresse IP du destinataire est encapsulée par l'en-tête IP de la connexion VPN. Elle est donc ignorée des routeurs.

Une fois la connexion établie au niveau liaison et réseau, la sécurisation est mise en œuvre en cryptant et en encapsulant les unités de données de niveaux supérieurs dans les paquets PPTP.

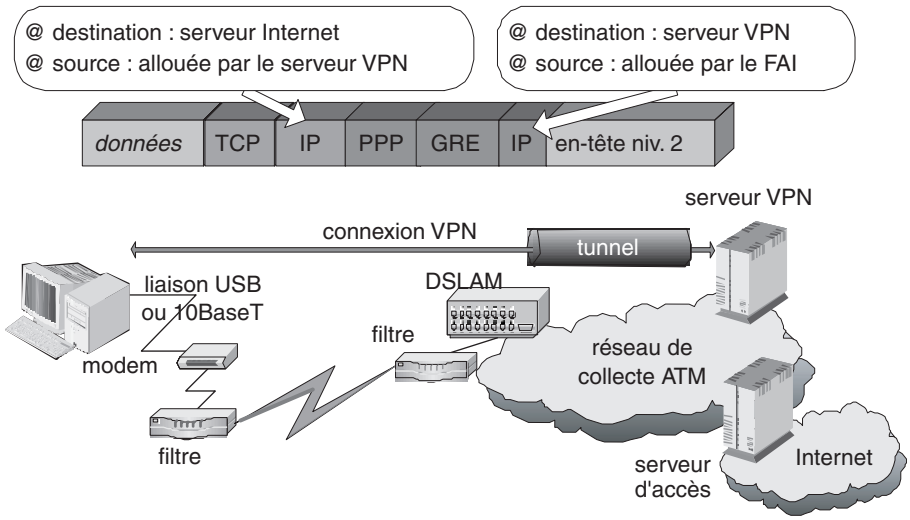

Figure 2.8 Encapsulation des paquets IP sur une connexion VPN.

La figure 2.8 montre que l'adresse IP circulant sur Internet est une adresse allouée par le serveur VPN et non celle du client allouée par le fournisseur d'accès Internet (FAI). Il y a donc sécurisation de l'identité du client. Le serveur VPN assure les translations d'adresses.

Sous Windows, l'installation d'une connexion VPN passe d'abord par l'installation d'une carte réseau VPN (carte virtuelle) et du protocole TCP-IP associé à cette carte.

Comme le montre la figure 2.9, la configuration utilise deux adresses :

– adresse IP du serveur VPN ;
– adresse IP privée pour l'accès au serveur du fournisseur d'accès Internet.

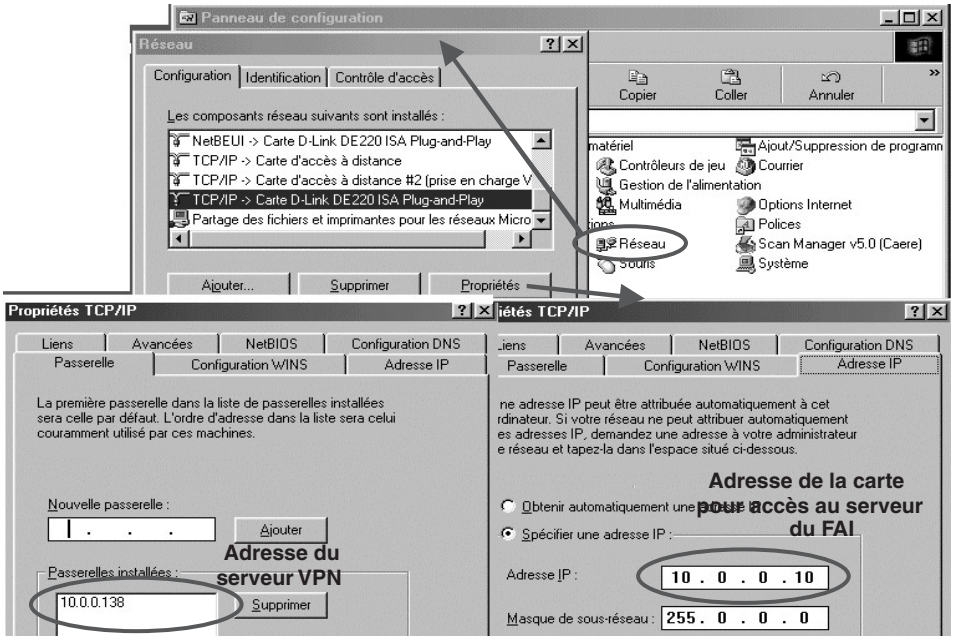

Figure 2.9 Paramétrage d'une connexion VPN sur l'ADSL.

L'adresse utilisée est une adresse privée non routable par les routeurs Internet. L'équipement du client est donc inaccessible par un piratage venant de l'extérieur.

L'accès à Internet par une connexion ADSL sous Windows s'initialise par le menu « accès réseau à distance ». Lors de la création d'une nouvelle connexion, le logiciel demande le type d'interface à utiliser. Après l'installation d'une carte réseau VPN, il sera possible de la sélectionner pour la connexion. Il faudra ensuite entrer le nom d'utilisateur et le mot de passe fournis par l'opérateur ADSL. La figure 2.10 montre les paramètres mémorisés après création.

2.4.3 Le protocole PPP avec l'ADSL

Contrairement au protocole de transmission asynchrone des modems utilisés sur le RTC, le protocole ADSL n'est qu'un mode de transmission. Il ne définit aucun format de trame de niveau 2. Il n'est donc pas suffisant à lui seul pour une détection d'erreurs de transmission à la réception. Le recours à un protocole de niveau 2 entre PPTP et ADSL s'avère nécessaire. Parmi les protocoles de niveau 2 possibles, les plus utilisés sont ATM et Ethernet.

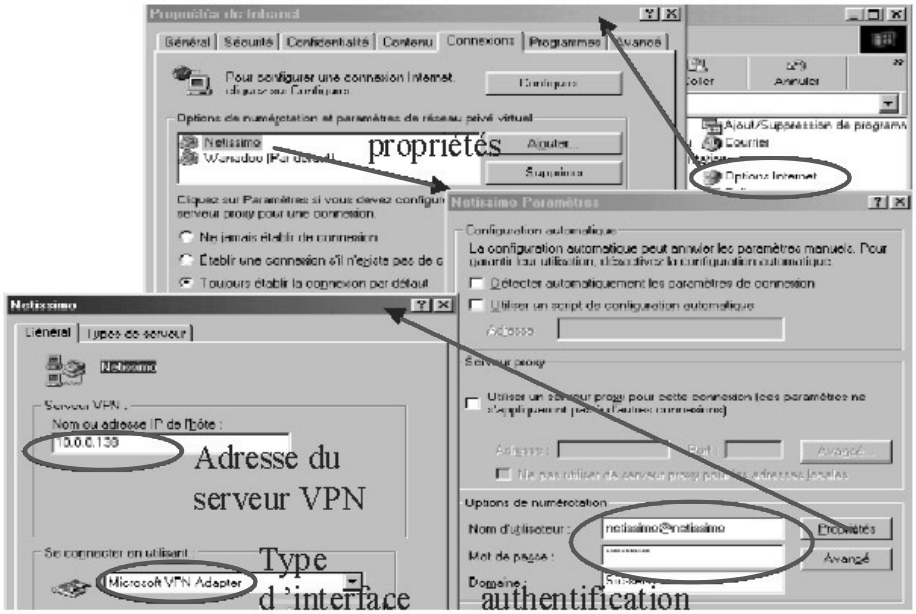

Figure 2.10 Paramètres d'une connexion par accès réseau à distance via ADSL.

Associé à ATM, le protocole PPP deviendra PPPoA (*PPP over ATM*), associé à Ethernet on aura PPPoE (*PPP over Ethernet*). Bien sûr, seules les fonctionnalités indispensables seront mises en œuvre. Pour Ethernet, par exemple, seront retenus le format de trame incluant la somme de contrôle d'erreur (*checksum*), la méthode d'accès au support de type CSMA/CD ne sera d'aucune utilité (figure 2.11).

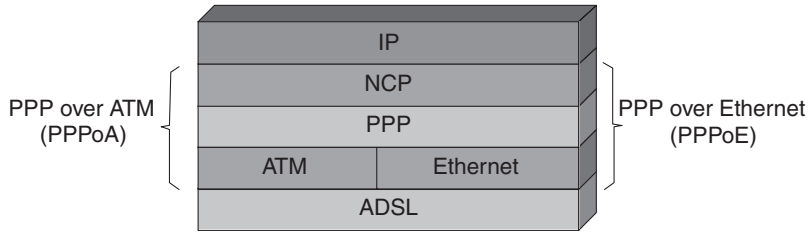

Figure 2.11 Association du protocole PPP avec ATM et Ethernet.

La figure 2.12 montre les requêtes transmises par le routeur d'un client ADSL lors de l'établissement d'une connexion avec son fournisseur d'accès à Internet.

L'étude de cas montre les phases d'établissement d'un tunnel PPP entre le client et le fournisseur d'accès Internet à travers les équipements du fournisseur d'accès ADSL français « Netissimo ».

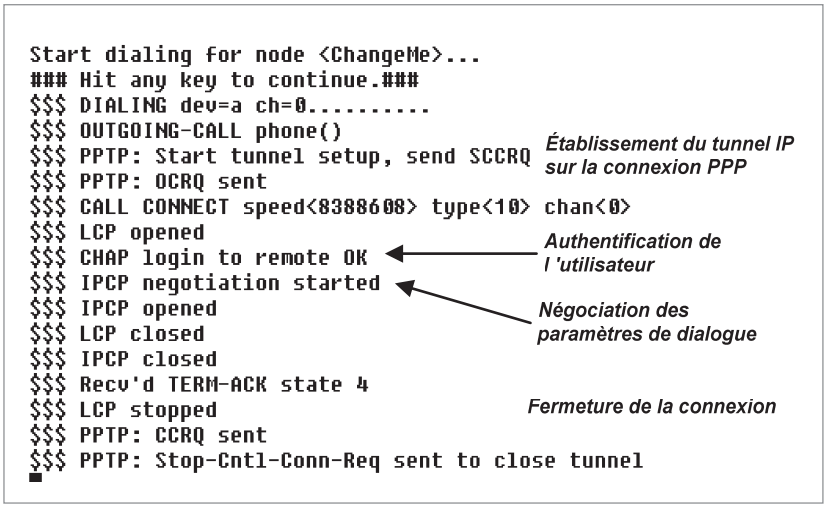

Figure 2.12 Dialogue d'établissement d'une connexion PPP via ADSL.

2.5 SE CONNECTER PAR LE CÂBLE

Ce type de connexion utilise les réseaux câblés de télévision présents dans les agglomérations denses. La technologie permet la retransmission de données numériques sur un ou plusieurs canaux de câble de 6 MHz. Les autres signaux, vidéo et audio (la télévision par câble et le son FM), peuvent ainsi être transmis sur d'autres canaux du même câble. La technologie du réseau local à large bande permet de faire coexister ces différents services simultanément.

Le réseau de transport en fibre optique distribue à partir d'une tête de réseau les données ainsi que les signaux TV en numérique et en analogique jusqu'à un centre local de distribution qui regroupe plusieurs habitations ou immeubles (figure 2.13). Les signaux sont ensuite transportés sur un câble coaxial type TV (CATV) vers chacun des foyers et la connexion est réalisée par un boîtier de raccordement, généralement appelé modem-câble. Ce dernier est spécifiquement dédié aux réseaux de type HFC (*Hybrid Fiber Optic and Coaxial*) qui est une norme pour les réseaux câblés autorisant un flux bidirectionnel.

Le modem-câble généralement loué au fournisseur d'accès et configurable uniquement à distance offre donc plusieurs fonctions :

– il assure la modulation/démodulation vis-à-vis des cartes TX (carte voie descendante) et RX (carte voie remontante) situées en tête de réseau ;
– il effectue une adaptation des trames Ethernet côté utilisateur en cellules ATM côté réseau câblé (figure 2.14) ;
– il réalise à chaque mise sous tension de l'équipement de l'utilisateur une identification de l'abonné (chaque modem-câble possède un numéro unique) avant de renvoyer une adresse IP ;

– il peut également proposer des fonctions de filtrage ou de sécurité suivant le choix de l'opérateur.

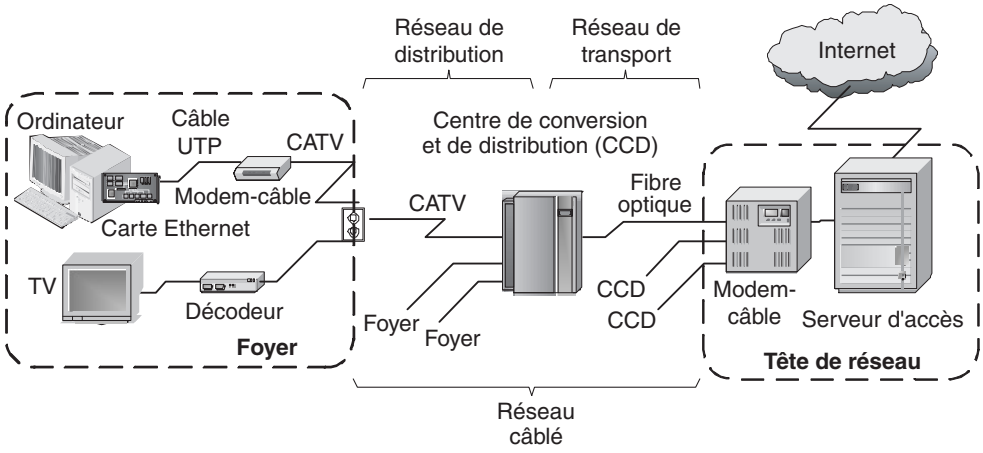

Figure 2.13 Architecture d'une connexion par câble.

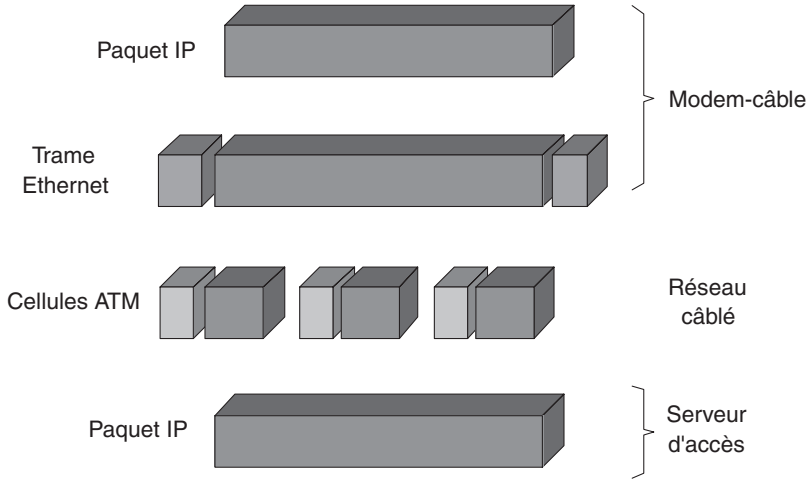

Figure 2.14 Format des données d'une connexion par câble.

Côté utilisateur, le raccordement et la configuration sont les mêmes que pour un réseau local à partir d'une carte Ethernet (figure 2.15). La connexion n'est sécurisée que par les équipements de type coupe-feu (*firewall*) du fournisseur d'accès ou éventuellement du particulier.

Les débits proposés sont généralement forfaitaires et peuvent atteindre 512 Kb/s en voie descendante (vers l'abonné) et 128 Kb/s en voie montante.

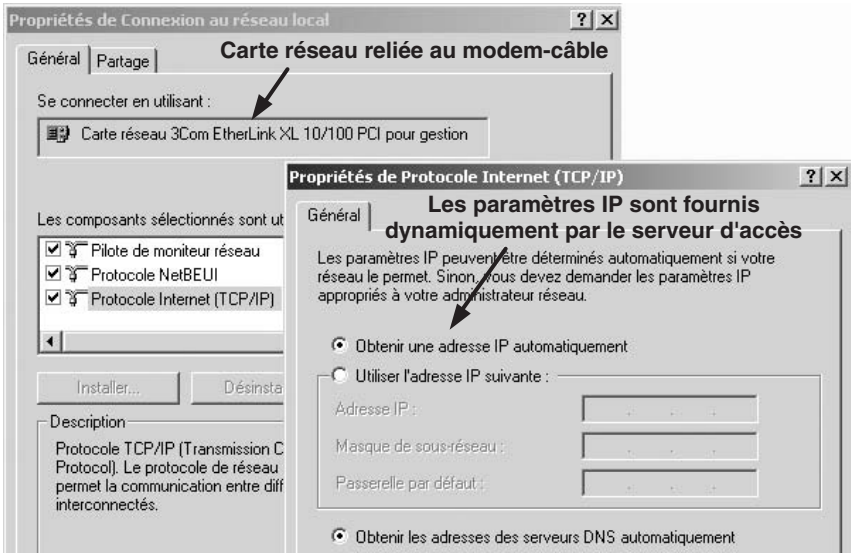

Figure 2.15 Paramétrage d'une connexion par câble.

2.6 SE CONNECTER PAR LIAISON SPÉCIALISÉE

Ce mode de connexion est particulièrement utilisé par les entreprises qui disposent de serveurs web devant être accessibles en permanence depuis Internet. La liaison entre le client et le fournisseur d'accès Internet sera assurée par un opérateur de télécommunication. Il mettra à disposition des deux contractants une structure de transport des données et un protocole de transmission garantissant le débit et la détection des erreurs. Ces fonctions regroupent les niveaux 1 et 2 de l'architecture OSI[1]. Les fonctionnalités de niveau supérieur sont à la charge des abonnés. Entrent dans ce champ, les protocoles d'adressage, d'adaptation de IP au protocole de transmission, de fragmentation/réassemblage, d'authentification et de sécurisation.

Les protocoles les plus utilisés aujourd'hui sont SDH (*Synchronous Digital Hierarchy*) et WDM (*Wavelength Division Multiplexing*). SDH est un protocole de transmission synchrone sur câble cuivre ou sur fibre optique. Il permet le transport de différents paquets de niveau 3. Il s'adapte facilement au transport de paquets IP[2]. WDM est un mode de transmission dans lequel chaque flux de données utilise une longueur d'onde. Ce protocole ne définit pas de format de trame, ni de détection d'erreur de transmission. Il doit être associé à un protocole de niveau 2 tel qu'ATM.

L'opérateur de télécommunication peut proposer des liaisons point à point ou point multipoint. Dans le premier cas, le FAI dispose d'un ETN (Équipement de Terminaison Numérique) pour chaque client (figure 2.16). Le débit de la ligne du

1. Cf. paragraphe 5.4 de l'ouvrage *Transmissions et Réseaux*.
2. Cf. paragraphe 3.6 de l'ouvrage *Transmissions et Réseaux*.

client est donc garanti jusqu'au FAI. Dans le second cas, le FAI dispose d'un seul ETN pour tous ses clients. Le débit de la ligne de raccordement de l'ETN au FAI est alors partagé par les clients. Cette seconde solution s'adapte bien aux fournisseurs d'accès ayant des clients ne nécessitant pas de gros débits.

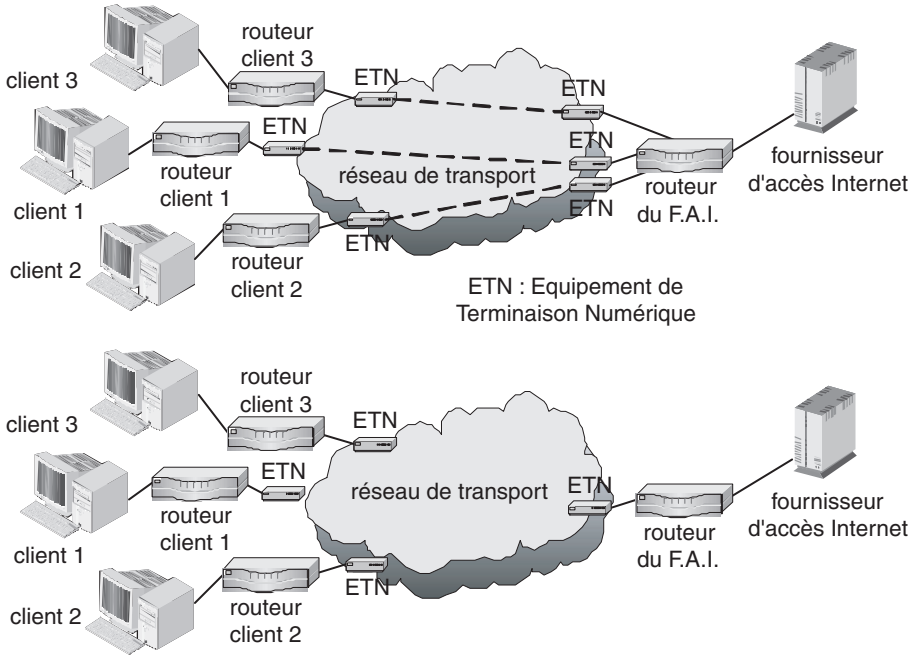

Figure 2.16 Architecture de liaisons monocanal et multicanaux.

Pour le raccordement, le client doit disposer d'un routeur et des logiciels et cartes d'interfaces compatibles :

– avec le mode de transmission et le protocole utilisés sur la liaison entre ses équipements et ceux de l'opérateur de télécommunication ;
– avec les protocoles utilisés par le fournisseur d'accès Internet.

Le coût de l'installation doit prévoir :

– l'investissement et l'amortissement des équipements de raccordement (routeurs + cartes réseaux) ;
– la maintenance de ces équipements ;
– l'installation de l'accès à la ligne spécialisée de l'opérateur (des équipements du client au réseau de l'opérateur) ;
– l'abonnement à la ligne spécialisée ;
– l'abonnement aux services du FAI.

Les débits proposés par la plupart des opérateurs de télécommunication vont de 64 Kb/s à 155 Mb/s. Pour sa part, l'offre France Telecom comporte des liaisons

Transfix jusqu'à 2 Mb/s sur des interfaces G.703, X.24 et V.35, ainsi que des liaisons Transfix HD à 34 Mb/s et 155 Mb/s sur interface synchrone G.703 (voir le site *www.francetelecom.com/fr/entreprises*).

Résumé

1. Quel type de connexion choisir ?

➢ le mode connecté nécessite l'établissement d'une liaison à travers un réseau commuté (RTC par exemple) ;
➢ le mode non connecté utilise une liaison permanente entre le client et l'opérateur Internet ;
➢ le choix doit s'intéresser aux taux de disponibilité des lignes, des services du prestataire, du débit entre le prestataire et Internet, au temps de remise en service des équipements ;
➢ le débit peut être garanti entre le client et le prestataire, pas au-delà ;
➢ le raccordement du client au prestataire de service se fait par une liaison point à point ;
➢ les protocoles côté client d'une part, prestataire d'autre part doivent être identiques.

2. Se connecter par le RTC

➢ le raccordement par le RTC nécessite un modem, le protocole PPP et le protocole TCP/IP ;
➢ le paramétrage par défaut d'un modem sous Windows donne un format de trame asynchrone avec 8 bits de données, pas de parité, 1 bit d'arrêt et un contrôle de flux matériel (RTS/CTS) ;
➢ le protocole PPP regroupe PPP, LCP et NCP ;
➢ les datagrammes IP sont fragmentés par NCP et transmis octet par octet par le modem.

3. Se connecter par Numéris

➢ le raccordement par Numéris nécessite un pseudo-modem et le protocole TCP/IP.

4. Se connecter par ADSL

➢ le raccordement par ADSL utilise un modem+filtre, une connexion VPN, le protocole PPP et le protocole TCP/IP ;
➢ le protocole PPTP ajoute l'encapsulation et le cryptage au protocole PPP ;
➢ une connexion VPN à besoin de 2 adresses IP : l'adresse du serveur VPN et l'adresse du serveur du FAI ;
➢ avec une connexion VPN, le client se voit attribuer une adresse privée non routable sur Internet ;
➢ sous Windows, une connexion VPN s'initialise par le menu « accès réseau à distance » ;

➢ PPPoA (PPP over ATM) et PPPoE (PPP over Ethernet) sont 2 protocoles de niveau 2 associés à ADSL.

5. Se connecter par le câble

➢ ce type de connexion utilise les réseaux câblés de TV avec un cablâge mixte coaxial et fibre optique ;
➢ un modem-câble spécifique réalise la transformation entre une liaison locale Ethernet côté abonné et les cellules ATM supportées par des signaux analogiques modulés côté réseau câblé ;
➢ les débits proposés par les opérateurs peuvent atteindre 512 Kb/s en voie descendante.

6. Se connecter par liaison spécialisée

➢ la liaison entre le client et le FAI est une liaison permanente assurée par un opérateur de télécommunication ;
➢ les protocoles de transmission les plus utilisés sont SDH (Synchronous Digital Hierarchy) et WDM (Wavelength Division Multiplexing) ;
➢ pour une liaison multicanaux, le débit disponible sur la liaison du FAI à l'opérateur télécom est partagé par les clients ;
➢ pour le raccordement, le client doit disposer d'un routeur et des cartes interfaces permettant la mise en œuvre des protocoles de l'opérateur de télécommunication et du FAI.

QCM

Une version électronique et interactive est disponible sur le site *www.dunod.com*.

1. Quel type de connexion choisir ?

Q1. Le mode connecté est utilisé par les réseaux (plusieurs réponses) :
a) RTC b) Ethernet c) ADSL d) GSM e) Internet

Q2. Dans le mode non connecté, la liaison du client avec le prestataire de service est :
a) permanente b) établie par le client c) établie par le prestataire

Q3. La liaison entre le client et le prestataire est de type :
a) point-multipoint b) point à point c) multipoint-multipoint

Q4. Dans un raccordement par le RTC, qui adresse le premier une demande d'établissement de connexion :
a) TCP/IP b) PPP c) le modem

Q5. Dans un raccordement par le RTC, qui établit le premier une connexion :
a) TCP/IP b) PPP c) le modem

2. Se connecter par le RTC

Q6. Le modem du prestataire utilisant le paramétrage par défaut, quel format utiliser sur le modem du client (bits de données ; parité ; bits de stop) ?
a) 7 ; paire ; 2 b) 8 ; impaire ; 1 c) 8 ; sans ; 2 d) 8 ; sans ; 1

Q7. Quel protocole active et teste la ligne ?
a) PPP b) LCP c) NCP

Q8. Quel protocole adapte les paquets du protocole de niveau 3 au format des trames de niveau 2 ?
a) PPP b) LCP c) NCP

3. Se connecter par Numéris

Q9. Quel(s) protocole(s) une connexion Internet par Numéris n'utilise-t-elle pas ?
a) trame asynchrone b) trame synchrone
c) TCP/IP d) PPP

4. Se connecter par ADSL

Q10. Quel(s) protocole(s) une connexion Internet par ADSL n'utilise-t-elle pas ?
a) trame asynchrone b) trame synchrone
c) TCP/IP d) PPTP

Q11. Avec une connexion VPN, quelle adresse IP circule sur le réseau Internet ?
a) du serveur VPN b) fournie par serveur VPN client
c) du poste d) du FAI

Q12. Entre quelles entités est établi le tunnel IP :
a) poste client et serveur VPN b) poste client et FAI
c) DSLAM et FAI d) DSLAM et serveur VPN

Q13. Quelles fonctionnalités du protocole Ethernet sont utilisées par le protocole PPPoE ?
a) accès au support b) format de trame
c) adressage d) détection d'erreur

5. Se connecter par le câble

Q14. Quel type de réseau emprunte une connexion par câble coaxial ?
a) RTC b) Réseau TV c) RNIS d) Transpac

Q15. Quel format de trame circule entre le modem-câble de l'abonné et la tête de réseau ?
a) Ethernet b) trame asynchrone c) ATM

6. Se connecter par liaison spécialisée

Q16. Indiquer quel(s) protocole(s) sont utilisés sur une liaison spécialisée ?
a) HDLC b) ADSL c) SDH d) V35 e) WDM

Q17. Quels sont les niveaux OSI gérés par les protocoles des opérateurs de télécommunication sur les liaisons point à point ?
a) niveau 1 b) niveau 2 c) niveau 3 d) niveau 4 e) niveau 5

Q18. Dans une liaison point-multipoint, comment peut être le débit sur la ligne client par rapport à celui de la ligne du FAI ?
a) inférieur et variable b) égal c) inférieur et constant

Exercices

➤ (*) : facile(**) : moyen(***) : difficile
Corrigés à la fin du livre et sur le site *www.dunod.com*.

2.1 (*) Un prestataire de service dispose d'une ligne spécialisée 2 Mb/s vers le réseau Internet. Il compte abonner 120 clients par le réseau commuté avec des modems 56 Kb/s.

a) Calculer le taux de surbooking (rapport du nombre de clients à celui des clients pouvant être connectés simultanément).

b) Combien de modems sont nécessaires ?

2.2 (**) Un fournisseur d'accès Internet veut abonner trois entreprises disposant chacune d'une liaison spécialisée à 512 Kb/s pour des serveurs web, deux prestataires de service disposant chacun d'une LS à 512 Kb/s pour leurs clients et 12 prestataires disposant de LS à 128 Kb/s. Il veut offrir aux entreprises un débit nominal égal à celui de leur LS. Il estime que les lignes des prestataires sont utilisées à 60 % de leur capacité.

a) Calculer le débit de la LS de type multicanaux qu'il doit louer.

b) Combien de prestataires disposant de lignes 128 Kb/s pourra-t-il abonner s'il dispose de 3 LS à 2 Mb/s ?

2.3 (***) Un prestataire veut évaluer le nombre d'abonnés nécessaires pour amortir sa connexion à une plaque ADSL distante de 30 km par le service de Collecte IP/ADSL de France Telecom. Il considère que le poids moyen d'une page web est de 60 Ko et que le nombre moyen de pages consultées est de 20 pages/mn.

a) Calculer le nombre de clients Netissimo 1 pouvant être connectés simultanément sur un lien à 500 Kb/s.

b) Combien de liens à 2 Mb/s sont nécessaires pour connecter simultanément un minimum de 10 clients Netissimo 1 (utiliser le tableau 2.1 de l'étude de cas).

c) À partir des tableaux 2.2 et 2.3, calculer le coût annuel de la liaison à la plaque ADSL (hors investissement matériel, et avec un amortissement de l'accès à la plaque sur 4 ans).

d) Combien faut-il d'abonnés si l'abonnement des clients est fixé à 25 €/mois.

2.4 (**) Un utilisateur hésite entre plusieurs types de connexions : un forfait RTC 20 heures à 15 € par mois ; un accès câble à 39 € par mois offrant un débit de 512 Kb/s ; un accès ADSL à 30 € par mois pour un débit de 128 Kb/s.

a) Calculer le coût du Ko/s pour les différents accès.

b) Comparez les différentes solutions si le volume des données reçues ne dépasse pas 600 Mo par mois.

Étude de cas : L'offre IP/ADSL de France Télécom

En France, aujourd'hui, l'offre ADSL s'appuie essentiellement sur le réseau de France Telecom. Il découpe le territoire en zones dénommées « plaques ADSL » (figure 2.17). Cette infrastructure permet le raccordement d'abonnés d'une part, de fournisseurs d'accès Internet (FAI) d'autre part.

Aujourd'hui les clients ADSL ont le choix entre deux solutions : raccorder un poste isolé (Netissimo 1) ou raccorder des postes en réseau (Netissimo 2).

Le raccordement d'un poste isolé utilise :

– une interface Ethernet ou USB ;

– le protocole PPTP, PPP ou PPPoA.

Le raccordement de postes en réseau utilise :

– un routeur disposant d'une interface ATM côté modem et d'une carte Ethernet côté réseau local ;

– des postes en réseau.

Le routeur doit supporter :

– le protocole PPTP ou PPPoE ;

– les authentifications PAP et CHAP[1] ;

– la connexion ATM sur le couple VPI/VCI 2/32 ;

– la translation d'adresse (*Network Adress Tranlation*).

En 2003, les débits (montant-descendant) proposés par Netissimo sont de 128 Kb/s – 512 Kb/s pour Netissimo 1 et 256 Kb/s – 1 Mb/s pour Netissimo 2.

1. Cf. paragraphe 9.5 de l'ouvrage *Transmissions et Réseaux*.

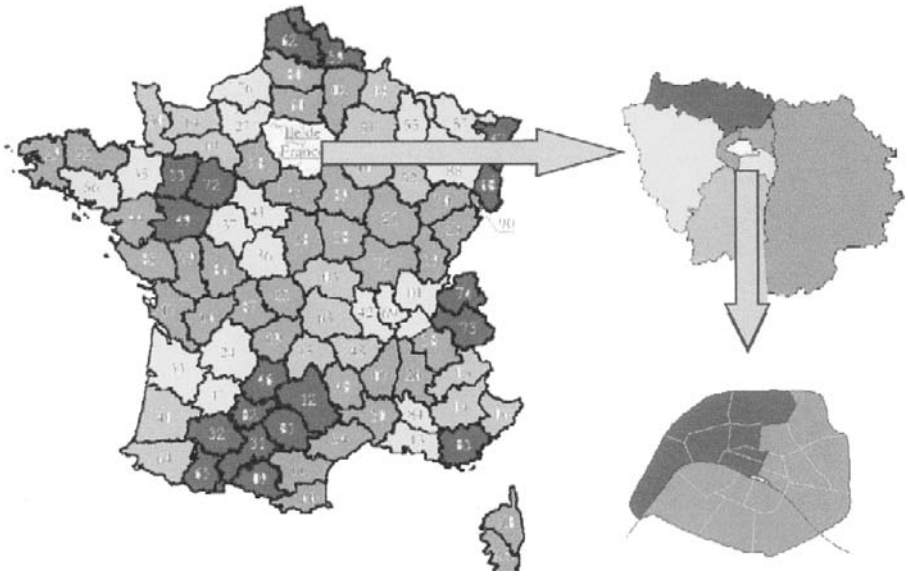

Figure 2.17 Les plaques ADSL.

Pour offrir des accès Internet aux clients ADSL d'une plaque, un fournisseur d'accès Internet doit raccorder ses équipements à un routeur de cette plaque. Il dispose pour cela du service Collecte IP/ADSL de France Télécom. La connexion utilise deux circuits virtuels ATM assurant une bande passante de 2 Mb/s, 34 Mb/s ou 155 Mb/s avec un débit garanti. La gestion des flux de service permettant le respect des performances utilise un serveur de type RADIUS. Le tableau 2.1 donne le nombre de clients ADSL pouvant être connectés sur chaque type de connexion IP/ADSL.

Tableau 2.1 Débits autorisés sur une connexion IP/ADSL.

Débit	D1	D2	D1 + D2
2 Mb/s	K*500 Kb/s	K*500 Kb/s	< 1,5 Mb/s
34 Mb/s	K*500 Kb/s	> 1 Mb/s	< 17 Mb/s
155 Mb/s	K*500 Kb/s	> 1 Mb/s	< 75 Mb/s

D1 : bande passante pour les utilisateurs Netissimo 1
D2 : bande passante pour les utilisateurs Netissimo 2

Les tarifs des services de Collecte IP/ADSL se composent du coût du raccordement (ouverture de la ligne + location mensuelle) et de l'abonnement mensuel correspondant au débit souscrit (celui-ci peut être modifié chaque mois pour s'adapter à l'évolution du trafic du client). Les tableaux 2.2 et 2.3

donnent une idée des coûts du service de collecte IP/ADSL tels qu'ils se présentaient en janvier 2001. Aujourd'hui, la tarification est adaptée à chaque client (voir *collecte IP/ADSL* ou *EQUANT IP VPN* sur le site *www.entreprises.francetelecom.com)*.

Tableau 2.2 Coût du raccordement au service de Collecte IP/ADSL (janvier 2001).

Raccordement	Frais d'accès (k€)	Abonnement mensuel (k€/mois)
2 Mb/s	00,61	02,9 + 2,29(d – 10)
34 Mb/s	12,20	06,1 + 0,46(d – 10)
155 Mb/s	12,20	12,2 + 0,69(d – 10)

d : distance à vol d'oiseau du site du client au cœur de plaque

Tableau 2.3 Coût de la composante Bande Passante IP d'une liaison au service de Collecte IP/ADSL.

Débit souscrit	Abonnement mensuel (K€/mois)
0 à 2 Mb/s	0,46
2 à 8 Mb/s	0,43
8 à 16 Mb/s	0,40
16 à 34 Mb/s	0,37
Au-delà de 34 Mb/s	0,34

Prix pour chaque tranche de 500 Kb/s

Le dialogue va donc s'établir entre les trois entités que sont le client, le fournisseur d'accès Internet et le fournisseur d'accès ADSL. Ce dernier doit établir la connexion entre les deux premiers.

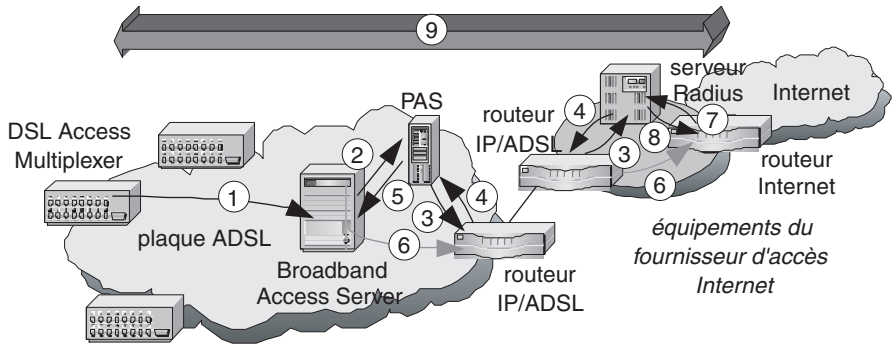

Figure 2.18 Établissement d'une connexion client-FAI à travers une plaque ADSL.

La figure 2.18 montre les phases d'établissement de la connexion :

1. Le client adresse une requête « client@fai.fr » par l'ouverture de sa connexion « accès réseau à distance » au fournisseur d'accès Internet.

2. Le BAS envoie une requête « access-request : client@fai.fr » à la Plate-forme d'Accès aux Services (PAS).

3. Le PAS transmet la requête au serveur Radius pour authentifier le client.

4. Le serveur Radius retourne en réponse le type de tunnel à établir « access-accept : tunnel type=L2TP ; tunnel medium type=IP ».

5. Le PAS retransmet la réponse au BAS.

6. Le BAS établit un tunnel L2TP avec les routeurs du FAI.

7. Le routeur d'accès Internet du FAI adresse une requête « access-request : client@fai.fr » au serveur Radius pour authentification.

8. Le serveur radius envoie en réponse le protocole de trame utilisé et l'adresse IP du client « access-accept : frame protocol=PPP ; service type= framed ; framed IP-adress=Y.Y.Y.Y ».

9. Une connexion PPP est établie entre le client et le routeur d'accès Internet du FAI.

Chapitre **3**

TCP/IP pour le routage et la qualité de service, PPP vers le client

3.1 CLASSIFICATION OSI

À l'origine, les protocoles TCP/IP font partie de la hiérarchie des protocoles ARPA (*Advanced Research Project Agency*), sous l'égide du DOD (*Department Of Defense*) aux États-Unis. Ils sont présents dans toutes les implantations du système d'exploitation UNIX et constituent des protocoles de référence pour l'interconnexion des réseaux locaux et des réseaux longue distance. Ils sont notamment utilisés en standard par les systèmes d'exploitation réseau *Windows* et *Netware* ainsi qu'à l'échelle mondiale par le réseau Internet.

Les protocoles TCP et IP servent de base à une famille de protocoles de niveau supérieur définis dans les RFC (*Requests For Comments*, demandes de commentaires), documents publiés par des organismes spécialisés. Chaque protocole ou procédure lié à TCP/IP fait l'objet d'une RFC référencée : RFC 791 pour IP, RFC 854 pour Telnet... Ces protocoles sont antérieurs aux travaux de normalisation de l'OSI, mais une correspondance est généralement admise (tableau 3.1).

Aux niveaux 1 et 2, se trouvent les protocoles liés aux architectures Ethernet, Arpanet ou autres. Les identifiants des sous-couches MAC et LLC peuvent prendre deux valeurs distinctes suivant l'architecture utilisée (figure 3.1).

Pour une architecture type 802.3, les champs DSAP et SSAP de la sous-couche LLC prennent la valeur 06_H pour indiquer le protocole IP au niveau supérieur.

Pour une architecture type Ethernet II, la sous-couche LLC n'existe pas, le protocole IP est indiqué directement dans le champ longueur de la sous-couche MAC par la valeur 0800_H.

Tableau 3.1 Architectures DOD et OSI des protocoles TCP/IP.

DOD							OSI
Process	Telnet	FTP	NFS	SMTP	SNMP	HTTP	**Niveaux 5, 6 et 7**
		RPC			XDR		
Host to Host		**TCP**			UDP		**Niveau 4**
Internet	ICMP	RIP	**IP**	ARP		RARP	**Niveau 3**
Network Access	Ethernet	FDDI	Arpanet	SLIP		**PPP**	**Niveaux 1 et 2**

Les procédures **SLIP** (*Serial Line Internet Protocol*) et **PPP** (*Point to Point Protocol*) sont des cas particuliers permettant d'adapter le réseau ou le poste de travail à une communication série asynchrone par l'intermédiaire d'un modem avec un serveur distant (cas du réseau Internet).

MAC				**LLC**		**IP**
Adr. Dest.	Adr. Src.	Longueur	DSAP=06_H	SSAP=06_H	Contrôle	

MAC			**IP**
Adr. Dest.	Adr. Src.	0800_H	

Figure 3.1 Trames Ethernet liées à IP.

Au niveau 3, se trouve l'implantation du protocole IP (*Internet protocol*). Ce protocole, en mode datagramme, va offrir les fonctions de routage. L'interconnexion entre deux machines situées n'importe où sur le réseau est possible. Le protocole IP gère également la fragmentation des données. La couche 3 contient quatre autres protocoles :

– **ARP** (*Address Resolution Protocol*) permet de faire la correspondance entre les adresses logiques (Internet) et les adresses physiques (MAC). Ce protocole permet de masquer les adresses nécessaires à l'acheminement des trames de niveau MAC. En effet, si une adresse IP permet d'envoyer des données à une machine quelconque sur le réseau, les adresses physiques n'ont que la portée du réseau local. Les adresses MAC sont aussi par construction uniques (numéro du constructeur, numéro de fabrication), mais leur allocation peut être vue comme aléatoire sur le réseau. Les adresses IP sont, elles, logiquement distribuées. Il est donc plus simple pour l'administrateur réseau de référencer ces machines avec une adresse IP. Les mécanismes ARP permettent de faire la recherche de l'adresse MAC correspondante.
– **RARP** (*Reverse Address Resolution Protocol*) permet d'établir la correspondance entre les adresses physiques (MAC) et les adresses logiques (Internet). Ce protocole peut être utile, par exemple, lorsqu'une station sans disque veut connaître, au

démarrage, son adresse Internet à partir de la seule information dont elle dispose, c'est-à-dire de l'adresse MAC qu'elle peut lire sur son coupleur.
– **ICMP** (*Internet Control Message Protocol*) n'est pas à proprement parlé un protocole de niveau 3, puisqu'il utilise l'encapsulation IP. Mais il sert à la gestion du protocole IP. Il permet, par exemple, de collecter les erreurs qui surviennent lors de l'émission de messages (réseau coupé, échéances temporelles...).
– **RIP** (*Routing Information Protocol*) est un protocole de routage utilisant le principe de la multidiffusion. Les routeurs utilisant RIP diffusent périodiquement leurs tables de routage aux autres routeurs du réseau.

Au niveau 4, se trouve le protocole **TCP** (*Transmission Control Protocol*) qui offre aux utilisateurs un transfert fiable sur connexion et le protocole **UDP** (*User Datagramme Protocol*) qui offre un transfert en mode datagramme.

Au niveau 5, se trouvent les routines de base des **RPC** (*Remote Procedure Call*) qui permettent de cacher aux couches supérieures les accès au réseau en utilisant la sémantique des appels de fonctions. Ces routines se trouvent dans des bibliothèques liées aux programmes d'application au moment de la compilation.

Les procédures **XDR** (*eXternal Data Representation*) de la **couche 6** permettent de rendre universelle la représentation des données et de s'affranchir des codages et de la structuration des données proposée par les différents constructeurs.

Le niveau 7 regroupe les différentes applications courantes dans le monde UNIX :
– Telnet (*Terminal Emulation Protocol*) pour la connexion et l'émulation de terminal ;
– FTP (*File transfert Protocol*) pour le transfert de fichiers ;
– NFS (*Network File Server*) pour la gestion de fichiers ;
– SNMP (*Simple Network Management Protocol*) pour l'administration et la gestion des machines du réseau ;
– SMTP (*Simple Mail Transfert Protocol*) pour les services de courrier électronique ;
– HTTP (*HyperText Transmission Protocol*) pour des recherches d'informations en mode hypertexte.

3.2 LE PROTOCOLE IP (*Internet Protocol*)

3.2.1 Fonctionnalités du protocole IP

Le protocole Internet est un protocole de niveau réseau. Il est responsable de :
– la transmission des données en mode sans connexion ;
– l'adressage et le routage des paquets entre stations par l'intermédiaire de routeurs ;
– la fragmentation des données.

Lors de l'émission, les fonctionnalités assurées sont :
– identification du paquet ;
– détermination de la route à suivre (routage) ;
– vérification du type d'adressage (station ou diffusion) ;

– fragmentation de la trame si nécessaire.

À la réception, les fonctionnalités sont :

– vérification de la longueur du paquet ;
– contrôle des erreurs ;
– réassemblage en cas de fragmentation ;
– transmission du paquet réassemblé au niveau supérieur.

3.2.2 Format du paquet

Le paquet IP, ou datagramme IP, est organisé en champs de 32 bits (figure 3.2).

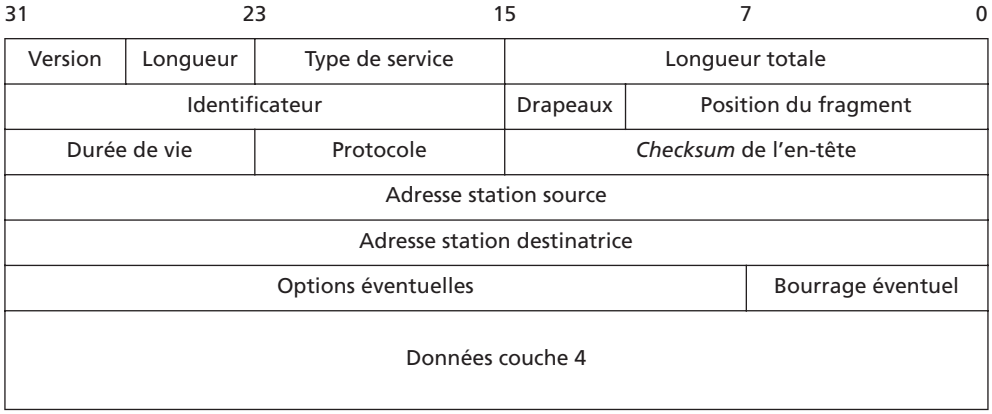

Figure 3.2 Format du paquet IP.

Les fonctionnalités IP se retrouvent dans chaque groupement de bits de l'en-tête :

– **Version** : numéro de version du protocole IP (actuellement 4).
– **Longueur** : longueur de l'en-tête codée sur 4 bits et représentant le nombre de mots de 32 bits (généralement 5).
– **Type de service** (TOS) : désigne la qualité de service qui doit être utilisée par le routeur. Par exemple, pour un transfert de fichier important, il est préférable de privilégier le débit par rapport au délai de transmission. Pour une session interactive, le délai de propagation sera primordial.
– **Longueur totale** : longueur totale du fragment (en-tête et données) exprimée en nombre d'octets.
– **Identificateur** : identifie le paquet pour la fragmentation (tous les fragments d'un même paquet portent le même numéro).
– **Drapeaux** : gère la fragmentation sur 3 bits suivant le format :
  – DF MF ;
  – le bit DF (*Don't Fragment*) demande au routeur de ne pas fragmenter le paquet ;
  – le bit MF (*More Fragment*) est positionné à 1 dans tous les fragments, sauf le dernier.

– **Position du fragment** : indique par multiple de 8 octets la position du fragment dans le paquet courant. Tous les fragments du paquet, sauf le dernier, doivent donc avoir pour longueur des multiples de 8 octets. Avec un codage sur 13 bits, le maximum pour un paquet est de 8 192 fragments.
– **Durée de vie** (TTL, *Time to live*) : indique en nombre de sauts le temps pendant lequel un paquet peut rester dans le système. Si ce champ contient la valeur 0, alors le paquet doit être détruit. Sa valeur est décrémentée à chaque passage dans un routeur même si le temps de traitement est inférieur à une seconde. La valeur par défaut est de 32, 64, 128 ou 256 suivant l'importance du réseau.
– **Protocole** : numéro du SAP destinataire du paquet, indique le protocole de la couche supérieure (1 pour ICMP, 6 pour TCP, 17 pour UDP).
– **Options** : utilisées pour le contrôle ou la mise au point.

3.2.3 L'adressage Internet

Chaque machine susceptible d'être connectée à l'extérieur de son réseau local possède une adresse IP en principe unique. Le réseau Internet, qui tient son nom du protocole utilisé, correspond à l'interconnexion de plusieurs millions d'ordinateurs à l'échelle mondiale et la gestion des adresses est bien entendu de toute première importance.

Une autorité internationale le NIC (*Network Information Center*) attribue des numéros à chaque réseau. Les adresses codées sur 32 bits comportent deux parties : le numéro de réseau (*Net_id*) et le numéro de la machine sur le réseau (*Host_id*). Le NIC n'alloue que les numéros de réseau. L'affectation des numéros complets est à la charge des administrateurs réseaux. Suivant l'importance du réseau, plusieurs classes d'adressage sont possibles (figure 3.3).

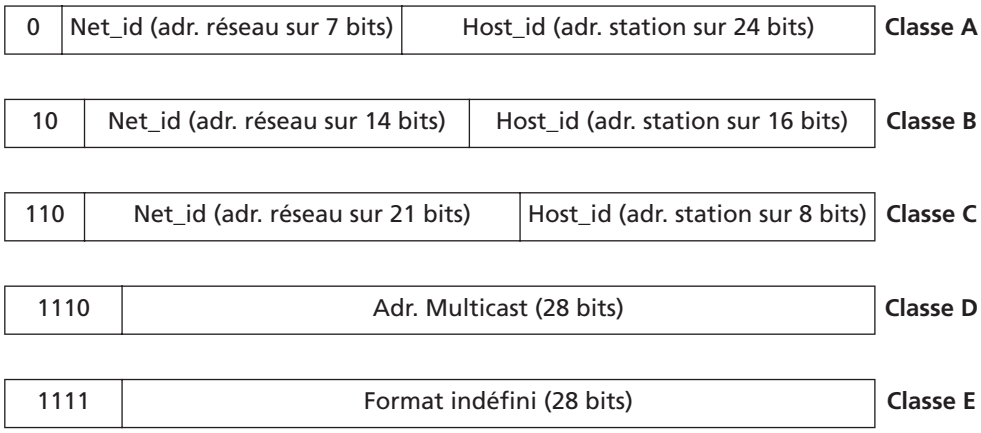

Figure 3.3 Format des adresses IP.

Les adresses sur 32 bits sont exprimées par octet (soit quatre nombres compris entre 0 et 255) notées en décimal et séparés par des points : 137.15.223.2.

Les différentes classes d'adresses correspondent donc à des nombres appartenant aux plages suivantes :

– classe A : 1.0.0.0 à 126.0.0.0, soit 126 réseaux ($2^{8-1} - 2$) et 16 777 214 machines par réseau ($2^{32-8} - 2$) ;
– classe B : 128.1.0.0 à 191.254.0.0, soit 16 382 réseaux ($2^{16-2} - 2$) et 65 535 machines par réseau ($2^{32-16} - 2$) ;
– classe C : 192.0.1.0 à 223.255.254.0, soit 2 097 150 réseaux ($2^{24-3} - 2$) et 254 machines par réseau ($2^{32-24} - 2$) ;
– classe D : 224.0.0.1 à 239.255.255.255, soit 268 435 455 adresses de groupe ($2^{32-4} - 1$) ;
– classe E : 240.0.0.0 à 255.255.255.254.

La classe A représente donc les réseaux de grande envergure (ministère de la défense, réseaux d'IBM, AT&T, DEC...) dont la plupart se trouvent aux États-Unis. **La classe B** désigne les réseaux moyens (universités, centres de recherches...).

La **classe C** représente les petits réseaux régionaux, les PME/PMI et en règle générale les sites comprenant moins de 254 machines.

Les adresses de **classe D** ne désignent pas une machine particulière sur le réseau, mais un ensemble de machines voulant partager la même adresse et ainsi participer à un même groupe : adresses de groupe de diffusion (*multicast*). Ces adresses sont choisies arbitrairement par les concepteurs des applications concernées (News, multimédia...).

Les autres adresses sont particulières ou réservées :

– l'adresse dont la partie basse est constituée de bits à 0 est une adresse réseau ou sous-réseau, 212.92.27.0 pour une classe C par exemple ;
– l'adresse dont la partie basse est constituée de bits à 1 est une adresse de diffusion (*broadcast*), 157.42.255.255 pour une classe B par exemple ;
– 127.0.0.1 est une adresse de bouclage (*localhost, loopback*) et permet l'utilisation interne de TCP/IP sans aucune interface matérielle ;
– 0.0.0.0 est une adresse non encore connue, utilisée par les machines ne connaissant pas leur adresse IP au démarrage ;
– pour chaque classe, certaines plages d'adresses sont réservées à un usage privé. Ces adresses ne sont pas gérées par les routeurs des réseaux Internet : 10.0.0.0, 172.16.0.0 à 172.31.0.0, 192.168.0.0. à 192.168.255.0.
– la partie basse de l'espace d'adressage de la classe C est divisée en 8 plages d'adresses affectées à des régions du monde :

192.0.0 – 193.255.255.255	Inter-régions
194.0.0.0 – 195.255.255.255	Europe
196.0.0.0 – 197.255.255.255	Autres régions
198.0.0.0 – 199.255.255.255	Amérique du Nord
200.0.0.0 – 201.255.255.255	Amérique du Sud et Amérique Centrale
202.0.0.0 – 203.255.255.255	Pacifique
204.0.0.0 – 205.255.255.255	Autres régions
206.0.0.0 – 207.255.255.255	Autres régions

3.3 GESTION DES ADRESSES ET ROUTAGE SUR INTERNET

3.3.1 Adapter la gestion des adresses aux besoins

Le nombre d'attributions d'adresses IP a suivi ces dernières années une croissance presque exponentielle, ce qui a conduit à une saturation. Une nouvelle norme IPv6 est en voie de remplacer la version 4 actuelle du protocole IP et offrira un codage des adresses sur 128 bits. En attendant la généralisation de cette version de IP, deux techniques ont été mises au point :

– la division des classes d'adressage en blocs plus petits (*Classless InterDomain Routing* – CIDR – RFC 1518 et 1519) ;
– la translation d'adresse (*Network Address Translation* – NAT – RFC 1631).

a) La division des classes d'adressage

L'utilisation des classes d'adresses laisse de nombreuses adresses inutilisées. Par exemple, une organisation demandant 1 000 adresses IP se verra attribuer une adresse de classe B, soit environ 64 000 adresses (une classe C avec près de 256 adresses est insuffisante).

Les tailles des masques[1] correspondant à un réseau, ont été adaptées à la demande des utilisateurs. Dans l'exemple donné l'organisation pourra se voir attribuer la plage 195.162.0.0 – 195.162.3.255 qui offre près de 1 024 adresses. Ce réseau sera représenté dans les tables des routeurs par l'adresse 195.162.0.0/22 où « 22 » correspond au nombre de bits à utiliser pour le masque de routage (255.255.252.0).

Il est également possible de diviser les blocs d'adresses de classe C en blocs plus petits que les 256 adresses initiales. Si une organisation a besoin de 80 adresses IP, il est possible de lui attribuer la zone d'adresses 200.154.210.0 – 200.154.210.126. Cette plage sera représentée par l'adresse 200.154.210.0/25, soit un masque de routage 255.255.255.128. Cette classe d'adresses pourra ainsi être attribuée à plusieurs clients.

b) La translation d'adresse

Cette technique est utilisable par un organisme qui ne peut obtenir une plage d'adresses suffisante pour toutes ses machines. Elle s'appuie sur la remarque que toutes les machines n'accèdent pas à Internet simultanément. Le routeur d'accès à l'opérateur Internet attribuera les adresses de manière dynamique au fur et à mesure des demandes. Prenons le cas d'une entreprise disposant de 400 postes clients et se voyant attribuer une plage d'adresses de classe C. la solution consiste à utiliser un adressage IP de classe privée dans l'entreprise (non reconnues par Internet) et de charger le routeur d'accès à Internet de remplacer l'adresse privée du poste demandant l'accès à Internet par une adresse de classe C. Bien sûr, seuls 250 postes environ pourront accéder à Internet simultanément.

1. Cf. paragraphe 7.2.2 de l'ouvrage *Transmissions et Réseaux*.

Cette technique offre également une protection des postes de l'entreprise contre des tentatives de piratage venant d'Internet.

3.3.2 Le routage sur Internet

a) Le routage IP sur réseau maillé

Le routage IP utilise des tables de routage pour trouver le chemin des paquets entre la source et la destination[1]. Le réseau Internet étant de type maillé, il existe plusieurs chemins possibles pour une même destination (figure 3.4). A son arrivée sur un routeur, le paquet est mis en mémoire en attendant d'être routé. Lorsque le débit entrant d'un routeur amène la saturation de sa mémoire, le routeur en amont doit trouver un autre chemin pour les paquets (le routeur ne peut retenir les paquets sortants au risque de bloquer tous les paquets en attente d'émission).

Dans l'exemple (a) de la figure 3.4, la saturation de la mémoire du routeur R2 oblige le routeur R4 à trouver un nouveau chemin pour les paquets. Ceux-ci traverseront les routeurs R4, R1, R3 et R5.

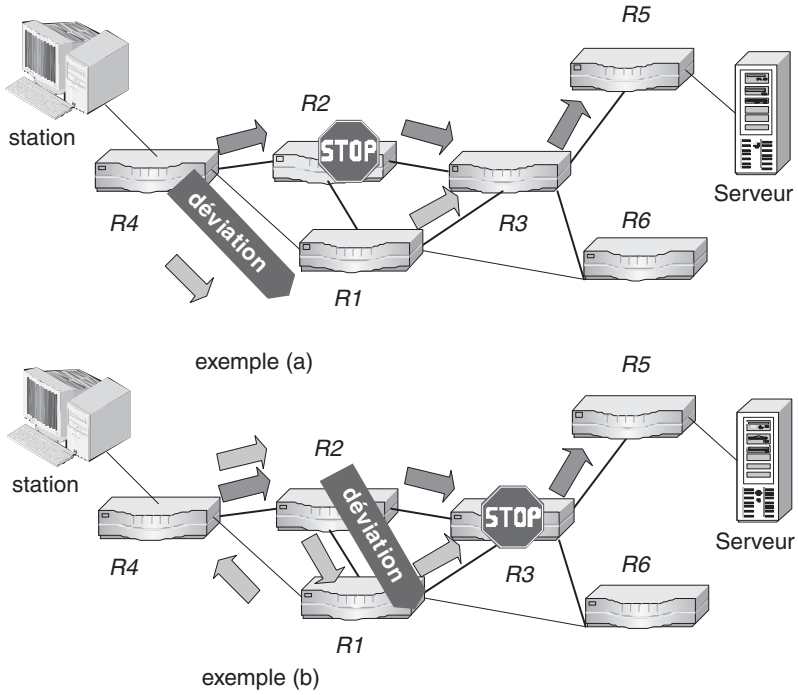

Figure 3.4 Routage des paquets IP dans un réseau maillé.

1. Cf. paragraphe 7.3 de l'ouvrage *Transmissions et Réseaux*.

L'exemple (b) est plus critique. La saturation de la mémoire du routeur R3 entraîne le re-routage des paquets. Le routeur R2, informé par le routeur R3 qu'il ne peut lui adresser de paquet (protocole RIP), va envoyer les paquets vers le routeur R1. Celui-ci, informé également par R3, va envoyer les paquets vers R4. Ceux-ci vont donc tourner entre les routeurs R2, R1 et R4, sans jamais atteindre leur destination, encombrant ainsi le trafic « normal ». Pour éliminer ces paquets, le compteur du champ « durée de vie » de l'en-tête IP (figure 3.2) est décrémenté à chaque traversée de routeur. À son passage à zéro, le paquet est détruit par le routeur.

Internet étant constitué d'interconnexions de réseaux d'opérateurs, le problème du routage se présente sous deux aspects (figure 3.5) :

– le routage à l'intérieur de leur propre réseau ;
– le routage d'interconnexion avec les autres réseaux d'opérateurs.

Ces deux types de routage font appel à des protocoles spécifiques :

– les protocoles de routage interne (*Interior Gateway Protocols*) tels que RIP (*Routing Information Protocol*) et OSPF (Open Short Path First) ;
– les protocoles de routage externe comme EGP (*Exterior Gateway Protocols*) ou BGP (*Border Gateway Protocol*).

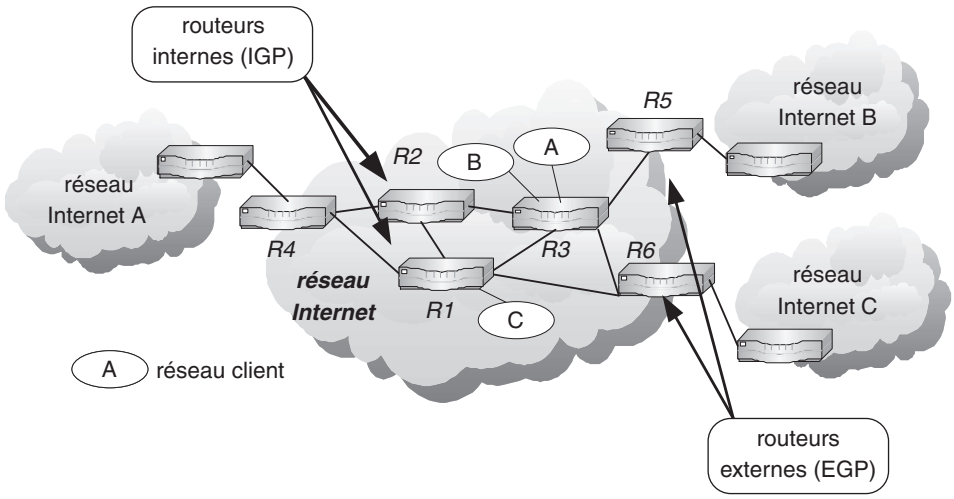

Figure 3.5 Organisation des routeurs d'un opérateur Internet.

b) Routage interne

Le protocole RIP (RFC 1058 et RFC 1723) utilise un algorithme de routage de type vecteur de distance. Les tables de routage indiquent pour chaque réseau client, le chemin optimal et la distance. Le tableau 3.2 montre le contenu de la table de routage du routeur R3 (distances : R3-R2=3 ;R1-R4=4 ;R1-R2=5 ;R3-R6=3 ; autres=1) de la figure 3.5.

Tableau 3.2 Table de routage d'un protocole RIP.

Réseau client	Routeur voisin	Distance
A	=	1
B	=	1
C	R1	2
Internet A	R2	5
Internet B	R5	2
Internet C	R6	4

Très facile à implémenter, cet algorithme présente des inconvénients :

– si plusieurs chemins existent pour un même client, la convergence (élimination des chemins pour obtenir un chemin unique) de l'algorithme peut être lente voire infinie (ex. : 4 chemins de R3 à R4 + une boucle R3-R2-R1 – figure 3.5) ;

– la taille des tables augmente rapidement avec le nombre de routeurs ;

– les routeurs échangent le contenu de leur table de routage toutes les 30 secondes par des messages de diffusion (*broadcast*).

Le protocole OSPF (RFC 2328) utilise un algorithme de routage basé sur la connaissance de l'état des liaisons entre routeurs (*Link State*). Les routeurs maintiennent une carte du réseau et testent régulièrement l'état des liaisons avec les routeurs voisins. Comme dans RIP, le calcul des chemins est local. Si l'on reprend l'exemple présenté sur la figure 3.5, avec des distances égales à 1, sauf pour R1-R2 = 5, R1-R4 = 4, R3-R6 = R2-R3 = 3. La table de routage des routeurs contiendrait les informations suivantes (tableau 3.3).

Tableau 3.3 Table de l'état des liaisons d'un protocole OSPF.

Source	Destination	Distance	Source	Destination	Distance
R1	R2	5	R2	R1	5
R1	R3	1	R2	R3	3
R1	R4	4	R2	R4	1
R1	R6	1	R3	R1	1
R4	R1	4	R3	R2	3
R4	R2	1	R3	R5	1
R6	R3	3	R3	R6	3
R6	R1	1	R5	R3	1

Cette table est identique pour tous les routeurs. Elle sert à chacun d'eux de base de calcul du plus court chemin (*Shortest Path First*) pour l'accès aux réseaux clients. Si le réseau client A émet un paquet à destination d'un serveur situé sur le réseau Internet A, le routeur R3 va calculer le plus court chemin vers R4, parmi tous les chemins possibles (tableau 3.4).

TABLEAU 3.4 CALCUL DU PLUS COURT CHEMIN.

chemin	voisin	coût	chemin	voisin	coût
R2-R4	R2	4	R1-R4	R1	5
R2-R1-R4	R2	12	R1-R2-R4	R1	7
R6-R1-R4	R6	8	R6-R1-R2-R4	R6	10

Dans le cas où plusieurs chemins ont le même coût, le programme du routeur choisira un chemin suivant les règles implémentées par le constructeur. Les valeurs des distances peuvent être modifiées par l'administrateur du réseau afin de réguler les flux sur les liens. Cette méthode présente plusieurs avantages :

– seules les modifications de l'état des liens sont adressées aux routeurs ;
– les chemins ne sont plus échangés entre routeurs ;
– l'algorithme SPF converge plus rapidement.

c) Routage externe

Les protocoles de routage externe sont destinés aux échanges d'information de routage entre routeurs externes ou routeurs de bord. Le protocole EGP (RFC 904) est réservé aux routeurs reliés par une liaison unique. Les deux routeurs échangent leurs tables de routage périodiquement. Chaque routeur connaît ainsi les destinations accessibles par le réseau voisin.

Lorsqu'un routeur externe est relié à plusieurs routeurs externes, il utilise le protocole BGP-4 (RFC 1771). Dans la figure 3.6 les routeurs R4, R5 et R6 sont des voisins « internes », reliés par les routeurs internes du réseau de l'opérateur.

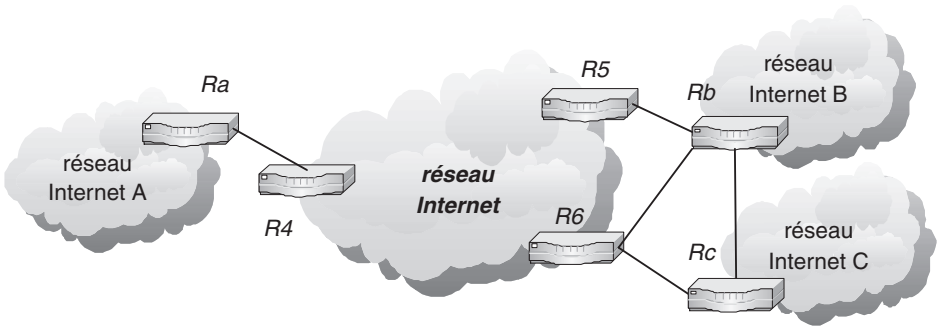

Figure 3.6 Interconnexion de réseaux d'opérateurs.

Le protocole BGP-4 utilise un algorithme de routage de type vecteur de distance. Les chemins multiples sont classés dans un ordre préférentiel. Seul le chemin ayant la préférence la plus élevée est transmis aux autres routeurs. Les messages sont échangés *via* le port 179 du protocole TCP. Le protocole BGP-4 supporte la division de classes (CIDR).

La taille de certains réseaux d'opérateurs nécessite de créer des sous-réseaux comportant leurs propres routeurs internes et externes. Ils constituent des systèmes autonomes de routage.

3.4 LES PROTOCOLES DE NIVEAU TRANSPORT : UDP ET TCP

Les protocoles de niveau transport sont chargés d'initialiser le dialogue avec les protocoles de même niveau du destinataire, à la demande des applications. Cette phase s'appelle l'ouverture de session. Elle est décrite dans la figure 3.7 :

1. Pour une application de type navigation, le navigateur demande l'ouverture d'une connexion sur le port 80 (ouverture de socket). Il fournit donc au protocole de niveau transport le numéro du protocole utilisé (port destination 80), l'adresse destination, le numéro de process local (port source) et l'adresse source.
2. Le protocole de niveau transport transmet une demande d'ouverture de connexion au protocole de niveau réseau. Il lui transmet les adresses sources et destination.
3. Le protocole de niveau réseau va transmettre sur le réseau Internet la demande de connexion au serveur.
4. Après un mécanisme similaire et une réponse positive du serveur, le protocole réseau informe le protocole de niveau transport de l'établissement de la connexion.
5. Le protocole de niveau transport initialise la connexion (dimensionnement des buffers, initialisation du numéro de séquence et de la régulation de flux).

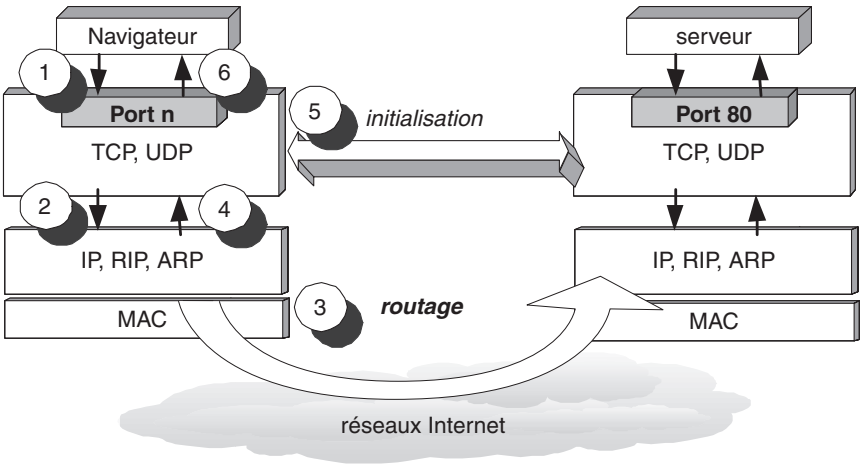

Figure 3.7 Ouverture de session.

6. Le protocole de niveau transport informe le navigateur que le dialogue avec le serveur est établi.

Les phases de cette procédure peuvent être suivies sur un navigateur Internet Explorer. Des messages s'affichent en bas et à gauche de la fenêtre du navigateur :

– à la phase 4 correspond le message « site web trouvé » ;
– à la phase 5 correspond le message « attente de réponse du site web » ;
– après la phase 6, le navigateur va charger la 1re page.

3.4.1 Le protocole UDP (*User Datagramme Protocol*)

UDP est un protocole sans connexion et permet à une application d'envoyer des messages à une autre application avec un minimum de fonctionnalités (pas de garanties d'arrivée, ni de contrôle de séquencement). Il n'apporte pas de fonctionnalités supplémentaires par rapport à IP et permet simplement de désigner les numéros de port correspondant aux applications envisagées avec des temps de réponse courts (figure 3.8).

Un message UDP est désigné dans un paquet IP par une valeur du champ protocole égal à 17.

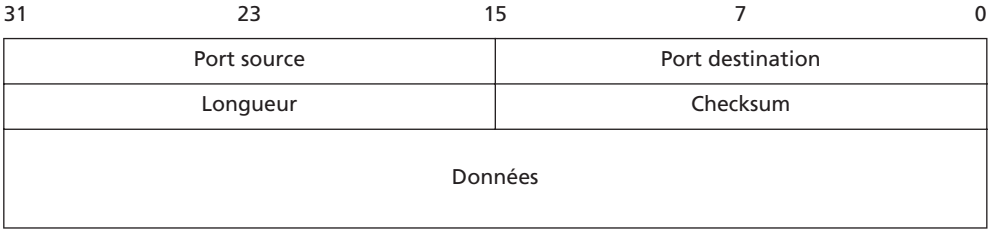

Figure 3.8 Format d'un message UDP.

Le **port source** et le **port destination** permettent de référencer les applications qui s'exécutent sur les machines locales et distantes. Les numéros de port des applications UNIX usuelles (*process*) sont donnés dans le tableau 3.5.

Les valeurs supérieures à 1 024 correspondent à des ports clients et sont affectées à la demande par la machine qui effectue une connexion TCP.

Tableau 3.5 Numéros de port UDP et TCP usuels.

N° de port	7	20	21	23	25	37	80	110	161
Process	Echo	FTP-data	FTP	Telnet	SMTP	Time	HTTP	POP3	SNMP

La **longueur** indique la longueur totale du message en octets (données et en-tête).

La **somme de contrôle** est calculée comme pour les paquets IP. Une somme à 0 indique qu'elle n'est pas gérée.

3.4.2 Le protocole TCP (*Transmission Control Protocol*)

Ce protocole de niveau transport recouvre globalement les fonctionnalités des communications de classe 4 avec connexion (normalisation ISO). Il est identifié par la valeur 6 dans le champ protocole du paquet IP. Ses principales caractéristiques sont :

– établissement et fermeture de la connexion virtuelle ;
– segmentation et réassemblage des données (S-PDU) ;
– acquittement des datagrammes reçus et retransmission sur absence d'acquittement (un reséquencement est effectué si la couche IP ne les délivre pas dans l'ordre) ;
– contrôle de flux ;
– multiplexage des données issues de plusieurs processus hôtes en un même segment ;
– gestion des priorités des données et de la sécurité de la communication.

a) Format des segments TCP

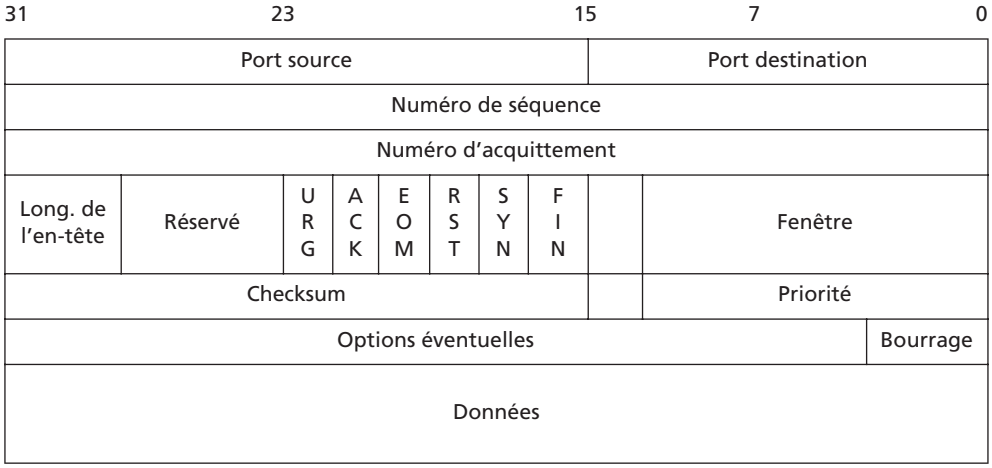

Figure 3.9 Format des segments TCP.

Les **numéros de port** permettent de référencer les applications (voir paragraphe 3.4.1, *Le protocole UDP*).

Le **numéro de séquence** indique le numéro du premier octet transmis dans le segment.

Le **numéro d'acquittement** contient le numéro de séquence du prochain octet attendu par le récepteur.

La **longueur de l'en-tête** est codée sur 4 bits et donne le nombre de mots de 32 bits.

Les **bits de contrôle** permettent de définir la fonction des messages ainsi que la validité de certains champs :

– URG = 1 si le champ des priorités est utilisé (pour des demandes d'interruption d'émission par exemple) ;
– ACK = 1 si la valeur du champ acquittement est significative ;
– EOM (ou PSH) indique une fin de message (*End of Message*), les données doivent être transmises (*pushed*) à la couche supérieure ;
– RST (*Reset*) : demande de réinitialisation de la connexion ;
– SYN : demande d'ouverture de connexion (les numéros de séquence doivent être synchronisés) ;
– FIN : fin de connexion.

Le champ **fenêtre** (*windows*) indique le nombre d'octets que le récepteur peut accepter à partir du numéro d'acquittement.

Le champ **checksum** correspond à une somme de contrôle de l'en-tête et du message.

Le champ **priorité** contient lors d'une interruption d'émission (URG=1) un pointeur sur les octets de données à traiter en priorité.

Le champ **options** permet de définir, par exemple, la taille maximale d'un segment.

b) Ouverture d'une connexion

Après autorisation locale sur chaque station et déclaration d'un identificateur permettant à l'application de référencer la connexion, la demande d'ouverture de connexion est transmise à la couche transport qui positionne son bit SYN à 1 (figure 3.10). Le numéro de séquence initial à l'émission (*Initial Send Sequence number*, ISS) est délivré, au moment de la demande, par un compteur incrémenté toutes les 4 ms (la taille du champ séquence étant de 32 bits, la période du compteur est supérieure à 4 heures). La station sollicitée répond avec les bits SYN et ACK à 1 et une dernière confirmation est effectuée par la station initiatrice avec le bit ACK à 1.

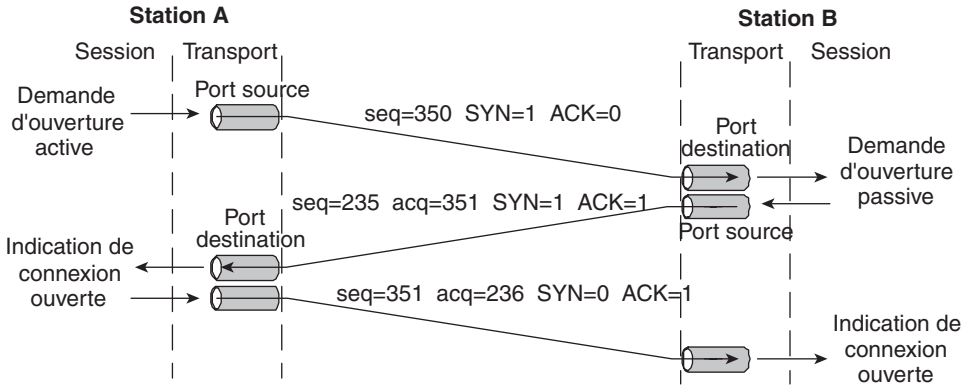

Figure 3.10 Exemple de connexion réussie.

c) Transfert de données

Le transfert de données peut alors commencer avec les numéros de séquence en cours (figure 3.11). Le contrôle de flux est réalisé dans les deux sens par les numéros d'acquittement (le bit ACK est alors positionné à 1). Chaque accusé de réception indique le nombre d'octets correctement reçus. La taille de la fenêtre de transmission sans acquittement (le nombre d'octets qu'il peut encore recevoir) est transmise par le destinataire lors de chaque acquittement en fonction de la place restante dans son tampon de réception. Lorsque l'émetteur n'a pas reçu d'acquittement après expiration d'un délai programmé, une retransmission des segments non acquittés est réalisée.

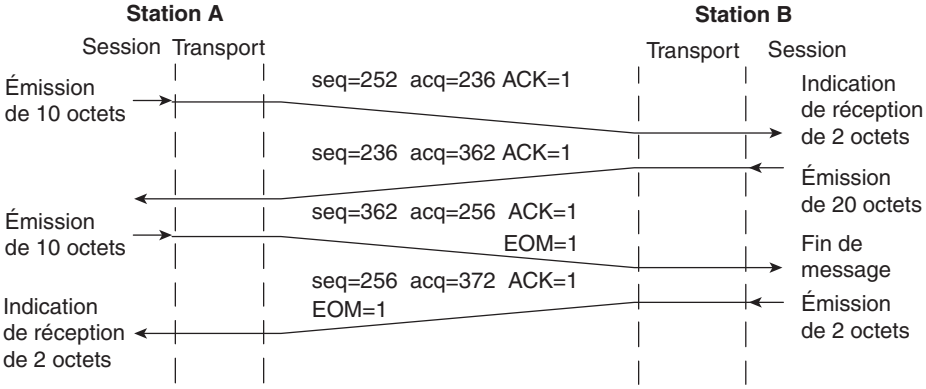

Figure 3.11 Exemple d'échange TCP.

d) Fermeture d'une connexion

La fermeture d'une connexion est réalisée lorsque le récepteur reçoit un en-tête TCP dont le bit FIN est positionné à 1 (figure 3.12). La demande est traitée dans les deux sens aux niveaux supérieurs avant acquittement.

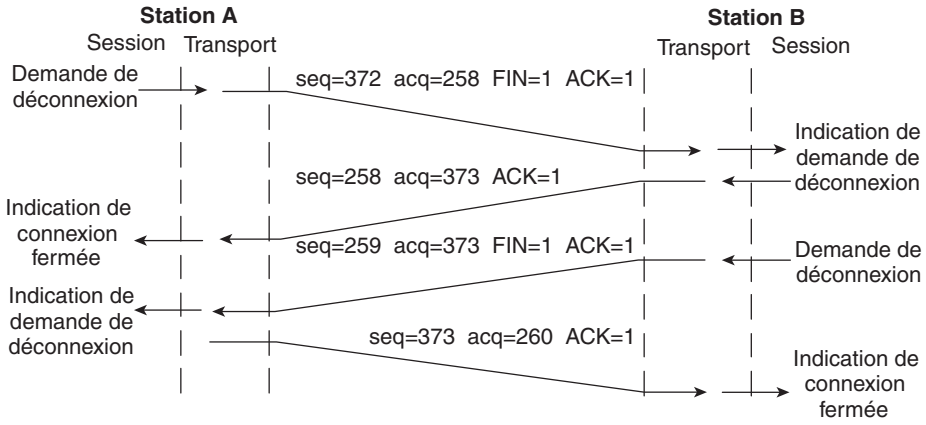

Figure 3.12 Exemple de fermeture réussie.

3.5 IP ET QUALITÉ DE SERVICE

3.5.1 Pourquoi de la qualité de service ?

Par un investissement massif dans le câblage optique des réseaux Internet, les opérateurs de transport ont contourné par le surdimensionnement l'épineux problème de la Qualité de Service (QoS) sur leurs réseaux. Les capacités en bande passante des fibres optiques permettaient la transmission des paquets IP sans ralentissement. Si l'on fait un parallèle avec les réseaux autoroutiers, le dimensionnement était largement supérieur au trafic de véhicules les empruntant. Ceux-ci n'étaient donc pas ralentis par des « bouchons » et la durée de leur trajet prévisible. Tout le monde sait que lorsque le trafic augmente, les retours de week-end ou de vacances par exemple, les bouchons ralentissent la vitesse des véhicules, et qu'il devient difficile voire impossible de prévoir la durée du trajet, ou les variations de celle-ci.

Après avoir répondu à la demande concernant l'information « texte » et « image fixe », Internet est confronté à une demande de plus en plus pressante d'informations de type voix ou vidéo. Les services de promotion des productions cinématographiques veulent diffuser des extraits de films et d'interviews d'acteurs ou de réalisateurs. Les entreprises souhaitent utiliser Internet pour leurs communications entre sites et réduire les coûts. Les sociétés d'organisation d'événements regardent du côté d'Internet pour la diffusion de concerts.

Sous la pression, les opérateurs cherchent parmi les solutions existantes, celles répondant le mieux à leurs contraintes. Celles-ci doivent prendre en compte le fait que l'information traverse plusieurs réseaux gérés par des opérateurs à statut privé. Les principales questions à résoudre sont :

– Quel intérêt pour mes abonnés peut apporter la mise en œuvre d'une qualité de service sur mon réseau, si les autres opérateurs ne la mettent pas en œuvre ?
– Puisqu'il est quasiment impossible que tous les opérateurs privés adoptent la même norme, quel protocole adopter sur mon réseau pour qu'il soit compatible avec le protocole adopté par les opérateurs voisins ?
– Quels sont les protocoles pouvant être mis en œuvre et quels paramètres permettent de mesurer les performances ?

3.5.2 Mesurer et garantir les performances

La transmission de son ou de vidéo implique que le destinataire dispose à intervalles réguliers des données pour reproduire le son à la fréquence de l'échantillonnage ou la vidéo au rythme de 25 images/seconde. Il faut définir des paramètres pour caractériser la qualité de la transmission des données :

– variation maximale entre cellules ou paquets (*peak-to-peak Cell Delay Variation* – CDV) ou gigue maximale ;
– temps de transfert maximum (*Maximum Cell Transfer Delay – Max* CTD) ;
– temps de transfert moyen (*Mean Cell Transfer Delay – Mean* CTD) ;
– taux de perte de cellules (*Cell Loss Ratio* – CLR).

Or ces paramètres vont varier notamment du fait de la variation des débits sur les liens (figure 3.13).

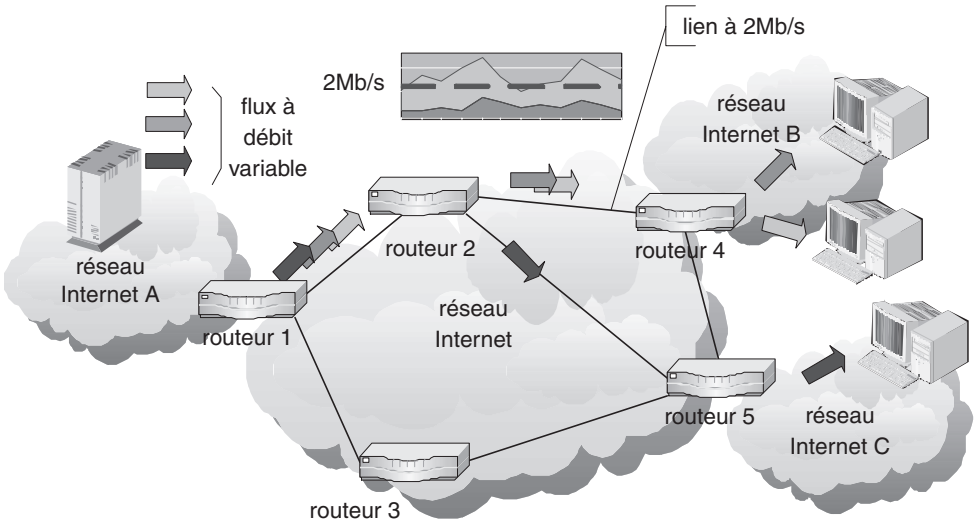

Figure 3.13 Variation des débits sur un lien d'un réseau d'opérateur Internet.

Les rafales peuvent amener le débit instantané à dépasser la bande passante du lien. Les paquets sont alors déroutés ou retardés, ce qui engendre de la gigue, ou encore détruits. Pour limiter ces inconvénients, il faut mettre en place des protocoles à plusieurs niveaux de l'architecture OSI :

– aux niveaux 1 et 2 avec des protocoles de transmission à performances garanties ;
– au niveau 3 avec des protocoles de routage réservant des ressources dans les routeurs ;
– aux niveaux 3 et 4 avec un protocole de signalisation contrôlant les performances et informant les équipements et les clients.

Aujourd'hui, les protocoles les plus avancés sont :

– Protocoles de transmission (niveaux 1 et 2) : ATM ; SDH ; Frame Relay ;
– Protocoles de routage (niveau 3) : IPv4 ; IPv6 ; ATM ;
– Protocoles de signalisation (niveau 4) :
  • Integrated Services – Intserv (RFC 1633) ;
  • Ressource reSerVation Protocol (RSVP) with Intserv (RFC 2210) ;
  • Guaranteed QoS in Intserv (RFC 2212) ;
  • Control Load QoS with Intserv (RFC 2211) ;
  • Differenciated services – DiffServ (RFC 2474) ;
– *MultiProtocol Label Switching* (MPLS) :
  • 4 classes de service (Platinium, Gold, Silver et Bronze) ;
  • ajout d'une étiquette aux paquets à l'entrée du réseau de l'opérateur ;
  • compatible avec Diffserv.

Pour assurer une qualité de service, il faut réguler le trafic à l'entrée du réseau de l'opérateur et dans les routeurs du réseau. Deux méthodes sont envisageables :

– l'écrêtage (*policing*) consiste à détruire les paquets lorsque le débit dépasse le seuil critique ;
– le lissage (*shaping*) consiste à stocker les paquets en excès et les transmettre lorsque le débit redevient inférieur au seuil critique.

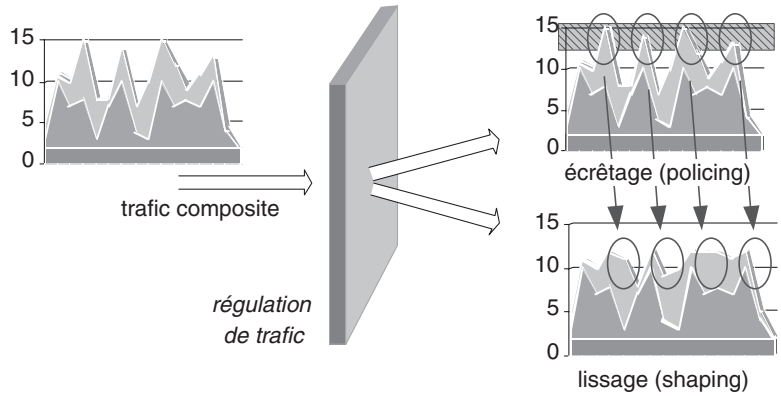

Figure 3.14 Régulation de flux par écrêtage et lissage.

La figure 3.14 montre que dans le cas d'un écrêtage, certains paquets seront détruits et le taux de perte augmentera. Dans le cas d'un lissage, certaines données sont retardées, leur latence sera donc augmentée. Les protocoles vont devoir décider quels paquets seront détruits ou retardés afin d'assurer le meilleur service aux clients. Il faut instaurer la notion de paquets plus prioritaires que d'autres, ou classes de services. Il faut également réserver dans les routeurs, des ressources capables de traiter les paquets suivant les règles définies.

3.5.3 Intserv s'appuie sur RSVP

Le protocole *Intserv,* en définissant une architecture de services intégrés, permet d'établir un mode « connecté » sur un réseau Internet. Il établit un chemin que suivront toutes les données de la connexion. Il va réserver dans les routeurs les ressources nécessaires en leur adressant des requêtes :

– *request PATH* pour trouver un chemin à travers le réseau ;
– *respons RESERVE* va indiquer que le routeur a les ressources nécessaires disponibles pour traiter les données de la connexion.

Chaque routeur concerné va créer une « machine d'état » pour le flux de données de la connexion (figure 3.15). Il utilisera les paramètres des protocoles *Real-time Transport Protocol* et *Real-Time Control Protocol* associé à TCP/IP pour gérer les données et faire connaître les performances obtenues aux clients et autres routeurs.

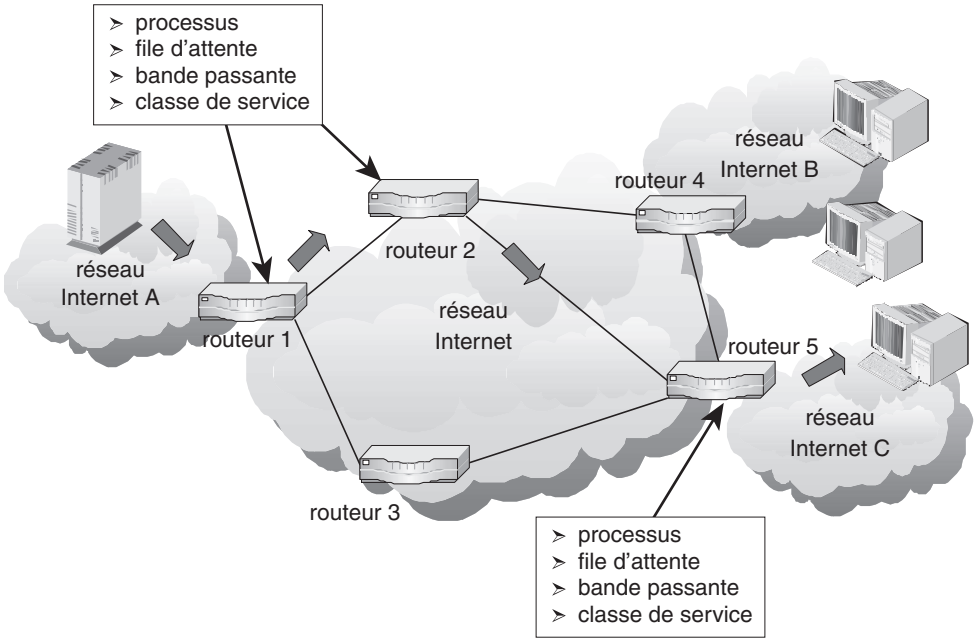

Figure 3.15 Inserv crée des « machines d'état » dans les routeurs traversés.

Le dialogue entre une application client « temps réel » et un serveur comporte trois phases (figure 3.16) :

1. Lors d'une demande de l'application client, le protocole RSVP envoie une requête aux routeurs du réseau pour réserver des ressources et créer un processus de gestion des flux.
2. Une fois la communication établie entre les deux applications, le serveur transmet les données en utilisant le protocole RTP.
3. Le protocole RTCP mesure les paramètres du flux de données reçues (gigue, temps moyen de transmission, taux de perte) et informe le serveur pour assurer une régulation du flux.

3.5.4 DiffServ définit quatre classes de trafic

À la différence du service intégré basé sur la réservation des ressources dans les routeurs, l'approche « services différenciés » cherche à mettre en place la QoS par un tri des paquets entrants à la frontière du réseau suivant différents critères (délai, bande passante, adresse…).

Les flux de données échangées entre les applications sont classés suivant deux catégories de service et quatre classes de trafic prédéfinies en fonction des performances demandées pour leur transmission. Les paquets sont « marqués » et gérés dans les routeurs par des files d'attente spécifiques à chaque catégorie ou classe.

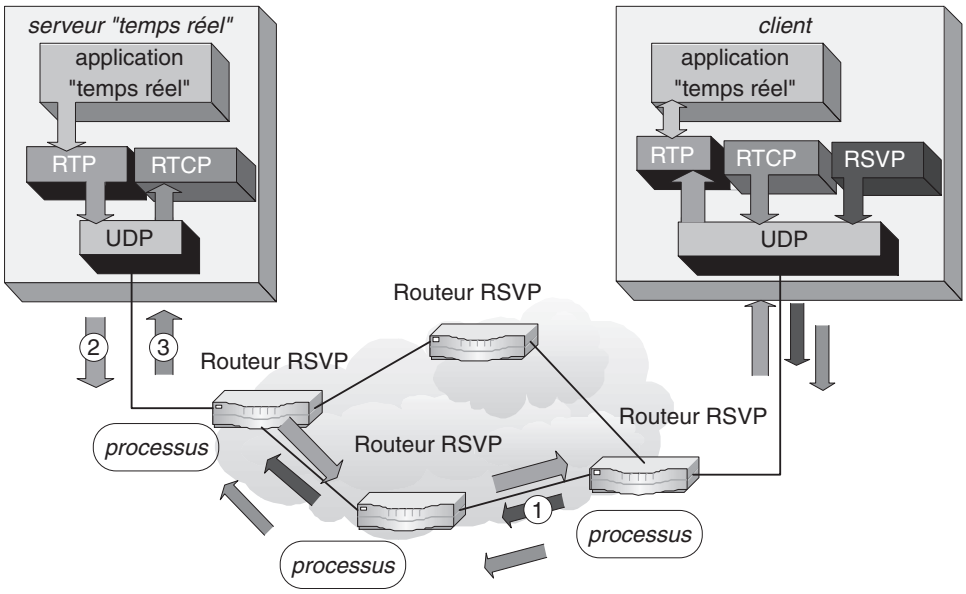

Figure 3.16 Dialogue entre application et serveur « temps réel ».

– Le premier service appelé parfois « premium » fournit un traitement accéléré (*Expedite Formarding* – EF) en assurant des garanties à tous les niveaux (débit, délai, taux de perte et gigue), ces garanties sont comparables à celles obtenues sur une ligne spécialisée et permettent des applications « temps réel ».
– Le deuxième service parfois appelé « olympic » assure l'acheminement des paquets (*Assured Forwarding* – AF) avec quatre classes de trafics différentes :
  • AF4 ou *platinium* cherche à réduire le délai de transmission des données ;
  • AF3 ou *gold* garantit un délai maximum et la délivrance des données au destinataire ;
  • AF2 ou *silver* garantit la délivrance des données sans garantir un délai de transmission ;
  • AF1 ou *bronze* offre un minimum de garanties en termes de délai ou d'erreurs.

Pour chacune de ces classes, les constructeurs implémentent dans les routeurs des règles de gestion des données dans les files d'attente. IP utilise l'octet « ToS » de l'en-tête pour indiquer la classe de trafic des données. Chaque classe peut utiliser trois niveaux de priorité (figure 3.17).

Les règles implémentées donneront une transmission prioritaire des paquets de type *premium*, par rapport aux paquets des autres classes. Ces paquets constituent une classe particulière (classe de trafic : 101) à laquelle est associée la priorité la plus haute (priorité : 110). En cas de congestion dans les files d'attente d'un routeur (manque de place en mémoire) ce sont les paquets de classe *bronze* qui seront détruits les premiers.

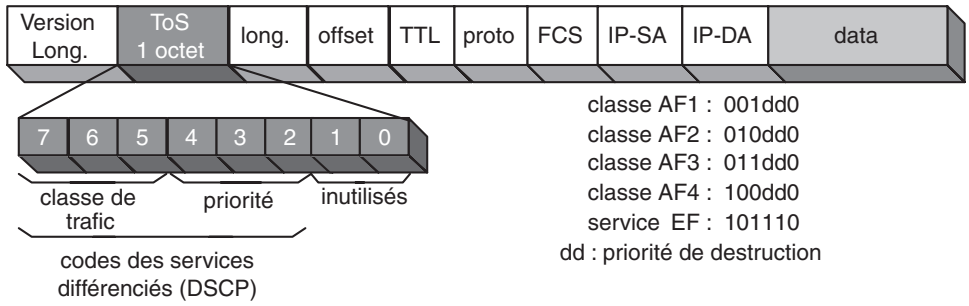

Figure 3.17 Classification des paquets dans l'en-tête IP.

Notons que lorsque le champ ToS n'est pas utilisé (tous les bits sont à 0), aucune qualité n'est demandée et l'on retrouve le fonctionnement par défaut de l'Internet du type « effort maximum » ou « best effort ».

L'absence de signalisation permet à chaque opérateur de gérer la QoS dans son réseau, indépendamment des réseaux des autres opérateurs. Le protocole MPLS est souvent utilisé par les opérateurs pour la mise en œuvre du protocole DiffServ dans leur réseau.

3.5.5 MPLS : une question d'étiquette

Un réseau d'opérateur de transport Internet comporte deux types de routeurs ou commutateurs (figure 3.18). Les routeurs de bordure (*Label Edge Routers*) traitent les paquets en provenance de réseaux d'autres opérateurs, les routeurs centraux (*Core Routers*) gèrent les paquets à l'intérieur du réseau de l'opérateur.

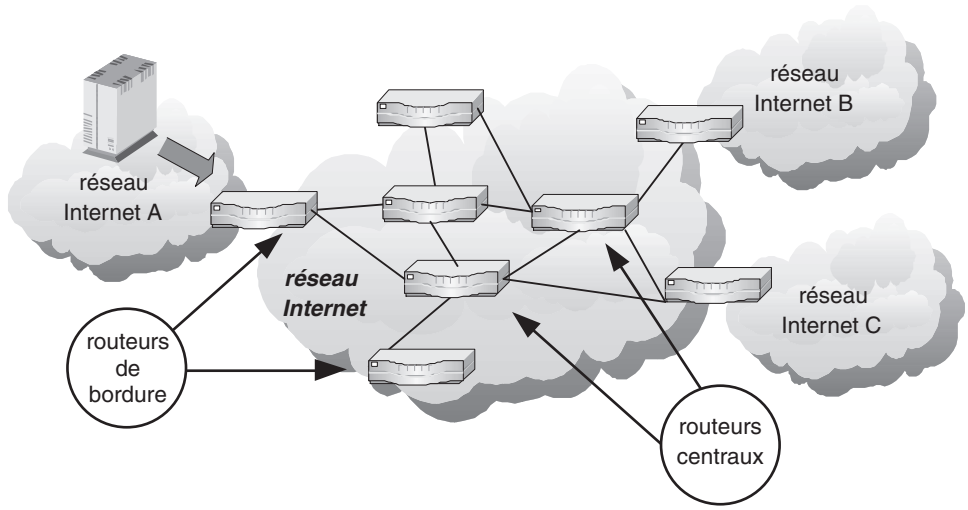

Figure 3.18 Organisation des routeurs dans un réseau d'opérateur.

À l'entrée sur le réseau d'un opérateur, chaque paquet se voit adjoindre une étiquette par le routeur de bordure. Le traitement des paquets dans les routeurs et commutateurs centraux va tenir compte des valeurs contenues dans cette étiquette.

La classe AF1 de DiffServ correspond à la classe bronze de MPLS, la classe EF correspond à la classe platinium. La classe et la priorité des paquets de l'en-tête MPLS sont déduites de l'en-tête IPv4 par copie des bits du champ ToS (figure 3.19).

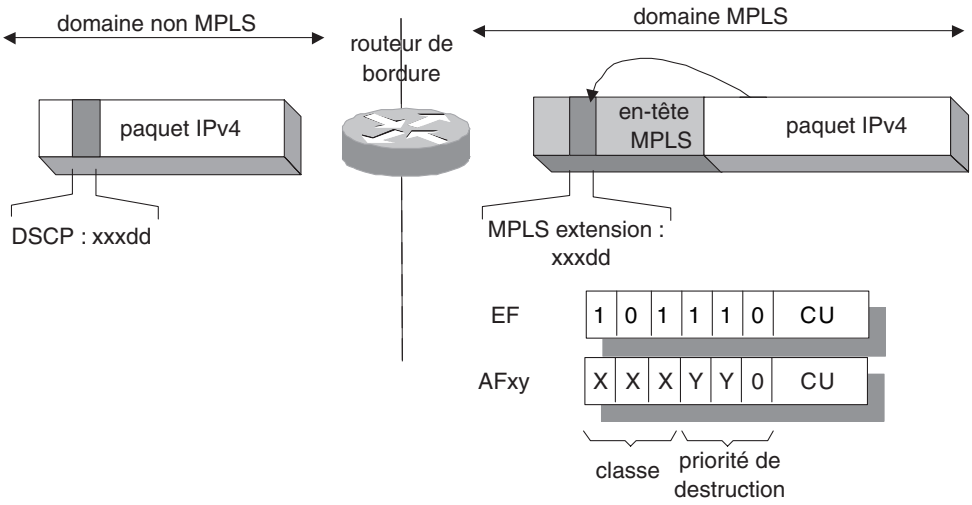

Figure 3.19 Classe et priorité dans l'en-tête MPLS.

Le routeur de bordure est également chargé de réguler le débit d'entrée sur le réseau MPLS. En cas de saturation des liens d'entrée ou de saturation de ses files d'attente, il détruira les paquets les moins prioritaires (figure 3.20).

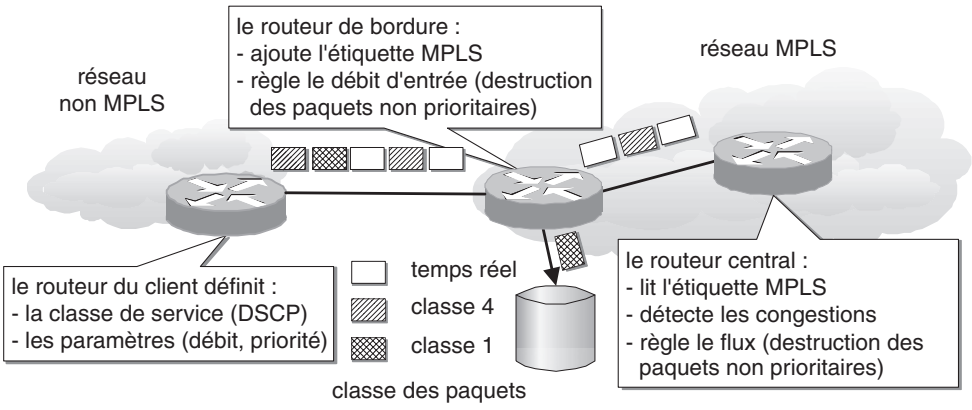

Figure 3.20 Rôle des routeurs dans un réseau MPLS.

Les routeurs centraux sont chargés de réguler les flux de données sur les liens du réseau. Pour cela, ils doivent détecter les congestions. Chaque routeur interroge ses voisins en utilisant un protocole de gestion (*Interior Local Management Interface*). Il tient à jour une base de gestion des liens (*Interior Link Management Interface – Management Information Base*).

3.5.6 Routage des « connexions à garantie de service »

Pour router une connexion, les routeurs établissent une liste des routeurs voisins disposant des ressources nécessaires (*Designated Transit List*). Les ressources sont réservées dans chaque routeur sélectionné, et une fonction de contrôle d'admission de trafic est activée (figure 3.21).

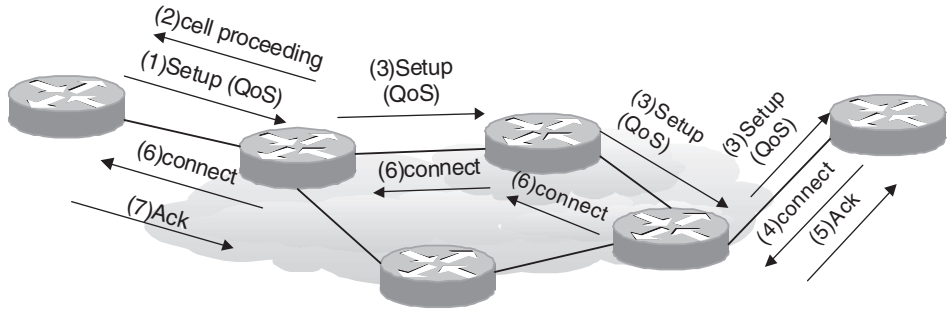

Figure 3.21 Établissement d'une connexion avec réservation de ressources.

Pour garantir des performances, les réseaux d'opérateurs doivent utiliser un protocole de transmission autorisant des classes de trafic et la mesure des performances. Les routeurs mémorisent les débits demandés sur chaque lien. Ils cumulent les débits de flux constants (flux *Constant Bit Rate* – CBR) et de flux variables (flux *Variable Bit Rate* – VBR). Pour toute nouvelle demande ils vérifient que le total des débits ne dépasse pas la bande passante du lien choisi :

$$Dtc = \sum_{i=1}^{n} dci\,; \quad Dtm = \sum_{i=1}^{k} dmi\,; \quad (Dtc)_{CBR} + (Dtm)_{VBR} < B$$

Dtc : débit crête total dc_i : débit crête de chaque flux CBR. Dtm : débit moyen total
Dm_i : débit moyen de chaque flux VBR B : bande passante du lien choisi

Les deux protocoles les plus adaptés actuellement sont ATM et le relais de trame[1].

1. Cf. paragraphes 8.4 et 8.6 de l'ouvrage *Transmissions et Réseaux*.

Le routage nécessite une vue globale des ressources du réseau. Elle est assurée par un algorithme « générique » de contrôle d'admission (GCAC). À la réception d'une demande de connexion :

– les liens qui n'ont pas le débit requis ou dont le taux de perte de cellules est supérieur à la demande sont éliminés de la liste des chemins possibles ;
– une liste des chemins les plus courts est établie ;
– de cette liste sont éliminés les chemins dont les performances globales sont inférieures à celles demandées. Dans le cas où plusieurs chemins sont trouvés, la répartition du trafic sur le réseau est prise en compte ;
– la description complète du chemin choisi est notée dans une liste (DTL) et transmise à tous les routeurs du chemin.

La garantie de service, implique la régulation des flux de données. Parmi les principales méthodes citons :

– la régulation de débit à l'admission dans le réseau (*Source Traffic Smoothing, Leaky Bucket*) ;
– le contrôle de bout en bout (*Rate Control for end-to-end Transport*) utilisant des cellules OAM ;
– le contrôle de congestion réactive ou préventive (*Connection Admission Control*).

a) Régulation à l'admission (Leaky Bucket)

Des jetons sont générés à intervalles réguliers. Le réseau n'admet pas plus de cellules que le nombre de jetons en stock. Les autres cellules devront attendre les jetons suivants pour être admises dans le réseau. Dans la figure 3.22, les trois premières cellules seront admises immédiatement, les deux autres devront attendre les prochains jetons.

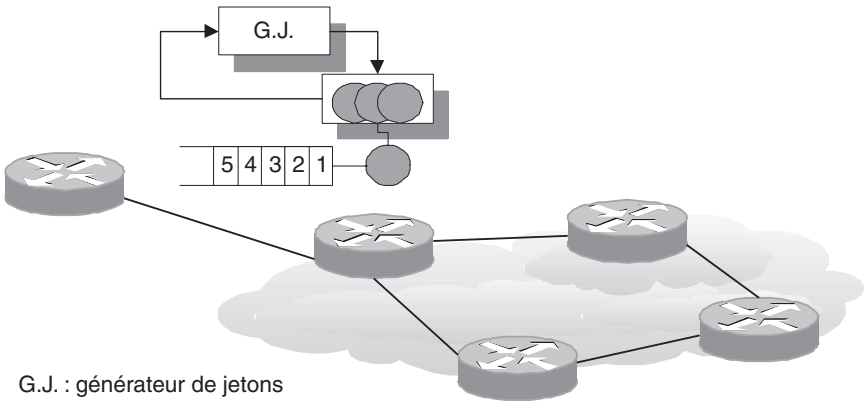

Figure 3.22 Contrôle de flux de type Leaky Bucket.

Il est ainsi possible de contrôler le nombre de cellules admises dans le réseau par unité de temps.

b) Régulation de bout en bout (Rate Control for end-to-end Transport)

Les méthodes à fenêtre sont peu efficaces du fait des temps de propagation. Les méthodes s'appuyant sur la prise en compte des congestions dans le réseau leur sont préférées. Les méthodes prédictives, telles que RCT, semblent plus performantes que les méthodes réactives.

La régulation par RCT utilise le bit CLP (*Cell Less Priority*) des cellules ATM pour déclasser celles-ci en cas de congestion. La figure 3.23 illustre cette méthode.

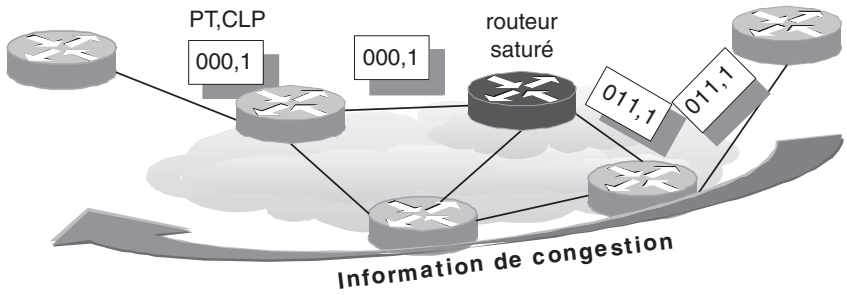

Figure 3.23 Régulation par information de congestion (RCT).

Lorsqu'une cellule portant un bit CLP à 1 traverse un routeur saturé, le champ PTI (*Payload Type Identification*) est marqué (010 ou 011). L'équipement terminal informe les équipements en amont de la congestion du routeur en utilisant les canaux de signalisation.

3.6 LE PROTOCOLE PPP (*Point-to-Point Protocol*)

Dans le cadre d'une connexion point à point par modem à l'Internet, il est nécessaire d'utiliser une procédure capable de transporter les datagrammes IP sur une liaison série. Le premier protocole conçu dans ce but est SLIP (*Serial Line Internet Protocol*) ; PPP (*Point to Point Protocol*) ajoute l'authentification et la détection d'erreurs et permet d'encapsuler plusieurs protocoles de niveau 3. PPP est défini par les RFC 1548, RFC 1661 et RFC 1662 de l'IETF.

Le protocole PPP est associé à deux autres protocoles dont les rôles sont les suivants :

– PPP encapsule les paquets de données pour les transmettre sur une liaison point à point. Son adaptation aux protocoles de niveau 3 les plus courants (IP, IPX, Appletalk, Xerox ou Decnet) et son autoconfiguration le rendent particulièrement performant ;
– le protocole LCP (*Link Control Protocol*) établit, configure, maintient et ferme la connexion ;
– un ensemble de protocoles dénommé NCP (*Network Control Protocol*) assure l'adaptation aux protocoles de niveau 3.

Le protocole PPTP (*Point-to-Point Tunneling Protocol*), combine l'encapsulation et le cryptage. Il permet de créer des liaisons sécurisées utilisées notamment dans les réseaux virtuels (*Virtual Private Network* – VPN).

Dans un premier temps, le protocole LCP va émettre des paquets pour établir la connexion et tester la liaison. Ensuite, PPP envoie des paquets NCP pour définir le protocole de niveau 3 utilisé et la taille des paquets échangés. À la fin de la transmission des données, des paquets LCP et NCP sont échangés pour fermer la connexion.

3.6.1 Gestion d'une connexion

a) Établissement d'une connexion

Pour ouvrir une connexion, LCP envoie une requête de configuration (code : 1). Il définit un identificateur pour la connexion (ID). Un paquet de confirmation positive (code : 2) ou négative (code : 3) est retourné par l'équipement distant. La figure 3.24 illustre ce dialogue d'établissement de connexion.

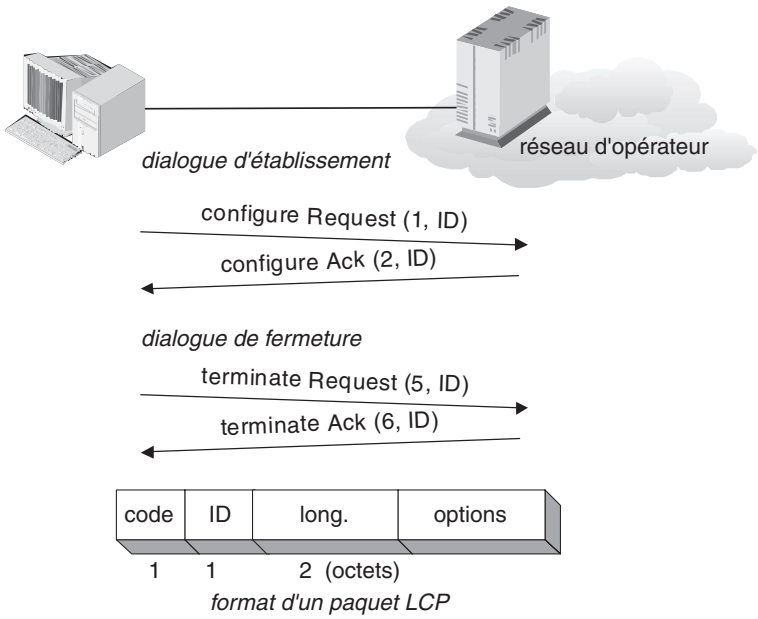

Figure 3.24 Dialogues de gestion d'une connexion par LCP.

Pour fermer une connexion, un paquet « terminate-request » est émis (code : 5). Un acquittement est envoyé en réponse (code : 6 pour un acquittement positif).

Des options peuvent être ajoutées. Le champ « longueur » indiquera la taille des options transmises. Parmi ces options, se trouve l'authentification par l'un des protocoles PAP (*Password Authentication Protocol*) ou CHAP (*Challenge Handshake Authentication Protocol*) définis par la RFC 1334 de l'IETF. Le protocole PAP repose

sur un identifiant associé à un mot de passe. Le protocole CHAP repose sur la connaissance d'un mot de passe (appelé « secret ») partagé par les deux utilisateurs. Ce mot de passe est utilisé comme clé de cryptage et de décryptage. La procédure d'authentification du protocole CHAP est activée périodiquement pendant l'ouverture de la connexion. La figure 3.25 montre le principe d'authentification périodique :

– le serveur envoie un premier paquet (*challenge*) qui contient un identifiant de la transaction, et un nombre aléatoire ;
– la station doit alors renvoyer (*response*) la version cryptée du nombre aléatoire ;
– le serveur décrypte le nombre reçu et compare sa valeur au nombre envoyé. En fonction du résultat, il renvoie un acquittement (*succes*) ou un refus (*failure*).

Par défaut, l'authentification des utilisateurs n'est pas activée.

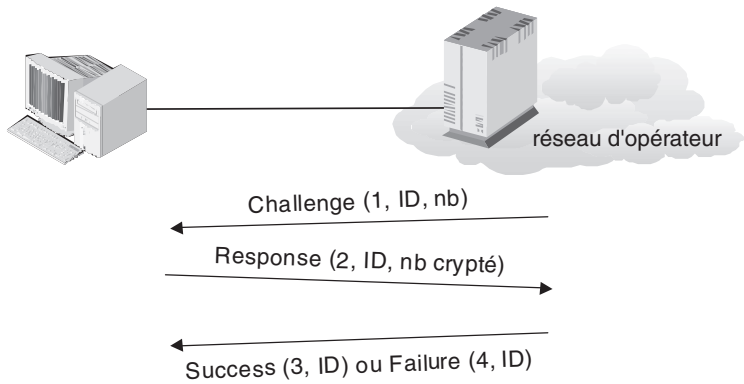

Figure 3.25 Dialogue d'authentification du protocole CHAP.

b) Configuration d'une connexion

Une fois la connexion établie, la configuration est à la charge du protocole NCP. Pour permettre l'échange de datagrammes IP, NCP échangera des paquets IPCP (*IP Control Protocol*) avec le site distant.

Le dialogue est identique à celui de l'établissement et de la fermeture avec les paquets « Configure-Request », « Configure-Ack », Configure-Nak », « Terminate-Request » et « Terminate-Ack ».

La taille des paquets échangés est fixée dans le champ des options. Par défaut, les paquets de données sont de 1 500 octets.

3.6.2 Trames PPP

a) Format des trames

Le format des trames PPP (figure 3.26) est proche de celui des trames HDLC. Non numérotées, elles ne permettent pas une procédure d'acquittement et de réémission. Les erreurs devront être traitées par les couches supérieures.

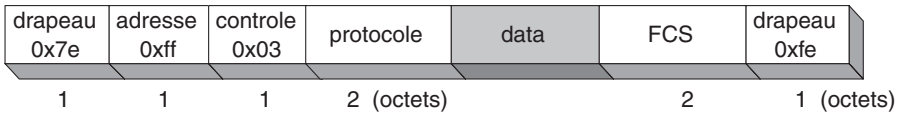

Figure 3.26 Format des paquets PPP.

Les champs **adresse** et **contrôle** ne sont pas utilisés. Les valeurs de ces deux octets sont respectivement 0xff et 0x03. Pour l'échange de paquets LCP, ces deux champs sont omis.

Le champ **protocole** indique le type de paquet ou le protocole de niveau 3 du champ **données**.

– Les codes des paquets des protocoles de gestion commencent par un « 1 » :

0xC021	Paquet LCP
0xC023	*Password Authentication Protocol*
0xC025	*Link Quality Report*
0xC223	*Challenge Handshake Authentication Protocol*

– Les codes des paquets d'un protocole de niveau 3 commencent par « 0 » :

0x0021	*Internet protocol*	0x0029	Appletalk
0x0025	Xerox NS IDP	0x002B	Novell IPX
0x0029	DECnet Phase IV	0x00CF	PPP « encapsulé »

Le champ **données** est de taille constante et fixée à la configuration de la connexion (1 500 octets par défaut). Les données sont complétées par des octets de bourrage si nécessaire.

b) Échange de datagrammes IP

Une fois la connexion établie et configurée, les datagrammes IP peuvent être échangés. Chaque datagramme est encapsulé dans un paquet PPP dont le champ protocole est fixé à la valeur 0x0021 pour IP. Le traitement des erreurs n'étant pas possible au niveau PPP, il devra être pris en charge par TCP.

Le protocole PPTP *(Point to Point Tunneling Protocol)*, basé sur l'encapsulation et le cryptage, permet de créer de manière sécurisée des réseaux privés virtuels (VLAN) sur l'Internet. Lorsque la connexion est établie au niveau liaison et réseau entre les deux systèmes distants, la connexion sécurisée est mise en œuvre en cryptant et en encapsulant les paquets IP.

3.6.3 Les protocoles PPPoE et PPPoA

Initialement mis en œuvre sur les liaisons du réseau téléphonique commuté, le protocole PPP a été adapté pour son utilisation sur des réseaux Ethernet (PPPoE) et ATM (PPPoA).

a) PPP over Ethernet

Le protocole PPPoE (RFC 2516) a pour objectif d'établir une session point à point sur un réseau Ethernet. Avant l'ouverture de session, la procédure débute par une phase de découverte destinée à obtenir l'adresse MAC d'un routeur. Le réseau Ethernet pouvant interconnecter plusieurs équipements configurés pour traiter le protocole PPPoE, l'ordinateur va devoir sélectionner celui avec lequel il va établir la session point à point. Cette phase est décrite figure 3.27 :

1. La station émet un paquet d'initiation (*PPPoE Active Discovery Initiation*) à tous les équipements (adresse de diffusion). Le code vaut 0x9, l'identificateur de session est à « 0 ».
2. Les routeurs retournent un paquet d'offre de session (*PPPoE Active Discovery Offer*) à la station source (code = 0x7 ; identificateur de session = 0).
3. La station envoie une demande d'ouverture de session (*PPPoE Active Discovery Request*) au routeur choisi (code = 0x19 ; identificateur de session = 0).
4. Le routeur retenu confirme l'ouverture de session (*PPPoE Active Discovery Session-confirmation*) à la station (code = 0x65) et affecte un identificateur de session.

Une fois la session point à point ouverte, l'échange de données s'effectue suivant le protocole PPP.

b) PPP over ATM

Le protocole ATM utilise un mode connecté[1]. Il se présente donc comme une connexion point à point, tout comme une connexion PPP. A l'établissement de la connexion, la couche ATM doit faire remonter à la couche LCP les informations d'établissement de la connexion (confirmation de la requête de connexion).

Le protocole PPPoA (RFC 2364) s'interface avec la couche AAL5 du protocole ATM. Cette couche traite des blocs de données jusqu'à 64 Ko. Les paquets PPP seront encapsulés dans un paquet LLC avant d'être transmis à la couche AAL5[2].

La figure 3.28 donne le détail des champs des paquets AAL5 encapsulant des paquets PPP. Ils se composent de trois parties :

1. l'en-tête LLC :
   - les adresses SAP destination et source sont fixées à 0xFE ;
   - la trame est de type non numérotée (0x03) ;
   - le champ *Network Layer Protocol Identifier* (NLPID) indique un protocole PPP encapsulé (0xCF).
2. Le paquet PPP :
   - l'identificateur de protocole sur 2 octets ;
   - les données PPP suivies d'un bourrage fonction de la taille des paquets définie à l'ouverture de la connexion par LCP.

1. Cf. paragraphe 8.6 de l'ouvrage *Transmissions et Réseaux*.
2. Cf. paragraphes 6.5.2 et 8.6.5 de l'ouvrage *Transmissions et Réseaux*.

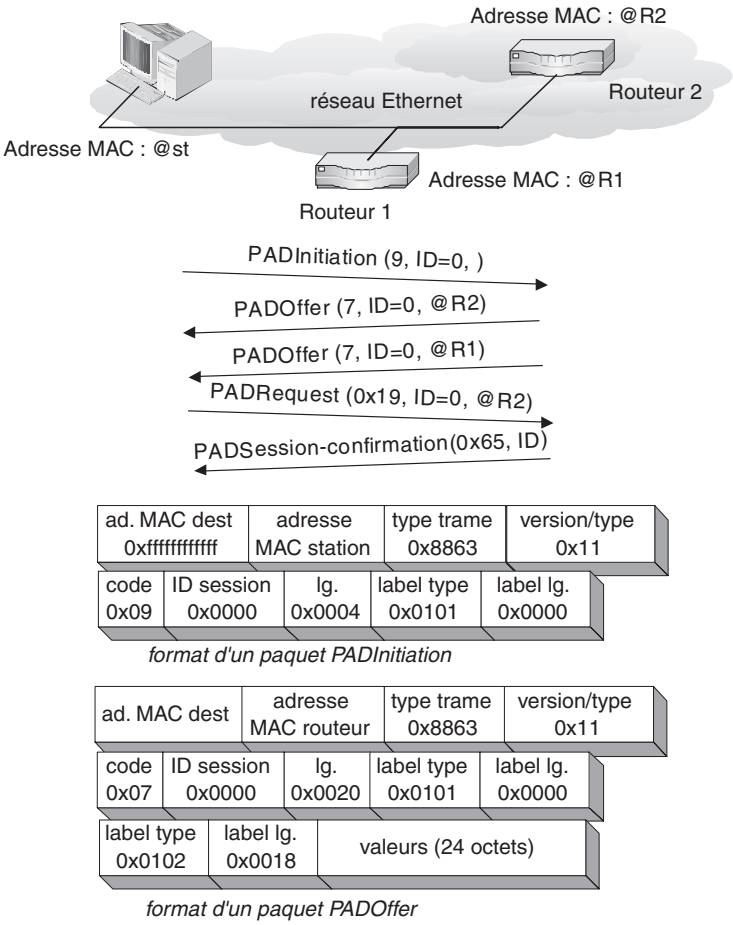

Figure 3.27 Établissement d'une session point à point par PPPoE.

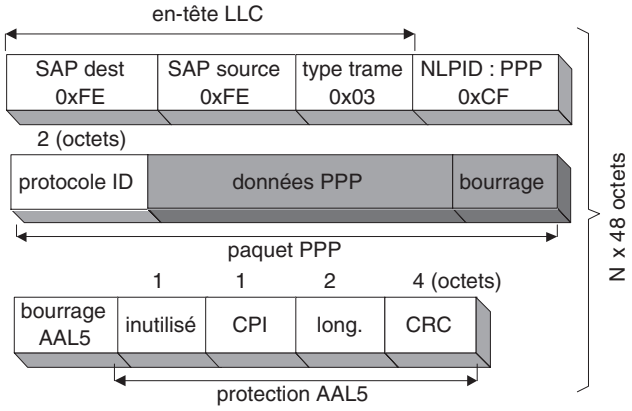

Figure 3.28 Format des paquets AAL5 transportant des paquets PPP.

3. Les octets de protection :
   – le champ *Common Part Indicator* (CPI) permet d'aligner la protection sur une longueur de 8 octets ;
   – la longueur est codée sur 2 octets (taille maximale 65 535 octets) ;
   – la somme de contrôle CRC est de 4 octets et porte sur l'ensemble du paquet.

Le protocole PPP et ses adaptations PPPoE et PPPoA s'intercalent entre le protocole IP et les protocoles de transmission. Si la valeur par défaut de la longueur des paquets (1 500 octets) est bien adaptée au format des trames Ethernet (1 500 octets de données), il n'en est pas de même pour le protocole ATM. En effet, AAL5 est prévu pour traiter les blocs de données IP sans les fragmenter. En interposant PPP entre IP et AAL5, un bloc de 64 Ko sera fragmenté en 44 unités à transmettre. Dans le cas de l'utilisation du protocole PPPoA, il peut être utile de paramétrer la taille des paquets PPP afin de réduire la fragmentation des datagrammes IP.

Résumé

1. Classification OSI
➢ les protocoles TCP/IP utilisés sur les réseaux Internet sont des protocoles respectivement de niveau 4 et de niveau 3 de l'architecture OSI ;
➢ le protocole IP offre des fonctions d'adressage et de routage. Il est associé aux protocoles ARP, RARP, ICMP et RIP ;
➢ le protocole TCP offre un transport en mode connecté. Le protocole UDP fonctionne en mode non connecté.

2. Le protocole IP
➢ les adresses IP sont codées sur 4 octets. Elles s'expriment en nombres décimaux séparés par un point (137.15.232.2) ;
➢ les adresses IP utilisées sur Internet sont réparties en cinq classes (A, B, C, D et E) ;
➢ certaines plages d'adresses ne sont pas routables sur Internet. Elles peuvent être utilisées sur des réseaux privés ;
➢ huit plages d'adresses sont affectées à des régions du monde.

3. Gestion des adresses et routage sur Internet
➢ les classes d'adresses peuvent être divisées en plages plus petites. Les routeurs utilisent des masques de taille variable (200.154.210.0/25) ;
➢ une entreprise utilisant une classe privée d'adresses IP utilisera la technique de translation d'adresses (NAT) pour l'accès à Internet ;
➢ les réseaux d'opérateurs utilisent des routeurs internes (IGP) pour le routage à l'intérieur de leur réseau. Ils font appel à des routeurs externes (EGP) pour l'interconnexion avec les réseaux des opérateurs voisins ;
➢ le protocole RIP est un protocole de routage interne s'appuyant sur un algorithme de type vecteur de distance ;

➢ le protocole OSPF est un protocole de routage interne utilisant un algorithme basé sur la connaissance de l'état des liaisons entre routeurs ;
➢ le protocole BGP-4 est un protocole de routage externe pour des routeurs connectés à plusieurs autres routeurs externes.

4. Les protocoles de niveau transport : UDP et TCP
➢ ils initialisent les dialogues à la demande des applications ;
➢ le protocole UDP utilise un mode non connecté et gère les ports permettant aux applications de dialoguer ;
➢ le protocole TCP utilise un mode connecté permettant la réémission des segments en erreur ;
➢ l'ouverture d'une connexion par TCP initialise le numéro de séquence et la taille de la fenêtre utilisée ;
➢ le transfert des données nécessite un acquittement (ACK).

5. IP et qualité de service
➢ la qualité de service permet de garantir les délais d'acheminement de flux « temps réel » ;
➢ pour garantir des performances, il faut quantifier et mesurer des paramètres ;
➢ les principaux paramètres sont le débit moyen et les rafales (débit max et durée) ;
➢ la qualité de service passe par la mise en place de protocoles de transmission (niveaux 1 et 2), de routage (niveau 3) et de signalisation (niveau 4) ;
➢ aux niveaux 1 et 2 les protocoles les plus adaptés sont ATM, SDH et Frame Relay ;
➢ au niveau 4 on trouve les protocoles IntServ, Diffserv, RSVP et MPLS ;
➢ le protocole IntServ permet d'établir un mode connecté à travers Internet ;
➢ les applications « temps-réel » utilisent les protocoles RSVP, RTP et RTCP pour la régulation des flux ;
➢ Diffserv définit quatre classes de trafic : *premium* pour les applications « temps réel », *gold* pour un délai garanti, *silver* et *bronze* qui ne garantissent pas la délivrance des données ;
➢ les classes de trafic et la priorité des paquets sont codées dans le champ ToS de IPv4 ;
➢ le protocole MPLS permet aux opérateurs de garantir des services sur leur réseau indépendamment des autres réseaux d'opérateurs ;
➢ à l'entrée sur le réseau, les routeurs de bordure ajoutent une étiquette (label) aux paquets. Cette étiquette servira au traitement des paquets dans les routeurs centraux ;
➢ le routage des « connexions à garantie de service » nécessite de réserver des ressources dans les routeurs traversés ;
➢ la régulation de flux peut se faire à l'admission des paquets (ex. : Leaky Bucket) ou de bout en bout (ex. : RCTP).

6. Le protocole PPP
➢ le protocole PPP assure la transmission sur des liaisons point à point de datagrammes de niveau 3 par encapsulation ;
➢ il est associé à deux autres protocoles : LCP pour la connexion, PPP pour le format des paquets et NCP pour traiter les paquets de niveau 3 ;
➢ le protocole PPTP ajoute un cryptage des paquets et permet de créer des réseaux privés virtuels (VPN) ;
➢ la version PPPoE va créer une liaison point à point avec un routeur à travers un réseau Ethernet ;
➢ la version PPPoA assure l'interfaçage avec la couche AAL5 d'ATM.

QCM

Une version électronique et interactive est disponible sur le site *www.dunod.com*.

1. Classification OSI

Q1. À quel niveau de l'architecture OSI correspond le protocole IP ?
a) niveau 1 *b) niveau 2* *c) niveau 3*
d) niveau 4 *e) niveau 5*

Q2. À quel niveau de l'architecture OSI correspond le protocole ICMP ?
a) niveau 1 *b) niveau 2* *c) niveau 3*
d) niveau 4 *e) niveau 5*

Q3. Quel est le protocole de même niveau que TCP ?
a) ARP *b) RIP* *c) RCTP* *d) UDP* *e) PPP*

Q4. Le protocole UDP utilise une connexion en mode :
a) connecté *b) non connecté* *c) point à point*

2. Le protocole IP

Q5. Les adresses IPv4 sont codées sur :
a) 2 octets *b) 3 octets* *c) 4 octets*
d) 5 octets *e) 6 octets*

Q6. Les adresses IP sont réparties en :
a) 3 classes *b) 4 classes* *c) 5 classes*
d) 6 classes *e) 7 classes*

Q7. Quelles sont les fonctionnalités assurées par le protocole IP ?
a) fragmentation *b) affectation des ports*
c) contrôle de flux *d) routage*

3. Gestion des adresses et routage sur Internet

Q8. Le routeurs appliquant le CIDR utilisent (plusieurs réponses) :
a) des sous-classes d'adresses *b) des masques de longueur variable*
c) des classes privées *d) le protocole NAT*

Q9. La translation d'adresse assure le passage d'adresses :
a) de classe privée à publique *b) de classe C à sous-classe*
c) de classe C à classe B

Q10. Les routeurs externes d'un opérateur Internet utilisent un protocole (plusieurs réponses) :
a) IGP *b) EGP* *c) BGP*

Q11. Le protocole RIP est un protocole utilisé par :
a) des routeurs internes *b) des routeurs externes*
c) les deux types

Q12. Le protocole OSPF (Open Short Path First) utilise un algorithme de type :
a) vecteur de distance *b) état des liens* *c) les deux*

Q13. Le protocole BGP-4 est un protocole utilisés par :
a) des routeurs internes *b) des routeurs externes* *c) les deux types*

Q14. Le protocole BGP-4 utilise un algorithme de type :
a) vecteur de distance *b) état des liens* *c) les deux*

4. Les protocoles UDP et TCP

Q15. Quelles sont les fonctionnalités assurées par le protocole UDP ?
a) la segmentation *b) l'affectation des ports*
c) le contrôle de flux *d) le routage*

Q16. Le champ « données » d'un datagramme UDP peut contenir au maximum :
a) 1 500 octets *b) 15 Ko* *c) 32 Ko* *d) 64 Ko*

Q17. Quelles sont les fonctionnalités assurées par le protocole TCP ?
a) la segmentation *b) l'affectation des ports*
c) le contrôle de flux *d) le routage*

Q18. Le champ « données » d'un datagramme TCP peut contenir au maximum :
a) 1 500 octets *b) 15 Ko* *c) 32 Ko* *d) 64 Ko*

5. IP et qualité de service

Q19. La qualité de service permet de garantir (plusieurs réponses) :
a) le délai d'acheminement *b) le taux de perte*
c) la retransmission sur erreur

Q20. Une rafale est définie par le(s) paramètre(s) :
a) le débit maximum *b) le débit moyen*
c) la durée *d) le taux de perte*

Q21. Quel(s) sont le(s) protocole(s) adapté(s) à la qualité de services ?
a) Ethernet *b) ATM* *c) FDDI*
d) HDLC *e) FastEthernet*

Q22. Quels sont les protocoles utilisés par les applications « temps réel » ?
a) UDP *b) RTP* *c) TCP*
d) RSVP *e) RIP*

Q23. Dans quel champ de l'en-tête IP se trouvent les paramètres utilisés par MPLS ?
a) version *b) drapeaux* *c) type de service* *d) durée de vie*

Q24. Quel protocole de régulation de flux est assuré par les seuls routeurs de bordure ?
a) Connection Admission Control *b) Leaky Bucket*
c) Rate Control end-to-end Transport

6. Le protocole PPP

Q25. À quel niveau de l'architecture OSI correspond le protocole PPP ?
a) niveau 1 *b) niveau 2* *c) niveau 3*
d) niveau 4 *e) niveau 5*

Q26. Quel protocole est chargé de l'établissement de la connexion ?
a) PPTP *b) NCP* *c) PPP*
d) IP *e) LCP*

Q27. Quel protocole est utilisé sur les réseaux privés virtuels (VLAN) ?
a) PPTP *b) LCP* *c) PPP*
d) IP *e) NCP*

Q28. Le protocole PPP over Ethernet établit une liaison point à point entre :
a) 2 postes clients *b) 1 poste client et 1 serveur*
c) 1 poste client et 1 routeur *d) 1 serveur et 1 routeur*

Q29. Avec quelle couche du protocole ATM s'interface le protocole PPPoA ?
a) ATM *b) AAL2* *c) AAL3-4*
d) AAL5 *e) PMD*

Exercices

➤ (*) : facile(**) : moyen(***) : difficile
Corrigés à la fin du livre et sur le site *www.dunod.com*.

3.1 (*) Calculer le nombre d'adresses Internet de classe C pouvant être distribuées par les organismes du NIC, en tenant compte des adresses réservées et non routables.

3.2 (**) Une entreprise demande une plage de 480 adresses Internet. Indiquer une adresse pouvant lui être attribuée par un organisme du NIC. Quel masque devra être utilisé dans les routeurs ?

3.3 (***) Une entreprise dispose de 110 ordinateurs clients et 4 serveurs. Elle souhaite disposer de 34 adresses sur Internet.

a) Indiquer une adresse pouvant lui être attribuée par un organisme du NIC.

b) Donner une table de translation possible si les postes connectés à Internet sont toujours les mêmes et comportent deux serveurs et deux routeurs.

3.4 (*) À partir de la figure 3.5, établir la table de routage du routeur R1 si les routeurs utilisent le protocole RIP.

3.5 (**) Dans la figure 3.5, le réseau client B est connecté au routeur R2 à la place du routeur R3.

a) Indiquer les modifications apportées dans la table de routage du routeur R3 (tableau 3.2).

b) Établir la table de routage du routeur R2.

3.6 (*) À partir de la topologie du réseau de la figure 3.5 et de la table de routage OSPF du tableau 3.3, établir le plus court chemin reliant le réseau client C au réseau Internet B.

3.7 (***) On considère la topologie du réseau de la figure 3.5 et la table de routage OSPF du tableau 3.3.

a) Établir le plus court chemin reliant le réseau client C au réseau Internet B dans le cas où le lien R1-R3 devient inutilisable.

b) Le trafic entre les réseaux Internet B et C augmente et sature le routeur R6. Comment modifier la table de l'état des liaisons du tableau 3.3 afin de faire passer le trafic du réseau client C vers le réseau Internet B par le routeur R2.

3.8 (***) À partir du réseau décrit à la figure 3.29 et de la table d'état des liens du tableau 3.7 (voir *Étude de cas* du présent chapitre), on analyse le trafic entre les réseaux clients A et B.

a) Déterminer le plus court chemin et son coût.

b) Le routeur R4 relié à l'Ebone est très chargé. Comment l'administrateur peut-il modifier la table d'état des liens pour que le trafic entre les réseaux clients A et B soit acheminé via les routeurs R5 et R6 ?

3.9 (***) Dans le réseau de la figure 3.29 (voir *Étude de cas* du présent chapitre), les liens partant des routeurs R1, R2 et R3 sont à 10 Mbit/s. Les liens entre les routeurs de bordure R4 à R7 sont de 50 Mbit/s. Les flux actuellement établis ont pour paramètres (total flux CBR ; total flux VBR) : R2-R1 (3 Mbit/s ; 5 Mbit/s) ; R1-R4 (2 Mbit/s ; 7 Mbit/s) ; R1-R7 (2 Mbit/s ; 2 Mbit/s) ; R4-R5 (15 Mbit/s ; 20 Mbit/s) ; R4-R7

(12 Mbit/s ; 15 Mbit/s) ; R5-R3 (1,7 Mbit/s ; 3,4 Mbit/s) ; R5-R6 (3,1 Mbit/s ; 4,8 Mbit/s) ; R6-R7 (2,4 Mbit/s ; 4,2 Mbit/s). Un poste du réseau client B veut établir une connexion avec un serveur vidéo du réseau A par un flux variable de paramètres 3,8 Mbit/s de débit crête et 2 Mbit/s de débit moyen.

a) Existe-t-il un chemin permettant de garantir les débits demandés ?

b) Même question si le trafic sur le lien R1-R2 passe à (3 Mb/s ; 2 Mb/s).

Exercices pratiques

➤ (*) : facile(**) : moyen(***) : difficile

Les logiciels utilisés sont disponibles sur le site *www.dunod.com* (versions d'évaluation ou gratuites).

3.10 (**) **Tests d'accès au prestataire de service par le RTC**

a) Relever l'adresse du DNS de votre prestataire. Vous pouvez afficher les propriétés ou les paramètres de la connexion réseau concernée et sélectionner le protocole Internet (TCP-IP). Une autre solution consiste à ouvrir une fenêtre de commandes en mode « DOS » (programmes, accessoires, Invite de commandes) et de taper « ipconfig /all » pour obtenir l'ensemble des paramètres TCP-IP pour toutes les connexions.

b) Après vous être connecté à votre prestataire, faire un « **ping** » sur l'adresse de son serveur DNS. Le logiciel **ping** est accessible par une fenêtre de commandes en mode « DOS ». Le serveur DNS vous retourne un paquet de réponse (paquet « echo ») et le logiciel mesure le temps de réponse du DNS (remarque : taper ping –p pour obtenir la syntaxe et les options de la commande).

3.11 (**) **Tests d'accès au prestataire de service par ADSL**

a) Relever l'adresse du DNS de votre prestataire. Vous pouvez procéder comme ci-dessus en identifiant la connexion correspondant à votre accès ADSL (généralement « carte d'accès distant » ou « modem ADSL »).

b) Après vous être connecté à votre prestataire, faire un « **ping** » sur l'adresse de son DNS (voir méthode dans l'exercice 3.10).

3.12 (**) **Routage Internet par l'utilitaire TRACERT**

a) Après vous être connecté à votre prestataire, lancer une commande « **tracert** » sur un serveur connu (serveur http par exemple). Le logiciel TRACERT est également accessible par une fenêtre de commandes en mode « DOS ». Relever l'URL et l'adresse IP de ce serveur, ainsi que l'itinéraire emprunté pour atteindre ce serveur.

b) Une option du logiciel permet de mesurer le temps de réponse (taper tracert –p pour obtenir la syntaxe et les options de la commande).

3.13 (***) **Routage Internet par le logiciel NeoTrace**

a) Installer le logiciel **Neotrace** sur votre ordinateur. NeoTrace est un logiciel de la société McAfee permettant de visualiser graphiquement le chemin emprunté par les paquets pour accéder à un serveur (serveur http par exemple). Le logiciel peut être obtenu gratuitement en version de démonstration.

b) Se connecter à plusieurs sites dispersés géographiquement (on peut utiliser les sites de Sony, tels que *sony.fr* ; *sony.it* ; *sony.fi* ; *sony.at* ; *sony.com*.au ; *sony.com.sg*.

c) Repérer le lieu de connexion avec le fournisseur d'accès Internet (FAI). Repérer le lieu d'interconnexion avec l'opérateur Internet suivant (lieu où le radical de l'adresse propre au domaine de l'opérateur Internet change) ; le nom du réseau d'interconnexion (e-bone) s'il existe.

d) Le logiciel permet de voir le nombre d'opérateurs et de routeurs traversés, ainsi que la durée moyenne (sur 10 paquets) du trajet et sa variation maximale.

e) Faire un relevé des routes et des durées de trajet sur un site, à des jours et heures différents (et si possible à partir de deux FAI différents). On note les différences dues aux variations de la charge des réseaux d'opérateurs Internet.

Étude de cas : Routage dans les réseaux d'opérateurs de transport

Les réseaux d'opérateurs sont organisés en domaines représentant des systèmes autonomes de routage (*Autonomous Systems*). Chaque plaque comporte des points d'accès au réseau permettant aux réseaux clients de se raccorder à Internet via les routeurs internes de l'opérateur (figure 3.29). Les plaques échangent leurs tables de routage et leurs trames par les routeurs de bordure (R4, R5, R6 et R7).

Les routeurs peuvent être configurés pour gérer une table de routage statique ou dynamique. Dans le cas d'un routage statique, l'administrateur remplit la table de routage manuellement (*net adress ; next hop ; metric*). Le paramètre « *metric* » est optionnel. En l'absence de paramètre, une valeur par défaut est utilisée par le logiciel de routage. Pour un routeur Cisco, la commande permettant de définir une route est « clns route ».

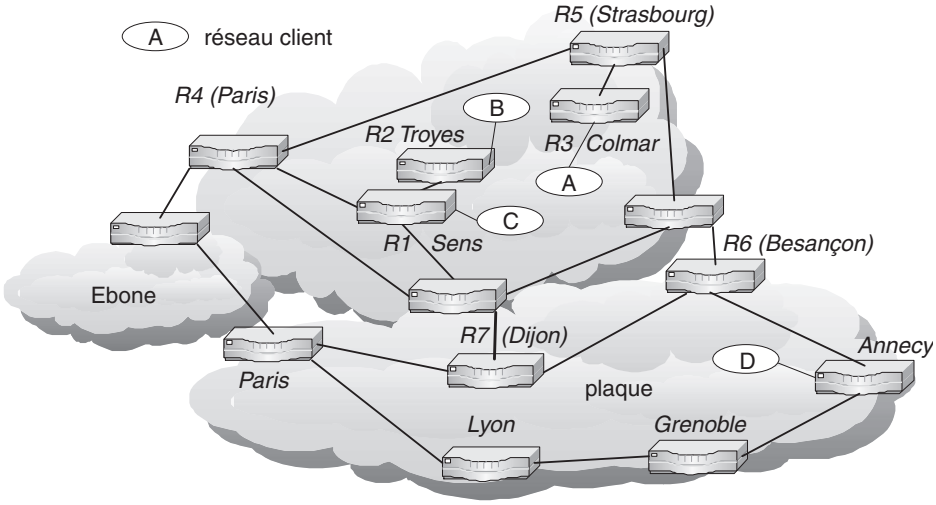

Figure 3.29 Organisation des routeurs d'un opérateur de transport Internet.

Les routeurs offrent souvent la possibilité de choisir entre plusieurs protocoles de routage dynamique. Les routeurs Cisco proposent le protocole ISO IGRP (*Interior Gateway Routing Protocol*) et le protocole IS-IS (*Intermediate System-to-Intermediate System*).Le protocole ISO IGRP dispose de trois niveaux de routage : *system routing, area routing et inter-domain routing*. Les deux premiers niveaux correspondent au routage interne à un domaine, le troisième niveau sera réservé aux routeurs de bordure. L'algorithme de routage est de type vecteur de distance. La table de routage du routeur R1 contiendra les informations du tableau 3.6.

Tableau 3.6 Table de routage du routeur R1 de la figure 3.29 au protocole ISO IGRP.

net	next hop	metric
A	R4	4
B	R2	2
C		1
D	R7	2

Pour configurer un routage dynamique au protocole ISO IGRP, il faut définir l'adresse du routeur et spécifier les interfaces qui vont utiliser ce protocole. Le paramètre « metric » ne correspond pas forcément au nombre de sauts et l'affectation de valeurs est facultative (commande : # metric weights qos k1 k2 k3 k4 k5). Les valeurs par défaut fournissent un bon routage dans la plupart des cas, et leur modification peut entraîner des baisses importantes de

performance. Il est donc nécessaire, avant de modifier ces paramètres, de mesurer les trafics sur les différents segments du réseau afin de vérifier si les modifications améliorent ou non les performances du routage.

Le protocole IS-IS autorise un routage dynamique utilisant une table d'état des liaisons (*Link state*). Les paramètres « *metric* » peuvent être entrés par la commande # isis metric value. La valeur est comprise entre 0 et 63, la valeur par défaut est 10. Le tableau 3.7 représente le contenu de la table d'état des liens.

TABLEAU 3.7 TABLE D'ÉTAT DES LIENS DE LA FIGURE 3.29 POUR LE PROTOCOLE IS-IS.

router	neigbourg	metric	router	neigbourg	metric	router	neigbourg	metric
R1	R2	10	R3	R5	10	R5	R4	10
R1	R4	10	R3	A	10	R5	R6	10
R1	R7	10	R4	R1	10	R6	R5	10
R1	C	10	R4	R5	10	R6	R7	10
R2	R1	10	R4	R7	10	R7	R1	10
R2	B	10	R5	R3	10	R7	R6	10
						R7	R4	10

Chapitre **4**

Les services sur Internet : messagerie, FTP et Web

4.1 LES SERVICES DE MESSAGERIE

Plus connus sous le nom de courrier électronique ou e-mail, ces services permettent d'échanger des messages et des fichiers. La taille des fichiers (pièces jointes) est limitée par les serveurs de messagerie (limitation d'environ 1 Mo) pour restreindre le stockage et préserver la bande passante. Au-delà, il faudra utiliser un service spécialisé dans le transfert de fichier utilisant un protocole adapté tel que FTP (*File Transfer Protocol*).

Il faut différencier la messagerie interne et la messagerie externe. La première permet l'envoi de messages entre les salariés de l'entreprise. La seconde interconnecte les salariés de l'entreprise aux messageries du monde Internet. L'architecture de la première étant la plus simple, elle sera étudiée en premier, même s'il est rare qu'elle soit dissociée de la seconde, sauf pour des raisons de sécurité. Dans ce cas, deux services distincts coexisteront, les postes permettant la messagerie interne étant dissociés de ceux autorisant l'échange de messages avec le monde Internet.

4.1.1 Architecture d'une messagerie interne

L'architecture de base tourne autour d'un serveur de messagerie disposant de boîtes aux lettres (BAL). Chaque utilisateur dispose d'une BAL à laquelle il peut accéder en lecture par un « nom utilisateur » et un « mot de passe » (figure 4.1). La liste des BAL est stockée dans une base de données de comptes. Cette base de données est le plus souvent compatible avec ODBC (*Open DataBase Connectivity*).

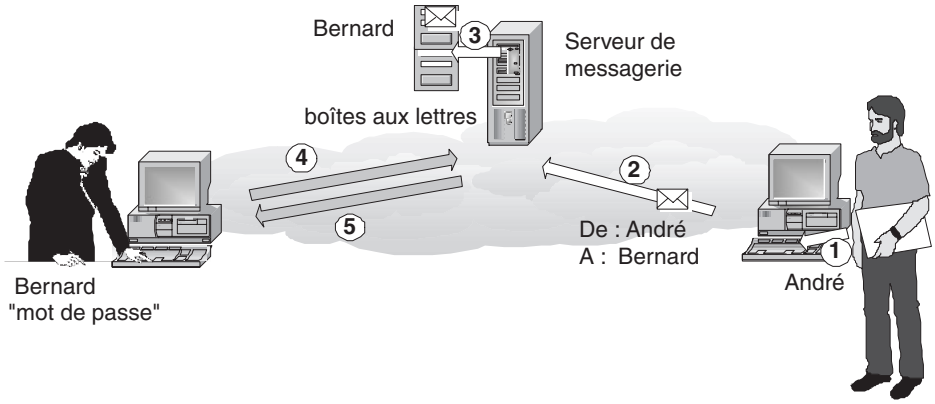

Figure 4.1 Architecture et fonctionnement d'une messagerie interne.

Le fonctionnement comprend deux phases distinctes : l'envoi du message d'une part, la lecture du message d'autre part. Ces deux phases sont indépendantes et décorélées dans le temps.

– Phases d'envoi :

1. L'expéditeur (André) rédige le message (texte + destinataire). Le poste peut être déconnecté du réseau.
2. L'expéditeur envoie le message au serveur de messagerie. Le poste doit être connecté au réseau. L'expéditeur n'a pas besoin de disposer d'une BAL sur le serveur, mais le poste doit connaître le nom du serveur (il doit posséder un compte si l'accès au réseau est contrôlé par un serveur de comptes).
3. Le serveur de messagerie vérifie l'existence d'une BAL au nom du destinataire (Bernard) et y stocke le message.

– Phases de réception :

4. Le destinataire (Bernard) interroge sa BAL. Le poste doit connaître le nom du serveur de messagerie (il doit d'abord ouvrir une session dans le cas d'un serveur de comptes).
5. Après vérification de son nom et de son mot de passe par le serveur, Bernard peut lire ou transférer les messages situés dans sa BAL. Dans le cas où le message est transféré vers l'outil de messagerie du poste client, la lecture du message peut se faire en différé (hors connexion au réseau).

Les protocoles utilisés par le serveur pour traiter le message et par le destinataire pour interroger sa Boîte aux lettres sont différents. Le plus souvent, le traitement des messages se fait avec SMTP (*Simple Mail Transfer Protocol*), alors que l'interrogation de la BAL utilise POP3 (*Post Office Protocol*).

Bien sûr, il s'agit du fonctionnement vu des utilisateurs. Nous allons affiner l'analyse pour comprendre les paramétrages nécessaires. Mais avant, examinons les logiciels constituant les applications client et serveur.

a) Architecture logicielle d'une messagerie

Une application de messagerie va installer sur un poste client 5 modules (figure 4.2) :

- une interface utilisateur fournissant les commandes permettant l'édition, l'envoi et la réception des messages ;
- une interface de service (*Service Provider Interface*) chargée d'exécuter les commandes transmises par l'interface utilisateur via le système d'exploitation. Ce module contient les paramètres de fonctionnement de l'outil de messagerie (nom du serveur, protocoles utilisés, planification des tâches) ;
- un module de stockage des messages contenant les messages des boîtes d'envoi et de réception ;
- un module de transport mettant en forme les messages en fonction des protocoles utilisés. Ce module dialogue avec le module TCP/IP des couches 3 et 4 du modèle OSI ;
- un annuaire permettant de stocker une liste de destinataires (carnet d'adresses, contacts).

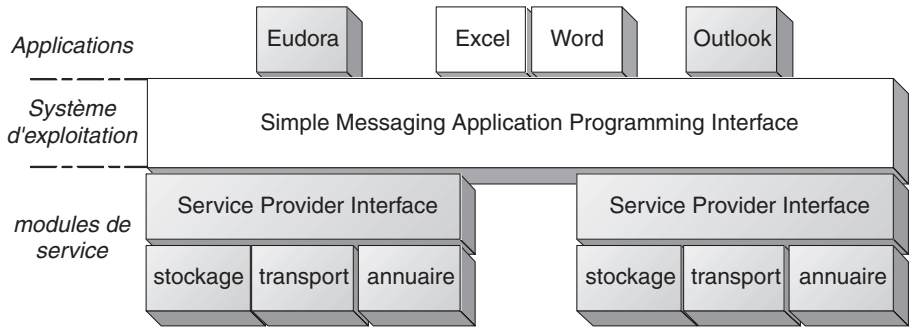

Figure 4.2 Éléments logiciels d'un outil de messagerie client.

Chaque outil de messagerie installe ses propres modules de service. Il faut noter que les formats de stockage des messages et informations ne sont pas normalisés. Chaque constructeur choisit son format, avec d'éventuels problèmes de compatibilité avec les autres applications.

Côté serveur de messagerie, la figure 4.3 donne les éléments logiciels installés :

- l'agent de transport des messages (*Message Transport Agent*) chargé de la réception et de l'envoi des messages avec d'autres serveurs ;
- le module de traitement des messages gère l'envoi et la réception des messages des clients, avec la mise au format de stockage ;
- l'annuaire contient la liste des BAL gérées par le serveur ;
- le module de passerelles intervient pour la mise au format des messages lors de l'envoi vers d'autres serveurs utilisant des protocoles différents ;
- le module de stockage des messages des clients (BAL).

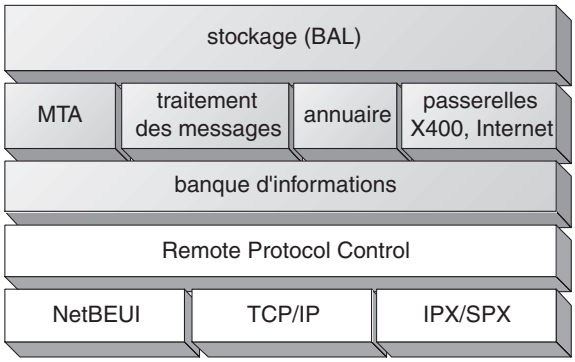

Figure 4.3 Éléments logiciels d'un serveur de messagerie.

On retrouve bien évidemment les modules du système d'exploitation assurant le transport des données (*Remote Protocol Control)* et les protocoles des couches 3 et 4 du modèle OSI.

b) Fonctionnement de l'émission de messages

Lors de la phase 1 de l'envoi d'un message (« clic » sur « envoi de message »), le message est stocké localement par le module de stockage (figure 4.4). La phase 2 de l'envoi a lieu immédiatement ou en différé, suivant le paramétrage.

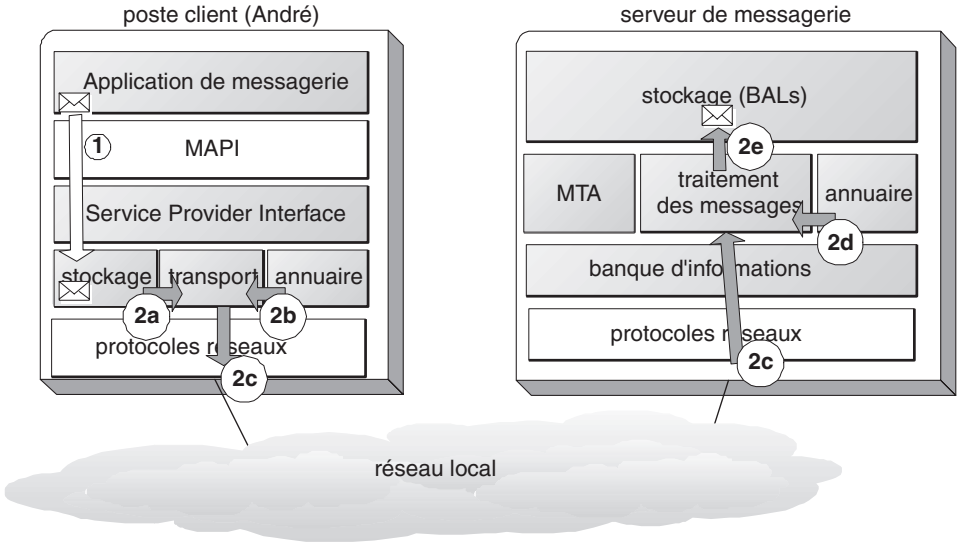

Figure 4.4 Phases d'envoi d'un message.

L'analyse de la phase 2 de l'envoi d'un message montre l'interaction des modules de service :

2*a* Le service « transport » charge le message à envoyer.

2*b* Le service « transport » récupère l'adresse du serveur de messagerie mémorisée lors du paramétrage.

2*c* Le service « transport » transmet aux services « réseau » une demande de connexion au serveur de messagerie.

2*d* Après connexion au serveur, le serveur vérifie dans l'annuaire l'existence d'une BAL au nom du destinataire.

2*e* Dans l'affirmative, le serveur demande le message et le stocke dans la BAL.

c) Fonctionnement de la réception de message

Le destinataire (Bernard) active la connexion à sa messagerie. La connexion peut être activée automatiquement par paramétrage. Cette demande est transmise par l'interface MAPI du système d'exploitation au service transport (figure 4.5).

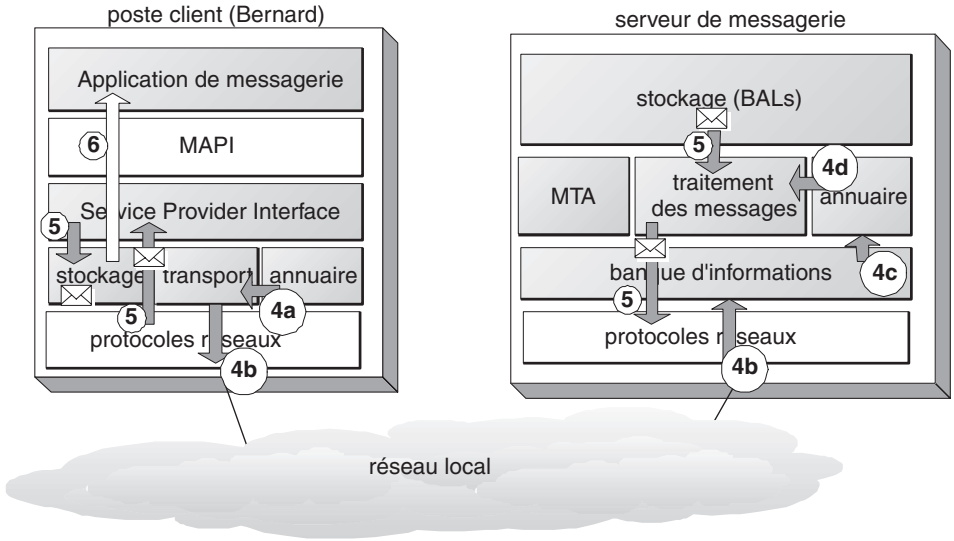

Figure 4.5 Phases de réception d'un message.

Lors des phases 4 et 5 de la réception d'un message, les étapes suivantes se succèdent pour le transfert du message sur le poste du client :

4*a* Le service « transport » récupère l'adresse du serveur de messagerie, ainsi que les noms et mot de passe de l'utilisateur, mémorisés lors du paramétrage.

4*b* Le service « transport » transmet aux services « réseau » une demande de connexion au serveur de messagerie.

4*c* Après connexion au serveur, la banque d'information authentifie l'émetteur de la demande dans l'annuaire par son nom et mot de passe.

4*d* Le service de traitement des messages localise la BAL auprès du service annuaire.
5 Le service de traitement des messages récupère le message dans la BAL et le transfère à l'interface du fournisseur de service (SPI) pour son stockage sur le poste client ou sa lecture « en ligne » (sans stockage sur le poste client).

La phase 6 représente la lecture du message transféré qui peut, dans ce cas, se faire en différé et hors ligne. Pour une lecture en ligne, l'interface du fournisseur de service ne stocke pas le message, mais le transmet directement à l'application de messagerie.

d) Les logiciels de messagerie

Il faut distinguer les logiciels de serveurs de messagerie et ceux destinés aux postes clients. Il n'est pas indispensable d'utiliser un outil de messagerie du même éditeur que le logiciel utilisé sur le serveur. Les protocoles d'échange normalisés (voir paragraphe 4.1.3, *Les protocoles de messagerie*) rendent compatibles les différentes versions. Des problèmes tels que l'affichage de certains caractères ou la gestion des pièces jointes ne sont toutefois pas à exclure.

Côté serveur, les logiciels les plus courants sont *Exchange Server* de Microsoft, *Netscape Messaging Server,* ou encore *Domino Mail Server* de Lotus.

Côté client, les outils de messagerie les plus utilisés sont *Netscape, Eudora, Mozilla,* bien évidemment *Outlook Express, Outlook* ou *Exchange* de Microsoft, mais également *Notes* de Lotus ou *Groupwise* de Novell.

À noter que des serveurs de liste de diffusion (serveur SYMPA par exemple) permettent de gérer des groupes de destinataires et d'assurer la diffusion d'un message à tous les membres (voir § 4.1.6, *Les services webmail et listes de diffusion*). L'abonnement et le désabonnement à la liste ou sa consultation s'effectuent automatiquement par l'abonné lui-même ou par l'administrateur de la liste grâce à l'envoi de commandes par courrier électronique. Un gestionnaire est souvent utile pour s'assurer que la liste est à jour.

4.1.2 Architecture d'une messagerie externe

La particularité d'une messagerie externe est que la boîte aux lettres du destinataire ne se trouve pas sur le serveur de messagerie auquel est connecté l'expéditeur du message. Pour atteindre la BAL du destinataire, les deux serveurs doivent s'échanger le message à travers un ou plusieurs réseaux d'opérateurs. Ces réseaux peuvent être de type Internet, mais également de type RTC, ADSL ou RNIS. Les deux serveurs vont devoir utiliser un protocole d'adressage compatible avec celui utilisé par les équipements de l'opérateur auquel ils sont raccordés. La figure 4.6 donne l'exemple le plus simple de l'architecture d'une messagerie externe.

Dans ce cas, la transmission du message va faire intervenir les agents de transfert (*Message Transfer Agent*) de chaque serveur de messagerie. La succession des phases se présente ainsi (figure 4.6) :

1. Transfert du message du poste de l'expéditeur (André) vers le serveur du réseau local A (réseau d'André) où il est stocké en attente d'émission par le MTA.

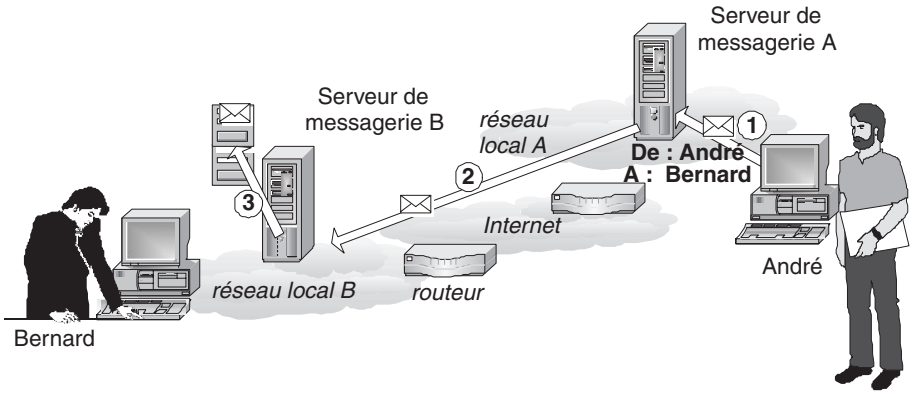

Figure 4.6 Architecture d'une messagerie externe.

2. Le serveur de messagerie A se connecte au serveur de messagerie B à travers le réseau de l'opérateur Internet. L'agent de transfert du serveur A transmet le message à l'agent de transfert du serveur B.
3. Le service de traitement du serveur de messagerie B stocke le message dans la BAL du destinataire (Bernard).

L'agent de transfert du serveur de messagerie B devra vérifier l'existence de la BAL du destinataire (Bernard). Si la BAL n'est pas trouvée, un message d'erreur est transmis par l'agent de transfert du serveur B vers l'agent de transfert du serveur A. celui-ci peut adresser à l'expéditeur un message d'erreur de transmission indiquant que le destinataire n'a pas été trouvé. Sur Internet, les agents de transfert utilisent le protocole SMTP (*Simple Mail Transfer Protocol*).

Lorsque le nombre de comptes de messagerie à gérer et que le volume de messages traités sont importants, le serveur d'émission des messages est physiquement séparé du serveur de réception.

4.1.3 Les protocoles de messagerie

a) SMTP pour la gestion du courrier

Le protocole SMTP (*Simple Mail Transfer Protocol*) est le plus couramment utilisé pour la gestion du courrier entre serveurs sur Internet, reliés en permanence. Un utilisateur connecté de façon intermittente (*Dial up*) à travers le RTC ou RNIS utilisera également SMTP pour l'expédition de son courrier (courrier sortant) et un protocole tel que POP3 (*Post Office Protocol*) pour lire son courrier (courrier entrant).

Le format des messages SMTP utilise le caractère « @ » comme séparateur du nom de la BAL de celui du serveur de messagerie. Ce dernier utilise le format commun des serveurs sur Internet tel que « mail.babaorum.fr » pour le serveur « mail » du domaine « babaorum.fr ». Ainsi l'adresse de Bernard sur ce serveur aura la syntaxe *bernard@mail.babaorum.fr*. Cette adresse devra apparaître dans le champ « destinataire » de l'éditeur de messages.

Les éditeurs proposent généralement les champs :

– Champ CC (*Carbone Copy* ou Copie Conforme) pour l'envoi d'une copie du message aux destinataires dont l'adresse se trouve dans ce champ. Les noms des destinataires apparaîtront sur tous les messages transmis.
– Champ BCC (*Blind Carbone Copy*) ou CCI (Copie Conforme Invisible) pour l'envoi aux destinataires indiqués dans ce champ. Les destinataires indiqués dans les autres champs ne verront pas ces destinataires dans la liste des destinataires.

Le tableau 4.1 donne une liste des principaux champs normalisés dans le format de messages SMTP, tels que définis par la RFC 822.

TABLEAU 4.1 CHAMPS NORMALISÉS DU PROTOCOLE SMTP.

Champ	Signification	Champ	Signification
To	Adresse destinataire principal	Date	Date et heure d'émission
Cc	Adresse destinataire secondaire	Reply To	Adresse de réponse
Bcc	Adresse destinataire caché	Message-Id	Numéro d'identification
From	Créateur du message	References	Numéros de messages liés
Received	Adresse émetteur	Subject	Résumé du message
Received :	Adresse des agents de transfert	Keywords	Mots clés de l'émetteur
Return-Path	Identifie le chemin de retour		

L'en-tête d'un message contient le chemin suivi et les serveurs et passerelles traversés. Dans l'exemple de la figure 4.6, en appelant ***andre.station*** le poste utilisé par André ; ***mail.alesia.f***r le serveur de messagerie d'envoi ; ***mail.babaorum.fr*** le serveur de messagerie où se trouve la BAL de Bernard, l'en-tête du message reçu par le serveur de messagerie destinataire contiendrait :

```
Received: from mail.alesia.fr
   by mail.babaorum.fr with ESMTP
   for <bernard@babaorum.fr>; Thu, 13 Nov 2003 18:14:08 +0100 (MET)
Received: from andre.station
   by mail.alesia.fr with SMTP
   for <bernard@babaorum.fr>; Thu, 13 Nov 2003 18:01:14 +0100
Message-ID: <002f01c16df8$9bf18be0$2a01005b@alesia>
From: "Andre" <andre@alesia.fr>
To: <bernard@babaorum.fr>
References: <01C16DFD.2470F2E0.bernard@babaorum.fr>
Subject:
```

La ligne 2 du premier bloc « received » indique le serveur final (contenant la BAL du destinataire). La ligne 1 indique le serveur en amont. Ce serveur se retrouve en ligne 2 du deuxième bloc « received ». La ligne 1 indique le poste/serveur en amont. On voit ainsi que le message, parti du poste d'André (*andre.station*) a traversé le serveur « mail.alesia.fr » pour arriver au serveur « mail.babaorum.fr ».

Les serveurs dialoguent en utilisant des commandes. Les tableaux 4.2 et 4.3 montrent quelques commandes normalisées constituées :

– D'un code de 4 lettres ou plus pour les commandes d'envoi ;
– D'un code de 3 chiffres pour les commandes de réponse :
  – Le premier chiffre signifie une exécution réussie (1, 2 ou 3) ou non (4 ou 5) ;
  – Les chiffres suivants précisent le code de retour de commande ou la nature de l'erreur.

Tableau 4.2 Commandes d'envoi du protocole SMTP.

Commande	Fonction
HELO « exp »	Requête de connexion provenant d'un expéditeur SMTP
MAIL FROM : « adr_exp »	Lance une transaction de courrier vers une ou plusieurs boîtes aux lettres
RCPT TP : « adr_dest »	Spécifie un destinataire du courrier. Pour plusieurs destinataires, la commande est répétée
DATA	Marque le début des données d'un message. La fin est marquée par la séquence <CRLF>.<CRLF>
QUIT	Demande au récepteur l'envoi d'une réponse OK et de fermer la connexion
RESET	Annulation du mail en cours
NOOP	Demande au récepteur l'envoi d'une réponse OK

Tableau 4.3 Réponses aux commandes du protocole SMTP.

Commande	Fonction
250	Action demandée bien effectuée (réponse OK)
251	Utilisateur non-local, message retransmis
354	Commencer à transmettre le mail (fin d'envoi par <CRLF>.<CRLF>)
450	Action demandée non-effectuée, BAL occupée
550	Action demandée non-effectuée, BAL inaccessible
451	Action demandée annulée : erreur pendant le traitement
551	Utilisateur non-local : rediriger le message
452	Action demandée non-effectuée : espace de stockage insuffisant
552	Action demandée non-effectuée : dépassement de quota disque
553	Action demandée non-effectuée : nom de BAL illégal
554	Echec de la transaction

Le dialogue entre les serveurs SMTP utilise le port 25 (port TCP par défaut). Il comporte 3 phases :

1. Établissement de la connexion entre les serveurs et identification de la source et de la destination du message.
2. Envoi du message avec les en-têtes aux normes RFC 822 et RFC 1521.
3. Libération de la connexion.

La figure 4.7 montre un dialogue entre deux serveurs pour l'envoi d'un message. Ce dialogue suppose les serveurs prêts à recevoir une demande de connexion. Cet exemple fait apparaître les échanges de type requête-réponse ainsi que les quatre phases d'établissement de connexion, identification du destinataire, transfert du message et libération de la connexion serveur-serveur.

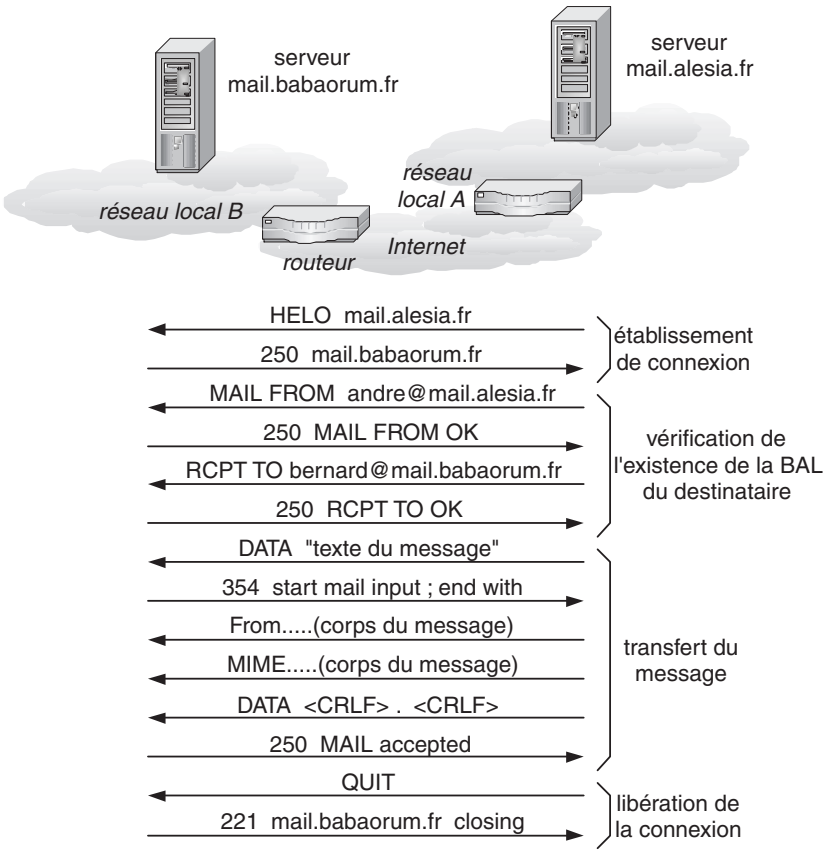

Figure 4.7 Dialogue de transfert de message entre serveurs SMTP.

Les deux relevés de trames présentés dans la figure 4.8 montrent un échange pour l'établissement de connexion entre deux serveurs SMTP. À la commande **HELO**

émise par le serveur *mail.alesia.fr*, le serveur destinataire *mail.babaorum.fr* transmet un acquittement positif d'exécution de la commande par la réponse **250**.

```
FRAME : Base frame properties
ETHERNET : ETYPE = 0x0800 : Protocol = IP : DOD Internet Protocol
IP : ID = 0xB600 ; Proto = TCP ; Len : 61
TCP : .AP…, len : 21, seq : 8841060-8841080, ack : 145295483, win : 8133,
SMTP : Cmd : Hello, host identifier, 21 bytes
SMTP: Command = HELO mail.alesia.fr

FRAME : Base frame properties
ETHERNET : ETYPE = 0x0800 : Protocol = IP : DOD Internet Protocol
IP : ID = 0xFDD4 ; Proto = TCP ; Len : 62
TCP : .AP…, len : 22, seq : 145295483-145295504, ack : 8841081, win : 9216,
SMTP : Rsp: Requested mail action okay, completed, 22 bytes
SMTP : Response = 250 mail.babaorum.fr
```

Figure 4.8 Trames échangées entre deux serveurs à l'établissement de la connexion.

b) POP3 et IMAP pour interroger la BAL

Ce protocole POP3 (*Post Office Protocol*) est destiné à récupérer le courrier sur un serveur pour un utilisateur non connecté en permanence à Internet, mais se connectant à travers un réseau d'opérateur de télécommunication tel que le RTC ou le RNIS. Il gère :

– l'authentification du client (vérification du nom et du mot de passe) ;
– la réception des courriers et fichiers attachés à partir du serveur de messagerie ;
– la réception de messages d'erreur ou d'acquittement.

Ce protocole ne permet pas l'envoi de messages. Il ne permet pas non plus la lecture des messages « en ligne ». Il est nécessaire de télécharger l'intégralité du message et des pièces jointes avant sa lecture. Il ne permet donc pas de manipuler les messages sur le serveur.

Pour lire le courrier « en ligne », il faut utiliser un protocole comme IMAP (*Interactive Mail Access Protocol*). Il permet également la manipulation sur les messages tels que les recherches selon critères, le tri, l'effacement, ainsi que la création sur le serveur de dossiers publics et privés pour le classement des messages. Les dossiers privés ne sont accessibles qu'à leur créateur ; les dossiers publics sont accessibles à tous ou à un groupe de clients. La version 4 du protocole est décrite dans les RFC 2060 et RFC 1733. Le protocole IMAP4 utilise le port 143 par défaut.

Les serveurs POP3 dialoguent par le port 110 (port TCP par défaut). Ils utilisent des commandes normalisées définies par la RFC 1939, comportant quatre lettres. Les réponses sont transmises sous forme d'une chaîne de caractères précédée des caractères +OK ou –RR suivant que celle-ci est positive ou négative. Le tableau 4.4 donne la liste des commandes disponibles sous POP3.

Tableau 4.4 Commandes du protocole POP3.

Commande	Fonction
STAT	Récupère le nombre et la taille des messages en attente
LIST (msg)	Demande d'information sur le message spécifié en paramètre (msg)
RETR msg	Récupère une liste de messages
DELE msg	Supprime le message spécifié
USER nom	Spécifie une boîte aux lettres
PASS password	Spécifie un mot de passe
QUIT	Supprime les messages lus et ferme la connexion

Détaillons les particularités de chacun de ces deux protocoles :

– Avec le protocole POP, les messages sont en général effacés du serveur après le téléchargement. L'espace disque nécessaire à chaque client sur le serveur peut être limité, et surtout reste à peu près constant, ce qui simplifie l'administration. Toutefois, en l'absence d'une commande d'effacement (DELE), un double du message est conservé sur le serveur après son téléchargement sur le poste client. Les messages sont rangés sur le poste client dans des dossiers créés localement. Le client ne crée donc pas de dossiers sur le serveur, ni n'effectue de manipulation de fichier. Ceci est vu comme une sécurité par beaucoup d'administrateurs. Pour envoyer un message à plusieurs destinataires, le message est dupliqué en autant d'exemplaires que de destinataires. C'est le cas par exemple dans les équipes de projet dont les membres veulent diffuser une information ou un document.
– Le protocole IMAP laisse les messages sur le serveur de messagerie. L'espace disque de chaque client risque donc de croître, si celui-ci ne fait pas le « ménage » dans ses messages. Les messages sont rangés sur le serveur par le client. Celui-ci a donc la possibilité de créer des dossiers sur le serveur. Un aspect intéressant du protocole consiste en la possibilité de créer des dossiers publics accessibles par un groupe de clients. La figure 4.9 montre un exemple d'organisation possible pour une entreprise. Le message est alors stocké en un seul exemplaire et peut être lu par tous les membres du groupe. La création de dossiers sur un serveur est parfois considérée par des administrateurs comme un risque de désorganisation du serveur.

Trois cas orientent le choix vers un serveur IMAP :

– la nécessité pour des collaborateurs de consulter leurs messages de plusieurs ordinateurs dans l'entreprise ou hors de celle-ci. Ils doivent alors trouver sur le serveur l'intégralité de leurs messages ;
– le souhait de permettre la consultation des messages à partir d'un navigateur web sur les postes clients. Le serveur de messagerie doit alors être interfacé à un module logiciel pour réaliser un Webmail comme expliqué au paragraphe 4.1.6, *Les services webmail et listes de diffusion* ;

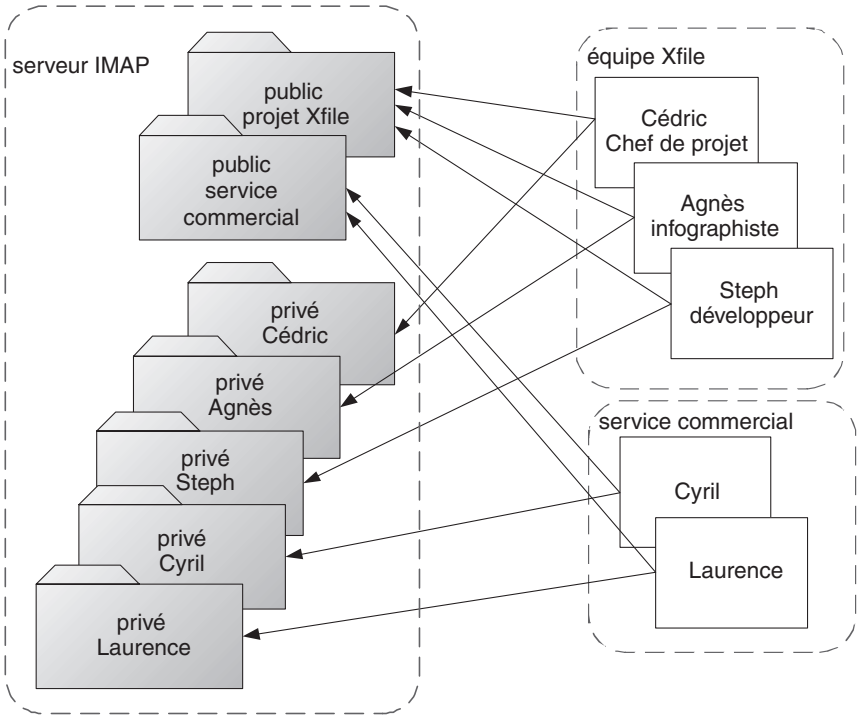

Figure 4.9 Organisation et accès des dossiers sur un serveur IMAP.

– la volonté d'assurer une transmission cryptée des messages. Cette solution permet de bénéficier du mode de transmission sécurisé SSL.

c) MIME pour la mise en forme des messages

Pendant longtemps, le codage des caractères était laissé au libre choix des éditeurs de logiciels de messagerie. Il s'ensuivait des affichages peu fiables lorsque le message était lu sur un logiciel d'un éditeur différent de celui utilisé pour la création du message. Aujourd'hui, les éditeurs proposent aux utilisateurs plusieurs choix de protocoles. Le plus utilisé actuellement est le protocole MIME (*Multipurpose Internet Mail Extension*). Ce protocole assure le codage du texte et l'insertion de fichiers joints, qu'ils soient de texte formaté, d'image ou de son.

Le protocole MIME reprend le codage ASCII sur 7 bits ou 8 bits (caractères accentués) de la RFC 822 et définit des règles pour le codage de messages non ASCII. Le codage utilisé pour la transmission peut être :

– un codage base64 pour les messages binaires (groupe de 24 bits segmentés en 6 bits et ASCII légal : A pour 0, B pour 1…) ;
– un codage QP (*Quoted Printable*) pour les messages texte (codage ASCII sur 7 bits et une séquence spécifique composée du signe égal et de la valeur du caractère pour les codes supérieurs à 127 – par exemple =E9 pour le caractère « é ») ;

– un codage permettant de spécifier le type de fichier et sous-type contenu dans le message (texte, son ou vidéo…).

Ce codage permet la transmission de nombreux types de fichiers, spécifiés par un en-tête suivi du type et du sous-type, comme le montre le tableau 4.5.

Tableau 4.5 Description des types des messages au protocole MIME.

En-tête	Signification	
MIME-Version	Identification de la version du protocole	
Content-Description	Chaîne de caractères donnant de façon lisible le contenu	
Content-Id	Identificateur unique	
Content-Transfer-Encoding	Façon dont le corps est emballé pour la transmission	
Content-Type	Nature du message	
Type	**Sous-type**	**Description**
Text	Plain	Texte non formaté
	Richtext	Texte avec formatage simple
Image	Gif	Image au format GIF
	Jpeg	Image au format JPEG
Audio	Basic	Son audible
Video	Mpeg	Film au format MPEG
Application	Octet-stream	Suite d'octets interprétés
	Postscript	Document imprimable en PostScript
Message	Rfc822	Message MIME au format RFC 822
	Partial	Message découpé pour la transmission
	External-body	Message à récupérer sur le réseau
Multipart	Mixed	Parties indépendantes dans l'ordre spécifié
	Alternative	Même message en différents formats
	Parallel	Parties à voir simultanément
	Digest	Chaque partie est un message RFC 822

4.1.4 Se connecter à distance

Deux cas peuvent se présenter. Le réseau local sur lequel se trouve le serveur de messagerie est accessible par un réseau d'opérateur téléphonique (RTC ou Numéris). La connexion se fera alors à travers le serveur d'accès distant de l'entreprise. Si le serveur de messagerie n'est accessible qu'à partir d'Internet, le client devra se

connecter en mode *Dial-up* par l'intermédiaire d'un prestataire de service. Dans les deux cas, sous Windows, l'accès du client se fera par l'intermédiaire du logiciel « connexions réseaux et accès distants ». Les protocoles mis en œuvres dans ce type de connexion sont décrits dans le chapitre 2, *Se connecter à Internet.*

a) Connexion par serveur d'accès distant

Lorsque le logiciel de messagerie du client veut envoyer une requête de connexion au serveur de messagerie, le modem du client doit d'abord établir une connexion avec le serveur d'accès distant (figure 4.10 – phase 1) en utilisant un identifiant et un mot de passe. Le client sera ensuite connecté au serveur de messagerie, via le routeur, et identifié en utilisant le nom du serveur (ou son adresse), son nom de client (nom de la BAL) et son code d'accès à sa boîte aux lettres (figure 4.10 – phase 2).

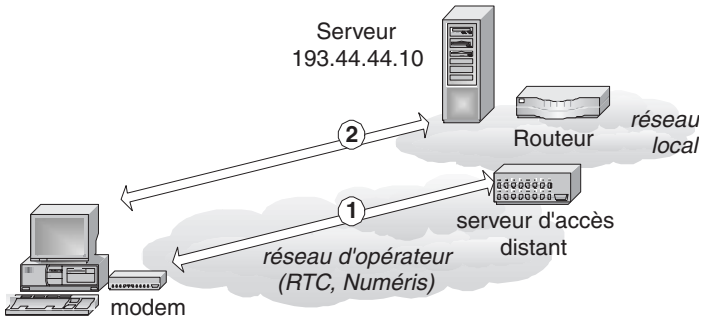

Figure 4.10 Connexion par serveur d'accès distant.

Le poste client doit donc connaître le numéro de téléphone du serveur d'accès distant, le protocole utilisé par le réseau local de l'entreprise, les adresses du serveur de messagerie, éventuellement celles du serveur DNS (sous TCP/IP), les protocoles utilisés par le serveur de messagerie, le nom de la BAL et du code d'accès.

Le paragraphe 4.1.5, *Installer, configurer les outils de messagerie*, indique les étapes de la configuration d'un client. Cette situation correspond également au cas d'un utilisateur dont la BAL est hébergée par le serveur de messagerie d'un prestataire de services.

b) Connexion par prestataire de service

Lorsque le logiciel de messagerie du client veut envoyer une requête de connexion au serveur de messagerie, le poste client doit d'abord établir une connexion avec son prestataire de service (figure 4.11 – phase 1). Il est authentifié par son nom client et son mot de passe. Le prestataire le connecte à Internet.

L'outil de messagerie du client va alors transmettre la demande de connexion (figure 4.11 – phase 2), via Internet, au serveur de messagerie de l'entreprise. Ce sont les serveurs DNS locaux du prestataire qui auront la charge de relayer la requête vers les DNS distants pour localiser le domaine où se situe le serveur de messagerie.

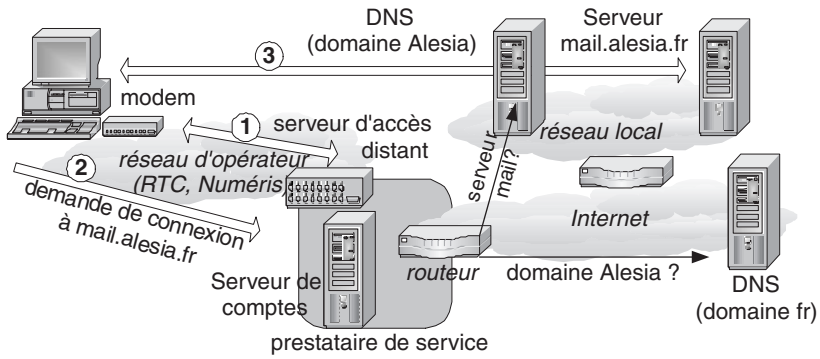

Figure 4.11 Connexion par prestataire de service.

Le client sera authentifié par son nom de compte et son mot de passe de messagerie et la connexion sera établie (figure 4.11 – phase 3). Outre le paramétrage de la connexion au prestataire de service, le poste client doit configurer sa messagerie pour fournir au prestataire les informations nécessaires à la localisation du serveur de messagerie (le mode de connexion ; les noms des serveurs de messagerie POP et SMTP ; le nom d'utilisateur et le mot de passe ; l'adresse de messagerie du client).

4.1.5 Installer, configurer les outils de messagerie

a) Configuration du client Outlook

La solution retenue pour créer et paramétrer une connexion du client Outlook, utilise l'assistant de création de compte. Pour y accéder, sélectionner l'icône « Outlook », cliquer sur le bouton droit de la souris et sélectionner l'option « propriétés » du menu (il est possible d'y accéder en ouvrant Outlook, puis en sélectionnant l'option « comptes » du menu « outils »). La fenêtre donne la liste des comptes créés. L'assistant démarre en cliquant sur le bouton « ajouter ». La création du compte comporte trois étapes. La première consiste à fournir les paramètres de connexion au serveur de messagerie (phase 2 de la figure 4.10). Les quatre fenêtres successives de la première étape de l'assistant de connexion Internet sous Windows sont regroupées dans la figure 4.12.

La première fenêtre permet de mémoriser le nom qui sera associé à l'adresse mail de l'expéditeur, paramétrée dans la seconde fenêtre. La troisième fenêtre permet de mémoriser la ou les adresses des serveurs d'envoi (courrier sortant) et de réception (courrier entrant) des messages. Dans le cas présenté figure 4.12, les serveurs d'envoi et de réception sont deux serveurs distincts. Si le serveur d'envoi et de réception est unique, les champs comporteraient le même nom (ex. : *mail.alesia.fr*). La quatrième fenêtre stocke les coordonnées de la boîte aux lettres du client (nom de la boîte et mot de passe).

Les trois fenêtres suivantes de la première étape servent au paramétrage de la connexion au serveur d'accès distant (phase 1 de la figure 4.10). Elles ne sont pas utilisées dans le cas d'une liaison permanente (ligne spécialisée, ADSL ou réseau local).

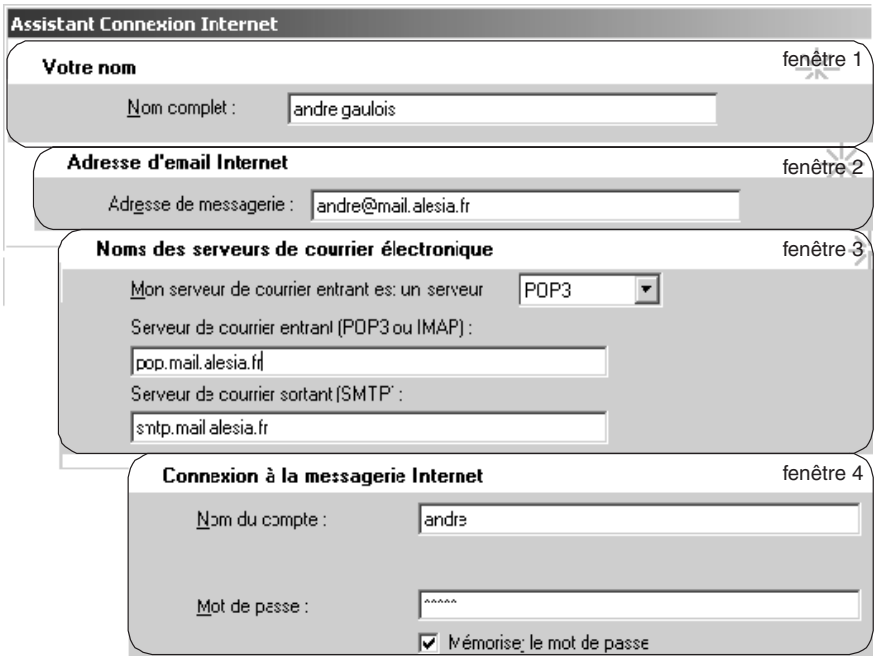

Figure 4.12 Paramétrage de la connexion au serveur de messagerie « mail.alesia.fr ».

La figure 4.13 montre le choix du mode de connexion (fenêtre 5), celui du modem (fenêtre 6) et le numéro d'appel du serveur d'accès distant (fenêtre 7).

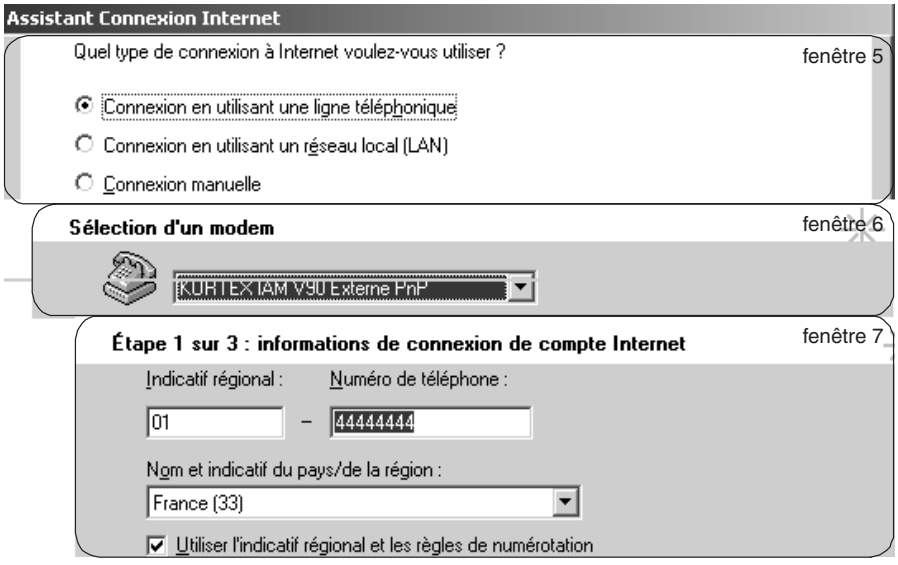

Figure 4.13 Paramétrage de la connexion au serveur distant.

Le bouton « avancés » de la fenêtre 7 permet le choix des protocoles de niveau 2 utilisés entre le poste client et le serveur d'accès distant, ainsi que du mode d'attribution d'adresse IP au poste client. Dans le cas d'un adressage fixe, l'adresse IP du poste client doit être entrée dans le champ correspondant, ainsi que celui du serveur DNS. La figure 4.14 montre la configuration pour un adressage dynamique (utilisation d'un serveur DHCP).

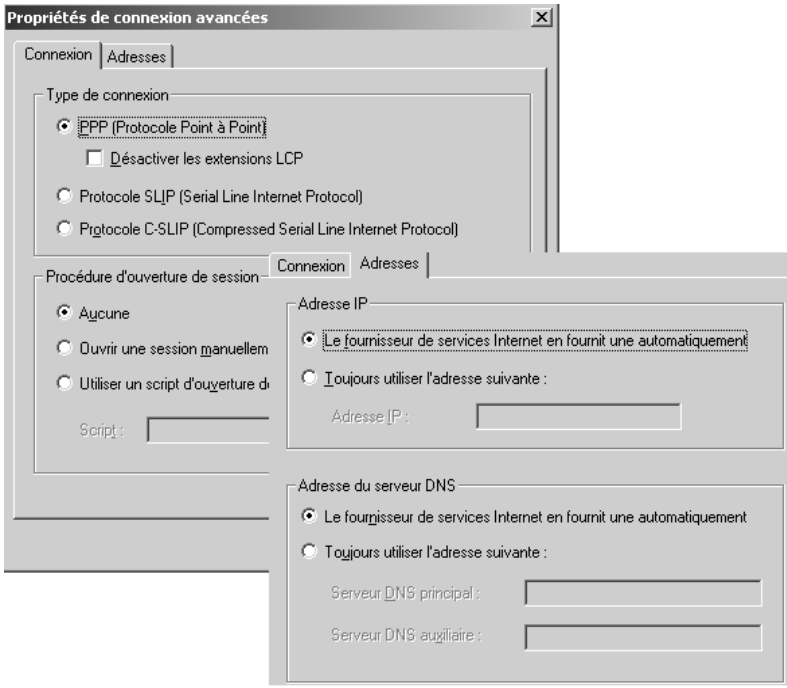

Figure 4.14 Configuration « avancée » de la liaison au serveur d'accès distant.

La 2e étape permet de mémoriser les paramètres d'identification du client par le serveur du prestataire de service ou le serveur de comptes distants de l'entreprise. On trouve le nom de compte et le mot de passe (figure 4.15).

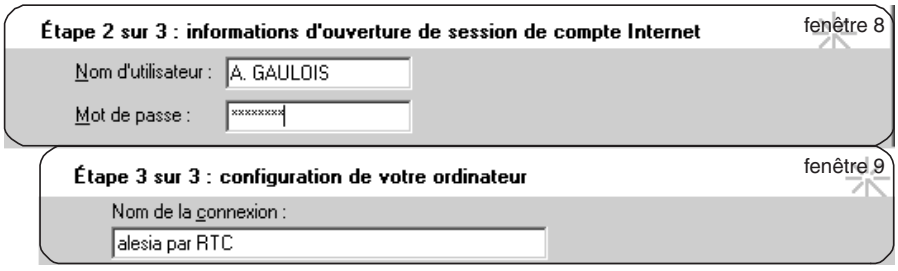

Figure 4.15 Paramétrage de la liaison avec le serveur de compte.

La dernière étape (fenêtre 9) mémorise le nom sous lequel apparaîtra la connexion dans la liste des comptes.

b) Installation, configuration, gestion d'un serveur

L'installation/configuration d'un serveur de messagerie nécessite :

- **l'identification du serveur** par son adresse IP, son nom, son nom de domaine et éventuellement le nom du serveur de domaine ;
- **l'identification des services** de messagerie avec le nom du serveur POP et celui du serveur SMTP, éventuellement les numéros de port utilisés s'ils sont différents des ports par défaut ;
- **l'identification des répertoires** de travail, répertoire des messages reçus en attente de stockage, celui des BAL, enfin des messages en attente d'envoi.

Il faut ensuite gérer les comptes clients en créant leur BAL. Pour chaque client, il faut définir son nom, le nom de sa boîte aux lettres et son mot de passe. Éventuellement, il sera nécessaire de paramétrer le chemin d'accès au répertoire de stockage des messages, celui des pièces jointes, la limitation du nombre de messages et l'espace disque de stockage. La figure 4.16 montre les paramètres d'un serveur de messagerie après sont installation.

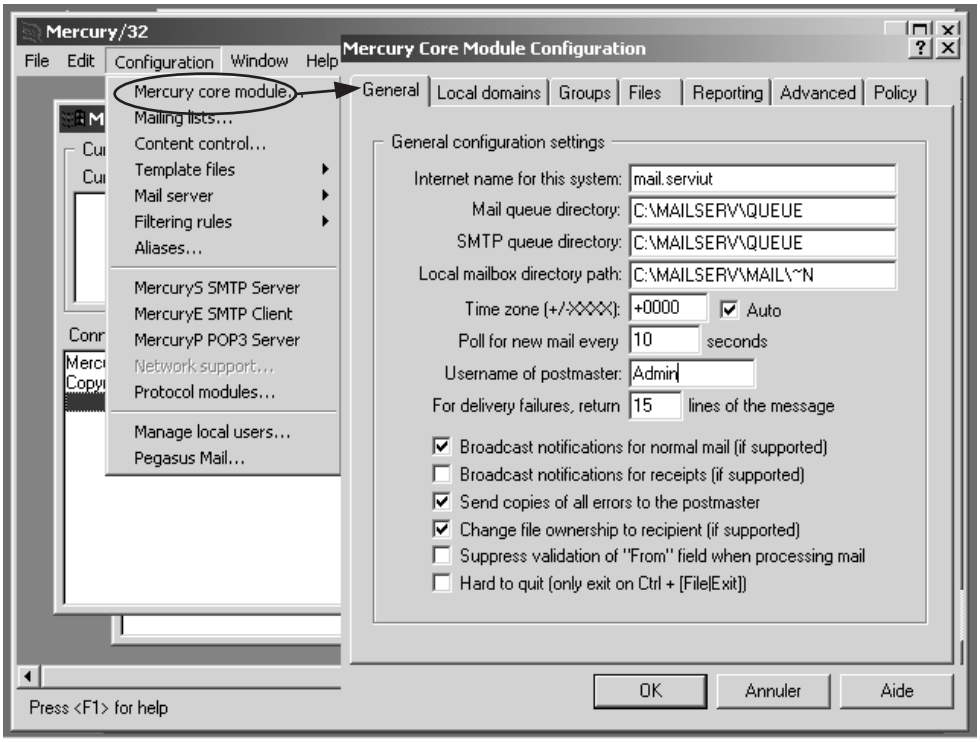

Figure 4.16 Paramètres d'installation d'un serveur de messagerie.

Un exemple d'installation/configuration de serveur de messagerie est détaillé en fin de chapitre dans l'étude de cas 1.

4.1.6 Les services webmail et listes de diffusion

a) Le Webmail

Ces serveurs permettent aux utilisateurs d'accéder à leurs boîtes aux lettres à partir de n'importe quel navigateur Internet. Le cœur du serveur webmail est un module logiciel d'interfaçage entre un serveur IMAP (plus rarement un serveur POP) et le navigateur du client. Ce logiciel, souvent écrit en PHP, code les messages en HTML et javascript, afin de les rendre compatibles avec les langages interprétés par les navigateurs. La figure 4.17 montre le principe de fonctionnement d'un module webmail.

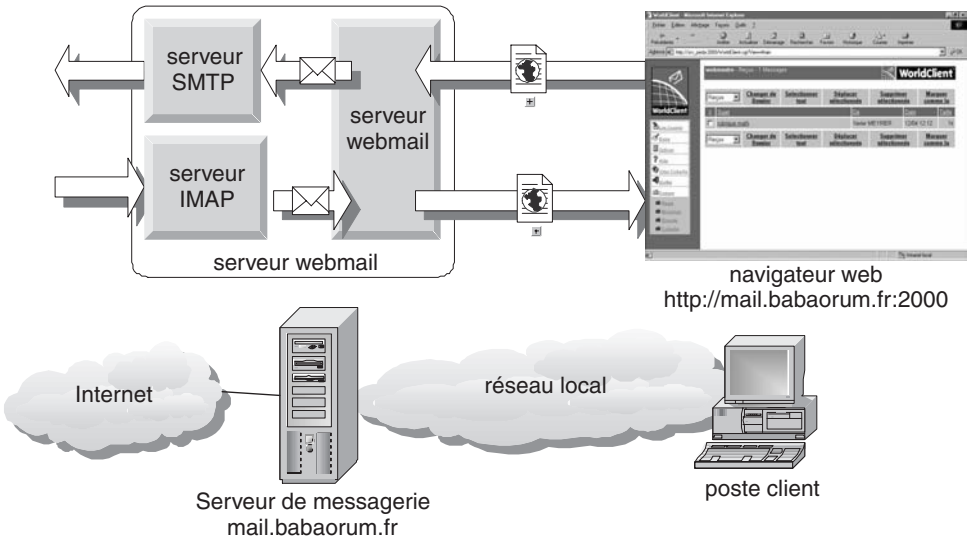

Figure 4.17 Principe d'un serveur Webmail.

Les messages étant stockés et rangés sur le serveur de messagerie, un serveur webmail s'interface plus naturellement avec un serveur IMAP. Les paramètres de session navigateur-serveur sont stockés dans une base de données (MySQL par exemple). Cette solution ne nécessite pas de configuration, ni d'installation sur les postes clients. La page de gestion des messages reçus et d'émission des messages est fournie par le serveur webmail lors de la connexion du client au serveur. L'étude de cas 2 en fin de chapitre montre les phases d'installation d'un tel serveur.

b) La liste de diffusion

Un serveur de liste de diffusion permet l'envoi d'un message à un ensemble de destinataires, sans que l'expéditeur n'ait besoin de connaître l'adresse de chacun

d'entre eux. Il associe à une adresse mail de diffusion une liste d'adresses mail. À réception du message dans la BAL, il retransmettra le message vers les BAL de chaque membre de la liste.

Le format de l'adresse de la liste est :

<nom de liste>@<nom.domaine du serveur de liste>

Si l'on veut envoyer un message à l'ensemble des professeurs du département SRC de l'IUT dont le domaine est iut.fr, en utilisant un serveur de diffusion comme le serveur « sympa », il suffira de créer une adresse *profs.src@sympa.iut.fr.* À cette adresse, une commande permettra d'inscrire les adresses mail des professeurs du département. Lors de l'envoi d'un message à l'adresse *profs.src@sympa.iut.fr,* le serveur dupliquera le message en autant de messages qu'il y a d'adresses mail de professeurs inscrits dans la liste. L'expéditeur du message n'a donc pas à connaître la liste exacte des destinataires, ni l'adresse de messagerie de chacun d'eux.

Le tableau 4.6 indique les commandes les plus courantes disponibles sur un serveur de liste de diffusion « sympa ». Elles sont envoyées dans le corps d'un message (une commande par ligne) adressé au serveur de liste (<nom du serveur>@<site du serveur>).

TABLEAU 4.6 PRINCIPALES COMMANDES D'UN SERVEUR DE LISTE DE DIFFUSION.

Commande	Objet	Commande	Objet
HELP	Liste des commandes	LIST	Liste des listes de diffusion
REVIEW *liste*	Liste des abonnés		
ADD *liste adresse nom prénom*	Ajouter un abonné par le propriétaire	DEL *liste adresse*	Enlever un abonné par le propriétaire
SUSCRIBE *liste prénom nom*	S'abonner sur liste ouverte	SIGNOFF *liste*	Se désabonner sur une liste ouverte

L'inscription/désinscription des destinataires sur la liste peut être libre (commandes SUSCRIBE/SIGNOFF). La liste est alors dite « ouverte ». Elle nécessite en général une mise à jour périodique par le propriétaire ou le modérateur de liste.

Dans certains cas, notamment pour des mesures de sécurité, les commandes d'inscription/désinscription seront bloquées pour les utilisateurs, et l'inscription ne se fera que par l'intermédiaire du propriétaire de la liste (commandes ADD/DEL). La liste est alors dite « fermée ».

Un troisième mode dit « contrôlé » peut être utilisé lorsque les demandes d'inscription de type SUBSCRIBE doivent d'abord être transmises au propriétaire avant d'être insérées ou non dans la liste par ce dernier.

Une liste de diffusion doit être créée par l'administrateur de la liste par la requête :

<nom de liste>-request@<site du serveur>

Il en devient le propriétaire. Les principaux paramètres à définir sont indiqués dans le tableau 4.7.

Tableau 4.7 Principaux paramètres d'une liste de diffusion.

Paramètre	Objet	Paramètre	Objet
Nom	Nom de la liste	Sujet	Résumé
Propriétaire	Responsable de la liste	Reply to	Adresse de liste, du propriétaire, autre
Utilisation	Publique, privée, modérée	Commande REVIEW	Tous, abonnés, propriétaire
Mode d'abonnement	Ouvert, contrôlé, fermé	Archivage	Oui/non, période

Outre le mode d'abonnement (ouvert, contrôlé ou fermé), il faut définir si l'utilisation de cette liste est pour tout le monde (liste publique), réservée aux abonnés (liste privée) ou si les messages doivent être adressés à un modérateur (liste modérée). De même pour la liste des abonnés qui peut être récupérée par tout le monde, les seuls abonnés ou uniquement le propriétaire.

4.1.7 Serveur de messagerie et sécurité

En tant que service le plus utilisé dans les entreprises, les serveurs de messagerie sont soumis à de nombreuses attaques et malveillances. Les plus classiques sont les virus, le spam et la violation des droits d'accès sur le serveur. Le contenu des messages donnant une image assez fiable de l'activité de l'entreprise, ils peuvent faire l'objet d'une « surveillance » dans le cadre d'une veille concurrentielle.

Pour lutter contre les attaques, les outils mis en œuvre sont de trois sortes :

– les filtres de messages ;
– les passerelles de messagerie ;
– les firewall.

Pour se mettre à l'abri de la veille sur les messages, la mise en œuvre d'une transmission sécurisée par cryptage est la méthode la plus efficace. Toutefois, le cryptage nécessite qu'expéditeur et destinataire disposent des clés de cryptage et de décryptage. Il s'ensuit que ce mode de transmission est limité aux messages internes à l'entreprise (en Intranet) ou avec des clients identifiés tels que sous-traitants, clients réguliers (en Extranet par exemple ou pour des dialogues de type *Business to Business*). Ce type de transmission n'est pas utilisable dans le cas de clients occasionnels ou du grand public. Dans ce cas, il peut être intéressant d'utiliser un serveur de messagerie pour chacune de ces deux familles d'interlocuteurs. Le mode SSL de transmission proposé pour les connexions TCP/IP est applicable dans le cas du dialogue entre les postes clients et un serveur webmail. L'utilisation d'un firewall est expliquée au paragraphe 5.4.3, *Les serveurs HTTP : configuration et sécurisation*.

Les passerelles de messagerie permettent de centraliser la réception des messages. Leur intérêt est réel pour une entreprise disposant de plusieurs serveurs de messagerie ou pour un fournisseur d'accès Internet (FAI) distribuant le courrier vers

plusieurs serveurs de messagerie « clients ». La figure 4.18 montre l'infrastructure d'un service de messagerie utilisant une passerelle dans les deux cas décrits.

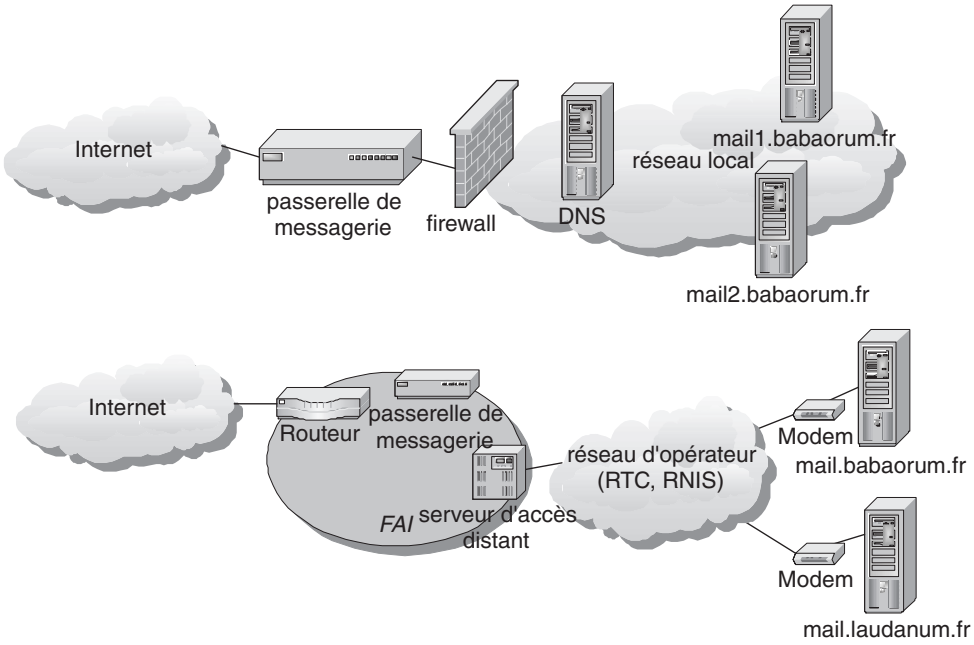

Figure 4.18 Utilisation d'une passerelle de messagerie.

Un ensemble de BAL est créé sur chaque serveur de messagerie pour recevoir l'intégralité du courrier en provenance de la passerelle. La passerelle est configurée pour associer cette BAL au serveur auquel est destiné le courrier entrant. Dans le premier exemple de la figure 4.18, une BAL « mailin » serait créée sur le serveur « mail1.babaorum.fr ». La configuration de la passerelle serait alors :

Serveur de messagerie	Adresse de transfert	Adresse d'expédition
Mail1.babaorum.fr	mailin@mail1.babaorum.fr	Mailbridge.babaorum.fr

Le message dont les adresses source et destination seraient :

```
From : asterix@mail.laudanum.fr
To : obelix@mail1.babaorum.fr
```

serait retransmis par la passerelle dans un message dont l'en-tête contiendrait :

```
Received: from mailbridge.babaorum.fr
   by mail1.babaorum.fr
   for <mailin@mail1.babaorum.fr>
```

```
Received : from mail.laudanum.fr
   by mailbridge.babaorum.fr
   for <obelix@mail1.babaorum.fr>
Received : from asterix.laudanum.fr
   by mail.laudanum.fr
for <obelix@mail1.babaorum.fr>
```

Les passerelles peuvent assurer l'archivage périodique et automatisé des messages. Elles proposent également les fonctionnalités de filtrage des messages. Ces filtres effectuent la détection des virus, des spam et les violations de droits d'accès. Le filtrage consiste à analyser les en-têtes et les contenus des messages entrants et vérifier s'ils ne sont pas incompatibles avec les configurations interdites dans les règles du filtre (fichiers « exe », « gif », adresses interdites…). En cas de détection d'anomalie, les messages peuvent être détruits ou stockés dans un répertoire particulier pour être traités par l'administrateur. Certains filtres attribuent un « coefficient de confiance » aux messages. Les règles d'analyses sont fixées par l'administrateur. Elles doivent être actualisées régulièrement.

4.2 LE SERVICE DE TRANSFERT DE FICHIERS

4.2.1 Architecture et fonctionnement d'un serveur de fichiers

Il permet à un client d'échanger des fichiers avec un serveur de fichiers en accédant directement et de manière sécurisée (sauf connexion « anonymous ») à l'arborescence des répertoires de ce dernier. C'est un outil très utile pour le travail coopératif (*groupware*). Il permet à un groupe (équipe de projet par exemple) de travailler et de s'échanger des documents de travail sans multiplier les copies, comme cela se passe dans le cas d'un échange par messagerie (sauf avec le Webmail). Son utilisation permet également la mise à jour à distance de pages d'un serveur web (voir *Étude de cas 3* du présent chapitre).

La procédure commence par l'établissement d'une connexion (niveau TCP) entre un client et le serveur. Une fois la connexion établie, le client dialogue avec le serveur en lui envoyant des « commandes » à exécuter. La connexion et le dialogue entre la station du client et le serveur utilisent le protocole FTP (*File Transfer Protocol*). Le serveur FTP dispose de deux types de répertoires : les répertoires « privés » accessibles uniquement aux clients possédant un compte sur le serveur, compte auquel sont associés des droits d'accès sur certains répertoires « privés », et les répertoires « publics » accessibles aux autres clients (comptes « anonymous »).

Après qu'un client se soit connecté au serveur, celui-ci demande un nom de compte et un mot de passe (figure 4.19). Le compte *anonymous* permet au client d'accéder aux fichiers des répertoires « public ». Dans ce cas, le mot de passe demandé est généralement l'adresse e-mail du demandeur.

Les logiciels sur la station du client disposent des commandes permettant de se déplacer dans l'arborescence du disque du serveur, de définir le type des données

transférées (binaire ou ASCII), de manipuler des fichiers (écrire, lire, effacer, renommer, transférer…). Le protocole FTP fonctionne, côté serveur, avec deux canaux distincts. Par défaut, ces canaux sont ouverts sur les ports TCP (figure 4.19) :

– 20 pour le canal de données ;
– 21 pour le canal de commande.

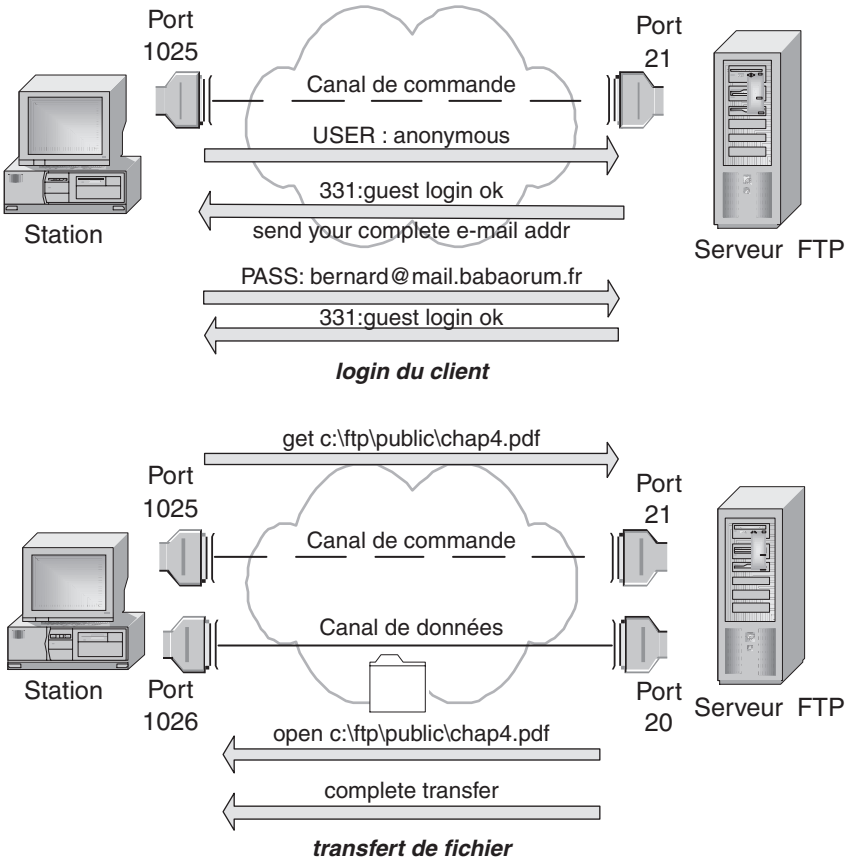

Figure 4.19 Connexion FTP.

La connexion peut donc être effectuée de deux façons :

– en anonyme (name : *anonymous*, password : *bernard@babaorum.fr*) pour un accès limité aux répertoires publics ;
– en compte authentifié pour un accès associé à des permissions sur des fichiers ou des répertoires particuliers.

Les commandes de l'utilisateur (user, password, dir, get…) utilisées sur le logiciel client sont traduites en commandes internes FTP (USER, PASS, LIST, RETR...)

suivies éventuellement d'arguments (nom d'utilisateur, nom de répertoire) ou de données correspondant au fichier transféré. Ce protocole défini par les normes RFC 959 et 1123 est décrit au § 9.5 de l'ouvrage *Transmissions et Réseaux*[1].

La plupart des logiciels de navigation sur le Web intègrent les fonctions permettant la connexion aux serveurs et le transfert des fichiers.

Dans ce cas, l'URL spécifié sera du type *ftp://ftp.babaorum.fr/public* pour une connexion anonyme, ou *ftp://name:password@ftp.babaorum.fr/public* pour une connexion identifiée. Il faut noter toutefois que si la lecture et le téléchargement de fichiers se font aisément à l'aide du « glisser/déposer », l'écriture de fichiers vers le serveur n'est pas toujours possible à partir d'un navigateur. Il est préférable d'utiliser un logiciel client, graphique ou non, spécialisé dans le transfert bidirectionnel FTP.

Toutes les versions de Windows ou d'Unix disposent d'un exécutable « ftp » en mode « ligne de commande ». D'autres logiciels clients tels *WS_FTP* de Ipswitch Inc ou *CuteFTP* de GlobalSCAPE Inc fonctionnent en mode graphique et présentent quelques fonctionnalités supplémentaires (répertoire des sites FTP, programmation et reprise automatique du téléchargement en cas de déconnexion, recherche de fichiers…).

Internet Information Server de Microsoft, *WS_FTP Server* de Ipswitch Inc, *wu-ftpd* et *proftpd* en version libre pour Linux sont quelques-uns des logiciels serveurs FTP.

Les caractéristiques des serveurs FTP porteront principalement sur :

– le nombre de clients pouvant être servis simultanément. Cette capacité tient également compte de l'architecture de l'ordinateur sur lequel le service est implémenté (voir § 5.1.2, *Les serveurs HTTP : configuration et sécurisation*) ;
– la sécurisation des transferts de fichiers, et notamment la possibilité de supporter les transmissions utilisant le protocole SSL et la limitation du nombre de login erronés ;
– l'utilisation par le serveur d'une base de données de comptes existante (base ODBC ou *Windows Active Directory* par exemple) ;
– la souplesse d'affectation des permissions (par fichier, par répertoire, par client…).

4.2.2 Configuration d'un serveur FTP

a) Principe

Un serveur FTP comporte généralement trois répertoires :

– le répertoire d'installation de l'application (*binary direct*ory) ;
– le répertoire de stockage des fichiers et sous-répertoires accessibles (*FTP directory*) ;

1. Lohier S. et Présent D., *Transmissions et Réseaux*, 3e édition, Dunod, 2003.

– le répertoire de « login » où sont stockés les fichiers liés à l'identification des clients ou à la base de donnée (*log directory*).

La configuration d'un serveur FTP comporte quatre phases :

1. Créer l'arborescence des sous-répertoires et des fichiers dans le répertoire de stockage.
2. Créer les comptes des clients identifiés.
3. Associer des droits d'accès à chaque client, groupe de clients et aux utilisateurs du compte « anonymous ».
4. Créer les outils d'administration qui donneront des informations sur l'activité du serveur (journaux de login, des téléchargements, d'alerte…).

L'arborescence des répertoires sera choisie pour simplifier la gestion des droits d'accès des clients. Cette arborescence est liée à la manière dont le serveur sera utilisé par les clients. Les solutions sont nombreuses, mais il est important de planifier sur papier cette arborescence avant de la créer sur le serveur. Il est possible de donner quelques points de repère. Pour un serveur FTP interne à une entreprise, l'arborescence s'inspire souvent de l'organisation fonctionnelle de celle-ci. Les salariés ayant une même fonction auront souvent les mêmes droits d'accès sur les répertoires et fichiers. Par contre pour un serveur ouvert au grand public (serveur d'un éditeur, d'un organisme public par exemple), l'arborescence sera thématique afin de faciliter la recherche du client.

Il faut rappeler que dans l'arborescence du serveur, des fichiers et/ou répertoires peuvent être « cachés », c'est-à-dire invisibles et inaccessibles des clients identifiés ou non. En général, le nom d'un fichier ou répertoire caché commence par le caractère « $ ».

Si vous utilisez la base de données du serveur FTP, vous créerez les comptes clients avec l'outil d'administration du serveur. Sinon, il vous faudra les créer avec l'outil d'administration associé à la base de données de comptes. Le serveur FTP aura été configuré pour utiliser cette base (chemin d'accès à la base de données, son nom, nom de la table à utiliser, éventuellement le nom du domaine où se trouve le serveur). Par contre, le compte *anonymous*, créé à l'installation, sera en général configuré avec les outils de gestion des comptes du serveur FTP.

Pour chaque utilisateur ou groupe d'utilisateurs, il faut définir le répertoire auquel il aura accès à l'issue de son « login ». Par défaut, un utilisateur aura accès au répertoire qui porte son nom avec tous les droits (créer/lire/effacer des fichiers, des répertoires). Il est possible de spécifier un autre répertoire (répertoire du projet auquel travaille l'utilisateur). Il est également possible de limiter l'espace disque alloué à l'utilisateur, ainsi que le nombre de fichiers.

Il faut ensuite définir les droits d'accès aux répertoires. Cela se fait répertoire par répertoire, soit avec l'outil d'administration du serveur FTP, soit avec celui de la base de données (base de Windows par exemple). Pour chaque utilisateur ou groupe autorisé à accéder au répertoire, on définira les droits associés. Ces droits de base sont : lister, lire, écrire, effacer ou renommer. De nombreux serveurs FTP offrent la

possibilité de travailler avec les droits définis avec les outils d'administration du système d'exploitation (Windows NT, Windows 2000 ou Linux).

Il reste à déclarer le serveur FTP et paramétrer les outils d'administration. Déclarer le serveur consiste à lui donner un nom, une adresse IP visible de tous les utilisateurs potentiels et le domaine dans lequel il se trouve. Il est également possible de paramétrer la déconnexion d'un client après un temps programmé d'inactivité de la connexion ; le nombre d'utilisateurs connectés simultanément (clients identifiés et « anonymous ») ; le mode de transmission (sécurisé ou non) ; l'utilisation ou non des connexions « anonymous ». Il est souvent possible d'interdire l'exécution de certaines commandes et de contrôler l'accès par les adresses IP (seules certaines plages d'adresses IP seront autorisées à se loguer). Il est recommandé de définir un fichier « log » qui mémorisera tous les accès au serveur, les accès et commandes refusées. Certains serveurs proposent d'établir des statistiques sur les performances du serveur (taux d'accès, bande passante utilisée…). Ces outils sont très utiles pour comprendre les dysfonctionnements pouvant se produire.

b) Exemple de configuration

L'exemple suivant utilise le logiciel serv-U de Cat-soft (*www.cat-soft.com*). Il permet d'installer un serveur FTP sur un poste de travail sous Windows. Il comporte de nombreuses fonctionnalités d'un service FTP. Le serveur installé se nommera *ftp.iut.fr*. Les utilisateurs disposeront d'un répertoire propre (à leur nom) et auront accès à un répertoire de groupe (espace de travail de *groupware*). Seul le chef du groupe aura la possibilité d'effacer des fichiers ou des répertoires. Les membres d'un groupe pourront consulter les données des autres groupes, mais ne devront pas pouvoir modifier quoique ce soit.

Après installation du logiciel, il faut lancer la console d'administration. La configuration comporte trois étapes :

1. Création d'un domaine associé au serveur.
2. Configuration du domaine.
3. Création et configuration des droits d'accès des clients.

➤ 1. Création d'un domaine associé

Dans la fenêtre qui s'affiche (figure 4.20) il faut créer un (plusieurs) domaine(s) associé(s) au serveur. Cela peut se faire dans le menu « domaine » par l'option « new domain », ou en sélectionnant l'icône « domains » dans l'arborescence de la fenêtre de gauche et en actionnant la touche « Inser » au clavier. Un assistant permet de définir les paramètres du domaine (figure 4.20 fenêtre de droite).

Le champ « security » permet de paramétrer des transferts cryptés.

➤ 2. Configuration d'un domaine

L'icône « setting » du domaine créé, permet de le configurer. Les paramètres des deux principaux onglets de configuration sont présentés figure 4.21.

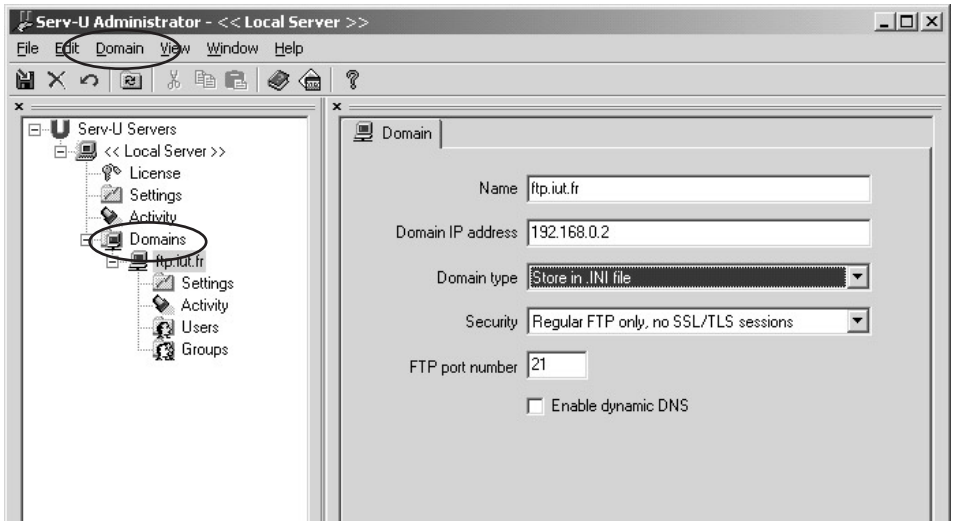

Figure 4.20 Paramètres du domaine associé au serveur.

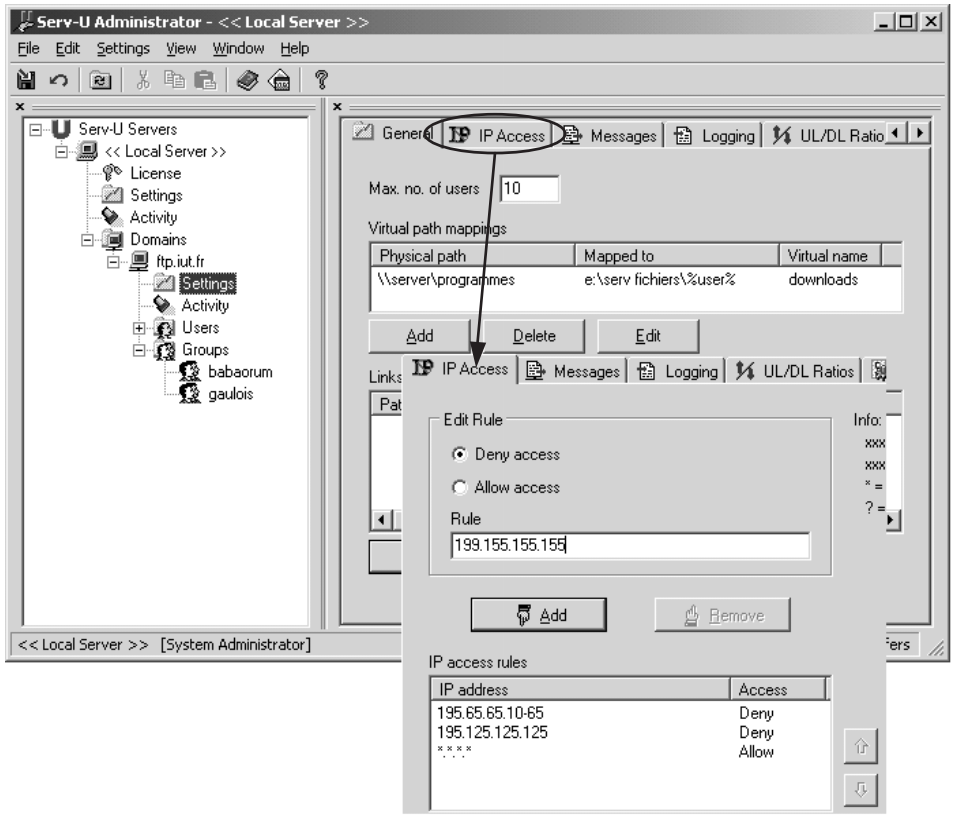

Figure 4.21 Configuration du domaine.

L'onglet « general » permet d'associer des répertoires locaux ou distants qui apparaîtront au client sous un nom de répertoire virtuel. L'exemple montre comment associer le répertoire « programmes » situé sur le serveur « server » au répertoire du client situé sur le serveur ftp. Ce répertoire apparaîtra dans l'arborescence accessible par le client sous le nom « download ». Cette procédure permet de restreindre l'accès du client à son propre répertoire tout en lui donnant accès à des répertoires situés sur d'autres unités de stockage locales ou distantes, augmentant ainsi la sécurité du site.

Dans l'onglet « IP Access » seront définies les règles d'autorisation et d'interdiction d'accès au domaine pour des machines dont les adresses IP sont connues. Les règles sont appliquées dans l'ordre où elles sont affichées. Il faut donc commencer par valider toutes les adresses qui ne sont pas interdites. Cette action est représentée par la dernière ligne de la fenêtre (*.*.*.* allow). Pour entrer une règle, il faut choisir celle-ci en validant « deny access » ou « allow access », puis entrer l'adresse ou le bloc d'adresses dans le champ « Rule », et enfin valider en cliquant sur le bouton « add ». Dans l'exemple de la figure 4.21, l'accès des machines utilisant une adresse du bloc 195.65.65.10 à 195.65.65.65 (1re ligne) ou l'adresse 195.125.125.125 (2e ligne) est interdit.

➤ 3. Création et droits d'accès des clients

L'assistant à la création d'un client s'obtient à partir du menu « users » par l'option « new user », ou en sélectionnant l'icône « users » dans l'arborescence de la fenêtre de gauche et en actionnant la touche « Inser » au clavier. L'assistant permet de remplir les champs de la fenêtre « account » (figure 4.22 fenêtre de droite).

L'assistant permet de configurer les nom, mot de passe, groupe d'appartenance, répertoire propre, ainsi que les droits d'administration éventuels du client. L'onglet « general » contient les paramètres définissant le temps de login sans action et la bande passante attribuée aux téléchargements du client. Les répertoires et fichiers accessibles au client, et les droits d'accès sont configurés dans l'onglet « Dir Access » (figure 4.22). Dans le cas présenté, le client « Abraracourcix », chef du groupe « gaulois » a accès à son répertoire propre et au répertoire du groupe « gaulois » avec tous les droits. Les autres membres du groupe gaulois auront accès à ces deux répertoires, mais sans les droits d'effacer un fichier ou un répertoire.

L'onglet « IP Access » autorise l'accès aux répertoires et fichiers aux seuls postes dont l'adresse IP est répertoriée. Un onglet « Quota » permet de fixer la taille maximum de l'espace disque affecté au client et d'indiquer l'espace disque réellement occupé.

Les fichiers et répertoires, les droits d'accès et le filtrage des adresses IP peuvent être définis pour des groupes d'utilisateurs. La création de ces groupes utilise la même procédure que celle utilisée pour la création des clients.

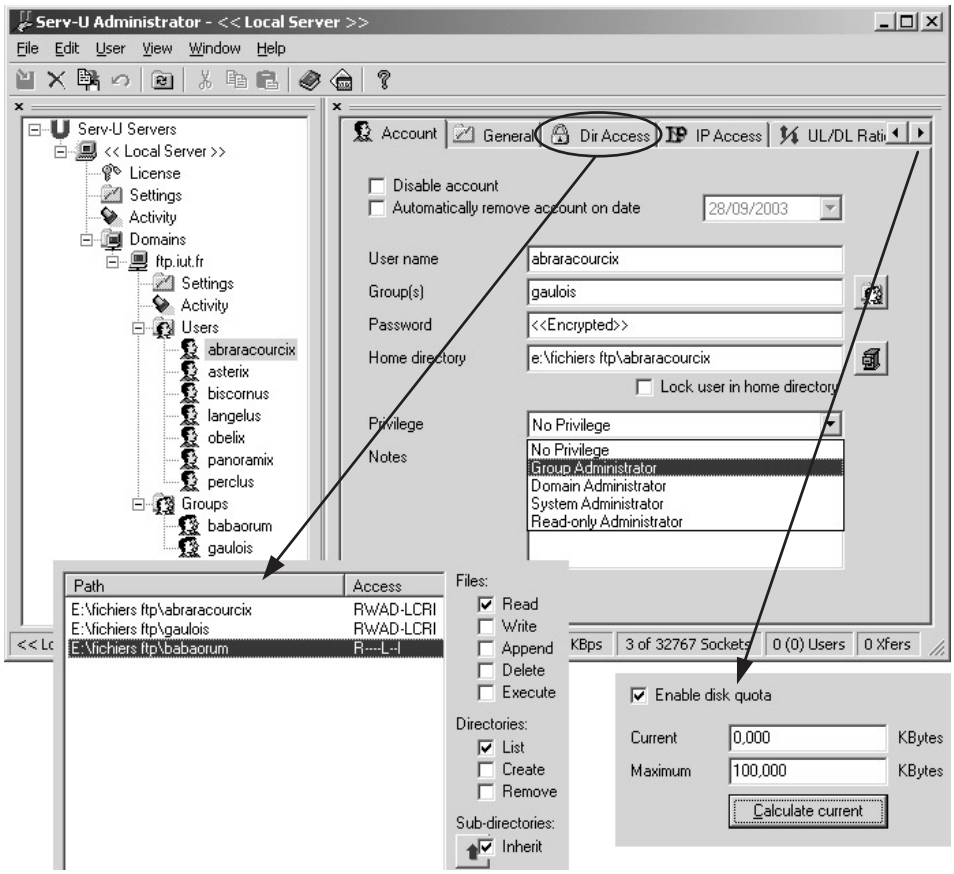

Figure 4.22 Création et configuration des droits d'un client.

4.3 LE SERVICE WEB

4.3.1 URL et protocole HTTP

a) Service web et hypertexte

Il permet d'accéder à des documents au format HTML (*Hyper Text Markup Language*) stockés sur un serveur, en utilisant pour la connexion et les échanges le protocole HTTP (*Hyper Text Transfer Protocol*). Les documents sont accessibles par un URL (*Uniform Ressource Locator*) comportant le nom du serveur http contenant le document, le chemin d'accès au document et le nom de celui-ci.

Les serveurs HTTP les plus courants sont Netscape Entreprise Server, Apache HTTP Server, Microsoft Internet Information Server et NetWare Web Server de Novell.

Pour accéder aux serveurs web, les stations doivent être équipées de navigateurs Internet. On trouve *Internet Explorer* de Microsoft, *Netscape Navigator* ou *Netsurfer* de NetManage.

Le protocole de communication HTTP (*HyperText Transmission Protocol*) utilisé entre le navigateur du client et les serveurs web est basé sur le principe des liens hypertextes. Ces liens sont repérés par des mots de couleur différente (bleu en général) ou des images qui servent de liens entre les documents. Il suffit de cliquer sur un lien pour accéder à un autre document localisé sur le même serveur ou sur un autre, pouvant être situé n'importe où sur le réseau Internet. Ces liens hypertextes rendent la lecture dynamique et permettent de « naviguer » sur une bibliothèque à l'échelle planétaire.

Un mécanisme de changement de couleur est utilisé pour savoir qu'un lien a déjà fait l'objet d'une visite (en général violet), le changement de couleur est réalisé non seulement sur la page de départ mais aussi sur toutes les pages qui font référence au même document. Les liens hypertextes peuvent adresser d'autres documents de type web (images, sons, vidéos…) mais aussi des serveurs de fichier, des serveurs de News…

Les URL (*Uniform Resource Locators*) sont les noms donnés aux liens hypertextes. Un URL peut relier à un fichier sur un serveur ftp, une image, une adresse courrier, un serveur de News, un serveur telnet et bien sûr un serveur http, c'est-à-dire un serveur web. La figure 4.23 donne des exemples de fichiers accessibles par URL à partir d'une page HTML : l'image (fichier gif ou jpeg par exemple) se trouve sur un serveur accessible par le réseau Internet, alors que le fichier son (fichier wav par exemple) et le fichier texte (fichier html par exemple) sont localisés sur le serveur http du réseau de l'entreprise. Quelques syntaxes d'URL :

– *http://www.babaorum.armor.fr* donne accès à la page par défaut du serveur web *babaorum.armor.fr* ;
– *ftp://ftp.laudanum.fr* permettra d'accéder au serveur de fichiers *ftp.laudanum.fr* ;
– *http://serveur/directory/fichier.htm* adresse le fichier au format html stocké sur le serveur « serveur » situé sur le réseau local ;
– *file:///c:/temp/fichier.txt* donne accès à un fichier texte situé sur le disque du poste du client (disque local).

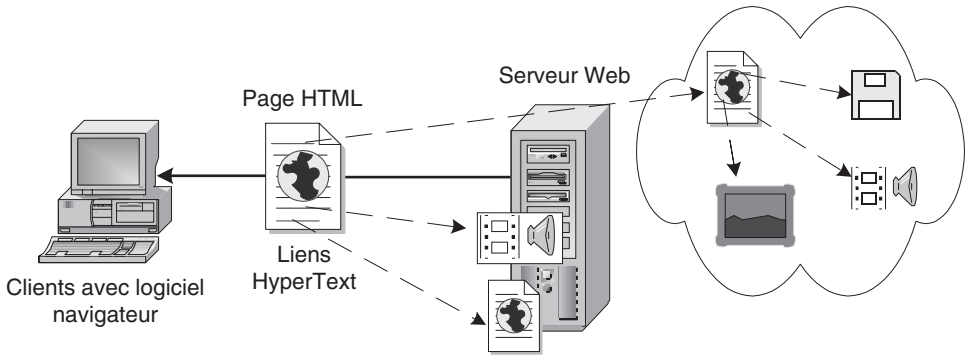

Figure 4.23 Localisation de fichiers par URL.

b) Dialogues du protocole HTTP

Le navigateur web du client utilise le port TCP 80 (par défaut) pour établir une connexion avec le serveur web. Un port non standard peut être utilisé. Il doit être précisé dans l'URL exemple :

```
http:// www.someorg.com:8080
```

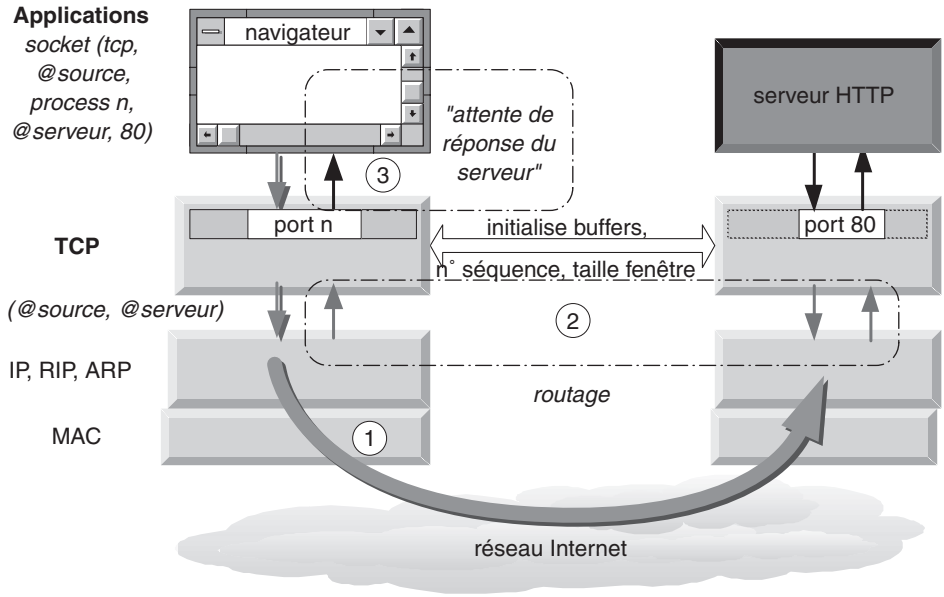

Figure 4.24 Phases de connexions d'un navigateur à un serveur http.

La figure 4.24 montre les phases de connexion d'un navigateur :

– 1. Le navigateur ouvre une session TCP en utilisant une « *socket* ». Cette fonction logicielle contient tous les paramètres nécessaires à la demande de connexion de niveau 4 au serveur http. Le protocole transmet la demande à la pile de protocoles réseaux (IP, RIP, MAC) qui assure le routage de la demande jusqu'au serveur.
– 2. Le protocole TCP initialise la session en échangeant avec le protocole TCP du serveur les paramètres de dialogue (voir paragraphe 3.4, *Les protocoles de niveau transport : UDP et TCP*).
– 3. Le protocole TCP avertit l'application que la session est ouverte avec le serveur et qu'il attend la page par défaut (message « attente de réponse du serveur »).

Une fois la connexion établie avec le serveur, le client va, en sélectionnant des liens hypertextes, envoyer des requêtes au serveur. Les requêtes contiennent la méthode à utiliser pour récupérer le document, le nom de l'objet demandé et la version du protocole HTTP à invoquer. Le protocole HTTP communique ses informations au format texte afin de ne pas être gêné par les différences d'implémentation

des jeux de caractères d'une plate-forme à l'autre. Exemple de requête HTTP envoyée par un navigateur web demandant un document :

```
GET /Web/docs/index.html HTTP/1.0
```

La figure 4.25 montre le principe de dialogue par requêtes entre le navigateur et le serveur pour l'obtention des documents à visualiser sur le poste client.

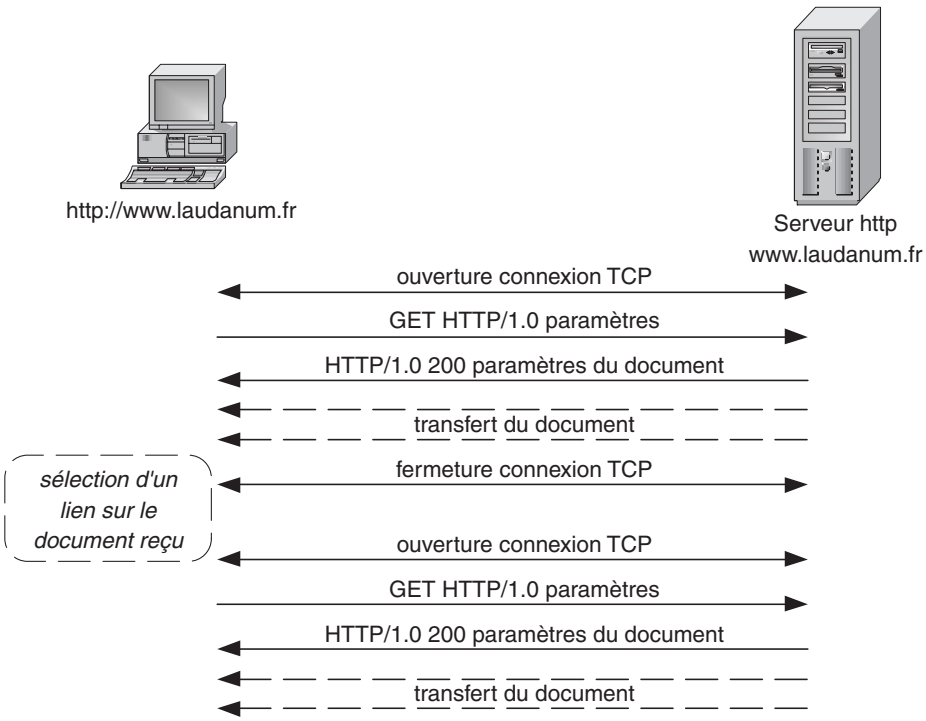

Figure 4.25 Dialogue par requêtes du navigateur et du serveur http.

D'autres commandes peuvent être utilisées pour n'obtenir que l'en-tête associé à la ressource demandée (commande HEAD) ou pour envoyer des données de type formulaire au serveur (commande POST). Le serveur répond à la requête en envoyant une réponse HTTP composée de trois parties : état de la réponse/en-tête de réponse/données. L'état de la réponse est une ligne de texte avec la version de HTTP utilisée par le serveur, un code d'état décrivant le résultat du serveur (200 pour un acquittement, 400 pour une erreur due au client, 500 pour une erreur due au serveur…) et quelques informations supplémentaires. Par exemple :

```
HTTP/1.0 200 OK
```

L'en-tête de réponse contient des informations relatives au type du serveur, à la version de MIME utilisée pour décrire le type de contenu, et une ligne vide (elle sert de séparateur entre l'en-tête de réponse et les données).

Par exemple :

```
Date: Tuesday, 05-Nov-96 23:42:34 GMT
      Server: Novell-HTTP-Server/2.5
      MIME-version: 1.0
      Content type:text/html

      « données » (notez la présence d'une ligne vide)
```

MIME est une méthode d'encodage des données (voir paragraphe 4.1.3, *Les protocoles de messagerie*) utilisée par html pour décrire les différents types de données qu'il doit manipuler. La ligne *Content type* est une description MIME des données transférées ; *text/html* indique que les données sont de type texte, sous-type HTML.

Un autre type courant est text/plain, qui indique que la réponse est à traiter comme du texte brut. Si le document demandé est un document HTML, les données de réponse contiendront le texte du document HTML. Exemple de données de réponse :

```
<HTML>
<HEAD><TITLE>Document HTML simple</TITLE></HEAD>
<BODY> <P> Cela est un document HTML minimaliste.</P> </BODY>
</HTML>
```

Il faut noter qu'une page est constituée de plusieurs fichiers textes et images. Ces fichiers sont disposés sur une trame découpant la surface de la page en zones matérialisées par les cases d'un tableau. Pour chaque fichier à charger pour afficher dans la page, le navigateur va créer un processus. Ce processus va, par l'intermédiaire d'une « socket » amener l'établissement d'une connexion par TCP.

La figure 4.26 montre les connexions établies par TCP pour le chargement du fichier texte et du fichier image constituant la page à visualiser. Le premier processus (process 1) gère l'initialisation de la connexion avec le serveur http. Les deux autres processus (process 2 et process 3) permettent le chargement des deux fichiers constituant la page. Il est facile de comprendre que la rapidité de chargement d'une page sur un navigateur dépend non seulement du débit sur le réseau de transmission (réseaux Internet et lignes ou réseaux de connexion à Internet), mais également de la complexité de la page à afficher, et de la rapidité et de la charge du ou des serveurs sur lesquels sont stockés les fichiers constitutifs de la page.

Certaines pages étant affichées plusieurs fois au cours de la navigation sur un site, le navigateur accélère l'affichage en stockant les fichiers chargés sur le disque local. Deux conséquences principales pour la station client :

– sans précaution particulière les fichiers s'entassent sur le disque du poste client ;
– des malveillances peuvent être opérées en stockant sur le disque des fichiers qui vont s'exécuter sur le poste du client et apporter des perturbations, voir des dysfonctionnements pouvant aller jusqu'à des pannes de l'ordinateur.

Il faut donc apporter un soin particulier à la configuration du navigateur d'une part et à la protection du poste par « firewall » personnel d'autre part. Ces deux points sont abordés dans les paragraphes suivants.

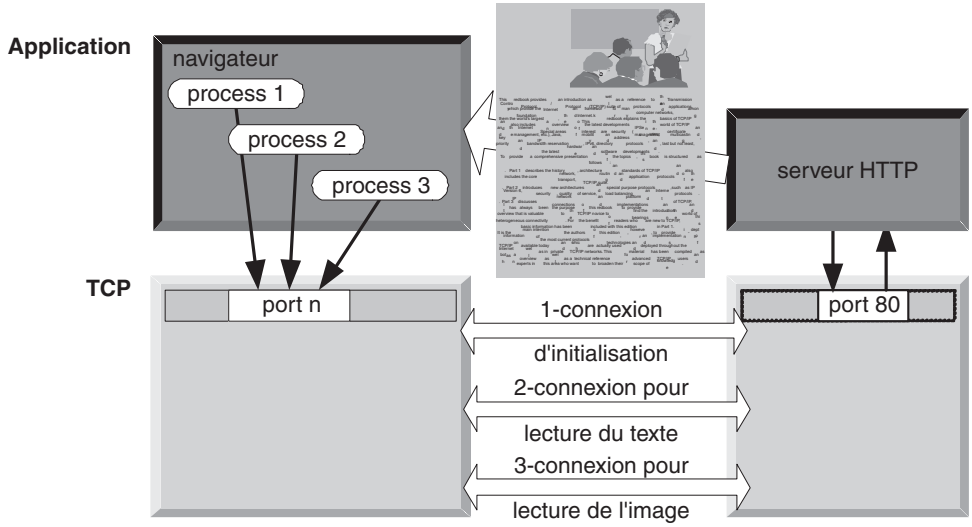

Figure 4.26 Chargement des fichiers d'une page.

4.3.2 Configuration d'un navigateur

Il s'agit de montrer ici la configuration de paramètres permettant de protéger le poste de l'envahissement du disque par stockage de fichiers inutiles. Deux types de fichiers sont visés : les « cookies » et les fichiers temporaires. La configuration est accessible dans la fenêtre des « propriétés » d'Internet Explorer (menu « propriétés » après un clic droit sur l'icône de l'application). La gestion des « cookies » est paramétrable dans la fenêtre « paramètres de sécurité ». Dans Windows 2000, trois niveaux de sécurité sont disponibles (figure 4.27). Le paramètre « demander » affichera, lors de l'arrivée d'un « cookie » un message d'alerte, demandant à l'utilisateur s'il accepte ou non le stockage du fichier sur le disque dur.

Sous Windows, les « cookies » sont stockés par défaut sur le disque dur dans l'un des deux répertoires suivants propre à chaque « client » : « c:\documents and settings\« client »\cookies », ou « c:\ documents and settings\ « client »\local settings\ temporary Internet Files ». Ce dernier répertoire est un répertoire caché. Certains sites web refusent l'affichage des pages lorsque le client refuse les cookies. Parmi ceux-ci, certains utilisent les « cookies » pour obtenir des informations sur le fonctionnement du navigateur, nécessaires au paramétrage des données qu'ils envoient. Cette méthode est utilisée pour certaines liaisons « sécurisées » de paiement électronique par exemple, ou des serveurs de vidéo utilisant la technique du « streaming ». Par contre, beaucoup de sites utilisent les « cookies » sans qu'ils soient nécessaires au bon fonctionnement du navigateur. Les informations récupérées par le serveur web peuvent occasionnellement servir d'informations « commerciales » sur les habitudes et le type de matériel de l'internaute, pouvant éventuellement être « revendues » à des entreprises. Mais ceci relève du domaine de la sécurité informatique et de l'intelligence économique.

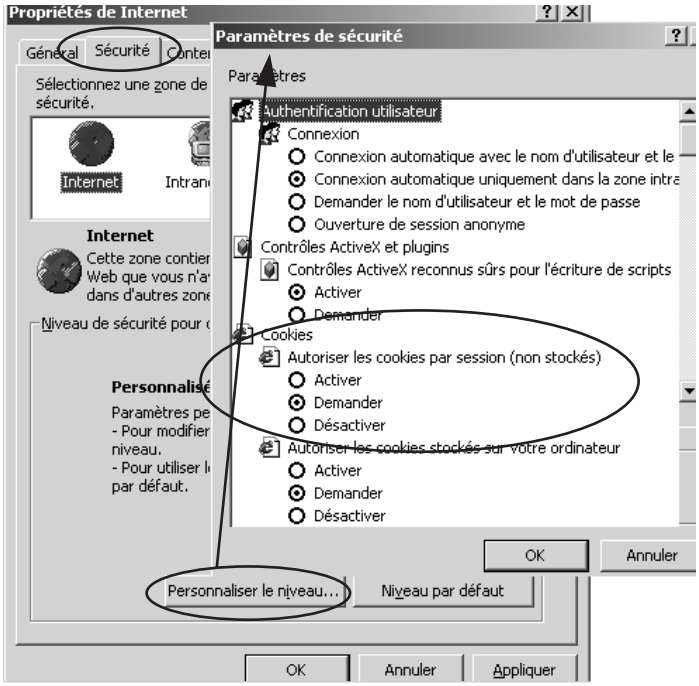

Figure 4.27 Configuration de la gestion des « cookies » dans un navigateur.

Lors de la navigation sur un serveur web, certaines pages ou objets sont stockés temporairement sur le disque dur de l'internaute. Le répertoire par défaut utilisé par Internet Explorer est un répertoire caché propre à chaque client « c:\documents and setting\ « client »\local settings\temporary Internet Files ». Ces fichiers peuvent encombrer inutilement le disque dur, et ralentir le fonctionnement de l'ordinateur. Deux méthodes permettent de les supprimer : paramétrer le navigateur pour supprimer ces fichiers lors de la fermeture du navigateur, ou effectuer un nettoyage du disque. La figure 4.28 montre le paramétrage du navigateur permettant la suppression automatique des fichiers temporaires stockés.

L'utilitaire « nettoyage de disque » (menu « outils système » de « accessoires » dans « programmes ») permet d'effacer les fichiers temporaires Internet. Il faut noter que cet utilitaire ne supprime que les fichiers du client de la session en cours, et n'efface pas les fichiers stockés dans le répertoire « cookies ».

4.3.3 Configuration d'un « firewall » personnel

Cet outil logiciel permet de contrôler les données entrantes et sortantes d'un client et plus généralement de tout poste d'extrémité « client » ou « serveur ». Il est le complément utile d'un pare-feu matériel. Il s'agit d'une application qui intercepte tous les paquets transitant entre la carte réseau et le système d'exploitation et pour certains entre l'application et le système d'exploitation, comme le montre la figure 4.29.

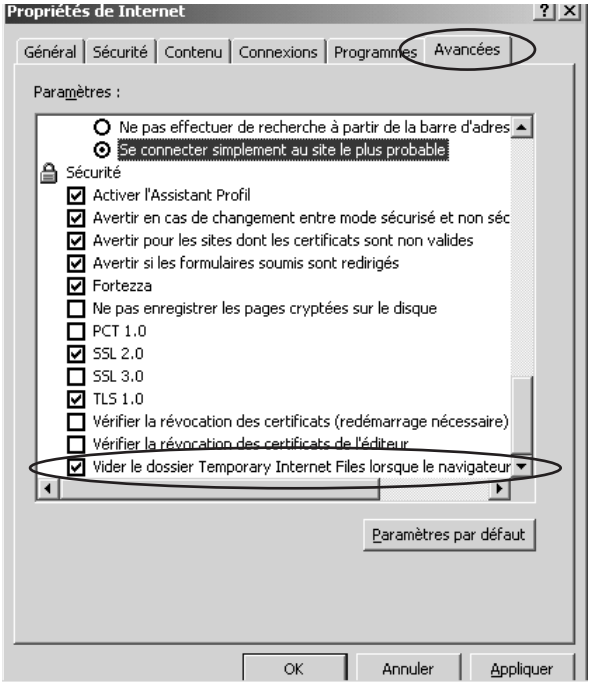

Figure 4.28 Paramétrage de la suppression automatique des fichiers temporaires.

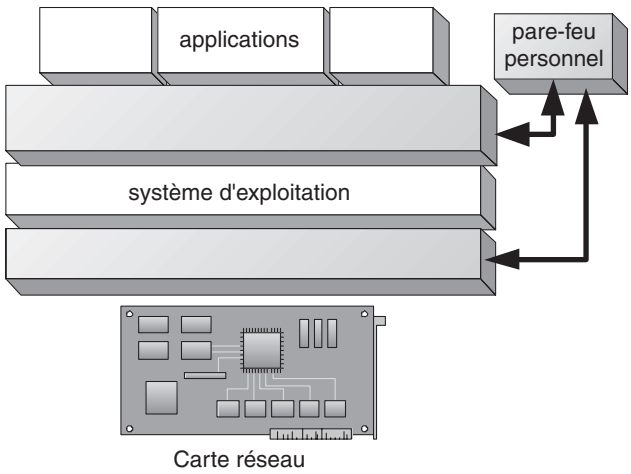

Figure 4.29 Architecture logicielle d'un « firewall » personnel.

Bien sûr, cette application va ralentir légèrement le traitement des données échangées avec le réseau. Elle fonctionne comme un pare-feu classique, en comparant les en-têtes des paquets entrant et sortant à une liste de règles établies par l'utilisateur. Pour chaque application et logiciel réseau, les règles vont autoriser ou interdire le traitement des paquets suivant leur adresse source, destination, protocole et/ou port source ou destination. La figure 4.30 donne un exemple de telles règles éditées dans la fenêtre d'administration du pare-feu. « Kério Personnal Firewall » de Kério Technologies Inc. (*www.kerio.com*).

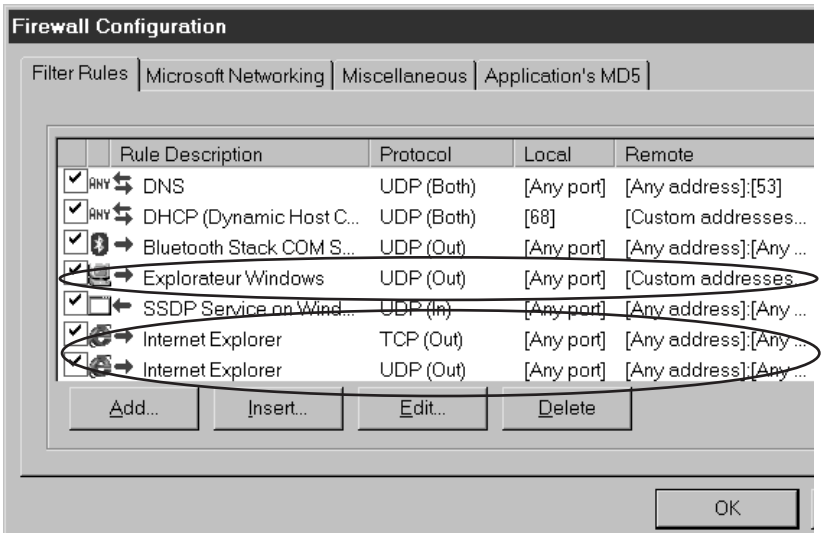

Figure 4.30 Règles de traitement des paquets par « Kério personnal firewall ».

Dans l'exemple présenté, le filtrage des paquets ne se fait que sur les adresses IP. La première règle entourée concerne l'application « Explorateur Windows ». Cette application ne doit se connecter qu'aux ordinateurs du réseau local ou à un groupe d'ordinateurs bien défini. Les adresses IP autorisées en adresse source ou destination sont donc celles du réseau local ou sous-réseau local définies dans l'onglet « Miscellaneous ». La seconde règle concerne l'application « Internet Explorer ». Celle-ci doit pouvoir se connecter à tout serveur du réseau Internet. Dans l'exemple, toutes les adresses IP destination sont autorisées. Pour cette application, il est possible d'éditer d'autres règles, en fonction de la topologie du réseau local, suivant que le réseau utilise ou non une passerelle, un translateur d'adresse IP (NAT) ou un pare-feu de réseau.

Les règles peuvent être éditées automatiquement ou manuellement. Le filtrage assuré par l'éditeur automatique est peu puissant, puisqu'il ne connaît pas la topologie du réseau. La figure 4.31 montre l'éditeur de règle de ce pare-feu.

L'éditeur permet de définir :

– le protocole utilisé par l'application (UDP ou TCP) ;
– le sens de filtrage des paquets (entrants ou sortants) ;
– le port TCP utilisé ;
– les adresses IP et le port du poste distant autorisés.

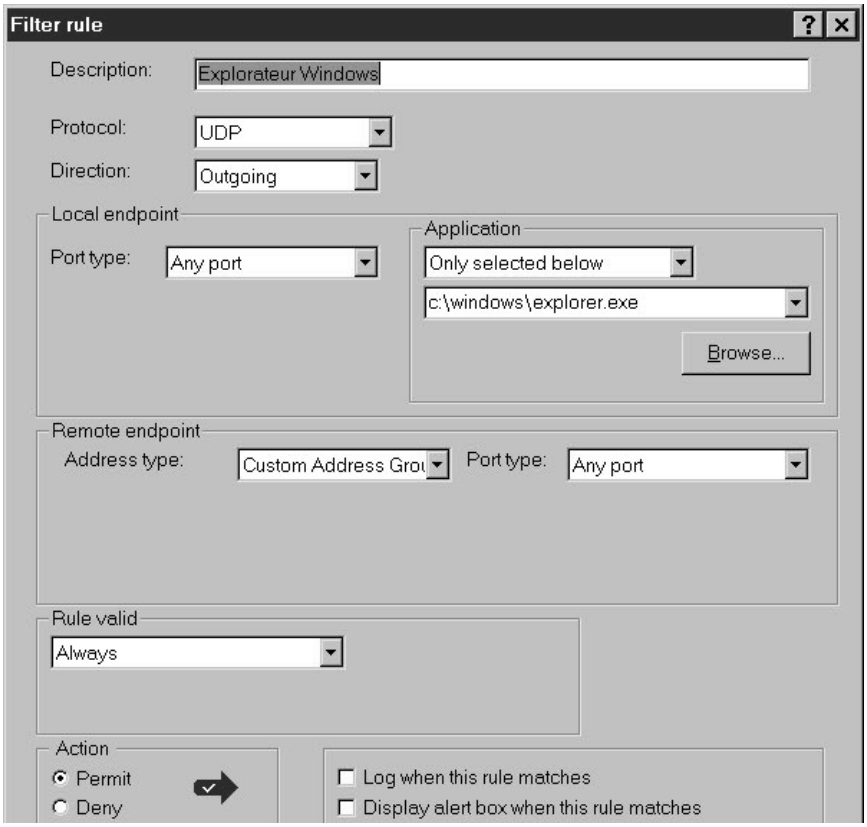

Figure 4.31 Fenêtre de l'éditeur des règles de filtrage.

Dans l'exemple de l'Explorateur Windows, la mention « Custom Address Group » indique que ces adresses sont définies dans l'onglet « Miscellaneous » (figure 4.32).

Les groupes d'adresses sont indiqués en utilisant l'adresse de réseau ou de sous-réseau, avec le masque de réseau ou de sous-réseau délimitant les adresses autorisées pour les connexions. Des exemples de paramétrages de règles sont présentés au paragraphe 5.4, *Les serveurs HTTP : configuration et sécurisation*, illustrés par des exercices.

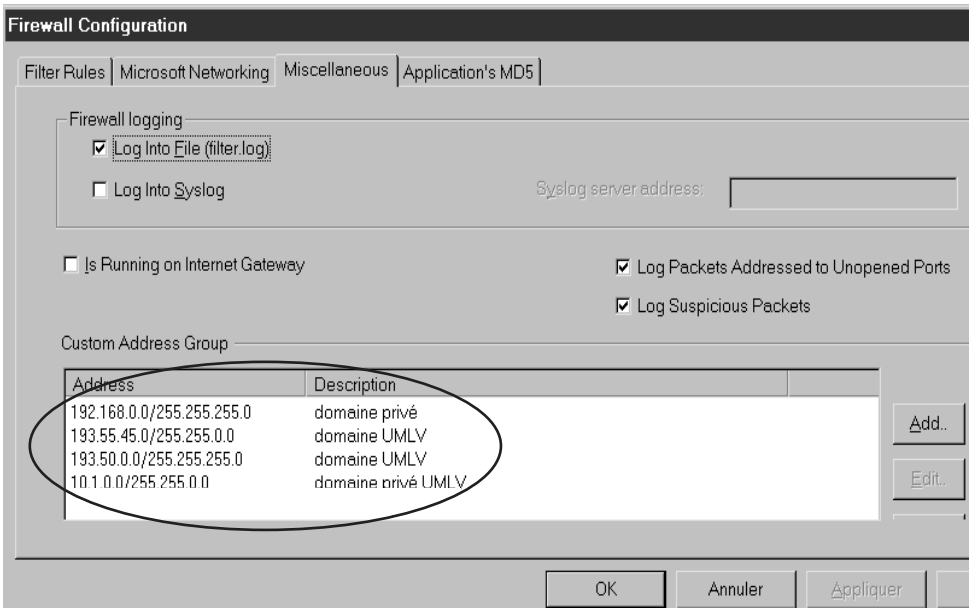

Figure 4.32 Fenêtre d'édition des groupes d'adresse de filtrage.

Résumé

1. Les services de messagerie

➢ un serveur de messagerie gère des boîtes aux lettres (BAL) ;
➢ chaque client dispose d'une BAL à laquelle il peut accéder en lecture après identification ;
➢ la liste des BAL est stockée dans une base de données de comptes ;
➢ la rédaction du message peut se faire hors connexion au serveur. Le message est ensuite envoyé au serveur qui le stocke dans la BAL du destinataire ;
➢ le destinataire se connecte au serveur et est identifié par son nom et un mot de passe. Il peut ensuite lire ou transférer son message sur son poste ;
➢ le protocole SMTP est utilisé pour l'envoi des messages. Pour la réception, les protocoles sont POP3 ou IMAP ;
➢ un client de messagerie installe : une interface utilisateur, une interface de service, un module de stockage, un module de transport et un annuaire ;
➢ un serveur de messagerie dispose : d'un agent de transport des messages, d'un module de traitement des messages, d'un annuaire, d'un module de passerelle et d'un module de stockage ;
➢ le service transport charge le message, récupère l'adresse du serveur et demande l'établissement d'une connexion ;

➢ lorsque le message change de serveur de messagerie, il est traité par les agents de transfert (MTA) ;
➢ l'en-tête des messages SMTP utilise le caractère « @ » comme séparateur du nom de la BAL de celui du serveur de messagerie ;
➢ les serveurs SMTP utilisent le port 25 par défaut ;
➢ pour la lecture d'un message « en ligne », le message est ouvert sur le serveur. Il n'est pas transféré sur le poste client. Le poste client doit rester connecté au serveur pendant toute la lecture ;
➢ pour la lecture « hors ligne », le fichier est d'abord transféré du serveur vers le poste client. Il est ensuite ouvert sur le poste client. Ce dernier peut être déconnecté du serveur pendant la lecture ;
➢ le protocole POP3 permet le transfert des messages du serveur vers le poste client. Il ne permet pas la lecture « en ligne » des messages ;
➢ le protocole IMAP permet la lecture « en ligne » des messages par le poste client ;
➢ le protocole POP3 utilise le port 110 par défaut et IMAP4 le port 143 ;
➢ le protocole MIME assure le codage du texte et l'insertion de nombreux types de fichiers ;
➢ pour se connecter par le RTC, le poste client est d'abord identifié par le serveur d'accès distant, puis par le serveur de messagerie ;
➢ la configuration d'un client de messagerie consiste à définir les paramètres de connexion au serveur de messagerie et d'identification du client ;
➢ la configuration d'un serveur de messagerie nécessite l'identification du serveur, des services et des répertoires utilisés ;
➢ un serveur webmail permet aux clients d'accéder à leur BAL à partir d'un navigateur Internet. Il ne nécessite pas de configuration du poste client ;
➢ un serveur de liste de diffusion assure l'envoi d'un message à chacun des membres de la liste. L'inscription peut être libre, fermée ou contrôlée par l'administrateur ;
➢ les serveurs de messagerie peuvent être sécurisés par l'utilisation de filtres, de passerelles de messagerie et de firewall ;
➢ la transmission des messages peut être sécurisée par cryptage ;
➢ une passerelle de messagerie permet de centraliser la réception des messages et de les transmettre sur plusieurs serveurs.

2. Le service de transfert de fichiers

➢ il permet l'échange de fichiers entre clients identifiés ou anonymes (compte « anonymous ») et le serveur ;
➢ la connexion et le dialogue utilisent le protocole FTP ;
➢ le client dispose des commandes lui permettant de se déplacer dans l'arborescence du disque du serveur et de manipuler les fichiers et répertoires ;

➢ par défaut, le serveur reçoit les commandes sur le port 21 et transmet les données sur le port 20 ;
➢ à chaque client ou groupe est associé la liste des répertoires et fichiers auxquels il peut accéder, ainsi que ses droits (lister, lire, écrire…) sur ces fichiers ou répertoires ;
➢ un serveur FTP comporte trois répertoires : installation de l'application, stockage des données et identification des clients ;
➢ pour configurer un serveur FTP, il faut : créer l'arborescence des répertoires, créer les comptes, associer les droits d'accès, créer les outils d'administration ;
➢ les comptes peuvent être importés d'une base de données.

3. Le service web
➢ il permet d'accéder à des documents au format HTML par l'intermédiaire d'un navigateur Internet ;
➢ le dialogue utilise le protocole HTTP basé sur le principe des liens hypertextes ;
➢ les liens hypertextes permettent de relier des documents situés sur n'importe quel serveur accessible par Internet ;
➢ les documents sont accessibles par un URL ;
➢ le serveur HTTP utilise le port 80 par défaut ;
➢ une fois connecté au serveur HTTP, le client envoie des requêtes au format texte ;
➢ une requête HTTP contient la méthode à utiliser pour récupérer le document ;
➢ pour chaque fichier constituant un document, un processus est créé et une connexion TCP ouverte entre le poste client et le serveur ;
➢ dans Windows, les « cookies » sont stockés par défaut sur le répertoire « documents and settings\ « client »\cookies » ;
➢ dans Windows, les pages sont stockées par défaut dans le répertoire « documents and setting\ « client »\local settings\temporary Internet Files » ;
➢ le navigateur peut être paramétré pour effacer ces fichiers lors de la fermeture du navigateur ;
➢ un « firewall » personnel est un logiciel de contrôle des paquets entrants et sortants de l'ordinateur ;
➢ un « firewall » personnel se situe entre le pilote de la carte réseau et le système d'exploitation ;
➢ il autorise les applications référencées par un numéro de port à échanger des paquets avec l'extérieur ;
➢ pour chaque application, les adresses IP ou groupes d'adresses autorisées en adresse source ou destination sont précisées dans une règle ;
➢ le pare-feu personnel est un complément utile du pare-feu placé à l'interconnexion du réseau local et du réseau Internet.

QCM

Une version électronique et interactive est disponible sur le site *www.dunod.com*.

1. Les services de messagerie

Q1. Le protocole POP3 est utilisé :
a) pour envoyer les messages *b) pour lire les messages*
c) pour coder le contenu des messages

Q2. La BAL est gérée par :
a) le serveur POP3 *b) le serveur IMAP* *c) le serveur SMTP*

Q3. Pour envoyer un message, il est nécessaire :
a) de disposer d'une BAL sur le serveur auquel se connecte le poste
b) de disposer d'une BAL sur le serveur du destinataire du message
c) il n'est pas nécessaire de disposer d'une BAL

Q4. Un serveur de liste de diffusion permet d'envoyer un message :
a) aux destinataires dont l'adresse figure dans le champ « destinataire »
b) à tous les clients gérés par le serveur de messagerie de l'expéditeur
c) aux membres de la liste gérée par le serveur de messagerie des destinataires
d) à tous les clients gérés par le serveur de liste de diffusion

Q5. Les professeurs d'un IUT ont une BAL sur le serveur de messagerie *mail.iut.fr*. un serveur de diffusion *sympa.iut.fr* gère les listes des professeurs de chaque département. Indiquer une adresse correcte pour envoyer un message aux professeurs du département SRC :
a) profs.src@sympa.iut.fr *b) profs.src@mail.iut.fr*
c) profs@src.mail.iut.fr *d) profs@sympa.mail.iut.fr*
e) profs@src.iut.fr

Q6. L'échange de messages entre les serveurs utilise :
a) le protocole POP3 *b) le protocole SMTP*
c) le protocole MIME *d) le protocole IMAP*

Q7. L'échange de messages entre serveurs est géré :
a) par l'agent de transport *b) par le module de stockage*
c) par l'agent de traitement *d) par l'agent de transfert*

Q8. La lecture d'un message « en ligne » nécessite :
a) la connexion du poste client au serveur pendant la durée de la lecture
b) la connexion du poste client au serveur pendant le transfert du message
c) ne nécessite pas la connexion du poste client au serveur

Q9. Le protocole IMAP est une alternative :
a) au protocole POP3 *b) au protocole SMTP*
c) au protocole MIME

Q10. Le serveur Webmail :
a) remplace un serveur SMTP *b) remplace un serveur POP3*
c) s'intercale entre un serveur SMTP et le poste client
d) s'intercale entre un serveur web et un poste client

Q11. Une passerelle de messagerie :
a) se place entre 2 serveurs de messagerie d'une entreprise
b) se place entre les serveurs de messagerie d'une entreprise et Internet
c) remplace les serveurs de messagerie d'une entreprise

2. Le service de transfert de fichiers

Q12. Le protocole FTP permet :
a) le chargement de fichiers *b) la lecture de messages*
c) la visualisation de pages HTML

Q13. L'identification d'un client utilisant le compte « anonymous » se fait le plus souvent :
a) par son compte FTP *b) ne se fait pas*
c) par son adresse mail

Q14. Les répertoires « publics » :
a) sont réservés aux clients disposant d'un compte FTP
b) sont réservés aux clients ne disposant pas de compte FTP
c) sont accessibles par tous les clients se connectant

3. Le service web

Q15. Le protocole HTTP permet :
a) de gérer les échanges avec les serveurs web
b) de définir le format des pages web
c) de localiser un document sur un serveur web

Q16. Le langage HTML est :
a) un langage de programmation
b) un ensemble de règles de mise en forme d'un document
c) un langage de script

Q17. L'URL permet de localiser :
a) un document *b) un serveur web*
c) un navigateur Internet

Q18. Pour charger une page comportant quatre fichiers, le navigateur Internet va ouvrir :
a) aucune session *b) une session*
c) 4 sessions *d) 8 sessions*

Q19. Les « cookies » sont :
a) les éléments de publicité affichés dans une page HTML
b) les objets permettant la navigation hypertexte
c) des requêtes envoyant des renseignements au serveur http
d) l'ensemble de fichiers constituant une page HTML

Q20. Les pages ou objets stockés sur un répertoire temporaire sont :
a) sur un répertoire propre à chaque utilisateur ;
b) sur un répertoire commun à tous les utilisateurs ;
c) sur le répertoire où se situe le navigateur ;

Q21. Un pare-feu personnel est :
a) une application logicielle ;
b) un pilote de périphérique ;
c) un équipement matériel de sécurité du réseau

Q22. Les règles de filtrage portent sur (plusieurs réponses) :
a) les adresses MAC ;
b) les protocoles de la couche « liaison » ;
c) les adresses IP ;
d) les protocoles de la couche « transport » ;
e) les paramètres de régulation de flux ;
f) les ports de la couche « transport » ;
g) les sites web

Exercices

➤ (*) : facile(**) : moyen(***) : difficile
Corrigés à la fin du livre et sur le site *www.dunod.com*.

4.1 (*) Dans l'en-tête ci-joint, retrouver le chemin emprunté par le message.

```
Received: from vega.masson.fr
   by univ-mlv.fr with ESMTP id SAA20646
  for <present@univ-mlv.fr>; Thu, 15 Nov 2001 18:14:08 +0100 (MET)
Received: from blanc.dunod
   by vega.masson.fr with SMTP id SAA09628
   for <present@univ-mlv.fr>; Thu, 15 Nov 2001 18:01:14 +0100
Message-ID: <002f01c16df8$9bf18be0$2a01005b@dunod>
From: "Jean-Luc Blanc" <jl.blanc@dunod.com>
To: <present@univ-mlv.fr>
```

4.2 L'en-tête ci-dessous correspond à un message transmis par l'intermédiaire de la liste de diffusion « src » gérée par un serveur sympa situé sur le domaine *univ-nlt.fr.*

```
Received: from mail.univ-nlt.fr
   by univ-mlv.fr (8.9.3 with ESMTP id QAA04697
  for <present@univ-mlv.fr>; Tue, 19 Feb 2002 16:47:03 +0100 (MET)
Received: by mail.univ-nlt.fr from userid 732); Tue, 19 Feb 2002
16:42:11 +0100 (MET)
Delivered-To: profs-src@univ-nlt.fr
```

```
Received: from univ-mlv.fr
   by mail.univ-nlt.fr with ESMTP id 054CE9786
   for <src@univ-nlt.fr>; Tue, 19 Feb 2002 16:42:07 +0100 (MET)
Received: from src-dept
   by univ-mlv.fr with SMTP id QAA04634
   for <src@univ-nlt.fr>; Tue, 19 Feb 2002 16:46:27 +0100 (MET)
Received: by localhost with Microsoft MAPI; Tue, 19 Feb 2002
16:51:28 -0000
Message-ID: <01C1B965.AD070B40.present@univ-mlv.fr>
From: Dominique PRESENT <present@univ-mlv.fr>
Reply-To: "present@univ-mlv.fr" <present@univ-mlv.fr>
   To: "'src@univ-nlt.fr'" <src@univ-nlt.fr>
   Date: Tue, 19 Feb 2002 16:51:27 -0000
```

a) Retrouver l'adresse de la liste de diffusion et justifiez sa syntaxe.

b) Indiquer le chemin emprunté par le message.

4.3 (***) Un IUT relié à Internet par une ligne louée et un FAI, dispose d'un serveur de messagerie « mail.iut.fr ». Pour des raisons de sécurité, il souhaite dissocier les comptes des étudiants de ceux du personnel en installant un second serveur de messagerie « mail2.iut.fr » pour les comptes étudiants.

a) Proposer une architecture.

b) Les étudiants pourront-ils garder leur adresse e-mail initiale ? Justifier la réponse.

4.4 (*) La liste de diffusion « administratifs.src » du serveur « sympa.iut.univ-mlv.fr » doit être modifiée comme suit : le membre « jean.tasse » doit être remplacé par « maud.aile ».

a) Établir la liste des commandes à exécuter pour opérer les modifications de la liste.

b) Quelle commande exécuter pour vérifier la mise à jour de la liste ?

4.5 (**) Imaginez qu'un étudiant de l'université de Marne la vallée vienne d'écrire un nouveau programme qu'il souhaite rendre accessible à tous par le serveur FTP *univ-mlv.fr*. Il place le programme dans le répertoire FTP ftp/pub/maitrise/newprog.c. Quelle sera l'URL permettant d'atteindre ce programme ?

4.6 (**) Quels sont les avantages et les inconvénients des connexions « anonyme » et « non anonyme » sur un serveur FTP ? Peut-on utiliser une connexion « non anonyme » sur un serveur web ?

4.7 (***) Dans un réseau local d'entreprise, les postes clients ont des adresses IP comprises dans la plage 10.50.0.30 à 10.50.0.120. L'adresse du réseau est 10.50.0.0, le serveur de comptes a l'adresse 10.50.0.2, le serveur de messagerie 195.50.50.2 et le routeur

195.50.50.1. Le serveur de comptes est également serveur Intranet, et le routeur assure la translation des adresses privées.

Établir les règles de filtrage à installer sur le pare-feu personnel d'un poste client pour l'application de messagerie d'une part et pour l'explorateur Windows d'autre part.

Exercices pratiques

➤ (*) : facile(**) : moyen(***) : difficile

Les logiciels utilisés sont disponibles sur le site *www.dunod.com* (versions d'évaluation ou gratuites).

4.8 (*) **Analyse des en-têtes de messages** : en utilisant votre outil de messagerie :

a) Envoyer un message à votre adresse. Récupérer l'en-tête et indiquer le chemin suivi par le message. (sous Outlook, l'en-tête est accessible lorsque le message est ouvert, par le menu « affichage », puis « options ». l'en-tête s'affiche en bas de la fenêtre).

b) Envoyer un message avec pièce jointe à votre adresse. Récupérer l'en-tête et retrouver la partie de l'en-tête caractérisant la pièce jointe.

4.9 (*) **Accusés de réception :** en utilisant votre outil de messagerie :

a) Envoyer un message à votre adresse en demandant un accusé de réception (pour Outlook : menu « affichage », « options », valider la case « demander une confirmation de lecture »).

b) À la lecture du message, un message s'affiche. Si vous validez la confirmation, que se passe-t-il dans la boîte d'envoi ?

c) En déduire qui du poste destinataire ou du serveur de messagerie de la BAL du destinataire crée le message de confirmation.

4.10 (*) Utilisation d'un Webmail

a) Connectez-vous au site **www.freesurf.fr** (paramètres de connexion : No d'accès : 0860 91 26 00 ; DNS Primaire : 212.43.206.2 ; DNS Secondaire : 212.43.206.3 ; Domaine de recherche : freesurf.fr ; Serveur POP : pop.freesurf.fr ; Serveur SMTP : smtp.freesurf.fr)

b) Loguez-vous sur le compte **lohpres@freesurf.fr** mot de passe dunod.

c) Le compte Webmail est à votre disposition pour vous familiariser avec les commandes. Effectuer le même travail qu'à l'exercice 4.9.

4.11 (**) Configuration **d'un serveur FTP**. L'entreprise souhaite disposer de répertoires pour les utilisateurs des deux services, « commercial »

d'une part et « développement » d'autre part. Les utilisateurs du premier service se nomment Claude et Charles, ceux du second Didier et Deborah. Chaque utilisateur devra avoir tous les droits sur son répertoire et les sous-répertoires créés, et le droit de lecture sur les répertoires de son collègue du service. Il ne devra pas pouvoir accéder aux répertoires de l'autre département.

a) Télécharger le logiciel serv-U de Cat-soft (*www.cat-soft.com*) et l'installer sur votre poste.

b) Sélectionner le serveur et configurer le domaine en lui donnant le nom ftp.server.fr et lui attribuer l'adresse IP de votre poste.

c) Créer les comptes des utilisateurs et les deux groupes « commerciaux » et « développeurs ».

d) Créer les deux répertoires « commerce » et « développement » dans lesquels se trouveront les répertoires des utilisateurs.

e) Donner les droits d'accès à chaque utilisateur.

f) Procéder aux vérifications des droits des utilisateurs en vous connectant au serveur FTP à partir de votre navigateur (ou d'un client FTP tel que FTP Works de Corban Software *http://www.corbanware.com*).

4.12 (***) Configuration d'un pare-feu personnel. L'exercice analyse les paquets entrant et sortant d'un poste pour comprendre l'édition des règles de filtrage. Il s'appuie sur le logiciel « Kério Personnal Firewall » de Kério Technologies Inc. (*www.kerio.com*).

a) Télécharger et installer le logiciel sur votre poste.

b) Redémarrer l'ordinateur. Des fenêtres vont s'afficher, indiquant le nom de l'application émettant ou recevant le paquet, l'adresse IP distante ainsi que le port utilisé. Le client a la possibilité d'accepter ou de refuser le paquet. Relever les éléments affichés.

c) Dans la fenêtre d'administration, cliquer sur « advanced ». la fenêtre de configuration s'ouvre. Cliquer sur « add » pour ouvrir l'éditeur de règles. Reporter les éléments notés dans la question précédente.

d) Redémarrer l'ordinateur. Les paquets ayant fait l'objet de relevés ne doivent plus provoquer l'affichage de messages.

e) Supprimer une règle. Redémarrer l'ordinateur. À l'affichage de la fenêtre d'alerte, cochez la case de création de la règle appropriée (*create approriate filter*). Aller dans l'éditeur de règles et comparez la règle créée avec celle éditée à la question « c ». Quelles sont vos constatations ?

Étude de cas 1 : Installation/configuration d'un serveur SMTP/POP3 sous Windows

a) Installation

L'IUT veut installer un serveur de messagerie. Le logiciel choisi est le freeware Mercury/32 (téléchargeable à l'adresse *http://risc.ua.edu/pegasus/mercury32*). Avant l'installation, il faut décider du nom du serveur, du répertoire d'installation, du répertoire des BAL. Nous prendrons mailserviut pour le nom du serveur, *c:\mailserv* pour le répertoire d'installation et *c:\mailserv\mail* pour les BAL. Une fois l'installation lancée, le logiciel demande si le serveur sera ou non dans un environnement NetWare, ce qui n'est pas le cas.

Il faut ensuite indiquer le répertoire d'installation « c:\mailserv » (figure 4.33), puis le répertoire des BAL « c:\ mailserv\mail ».

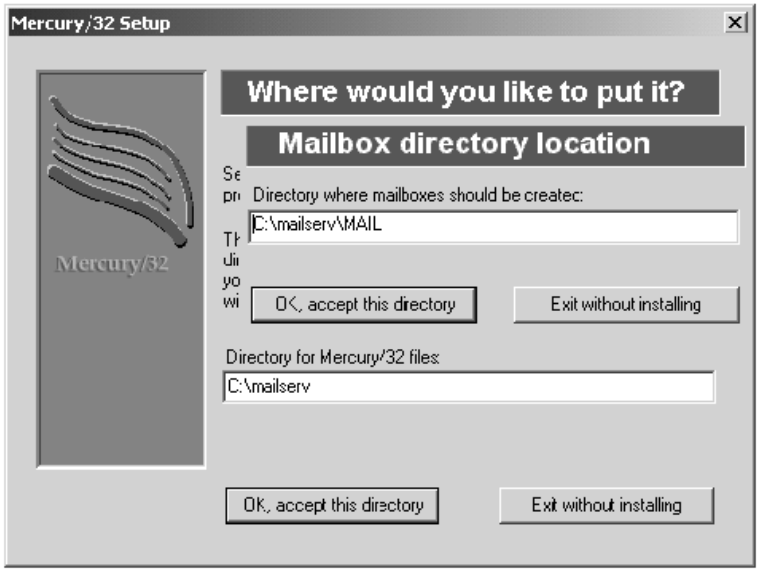

Figure 4.33 Définition des répertoires utilisés.

Il faut ensuite indiquer les protocoles utilisés (figure 4.34). Il faut bien sûr SMTP (module **MercuryS**) et POP3 (module **MercuryP**). Le module **MercuryD** n'est utile que si votre serveur doit aller chercher le courrier sur un serveur central (passerelle de messagerie par exemple) ; le module **MercuryX** permet de planifier le traitement du courrier ; le module **MercuryF** ne sert que pour utiliser un « annuaire » de type Finger ; le module **MercuryH** assure le dialogue entre le serveur et des clients Pegasus Mail ou Eudora.

Il est conseillé de charger le module **MercuryW** qui permet de changer le mot de passe d'accès à l'administration du serveur. Le module **MercuryI** chargera, s'il est validé, le protocole IMAP4, utile principalement pour interfacer un Webmail.

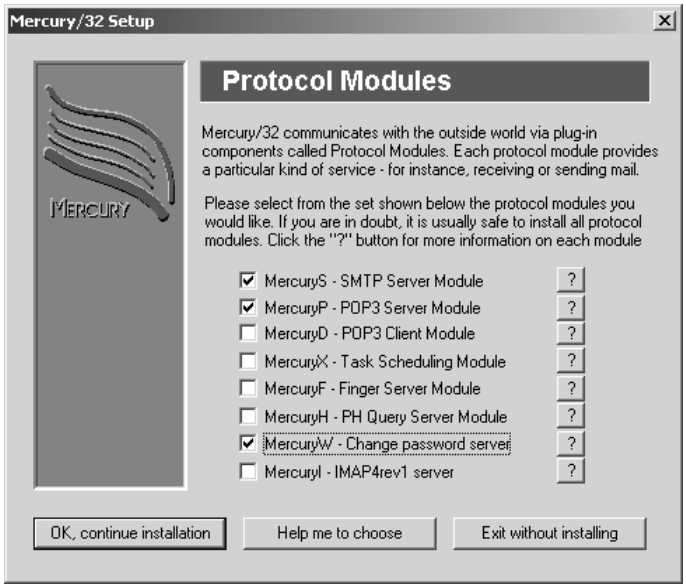

Figure 4.34 Fenêtre de validation des protocoles.

Le module SMTP client assure le dialogue du serveur avec les serveurs extérieurs. Le module **MercuryC** sera utilisé pour une connexion en mode « Dial-up » (figure 4.35) ; le module **MercuryE** dans le cas d'une connexion permanente.

Le nom du serveur « mail.serviut » terminera les paramétrages nécessaires. Dans le cas où il y a des clients Pegasus, il faut indiquer le nom de la file d'attente qui recevra les messages. Ce répertoire devra être partagé en lecture seule.

b) Configuration

Après lancement de Mercury32, il faut aller dans l'option « Mercury core module » du menu « configuration » (figure 4.36). L'onglet « general » regroupe les informations d'installation (adresse IP ou nom du serveur, répertoire des BAL et nom de l'administrateur).

Le nom du serveur sert de référence au serveur pour savoir si émetteur et destinataire d'un message sont « locaux » ou « non-locaux ». Ce nom est utilisé par le logiciel pour créer un compte administrateur (ici *postmaster @mail.serviut*). Cette adresse sera utilisée pour l'envoi de messages à l'émetteur si un problème de traitement est rencontré par le serveur.

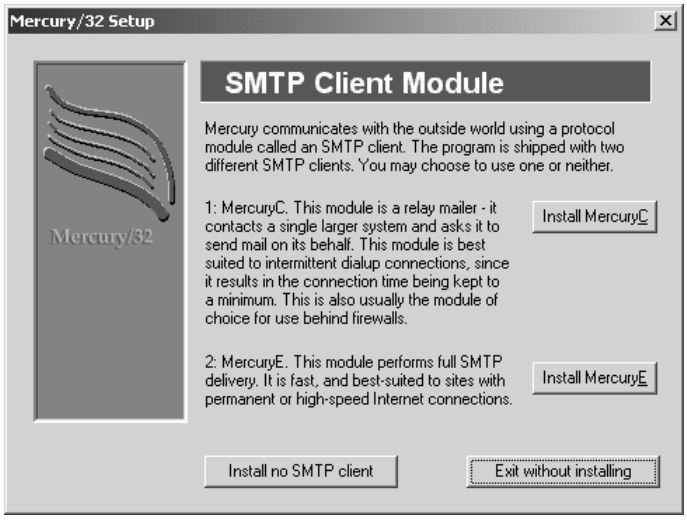

Figure 4.35 Choix des protocoles de connexion au serveur.

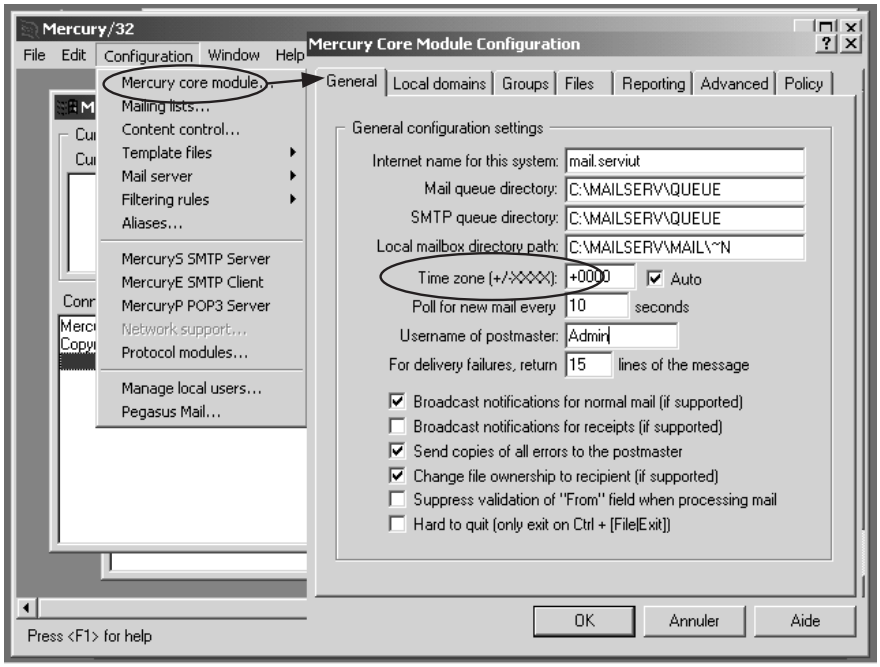

Figure 4.36 Informations d'installation du serveur.

Les autres paramètres sont les paramètres par défaut : notification au client de messages reçus, copie au responsable du serveur en cas de message en erreur. Vérifier le décalage de l'heure locale par rapport à l'heure universelle.

L'onglet « local domains » permet de paramétrer le serveur SMTP (figure 4.37). Sélectionner le serveur « mail.serviut » (double clic) et cliquer sur « local host or server ».

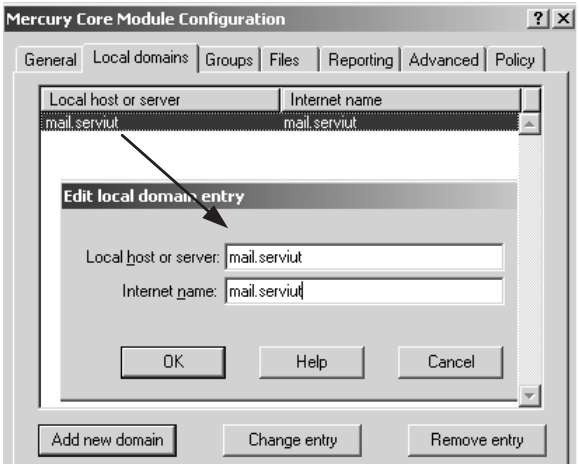

Figure 4.37 Définition des noms Internet et Intranet du serveur.

Dans l'option « Mercury SMTP Server » du menu « configuration », le champ « announce myself as » permet d'indiquer le nom du serveur tel qu'il apparaîtra dans les en-têtes de routage des messages (figure 4.38). Il est éthiquement correct d'indiquer le nom du serveur « mailserver » ou « mail.serviut ». Les paramètres par défaut correspondent au temps d'attente pour la réponse à une demande de connexion TCP/IP (30 secondes) et le numéro du port TCP utilisé (port 25).

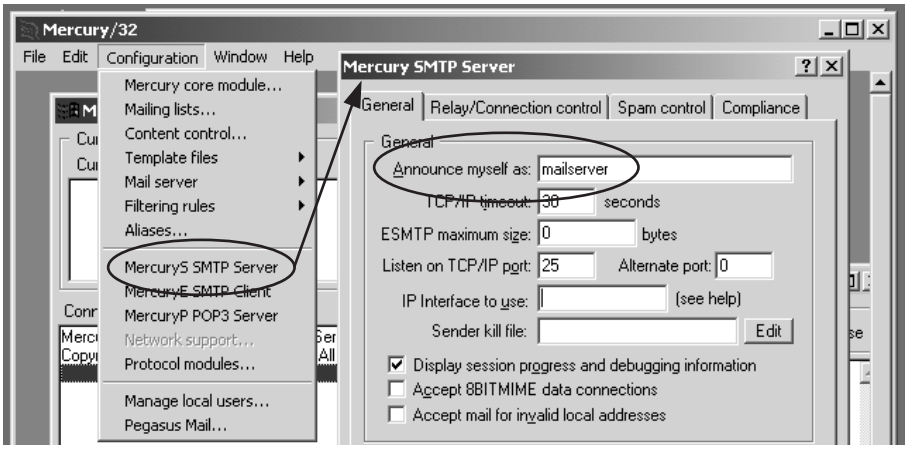

Figure 4.38 Paramétrage de l'identification du serveur dans les messages.

Dans l'option « Mercury POP3 Server » du menu « configuration » (figure 4.39), s'affichent les paramètres par défaut : l'adresse IP du serveur POP3 et le port TCP utilisé (port 110). L'adresse IP sera celle à utiliser pour paramétrer les postes clients. Les fonctions par défaut sont : « marquer comme lus les messages correctement transférés au client » et « ne proposer au client que les messages non transférés ». Il est possible d'ajouter « l'envoi des en-têtes de message » et « le blocage des commandes d'effacement ou non des messages sur le serveur ».

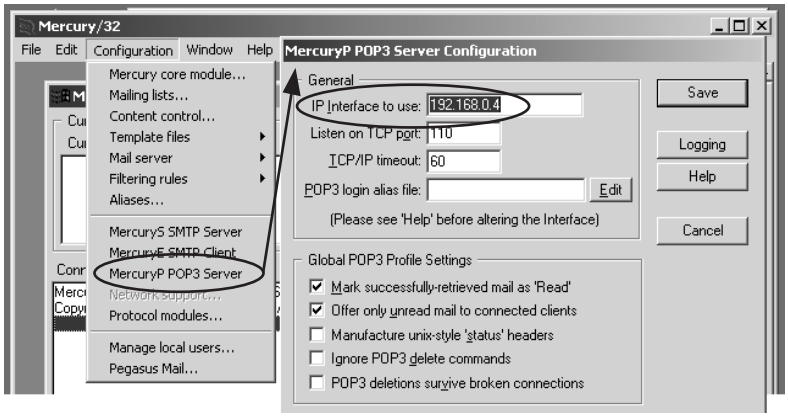

Figure 4.39 Configuration du serveur POP3.

Il faut enfin créer les BAL (figure 4.40) et paramétrer les clients.

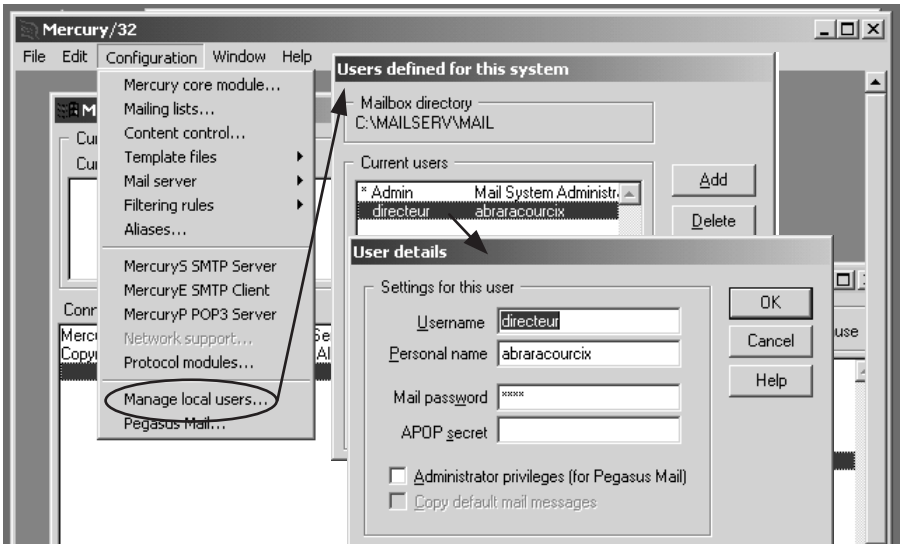

Figure 4.40 Création des BAL des clients.

Dans l'option « Manage local users » du menu « configuration », il suffit d'ajouter chaque client en définissant pour chacun : le nom, ses caractéristiques (en général sa fonction) et son mot de passe. La case en bas de la fenêtre permet de définir les clients qui disposeront des droits d'administration des comptes. À l'installation de la messagerie, une boîte est automatiquement créée pour l'administrateur (Admin ; *Mail System Administrateur*).

Il ne faut pas oublier de paramétrer les outils de messagerie des clients.

Une fois l'installation terminée, il est possible de tester le fonctionnement du serveur en envoyant un message par la fonction « send mail » (figure 4.41). Cette fonction envoie un message de la part de l'administrateur du serveur (From : *postmaster@mail.serviut*). L'adresse du destinataire est une des boîtes aux lettres créées, *directeur@mail.serviut* dans notre cas.

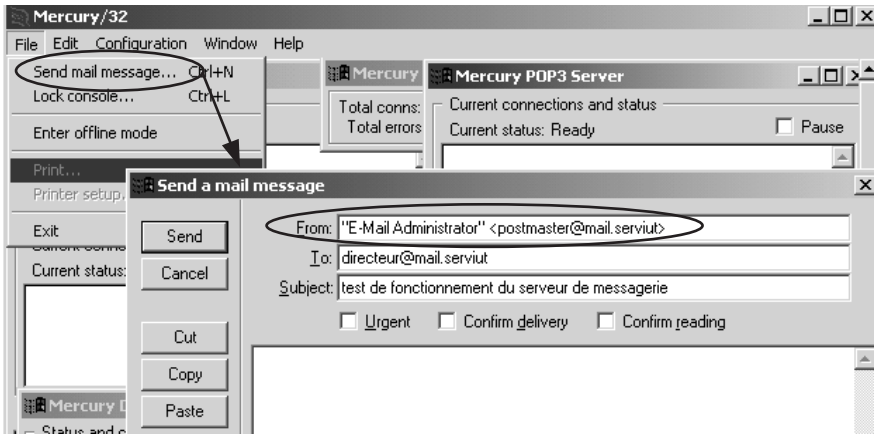

Figure 4.41 Envoi d'un message de test à partir du serveur.

Les fenêtres « Mercury Core Process » et « Mercury POP3 Server » permettent de suivre le traitement des messages envoyés pour la première, les connexions des clients pour la seconde. Sur la figure 4.42, la fenêtre de gauche montre l'envoi d'un message venant de « postmaster@mail.serviut » et destiné à « directeur ». Les deux adresses sont considérées comme locales, puisqu'elles utilisent toutes les deux le nom Internet « mail.serviut » défini dans l'onglet « general » de la fenêtre « Mercury Core Module » (figure 4.36).

La fenêtre de droite montre la connexion du client « directeur » au serveur et le nombre de messages transférés. L'en-tête (code source) du message test reçu par le directeur se présente ainsi :

```
Received: from spooler by mail.serviut (Mercury/32 v3.32);
➥ 22 Oct 03 16:43:33 +0200
X-Envelope-To: directeur@mail.serviut
```

```
From: "E-Mail Administrator" <postmaster@mail.serviut>
To: directeur@mail.serviut
Subject: test de fonctionnement du serveur de messagerie
Date: Wed, 22 Oct 2003 16:43:20 +0200
MIME-Version: 1.0
Content-type: text/plain; charset=US-ASCII
X-Mailer: Mercury/32 v3.32
```

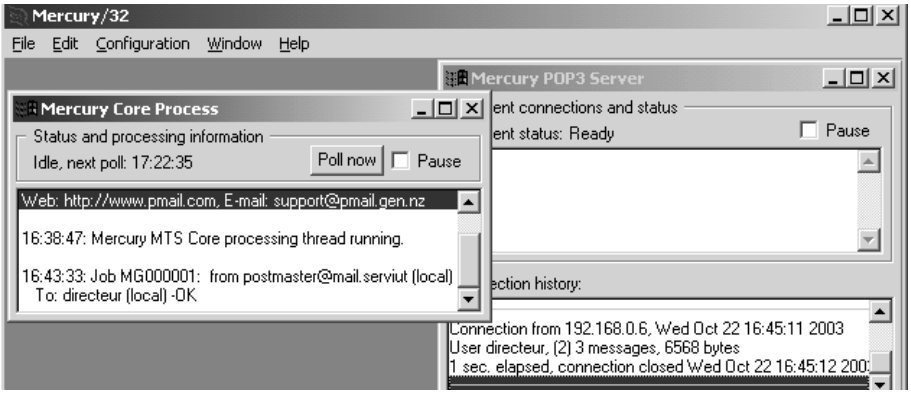

Figure 4.42 Fenêtre de suivi des messages et des connexions des clients.

Les deux premières lignes indiquent le destinataire local (*directeur@mail.serviut*) et le dernier serveur ayant transmis le message (*mail.serviut*). Les deux lignes suivantes (lignes 3 et 4) indiquent l'adresse de l'émetteur initial (*postmaster@mail.serviut*) et le destinataire final (*directeur@mail.serviut*). Entre ces deux blocs de lignes viendra s'ajouter l'identité des serveurs par lesquels le message a transité, permettant ainsi de suivre le trajet des messages.

Étude de cas 2 : Installation/configuration d'un Webmail sous Windows

Ce module, écrit en PHP permet d'interfacer à un navigateur, n'importe quel serveur de messagerie SMTP (Sendmail, Postfix…) et IMAP (Cyrus, Courier…). Le module Squirrelmail nécessite de disposer d'un serveur de messagerie et d'un serveur web (Apache par exemple). Une fois le fichier « tarball » ou « zip » décompressé, on trouve dans le répertoire initial les répertoires « *data* » pour les utilisateurs, « *config* » pour les paramètres de configuration, « *plugins* » pour les modules complémentaires, « *po* » pour les langages autres que l'anglais d'origine, et « *src* » où se trouvent les fichiers sources en PHP.

La configuration se fait dans le fichier ***config_default.php*** du répertoire *config* qui sera sauvegardé sous le nom ***config.php***. Les lignes suivantes doivent être modifiées (les modifications sont en gras) :

```
/* Organization's name */
global $org_name;
$org_name = 'webmail IUT';
.........
/**
 * Default language  This is the default language. It is used as a last
resort if SquirrelMail can't figure out which language to display.
Use the two-letter code. */
global $squirrelmail_default_language;
$squirrelmail_default_language = 'fr_FR';

/* The dns name and port for your imap server. */
global $imapServerAddress, $imapPort;
$imapServerAddress = '192.168.0.4';
$imapPort = 143;

/** The domain part of local email addresses. This is for all messages
sent out from this server.  Reply address is generated by
$username@$domain Example: In bob@foo.com, foo.com is the domain. */
global $domain;
$domain = 'mail.serviut';

/* Your SMTP server and port number (usually the same as the IMAP
server).*/
global $smtpServerAddress, $smtpPort;
$smtpServerAddress = '192.168.0.4';
$smtpPort = 25;


.........
/**
 * Path to the data/ directory. The path name can be absolute
or relative (to the config directory). It doesn't matter.
Here  are two examples:
 * Absolute:
 *   $data_dir = '/usr/local/squirrelmail/data/';
 * Relative (to the config directory):
 *   $data_dir = SM_PATH . 'data/'; */
global $data_dir;
$data_dir = 'c:\programmes\EasyPHP1-7\www\webmail\squirrelmail\data';
```

Le Webmail est prêt. Pour lancer le Webmail à partir du navigateur, il suffit de taper l'URL du serveur web, suivi du chemin d'accès au répertoire ***squirrelmail***. Une fenêtre demandant le nom de la boîte aux lettres de la messagerie et le mot de passe s'affiche (figure 4.43)

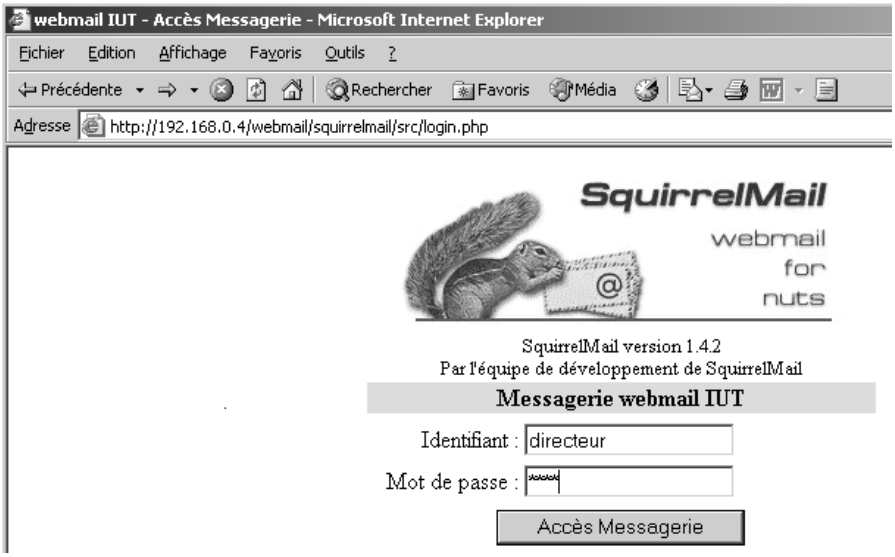

Figure 4.43 Fenêtre d'accueil du Webmail.

L'interface de la messagerie web s'affiche dans la fenêtre du navigateur comme le montre la figure 4.44. Les messages affichés ont permis de tester le bon fonctionnement du Webmail.

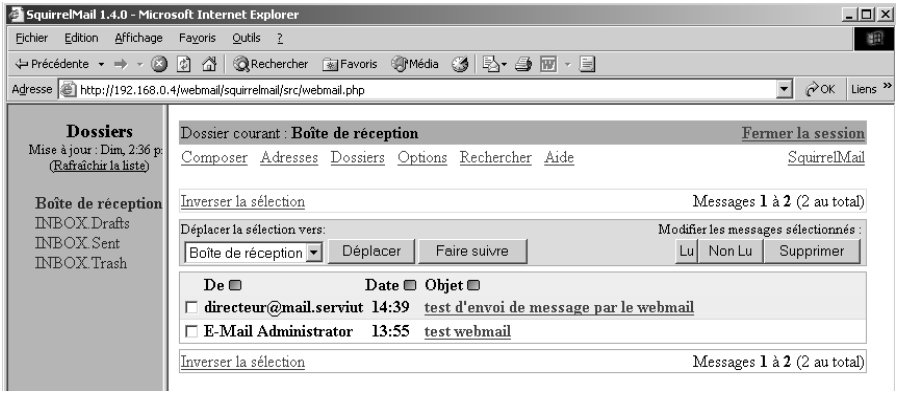

Figure 4.44 Fenêtre de réception de la messagerie web.

Le message « test webmail » a été envoyé au directeur par un client de messagerie classique. Le second message a été envoyé par le Webmail en activant le lien Composer. Le lien Dossiers permet de créer des dossiers dans la boîte aux lettres. La figure 4.45 montre la fenêtre des messages envoyés accessible en cliquant sur INBOX.sent dans la fenêtre de gauche.

Figure 4.45 Fenêtre des messages envoyés de la messagerie web.

Étude de cas 3 : Mise à jour d'un site web par transfert FTP

Lorsqu'un site web est hébergé sur un site distant, l'une des difficultés est la mise à jour. L'une des solutions les plus rapides consiste à transférer les fichiers de la nouvelle version vers le site web distant par un transfert FTP. Cela nécessite bien sûr que le site distant dispose d'un serveur FTP donnant accès aux répertoires où sont stockés les fichiers du site, et que vous ayez les droits pour aller écrire et modifier les fichiers et répertoires correspondants. Plusieurs précautions sont à prendre avant le transfert des fichiers :

– le nommage des fichiers et répertoires doit respecter les règles utilisées sur le serveur. Pour éviter les problèmes, il est prudent d'utiliser la convention DOS 8.3, en supprimant les majuscules, les espaces, les caractères accentués, et en se restreignant au strict alphabet et au caractère « sous-tiret » (*underscore*). Ainsi, les noms de fichiers et de répertoires seront compatibles avec les systèmes Windows et Linux.

– l'arborescence des fichiers devra être conservée. L'arborescence la plus courante consiste à disposer les fichiers html dans le répertoire et les images dans un sous-répertoire « *image* ». L'entrée dans le site passe par la page d'accueil habituellement nommée *index.htm*.

L'exemple montre la configuration d'un serveur FTP sur IIS, permettant la modification des pages du site web « serviut » (voir paragraphe 5.3, *Configuration d'un serveur IIS*) par un responsable du service administratif (compte *webadmin*) d'une part, un responsable du service informatique (compte *webinfo*) d'autre part. Chacun de ces services dispose dans l'arborescence du site web d'un répertoire propre (figure 4.46) situé dans le répertoire commun « www\ftp ».

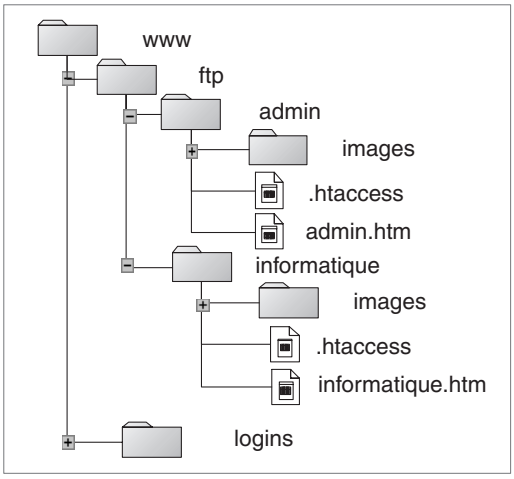

Figure 4.46 Arborescence des répertoires du site FTP.

La configuration du serveur FTP s'effectue à partir de la fenêtre « propriétés » du serveur FTP sélectionné dans le « gestionnaire des Services Internet » (figure 4.47). L'onglet « site FTP » permet de définir l'adresse IP du serveur, son descriptif et le nombre de connexions simultanées autorisées (le nombre doit être limité pour ne pas saturer les ressources du serveur). Le répertoire devant s'afficher au moment de la connexion d'un client est spécifié dans l'onglet « répertoire de base ». Ce répertoire sera le répertoire racine, et les clients ne pourront pas remonter dans l'arborescence du serveur. Le répertoire « ftp » protège ainsi la page d'accueil du site web et les fichiers de sécurisation placés dans le répertoire « logins » (voir chapitre 4, *Étude de cas 1*) contre toute modification. Dans l'onglet « comptes de sécurité », il faut préciser les comptes autorisés à administrer le serveur FTP. Il ne faut pas oublier d'ajouter ici les administrateurs du site. Dans l'exemple donné, il n'est pas nécessaire de prévoir un nom de compte et un mot de passe pour les clients sans compte « anonymous », puisque le transfert de fichier ne sera utilisé que par les responsables web des services. L'onglet « message » permet de prévoir des messages d'accueil s'affichant sur le moniteur du client FTP à l'établissement et la libération de la connexion au serveur. Enfin l'onglet « sécurité de répertoire » permet de limiter l'accès au serveur à partir de postes identifiés par leur adresse IP. Dans notre cas d'étude, il serait utile, pour la sécurité d'accès aux fichiers d'utiliser cette fonctionnalité en ajoutant les adresses IP des postes des deux responsables des pages web.

Le serveur est configuré. Il faut ensuite donner les droits d'accès aux responsables précités. Le serveur FTP de IIS utilise le système de droits d'accès au fichier de Windows 2000 Server. Il faut donc procéder en deux temps. Tout d'abord créer les comptes « webadmin » et « webinfo » dans le dossier « utilisateurs » du répertoire « outils système » du gestionnaire de l'ordinateur.

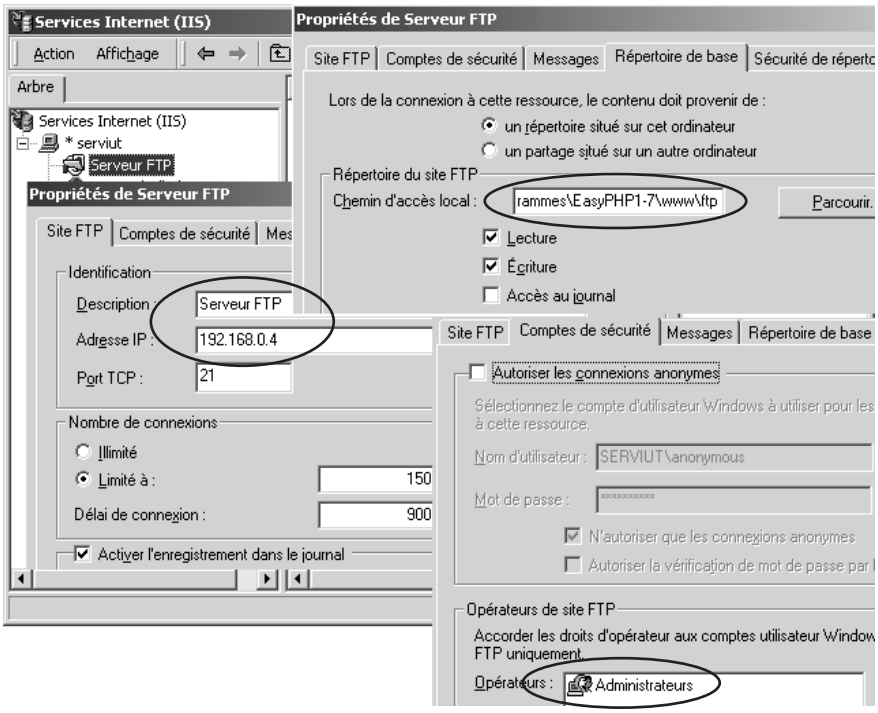

Figure 4.47 Configuration du serveur FTP de IIS.

Il faut ensuite aller dans les propriétés de chacun des dossiers et donner un accès aux responsables des pages pour qu'ils puissent écrire, créer et modifier des fichiers et des répertoires. La figure 4.48 montre les droits d'accès au répertoire « admin » affectés au compte « webadmin ».

Pour modifier les pages web, il ne faut pas oublier :

– que l'arborescence des répertoires sur le poste de l'administrateur des pages doit obligatoirement être le même que celle des pages du site web ;

– que le fichier d'entrée sur la page d'accueil « index.htm » doit toujours rester à la même place dans l'arborescence du serveur FTP et garder le même nom pour ne pas rompre le lien avec la page « index.htm » ;

– que les noms des fichiers modifiés ne doivent être changés que si cela s'avère nécessaire. Changer un nom de fichier nécessite une vérification exhaustive des liens, et rend caduques les chemins mémorisés dans le menu « *favoris* » des navigateurs des visiteurs habituels.

Il suffit ensuite de lancer le client FTP, indiquer le nom du serveur FTP distant, s'identifier par son nom de client et son mot de passe. La connexion au serveur FTP par le client « webadmin » est représenté figure 4.49 (le client FTP utilisé est FTP Expert de Visicom Media Inc. – *www.visic.com*).

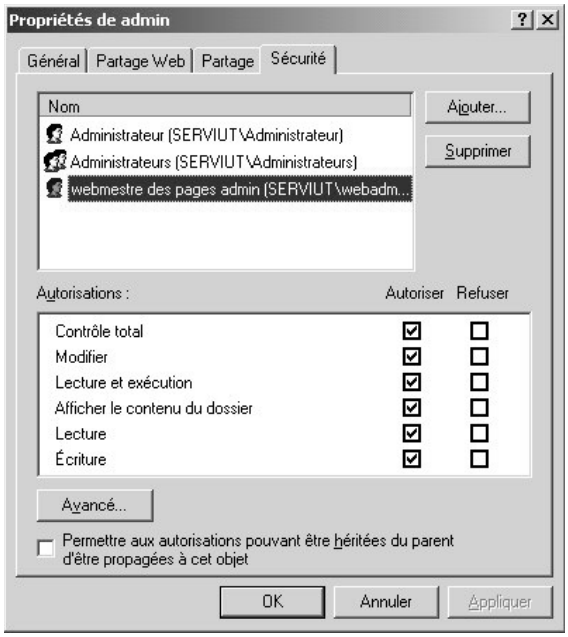

Figure 4.48 Droits du compte « webadmin » sur le dossier « admin ».

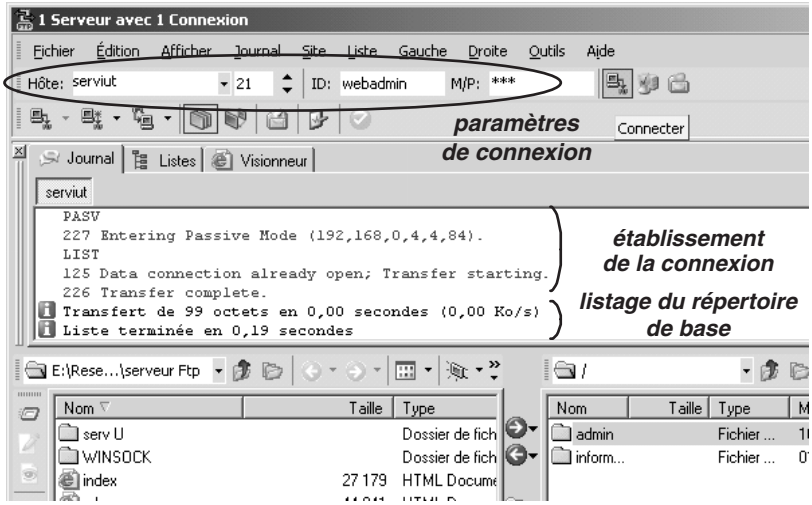

Figure 4.49 Connexion au serveur FTP par un client.

Les paramètres de connexion (nom du serveur/compte/mot de passe) apparaissent dans la barre en haut de la fenêtre. La première fenêtre montre le dialogue entre le client FTP et le serveur FTP sur le port 21 du serveur. On reconnaît les commandes d'établissement de la connexion se terminant par la

confirmation de l'ouverture du port 20 permettant l'échange de données. Puis le listage du contenu du répertoire de base (*www/ftp* dans notre cas). Les deux fenêtres du bas affichent le contenu du dossier du poste client (fenêtre de gauche) et celle du serveur (fenêtre de droite) où l'on peut reconnaître les deux répertoires de données « admin » et « informatique ».

Les anciens fichiers peuvent alors être remplacés par les nouveaux, les nouveaux fichiers sont chargés. Il ne reste plus qu'à supprimer les fichiers inutiles. Il faut toutefois se rappeler que supprimer un fichier peut casser des liens si ces fichiers sont pointés par d'autres serveurs. Il peut être utile de les remplacer, provisoirement du moins, par un fichier indiquant que cette page n'est plus utilisée et donnant l'URL de la page de remplacement.

Chapitre **5**

Les serveurs http : configuration et sécurisation

5.1 CHOIX D'UN SERVEUR HTTP

5.1.1 Logiciel et matériel

Disposant d'une version fonctionnant sous Linux et d'une version sous Windows, le serveur Apache est de plus en plus utilisé. Toutefois, le module http *d'Internet Information Server* peut être préféré pour garder une homogénéité dans l'interfaçage de l'application et du système d'exploitation. Les deux serveurs seront donc étudiés dans ce chapitre.

On ne peut parler des applications sans se poser la question de l'ordinateur sur lequel elles sont implantées. Certes, il est possible et économique d'utiliser un ordinateur classique pour réaliser un serveur http. On ne peut par contre attendre les mêmes performances que celles obtenues avec un serveur spécifique.

5.1.2 Architecture matérielle d'un serveur

Sans entrer dans le détail d'une telle architecture, en constante évolution, il est possible de guider le choix en donnant quelques points de repères fonctionnels et matériels. Tout d'abord se rappeler que, dans le cas d'un serveur http, un processus est créé et une connexion TCP ouverte pour chaque fichier constitutif d'une page web (voir paragraphe 4.3, *Le service web*). Plus le nombre de clients à servir « simultanément » sera élevé, plus le nombre de processus sera élevé et donc plus les ressources matérielles du serveur (temps processeur, mémoire) devront être importantes. Il est alors facile de comprendre que dans l'architecture matérielle d'un serveur, le

nombre de processeurs, la capacité de la mémoire et sa rapidité seront plus importants que sa capacité graphique ou multimédia. De même la capacité de stockage sur disques sera développée, et la rapidité de ces derniers optimisée pour tenir compte du nombre d'accès disques importants.

Pour construire un serveur, on cherchera à exploiter les capacités de « parallélisme » des processeurs actuels, ceux-ci se répartissant la gestion des processus. Pour le stockage, l'utilisation de disques SCSI sera préférée, non pour un débit plus important qu'une interface EIDE (les débits sont du même ordre, environ 160 Mo/s), mais pour le nombre de disques que cette interface peut gérer (jusqu'à 15 périphériques). La sécurité du stockage des données est également un point important, surtout si le serveur est amené à héberger des données de clients. La prudence incitant à ne pas mettre toutes les données dans la même unité de stockage, la technologie RAID (*Redondant Array of Inexpensive Disks*) répartit les données d'un fichier sur plusieurs disques (raid 1 de la figure 5.1). Certaines versions rajoutent des blocs de contrôle permettant de récupérer les données perdues par la déficience d'un disque (raid 4 de la figure 5.1).

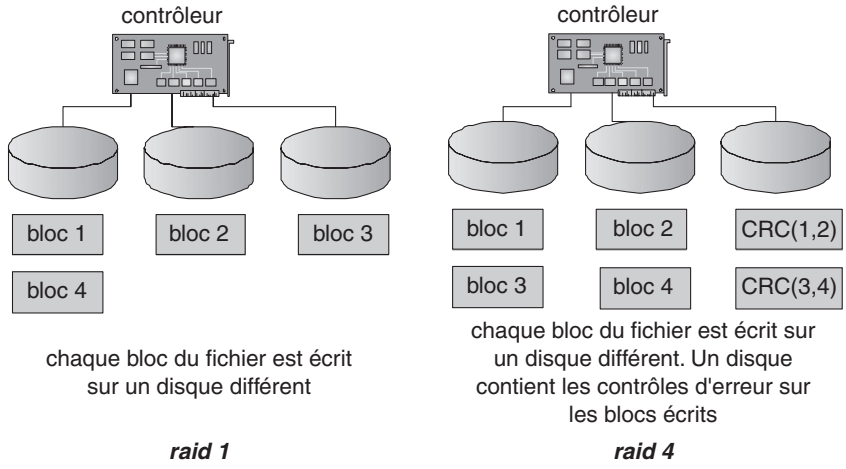

Figure 5.1 Technologie RAID de gestion des disques.

La sécurité et la fiabilité de fonctionnement seront prises en compte également. Il ne faut pas oublier que ces serveurs fonctionnent la plupart du temps sans interruption et que les parties « mécaniques » sont les plus sujettes à une panne. L'alimentation peut être doublée (alimentation de secours) voire secourue (onduleur et batterie incorporés). La ventilation doit aussi faire l'objet de soins particuliers. Si l'on résume les caractéristiques particulières des serveurs nous trouvons :

– le nombre de processeurs ;
– la capacité RAM et leur rapidité ;
– la capacité, le système de stockage et la rapidité des disques ;
– la fiabilité de fonctionnement.

Le tableau 5.1 illustre ces différences de spécifications de serveurs et de station dans la gamme PME d'un fabriquant.

TABLEAU 5.1 COMPARAISON DES SPÉCIFICATIONS SERVEURS/STATION.

Type	Processeur	Mémoire max.	F. bus (MHz)	Contrôleur	Stockage max.	Alim.	Sauvegarde
Station	1 Pentium 4	2 Go	400	IDE	60 Go	unique	
Serveur éco	1 Pentium 4	4 Go	800	Raid	300 Go	unique	option
Serveur pro	2 Xéon	24 Go	400	Raid	1,5 To	3 + 1 secours	sur bande

5.1.3 Architecture logicielle d'un serveur

Un serveur http est une application logicielle. Elle doit dialoguer avec le système d'exploitation. Le serveur devant être accessible à partir du réseau, l'ordinateur d'accueil devra être équipé d'une ou plusieurs cartes réseaux. Sa configuration réseau aura été validée avant de commencer l'installation du serveur http. Les applications actuelles vont chercher automatiquement les paramètres réseaux nécessaires, mais il sera toutefois préférable de relever le nom de la machine, son identité réseau (nom et adresse IP) son identité Internet (URL y donnant accès). L'installation des applications étant classique, elle ne sera pas développée dans les paragraphes suivants. Ceux-ci seront plus particulièrement consacrés à la configuration d'un serveur Apache sous Windows et Linux (paragraphe 5.2, *Configuration d'un serveur Apache*) et d'IIS4 (paragraphe 5.3, *Configuration d'un serveur IIS*).

5.2 CONFIGURATION D'UN SERVEUR APACHE

5.2.1 Exploitation sous Windows

L'installation se fait de façon classique en indiquant le nom du répertoire dans lequel l'application et les données seront installées. Le répertoire d'installation par défaut est *c:\Program Files\Apache\Group\Apache*. Une fois installée, l'arborescence du répertoire se présente comme dans l'exemple du tableau 5.2.

La configuration utilise le fichier texte *httpd.conf* qui sera modifié à l'aide du bloc-note ou d'un éditeur simple. Si « WordPad » est utilisé, ou a fortiori « Word », il faut **absolument sauvegarder en mode « texte seul »**, sinon ces éditeurs rajoutent des codes de mise en forme incompatibles. Dans les dernières versions d'Apache, il est déconseillé d'utiliser les fichiers *access.conf* et *srm.conf* pour la personnalisation de la configuration. Tout est décrit dans le fichier *httpd.conf*. Certaines versions commercialisées fournissent un logiciel de configuration qui facilite la modification de ce fichier. Il est organisé en commentaires (précédés du symbole #) et directives suivies d'arguments. Exemple de directive :

```
# nom du serveur
ServerName jeronimo
```

Tableau 5.2 Répertoires et fichiers d'un serveur Apache.

Répertoire		Contenu, Objet
bin		Programme pour créer les clients
cgi-bin		Utilitaires (horloge, compteur...)
conf		Fichiers de configuration
	Httpd.conf	Fichier texte de configuration
	Access.conf	Fichier de gestion des droits d'accès au serveur
	Srm.conf	Fichier de gestion des noms d'accès par les navigateurs
htdocs		Fichiers et répertoires du site web
	Index.html	Fichier ouvert quand aucune page n'est spécifiée
	manual	Répertoire de la documentation en anglais
icons		Icônes affichées lors des requêtes
log		Journaux de suivi du serveur
	Access.log	Journal des accès au serveur
	Error.log	Journal des erreurs, utile pour le débogage
modules		Modules complémentaires (Perl, Java…)
src		Sources du programme

La configuration va être effectuée en deux temps. Tout d'abord, les modifications minimales du fichier *httpd.conf* pour mettre le serveur en service. Ces modifications apparaissent en gras non-italique dans le fichier. Ensuite, une analyse plus détaillée du fichier permettra une personnalisation de la configuration. Les modifications sont en gras italique.

Le fichier de la figure 5.2 montre la structure du fichier *httdp.conf*. Seuls les blocs de paramètres apparaissent (#--<bloc>--). Pour une meilleure lisibilité certains paragraphes et commentaires ont été supprimés.

```
## httpd.conf -- Apache HTTP server configuration file

#---------------- Dynamic Shared Object (DSO) Support -------------

# définit les modules à charger pour utiliser des objets DSO
# Example:
# LoadModule foo_module libexec/mod_foo.so

#----------------- Name Space and Server Settings -----------------
# définit le nom des répertoires accessibles par les utilisateurs
# sur le serveur http. Définit aussi les paramètres indiquant
# comment les requêtes et les réponses seront formatées.
```

```
# DocumentRoot: le répertoire contenant les documents, tel qu'il
# sera vu par les utilisateurs.

DocumentRoot /home/httpd/html

# UserDir: nom du répertoire de réception des requêtes de chaque
# utilisateur déclaré.

UserDir public_html

# DirectoryIndex: liste des fichiers d'accueil par défaut

DirectoryIndex index.html index.htm index.shtml index.cgi  Default.htm
➥ default.htm index.php3

# AccessFileName: nom du fichier à lire dans chaque répertoire,
# pour connaître les droits d'accès

AccessFileName .htaccess

# permet le choix d'un ou plusieurs langues

AddLanguage en .en
AddLanguage fr .fr
AddLanguage de .de
AddLanguage da .da
AddLanguage el .el
AddLanguage it .it

LanguagePriority fr en

#---------------------- Global Access Configuration -------------------
# définit les services autorisés et leur environnement
# chaque répertoire auquel Apache a accès peut être répertorié en
# indiquant les caractéristiques d'accès ou d'interdiction.
# Indiquer en premier les permissions par défaut.

<Directory />
Options Indexes Includes FollowSymLinks
AllowOverride None
</Directory>

<Directory /home>

# contrôle quelles options le fichier « htaccess » des répertoires
# peuvent prévaloir. Peut aussi bien être « All » que toute combinaison
# de « Options », « FileInfo », « AuthConfig » ou « Limit »

AllowOverride All
```

```
# Controls who can get stuff from this server.

order allow,deny
allow from all

# autorise l'accès à la page server-status du serveur sur
# http://servername/server-status
# changer le « your_domain.com » pour rendre votre domaine accessible

<Location /server-status>
SetHandler server-status

order deny,allow
deny from all
allow from .your_domain.com
</Location>

# autorise l'accès aux répertoire docs du serveur à localhost

Alias /doc /usr/doc
<Directory /usr/doc>
order deny,allow
deny from all
allow from .your_domain.com
Options Indexes FollowSymLinks
</Directory>

# There have been reports of people trying to abuse an old bug from
# pre-1.1days.  This bug involved a CGI script distributed as a
# part of Apache.
# By uncommenting these lines you can redirect these attacks to a
# logging script on phf.apache.org.  Or, you can record them
# yourself, using the script support/phf_abuse_log.cgi.

#<Location /cgi-bin/phf*>
#deny from all
#ErrorDocument 403 http://phf.apache.org/phf_abuse_log.cgi
#</Location>

<Directory /home/lohier/public_html>
AuthName Répertoire_protégé
AuthType Basic
AuthUserFile /etc/httpd/conf/users.http
Require valid-user
</Directory>

</Directory>
```

```
#---------------------- Server Configuration ----------------------

# ServerType is either inetd, or standalone.

ServerType standalone
# If you are running from inetd, go to "ServerAdmin".
# Port: numéro du port utilisé

Port 80

# ServerName : nom permettant l'accès au serveur s'il est différent
# de la syntaxe "www"<nom du serveur> (l'adresse IP peut être
# utilisée ici)
# Note: le nom doit être un nom connu et reconnu des DNS

ServerName serviut

########################################
# SGI Performance Settings         #
########################################

########################################
# Add-on Modules and Virtual Hosts #
########################################
```

Figure 5.2 Structure du fichier de configuration *httpd.conf*.

a) Configuration de base

Le fichier comporte six parties. Les 1re, 5e et 6e parties concernent l'utilisation de modules optionnels et ne seront pas modifiées. En utilisant les noms de répertoires par défaut, rien n'est à modifier dans le second bloc. Les configurations de base sont à porter dans les 3e et 4e blocs. Le 3e bloc permet de contrôler l'accès des utilisateurs aux répertoires du serveur, le 4e bloc permet de l'identifier.

La 1re modification à effectuer est de donner un nom au serveur. Taper le nom après la directive **« ServerName »**. Il est possible d'utiliser l'adresse IP du serveur. Si un caractère « # » se trouve en début de ligne, il doit être supprimé. Ce caractère indique un commentaire. À défaut, la commande serait ignorée.

Exemple : **ServerName** serviut.

À partir de ce moment, le serveur existe et peut être lancé par le menu démarrer (démarrer ➠ programmes ➠ apache web server ➠ start Apache as console app). L'écran de la figure 5.3 doit apparaître.

À cette étape, le serveur n'est pas identifié sur le réseau et vulnérable. Ses répertoires sont accessibles à tous. Il faut donc le sécuriser. Cela consiste à identifier les utilisateurs devant avoir accès aux informations du serveur contenues dans le répertoire « htdocs ».

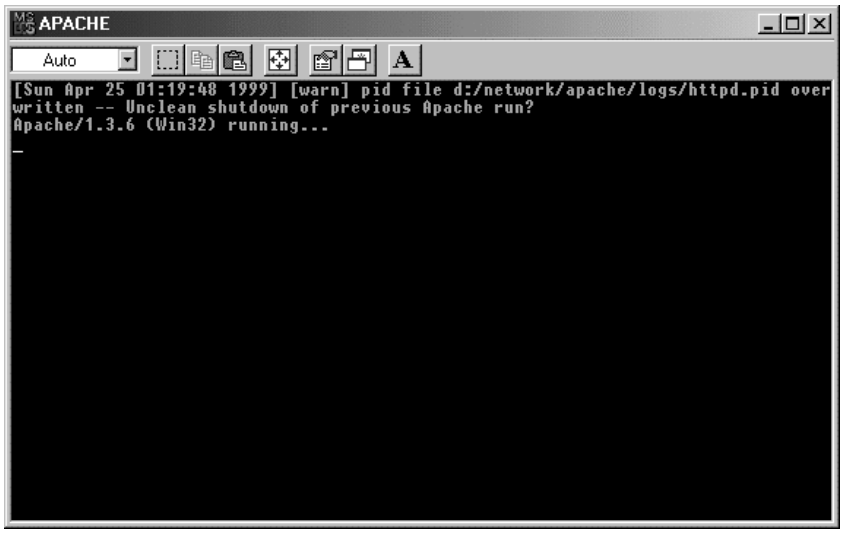

Figure 5.3 Écran de la console du serveur Apache.

Dans la partie « *Global Access Configuration* » du fichier httpd.conf et à la suite de la directive <Directory/> après « **Options »,** taper :

– **None** pour interdire à tous de lister les répertoires ;
– **Includes FollowSymLinks** pour autoriser l'exploitation des liens symboliques ;
– **All** pour autoriser l'accès à tous.

Après « **AllowOverride** » taper :

– **None** pas de droits d'accès particuliers pour le répertoire ;
– **htpaccess** restrictions d'accès dans ce fichier sur les droits d'accès système ;
– **Fileinfo** pour respecter les droits d'accès système ;
– **AuthConf** pour prendre les restrictions d'accès dans le fichier htaccess ;
– **All** pour prendre les droits d'accès uniquement dans le fichier htaccess.

Après « **order** » taper :

– **Allow,deny** pour tout autoriser sauf ce qui est interdit ;
– **Deny, allow** pour interdire tout ce qui n'est pas autorisé.

Dans notre exemple, les données ont été placées dans le répertoire www. Dans ce répertoire, il faut placer la page d'accueil (ou page par défaut). Le nom du fichier est l'un de ceux listés dans le fichier de configuration httpd.conf, dans la directive **DirectoryIndex**. Dans notre cas, il s'agit de ***index.htm*** (les images seront placées dans un sous-répertoire « images »).

Il reste à identifier le serveur sur le réseau en accédant à l'onglet « identification » de la fenêtre « propriétés » de l'icône « favoris réseaux ». Dans le champ « nom de l'ordinateur », il faut entrer le nom déclaré pour la directive **ServerName** du fichier *httpd.conf* (serviut dans notre exemple).

Le serveur est maintenant prêt. Pour le tester, il suffit de lancer le navigateur et d'entrer l'URL « http://serviut ». Le fichier index.htm doit s'afficher dans la fenêtre du navigateur (figure 5.4).

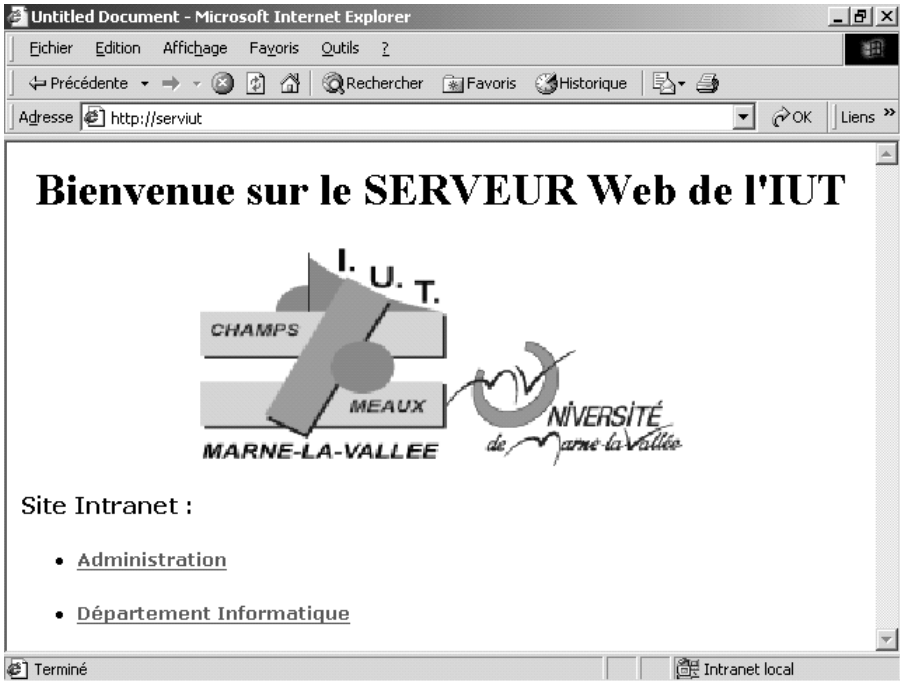

Figure 5.4 Page d'accueil du site « serviut ».

b) Configuration personnalisée

La personnalisation d'un site web peut être très poussée. Nous porterons l'étude sur la personnalisation de l'arborescence des répertoires des données, et de l'accès à des utilisateurs identifiés. Cette configuration correspond à un accès contrôlé pour un Intranet par exemple. Dans le cas du site « serviut », l'accès aux pages « administration » et « département informatique » sera contrôlé par mot de passe. La description est présentée dans l'étude de cas 1 en fin de chapitre.

L'accès à un répertoire est contrôlé par deux fichiers « .htaccess » et « .htpasswd ». le premier est placé dans le répertoire à contrôler, le second dans un répertoire spécifique. Ces fichiers sont des fichiers textes. La structure du fichier « .htaccess » est la suivante :

```
AuthUserFile  c:\programmes\easyphp1-7\www\logins\admin\.htpasswd
```

```
AuthGroupFile  /dev/null
AuthName   "accès protégé"
AuthType  Basic
<LIMIT GET POST>
Require valid-user
</LIMIT>
```

– **AuthName** est le libellé qui sera affiché dans la fenêtre de dialogue lors de l'authentification.
– **AuthType** défini le type d'authentification. Avec la valeur « basic », celle-ci correspondra à un simple encodage.
– **AuthUserFile** est le fichier contenant le nom des utilisateurs qui ont le droit d'accéder au répertoire ainsi que les mots de passe cryptés (ce fichier peut-être crée à l'aide du programme « htpasswd »).
– **Require** permet d'activer le contrôle d'accès. Avec la valeur « valid_user », le fichier défini par **AuthUserFile** sera utilisé.

Ce fichier peut être créé avec un simple éditeur de texte (sous Windows, le nom de sauvegarde doit avoir une extension .txt ; il faudra renommer le fichier). Il est possible d'utiliser une liste d'utilisateurs (directive « AuthUserFile ») ou de groupes (directive « AuthGroupFile »). Le nom et le chemin d'accès au fichier contenant la liste des utilisateurs autorisés et leur mot de passe est indiqué en paramètre. Le fichier « .htpasswd » sera créé sous Dos par la commande htpasswd se trouvant dans le répertoire apache\bin. L'exemple détaillé dans l'étude de cas 1 en fin de chapitre donne la procédure. Une fois ces fichiers créés, un clic sur le lien provoquera l'affichage d'une fenêtre demandant le nom d'utilisateur et le mot de passe (figure 5.5).

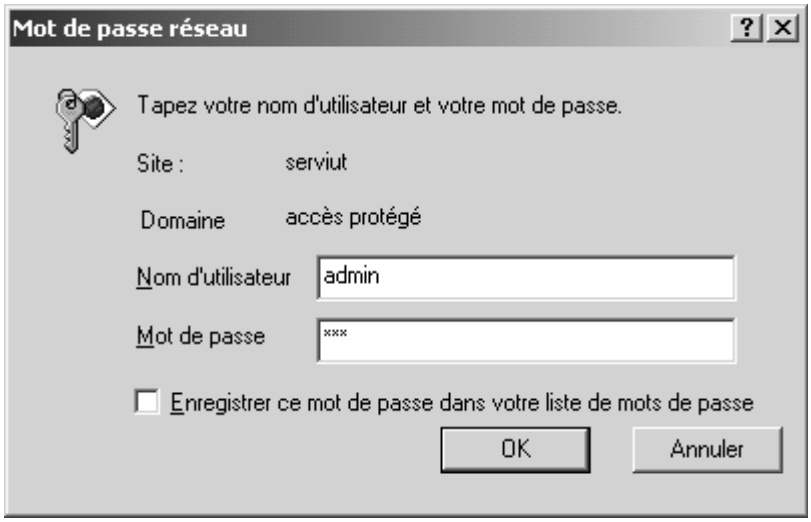

Figure 5.5 Fenêtre d'accès contrôlé au répertoire « admin ».

5.2.2 Exploitation sous Linux

Utilisé avec le système d'exploitation Linux ou Unix, le logiciel serveur Apache est immédiatement opérationnel après installation, il utilise les répertoires suivants :

– le programme serveur httpd (*daemon http*) est installé dans /usr/sbin ;
– les fichiers de configuration sont rangés dans /etc/httpd/conf ;
– les pages HTML sont rangées dans /home/httpd/html ou /var/www/html dans les dernières versions ;
– les programmes CGI sont placés dans /home/httpd/cgi-bin ou /var/www/cgi-bin;
– le répertoire /etc/httpd/logs (ou var/log/httpd) contient les fichiers « log » du serveur (journal d'accès et journal d'erreurs) ;
– le répertoire /usr/lib/apache contient tous les modules utilisables par Apache (un module est une extension logicielle à Apache, lui permettant par exemple d'interpréter le langage php)

Comme pour la plupart des programmes sous Unix ou Linux, la configuration passe par l'édition et la modification de fichiers textes à l'aide d'un éditeur de type « bloc-note » fonctionnant exclusivement en mode texte ou « ASCII ». Il existe cependant quelques programmes en mode graphique qui rendent plus simple la configuration d'Apache (utilitaire standard « Netconf » ou programme téléchargeable « Comanche »), ceux-ci ne sont en fait qu'une interface graphique rajoutée modifiant les fichiers de configuration utilisés par le « *daemon* » http.

Comme pour une installation sous Windows, le fichier de configuration */etc/httpd/conf/httpd.conf* est le fichier principal de configuration du programme serveur http il spécifie les attributs généraux du serveur.

Les différentes directives de ce fichier sont décrites dans l'aide en ligne, rubrique *Run-Time Configuration Directives*.

Lors d'une modification de directive, il est parfois nécessaire de redémarrer le serveur : */etc/rc.d/init.d/httpd restart*.

Le fichier de configuration */etc/httpd/conf/srm.conf* concerne les ressources du serveur et leur localisation (ce fichier est intégré dans la partie *Name Space and Server Setting* du fichier httpd.conf à partir de la version 1.3 de Apache).

C'est notamment dans cette partie que seront configurés les chemins d'accès au répertoire par défaut et aux pages personnelles des usagers du serveur. Trois directives, en autres, permettent ces configurations :

```
DocumentRoot /home/httpd/html
UserDir public_html
DirectoryIndex index.html index.htm index.shtml index.cgi  Default.htm
➥ default.htm index.php3
```

La première précise le répertoire d'accès par défaut associé à un URL du type **http://myserver.net**.

La deuxième donne le nom du sous-répertoire à créer dans le répertoire utilisateur /home/username associé à un URL du type : **http://myserver.net/~username** (avec

l'exemple donné un tel URL permettra d'atteindre directement la page par défaut du répertoire /home/username/public_html).

La troisième donne le nom de ou des pages par défaut situées dans le répertoire par défaut ou les répertoires utilisateurs. Pour adresser une autre page, il sera nécessaire de le préciser dans l'URL du client : **http://myserver.net/otherpage.htm.**

Le dernier fichier de configuration */etc/httpd/conf /access.conf* contrôle les accès aux différents répertoires du serveur http (ce fichier est intégré dans la partie *Global Access Configuration* du fichier *httpd.conf* à partir de la version 1.3 de Apache).

Les directives sont comprises entre deux balises d'ouverture et de fermeture des répertoires concernés. Par exemple :

```
<Directory /home/httpd/cgi-bin>
     AllowOverride None
     Options ExecCGI
</Directory>
```

Les différentes directives sont décrites dans l'aide en ligne du serveur Apache.

La directive « AuthUserFile » permet en particulier d'imposer un nom d'utilisateur et un mot de passe pour l'accès authentifié à un répertoire ou un fichier, comme détaillé dans l'étude de cas.

5.3 CONFIGURATION D'UN SERVEUR IIS

L'installation des services Internet se fait par ajout/suppression de composant windows (accessible par le panneau de configuration). Il faut cocher les Services Internet, puis dans la liste de ces services (cliquer sur le bouton « détails ») cocher le serveur *World Wide Web* (figure 5.6).

Une fois le service installé, il faut configurer le serveur web en utilisant le « gestionnaire des services Internet » des « outils d'administration ». La configuration est accessible à partir des « propriétés » du serveur web par défaut (sélectionner « propriétés » après un clic droit en pointant « serveur web par défaut »). La première étape consiste à attribuer un nom et une adresse IP au site web. Ces paramètres se situent dans l'onglet « site web » comme l'indique la figure 5.7.

Il faut ensuite indiquer le répertoire où se trouvent la page d'accueil, et les fichiers par défaut. Ces informations sont disponibles dans les onglets « répertoire de base » et « documents » (figure 5.8).

Dans ce répertoire, il faut placer la page d'accueil (ou page par défaut). Le nom du fichier est l'un de ceux listés dans l'onglet documents. Dans notre cas, il s'agit de *index.htm* (les images seront placées dans un sous-répertoire « images »).

Le serveur est maintenant prêt. Pour le tester, il suffit de lancer le navigateur et d'entrer l'URL « http://serviut ». Le fichier *index.htm* doit s'afficher dans la fenêtre du navigateur (figure 5.4).

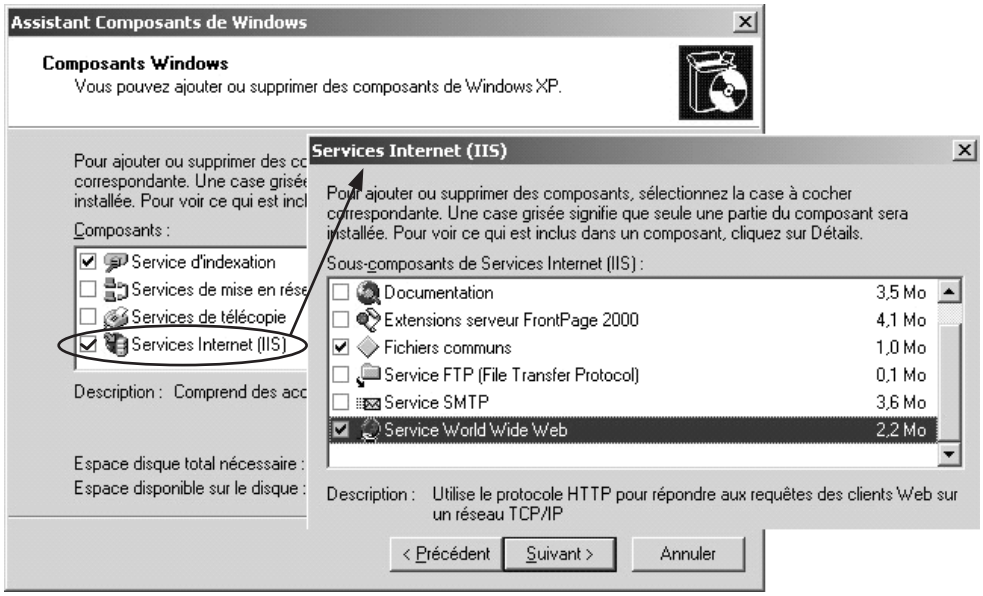

Figure 5.6 Installation des services Internet.

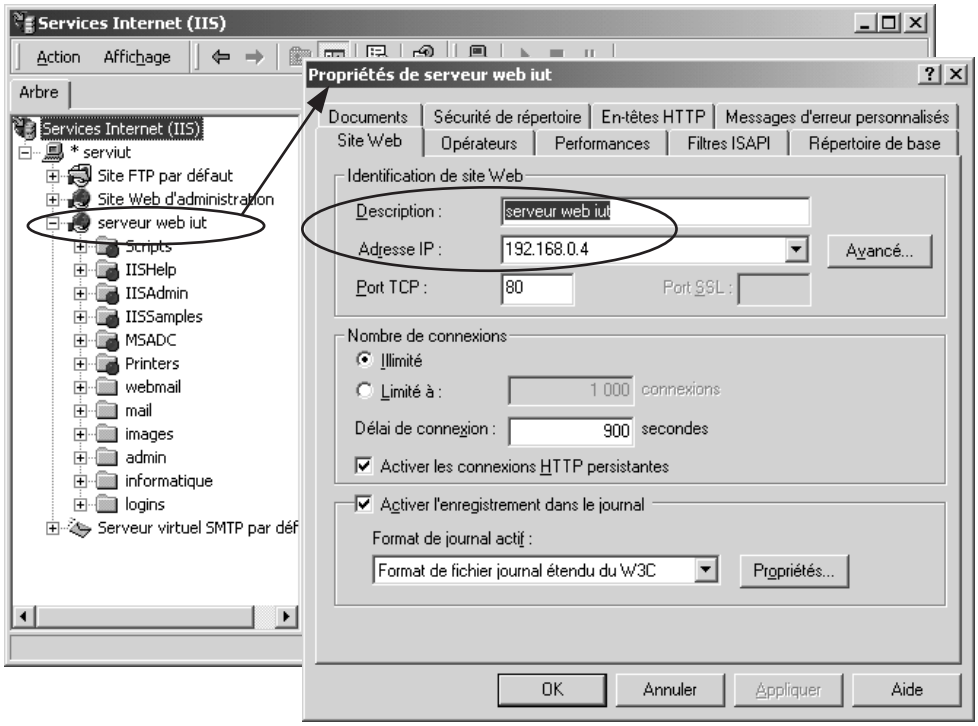

Figure 5.7 Configuration du serveur web – 1re étape.

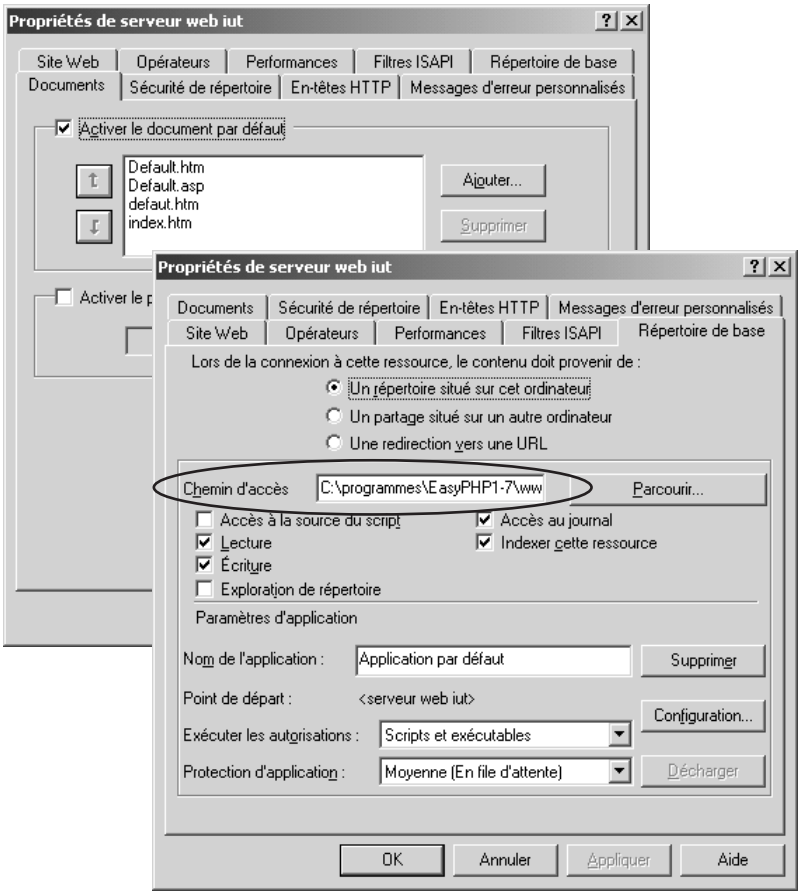

Figure 5.8 Configuration du serveur web – 2e étape.

5.4 SÉCURISATION D'UN SERVEUR HTTP

5.4.1 Pourquoi sécuriser ?

Dans le monde professionnel, il ne faut jamais oublier que les données et les informations sont souvent plus précieuses que les applications. Dès que le réseau d'entreprise s'ouvre au monde extérieur en se connectant à Internet, il peut être l'objet de malveillances. Deux types de problèmes peuvent se poser :

– les attaques destructives des données et applications de la part de « hackers » ;
– les surveillances et écoutes dues à une « veille économique » poussée.

Les attaques consistent à trouver un point d'entrée sur un système informatique, le plus souvent à partir d'un accès distant, en découvrant une identité et un mot de passe. Tous les systèmes informatiques connectés au réseau Internet ont un ou plusieurs points faibles.

Plusieurs modèles ou niveaux de sécurité existent :

– la sécurité par l'obscurité : le système est sûr car personne ne le connaît ;
– la sécurité par l'hôte : chaque machine est sécurisée à un certain niveau (serveurs ou stations avec nécessité d'authentification à la connexion, protections locales et sur l'accès aux ressources, cryptage interne des données…) ;
– la sécurité par le réseau : l'accès à l'ensemble des ressources du réseau est protégé par un coupe-feu (*firewall*) ou un filtre applicatif chargé de filtrer les accès et de sécuriser les données qui circulent.

Le paragraphe 5.4.2, *Sécurisation du serveur*, donne quelques exemples de sécurisation par l'hôte, en l'occurrence un serveur web. Le paragraphe 5.4.3, *Utilisation d'un coupe-feu* montre comment utiliser et mettre en œuvre un coupe-feu ou un filtre applicatif dans une architecture de réseau d'entreprise.

Par ailleurs, les surveillances et écoutes sont facilitées par le fait que les informations circulant sur les réseaux Internet sont accessibles à tout le monde. Se prémunir contre ce problème implique la sécurisation des échanges, en posant cinq questions :

– la confidentialité : l'information est cryptée et ne peut être déchiffrée que par le destinataire ;
– l'authentification : source et destinataire de l'information sont identifiés ;
– le contrôle d'accès : les interlocuteurs n'ont accès qu'aux informations qui leur sont destinées ;
– l'intégrité : les données reçues n'ont pas été altérées ou modifiées pendant la transmission ;
– la non-répudiation : l'échange d'informations a bien eu lieu.

Les serveurs web peuvent répondre aux deux premières questions avec le protocole HTTPS (*Hyper Text Transmission Protocole Secure*) s'appuyant sur le protocole SSL (*Secure Sockets Layer*), dont les principes et la mise en œuvre sur *Internet Information Server* sont présentés au paragraphe 5.4.4, *Utilisation d'une connexion sécurisée avec HTTPS/SSL.*

5.4.2 Sécurisation du serveur

a) Apache

Au niveau des ressources, il est possible, comme pour toute application sous Linux ou Windows, de renforcer les droits (lecture, écriture…) sur les répertoires et fichiers utilisés (répertoire /var/www/html, fichier index.html …) pour l'utilisateur par défaut se connectant sur le serveur (utilisateur anonyme) ou pour d'autres utilisateurs.

Au niveau des protocoles, pour une version d'Apache installée sur un serveur Linux, il est possible de mettre en place un certain nombre de filtres par adresse IP, par port TCP ou par application. L'outil logiciel utilisé dans ce cas est généralement « *ipchains* » en mode commande ou dans une version graphique. Le fonctionnement et la syntaxe d'*ipchains* sont décrits dans le paragraphe 5.4.3, *Utilisation d'un*

coupe-feu. Pour illustrer son utilisation dans le cadre d'une sécurisation de serveur web, l'exemple ci-dessous correspond aux commandes utilisées pour interdire la réception de courrier (port 25 SMTP) et la consultation de certaines pages : *www.sexe.com* pour toutes les adresses du réseau local et *http://games.net* seulement pour les adresses du réseau local commençant par 192.168.61.

```
$ IPCHAINS -A input -i eth1 -p TCP -s 0/0 -d 192.168.1.9 25 -l -j REJECT
$ IPCHAINS -A output -i eth1 -s 0/0 -d www.sexe.com -l -j REJECT
$ IPCHAINS -A output -i eth1 -s 192.168.61.0/24 -d games.net -l -j REJECT
```

b) IIS

Sous Windows également, la sécurisation d'accès au serveur ou à un répertoire de données suit les mêmes règles que la sécurisation des répertoires d'un disque. Les droits d'accès sont définis pour des listes d'utilisateurs, des groupes et des domaines définis dans Windows 2000.

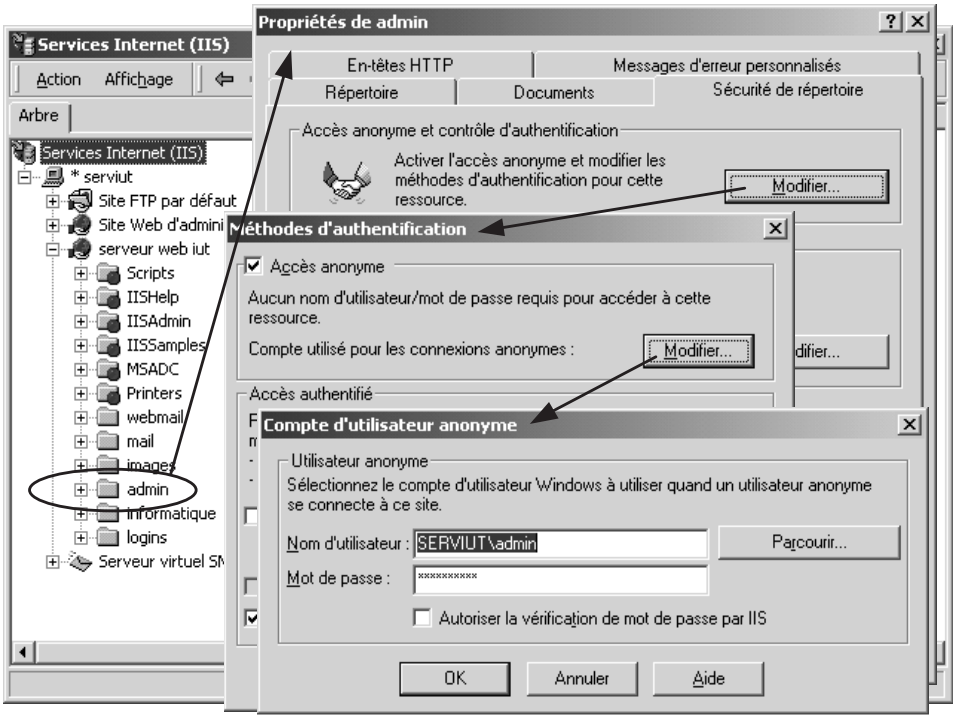

Figure 5.9 Sécurisation de l'accès à un répertoire.

L'onglet « Sécurité de répertoire » de la fenêtre des « propriétés » du répertoire « admin » permet de définir les utilisateurs ou groupes d'utilisateurs ayant accès aux données situées dans ce répertoire (figure 5.9).

5.4.3 Utilisation d'un coupe-feu

a) Coupe-feu sous Linux

Ipchains est le principal outil logiciel sous Linux permettant de filtrer les paquets. Il intervient au niveau de la pile IP pour contrôler quelles machines peuvent se connecter sur votre serveur, sur quels ports (filtrage entrant), mais aussi quelle machine du réseau peut aller sur tel serveur extérieur (filtrage entrant et sortant). *Ipchains* est également utilisé pour faire du « *masquerading* », c'est-à-dire pour masquer de l'extérieur les adresses IP de votre réseau local ; celles-ci pouvant éventuellement être privées (adresses de type 192.168.x.x pour une classe C par exemple) si vous souhaitez isoler votre réseau de l'extérieur pour des raisons de sécurité, de manque d'adresses publiques ou encore pour partager une connexion à Internet en utilisant une seule adresse IP.

Ipchains remplace *ipfwadm* dans les versions actuelles de Linux et sera remplacé par *netfilter* à partir de la version 2.4 du noyau.

➤ Principe du filtrage

Suivant la position sur le réseau et le rôle de votre coupe-feu, il faut définir les règles de filtrage à mettre en pace (figure 5.10). Un paquet entrant sur une machine (*INPUT*) peut être accepté, (*ACCEPT*), rejeté (REJECT) ou dénié (DENY). Lors d'un rejet, l'expéditeur est prévenu que son paquet a été refusé, ce qui n'est pas le cas avec un déni.

Une fois le paquet arrivé sur la machine, il peut être transféré (FORWARD) sur une autre interface réseau. Enfin arrivé sur cette deuxième interface (OUTPUT), il peut être autorisé ou non à poursuivre vers le réseau privé. Dans le mode FORWARD on dispose d'une option supplémentaire pour le « *masquerading* » (MASQ), ce qui permet de masquer les adresses IP des machines se trouvant dans le réseau local.

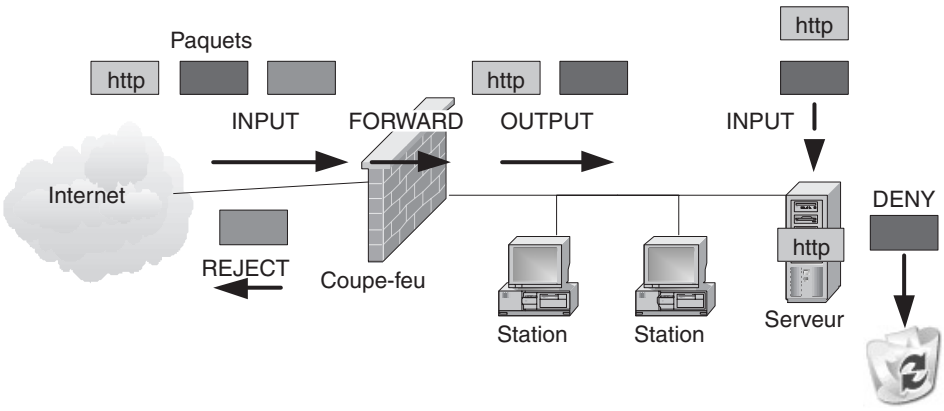

Figure 5.10 Exemple de filtrage Ipchains.

La configuration du filtrage à l'aide du programme *ipchains* peut se faire en ligne de commande. Pour chaque chaîne de filtrage de type « INPUT », « OUTPUT » ou « FORWARD », différentes règles peuvent être ajoutées au début ou à la fin de la chaîne. La syntaxe est la suivante :

```
ipchains -A|I chaîne -i interface -p protocole -s adresse source port -d
adresse destination port -j police -l
```

TABLEAU 5.3

A chaîne	Ajoute une règle à la fin d'une chaîne de type INPUT, OUTPUT ou FORWARD.
I chaîne	Ajoute une règle au début d'une chaîne.
-i interface	Indique l'interface réseau (eth0, eth1, ppp0, lo).
-p protocole	Indique le protocole (TCP, UDP, ICMP, ALL).
-s adresse source port	Indique l'adresse source du paquet (0.0.0.0/0 pour n'importe quelle origine ; 192.168.0.0/24 pour un réseau 192.168.0.0 avec un masque sur 24 bits). Indique le ou les ports concernés (sous forme www ou 80).
-d adresse destination port	Indique l'adresse destination et le port.
-j police	Indique la règle appliquée aux paquets : ACCEPT, DENY, REJECT ou MASQ pour une chaîne de type forward.
-y	Permet de vérifier que les paquets d'initialisation de la connexion viennent de la source (! –y dans l'autre sens).
-l	Message dans le fichier /var/log/messages lorsque la règle est satisfaite.

Exemples de règles :

```
ipchains -I input -s 0.0.0.0/0 -p icmp -j DENY
ipchains -A input -p tcp -y -i eth0 -s 192.168.1.45 -d 192.168.1.20 www -j
ACCEPT
```

La première règle est placée au début de la chaîne et interdit tous les « ping » entrants (les paquets d'écho envoyés suite à une commande « ping » sont générés par le protocole ICMP). La deuxième règle est placée à la fin de la chaîne et autorise une connexion venant de la machine 192.168.1.45 vers le serveur web 192.168.1.20.

Pour simplifier la mise en place des différentes règles, il est recommandé d'utiliser un fichier script que l'on pourra modifier simplement à l'aide d'un éditeur. Il est également possible d'utiliser des constantes afin de rendre la lecture du fichier plus simple (figure 5.11).

```
# Shell utilisé
#!/bin/sh

#  Emplacement de l'exécutable
IPCHAINS=/sbin/ipchains

# Définition des constantes
LOCALNET="192.168.1.0/24"      # le réseau privé de l'entreprise
ETHINSIDE="192.168.1.1"        # exemple d'adresse IP interne
ETHOUTSIDE="193.251.53.1"      # exemple d'adresse IP publique
LOOPBACK="127.0.0.1/8"         # adresse de bouclage
ANYWHERE="0/0"

# Effacement de toutes les règles avant d'en installer de nouvelles
$IPCHAINS -F

# Masquage des paquets à destination de l'extérieur ; ne pas
# masquer les paquets local vers local
# Pour pouvoir utiliser le masquerading, Il faut vérifier que le
# forwarding est activé (ligne « forward_ipv4=yes » dans le fichier
# /etc/sysconfig/network)

$IPCHAINS -A forward -s $LOCALNET -d $LOCALNET -j ACCEPT
$IPCHAINS -A forward -s $ETHOUTSIDE -d $ANYWHERE -j ACCEPT
$IPCHAINS -A forward -s $LOCALNET -d $ANYWHERE -j MASQ

# Définition des règles de filtrage :
$IPCHAINS -A input -s $LOCALNET -j ACCEPT
$IPCHAINS -A input -s $LOOPBACK -j ACCEPT
$IPCHAINS -A input -s $ETHOUTSIDE -j ACCEPT

# Refuser tout paquet venant de l'extérieur et ayant une adresse
# interne, pour éviter l'IP Spoofing :
$IPCHAINS -A outside -s $LOCALNET -j DENY
$IPCHAINS -A outside -s $LOOPBACK -j DENY

# Aucun paquet venant de l'extérieur ne doit pénétrer sur le réseau
# local, parce qu'à l'extérieur, personne n'est supposé connaître
# la plage d'adresses privée interne :
$IPCHAINS -A outside -d $LOCALNET -j DENY

# Refuser les connexions externes vers les ports NFS (111 et 2049),
# sur TCP ou UDP :
$IPCHAINS -l -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 111 -j DENY
$IPCHAINS -l -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 2049 -j DENY
$IPCHAINS -l -A outside -p UDP -s $ANYWHERE -d $ANYWHERE 111 -j DENY
$IPCHAINS -l -A outside -p UDP -s $ANYWHERE -d $ANYWHERE 2049 -j DENY
```

```
# Ne pas surcharger le port 80 TCP en évitant les connexions
# extérieures sur ce port :
$IPCHAINS -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 80 -j DENY

# Accepter les connexions FTP (ports 20 et 21) :
$IPCHAINS -A outside -p TCP -s $ANYWHERE 20:21 -d $ANYWHERE 1024: -j ACCEPT

# Accepter les paquets SSH d'administration à distance :
$IPCHAINS -A outside -p TCP -s $ANYWHERE -d $ANYWHERE ssh -j ACCEPT

# Accepter les paquets DNS venant de l'extérieur (port 53 TCP et
# UDP) :
$IPCHAINS -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 53 -j ACCEPT
$IPCHAINS -A outside -p UDP -s $ANYWHERE -d $ANYWHERE 53 -j ACCEPT

# Accepter tout le trafic SMTP sur le port 25 uniquement :
$IPCHAINS -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 25 -j ACCEPT

# Empêcher le ping des stations extérieures à votre réseau local
# sur celui-ci :
$ IPCHAINS -A input -b -i eth0 -p icmp -s 0/0 -d 0/0
```

Figure 5.11 Exemple de script.

Les interfaces graphiques **kfirewall** (fournie avec l'environnement graphique KDE) ou **gfcc** (disponible en version libre sur Internet) permettent une configuration plus aisée des filtres mais elles ne font au final que traduire en commandes *ipchains* les options choisies graphiquement (figure 5.12).

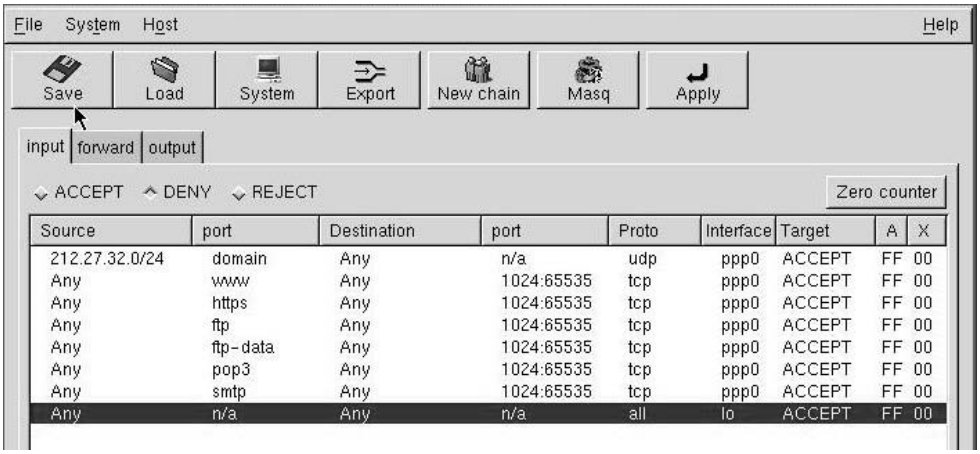

Figure 5.12 Interface graphique gfcc pour Linux.

b) Coupe-feu sous Windows

Comme pour Linux, un coupe-feu logiciel peut être installé sur le serveur web. Cet outil est décrit au paragraphe 4.3.3.

c) Coupe-feu CISCO

Le coupe-feu CISCO PIX 506 est muni de deux interfaces Ethernet, l'une vers le réseau local, l'autre vers Internet ou un autre réseau local. Dans un premier temps, il convient de connecter une console sur le port série standard pour effectuer les configurations de base (activation des interfaces Ethernet, création des adresses IP et des masques, nom du coupe-feu, adresse IP de la station utilisée pour l'administration).

La configuration des règles de filtrage se fait ensuite à partir d'une station connectée sur laquelle un navigateur est lancé avec comme URL celui du coupe-feu. Après saisie du nom d'utilisateur et du mot de passe, le PIX 506 délivre à la station une page web avec le logiciel graphique de configuration « *Cisco PIX Device Manager* ».

Dans l'exemple de la figure 5.13, la règle mise en place spécifie les machines autorisées à ouvrir une connexion sécurisée avec le protocole HTTPS.

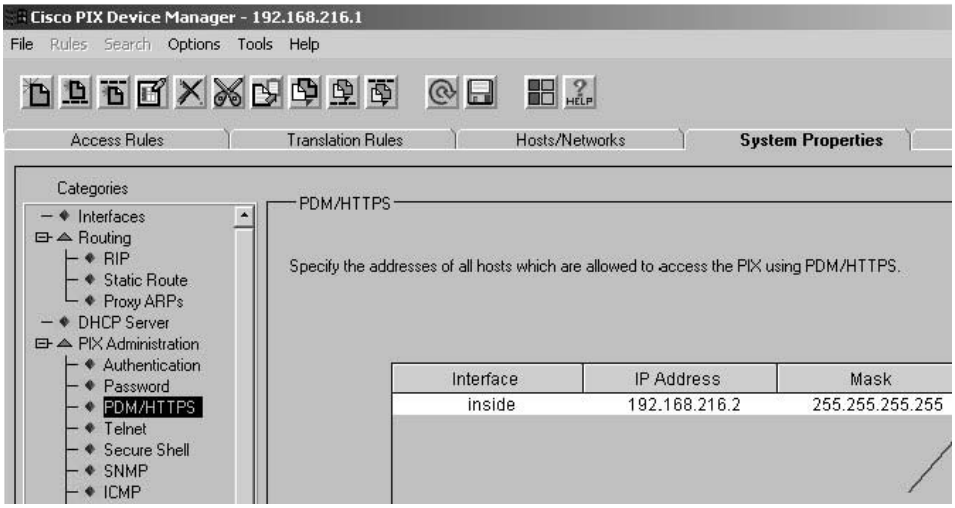

Figure 5.13 Interface graphique du coupe-feu CISCO PIX506.

5.4.4 Utilisation d'une connexion sécurisée avec HTTPS/SSL

a) Cryptage et authentification

La sécurisation de la connexion consiste à crypter les données transmises et/ou authentifier le serveur et/ou le client. Le cryptage est assuré par le protocole SSL, sollicité par le protocole HTTPS. L'architecture des protocoles est présentée figure 5.14.

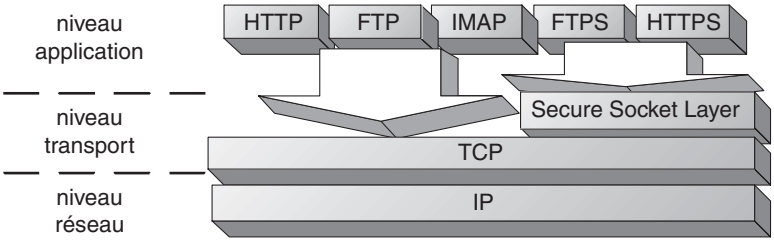

Figure 5.14 Architecture du protocole TCPIP + SSL.

Le protocole SSL autorise plusieurs méthodes de cryptage parmi lesquelles la méthode RSA (*Rivest-Shamir-Aldeman*). Ces méthodes utilisent le cryptage par clé publique/clé privée. Au moment de la connexion, le serveur envoie au client la clé publique (trame 2 de la figure 5.15). Le client se sert de cette clé pour crypter les données. Il envoie un message codé de test avec une signature (trames 3 et 4 de la figure 5.15). Le serveur retourne la signature qu'il a calculée pour valider le cryptage (trame 5 de la figure 5.15). L'échange des données cryptées peut alors commencer.

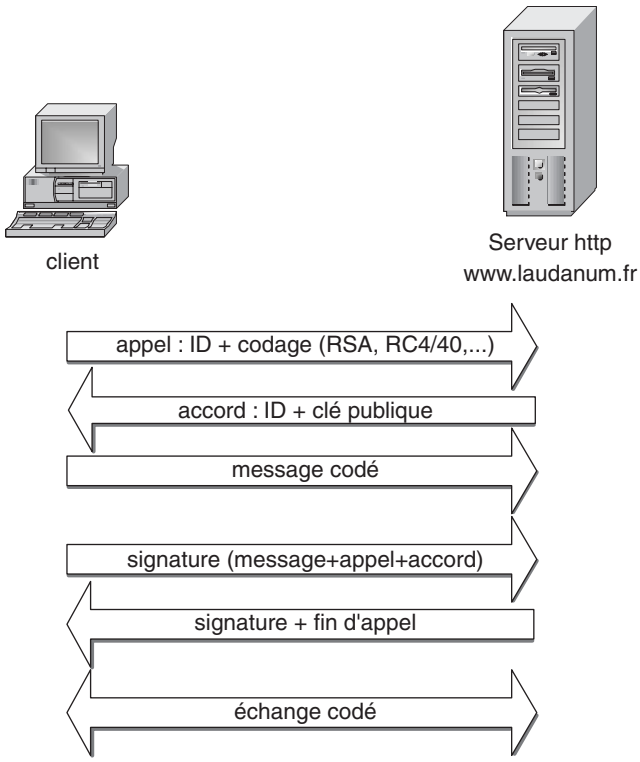

Figure 5.15 Dialogue d'initialisation d'une connexion sécurisée par cryptage SSL.

Cette sécurisation présente une lacune importante. Les entités client d'une part et serveur d'autre part ne sont pas authentifiées. Le client n'a pas la possibilité de vérifier que la clé reçue provient bien du serveur visé. De la même manière, le serveur ne peut vérifier l'identité du client qui se connecte. C'est la raison pour laquelle le cryptage est souvent associé à un certificat. Deux types de certificats existent : les certificats autogénérés et les certificats générés par une autorité de certification (*Certification Authority ou Root CA*). Le premier type de certificat est produit par le serveur d'une part, par le navigateur côté client d'autre part. Les informations sont éditées sous la responsabilité des deux entités qui en certifient la validité. Le format de certificat le plus utilisé est le certificat X.509. Un modèle de certificat est présenté figure 5.18. Bien sûr, un intrus peut générer un faux certificat qu'il adressera au client pour se substituer au serveur (*web spoofing*).

Pour augmenter la sécurité, le serveur, comme le client, peut demander à une autorité de certification de générer le certificat. Le serveur utilise en général un URL de type *https://www.serveur.domaine*. Dans ce cas, le dialogue de connexion comportera une phase d'authentification comme le montre la figure 5.16.

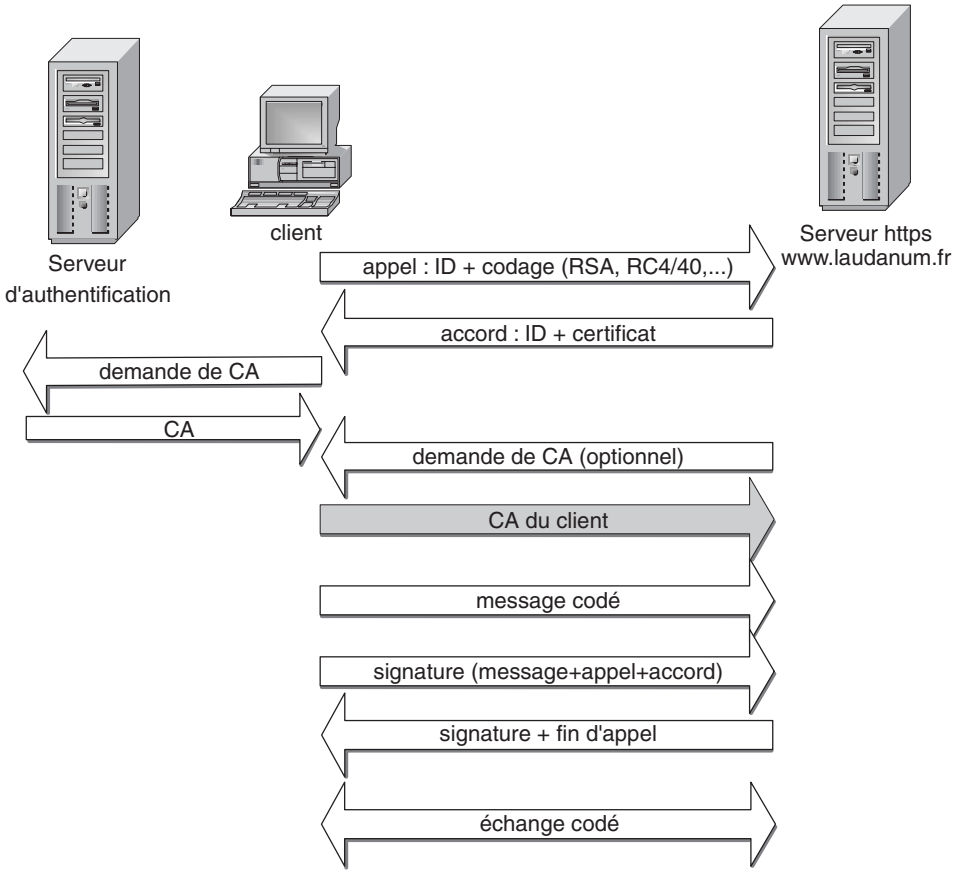

Figure 5.16 Dialogue d'initialisation d'une connexion sécurisée avec authentification.

Le dialogue commence par une requête du client au serveur contenant une chaîne de caractères (mot d'appel) et le type de codage qui sera utilisé. Le serveur répond en renvoyant la chaîne de caractères, la clé publique et un certificat. Celui-ci contient l'adresse d'un serveur de certification. Le client envoie à cette adresse une requête contenant les informations fournies par le serveur (figure 5.17).

```
Certificate Request :
Data:                                                    date d'édition
Version: 0 (0x0)
Subject: C=FR, ST=Paris, L=Paris, O=IUT, OU=serveur,
CN=www.serveur.iut.fr/Email=webmaistre@iut.fr                identité
                                                          du demandeur
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)                             type de cryptage
Modulus (1024 bit):
00:ac:45:e8:2a:6d:23:bc:2e:86:ee:d5:a0:e3:3b:             clé publique
55:c0:b2:96:41:8e:d1:c2:17:c3:2c:8b:be:c0:a5
d5:a2:ed:11:d9:e1:8c:8e:99:9c:05:59:28:23:8d:
8a:aa:a8:0d:de:47:ee:ac:b5:7f:73:4b:e0:15:c2:
ed:40:d0:0f:d4:c2:0a:b6:7e:80:a5:4c:a6:a5:15:
c5:b4:82:fc:53:18:c7:7c:3a:bd:48:ba:37:f6:99:
7c:57:fe:77:92:cf:ef:93:97:5e:2b:34:b1:aa:c3:
af:fd:ed:ef:df:e5:fc:c5:1b:b5:64:15:13:2d:42:
31:6c:0e:b0:e6:96:81:9c:83
Exponent: 65537 (0x10001)

Attributes:
a0:00
Signature Algorithm: md5WithRSAEncryption               signature du
68:49:0b:f0:fc:59:42:8c:7d:ba:01:f8:69:e1:1e:e6:9b:3f:    certificat
ad:3b:c3:9e:2f:eb:49:3c:dd:f7:dc:d5:74:e2:24:a5:ae:89:
27:a2:9f:4f:9a:a6:54:39:de:57:a5:9d:cf:c4:35:96:c0:27:
29:45:ad:3d:3c:80:03:d4:e8:35:c2:1c:e9:fa:3c:09:25:93:
1c:1b:0f:48:1e:f9:12:85:2a:a2:5c:56:d2:6c:28:70:69:7f:
eb:40:30:af:55:a9:e9:aa:f8:f8:1e:c7:f1:a1:e1:be:64:73:
a0:28
```

Figure 5.17 Exemple de demande de certificat.

Après vérification de la validité du certificat demandé, l'autorité de certification retourne celui-ci au client qui le comparera à celui reçu du serveur. Il saura alors si la clé de cryptage peut être utilisée (figure 5.18).

```
Certificate :
Data:                                                    date d'édition
Version: 3 (0x2)
Serial Number: 2 (0x2)
Signature Algorithm: md5WithRSAEncryption
Issuer: OU=Certificate Authority /Email=     identité de l'autorité
                                                    de certification
Validity
Not Before: Mar 26 13:53:26 2002 GMT      date de début de validité
Not After : Mar 26 13:53:26 2003 GMT        date de fin de validité
Subject: C=FR, ST=Paris, L=Paris, O=IUT, OU=serveur,
CN=www.serveur.iut.fr/Email=webmaistre@iut.fr identité du demandeur
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)                          type de cryptage
Modulus (1024 bit):
00:ac:45:e8:2a:6d:23:bc:2e:86:ee:d5:a0:e3:3b:          clé publique
55:c0:b2:96:41:8e:d1:c2:17:c3:2c:8b:be:c0:a5:
d5:a2:ed:11:d9:e1:8c:8e:99:9c:05:59:28:23:8d:
8a:aa:a8:0d:de:47:ee:ac:b5:7f:73:4b:e0:15:c2:
ed:40:d0:0f:d4:c2:0a:b6:7e:80:a5:4c:a6:a5:15:
c5:b4:82:fc:53:18:c7:7c:3a:bd:48:ba:37:f6:99:
7c:57:fe:77:92:cf:ef:93:97:5e:2b:34:b1:aa:c3:
af:fd:ed:ef:df:e5:fc:c5:1b:b5:64:15:13:2d:42:
31:6c:0e:b0:e6:96:81:9c:83
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Alternative Name:
email:tron_yoyo2000@yahoo.fr
Netscape Comment:
mod_ssl generated test server certificate
Netscape Cert Type:
SSL Server
Signature Algorithm: md5WithRSAEncryption              signature du
86:c3:0c:0b:49:d1:29:93:03:de:51:f8:99:64:a7:25:3d:78:   certificat
a8:20:41:a7:32:8a:c3:02:6a:6b:66:c8:00:9d:49:18:54:11:
6d:5c:c1:c9:69:d8:42:e5:b7:2a:95:f3:ad:11:97:29:65:bc:
a2:83:e9:ff:5f:eb:9e:2d:28:82:69:13:67:0d:1d:20:80:82:
68:a6:f8:a7:8b:ec:02:0c:8c:a2:c9:56:13:87:ce:fb:58:3c:
e2:b6:44:35:37:55:0b:4b:e7:7a:13:cc:d6:f4:59:b5:ab:15:
05:a0:e4:2f:41:cd:53:db:85:5f:90:a3:2d:83:d7:1e:b4:1c:
35:17
```

Figure 5.18 Exemple de certificat délivré.

b) Mise en œuvre du cryptage sous Windows

L'encryptage/décryptage est assuré par l'utilitaire SCHANNEL.DLL se trouvant dans le répertoire *windows/system32*. Cet utilitaire doit être chargé côté client ET côté serveur. Pour mettre en œuvre le cryptage dans Internet Explorer, il faut sélectionner le menu « outils » et l'option « options Internet ». Dans l'onglet « avancés » la section « sécurité » permet de valider les protocoles de cryptage SSL 2.0 et SSL 3.0 (figure 5.19).

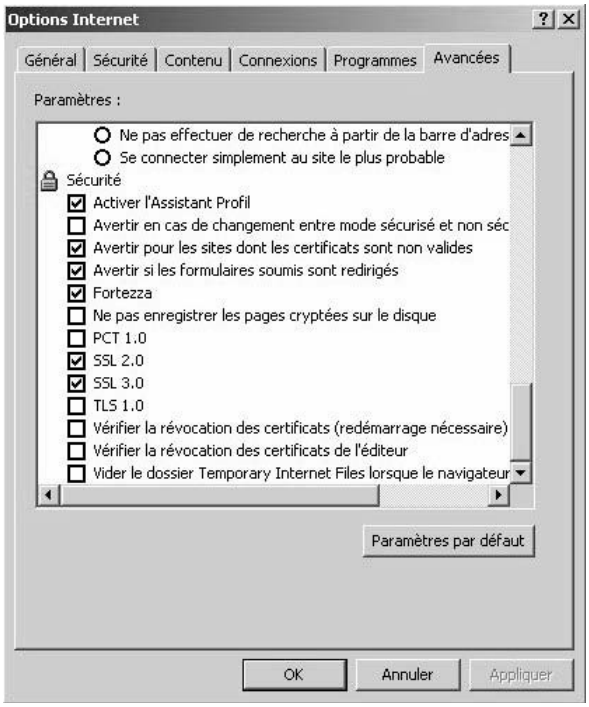

Figure 5.19 Validation des protocoles de cryptage SSL.

Internet Explorer propose plusieurs algorithmes de cryptage, différents suivant les versions et les mises à jour utilisées. La procédure d'activation pour Windows NT et Windows 2000 est décrite dans la notice technique Q245030 disponible sur le site Microsoft.

Pour connaître le type de clé utilisable, il suffit de lancer le navigateur et de sélectionner, dans le menu « ? », l'option « à propos de ». La taille de la clé se trouve dans la fenêtre (figure 5.20).

Lorsqu'une connexion sécurisée par cryptage est établie, le navigateur affiche un symbole représentant un cadenas à droite dans la barre d'état (figure 5.21).

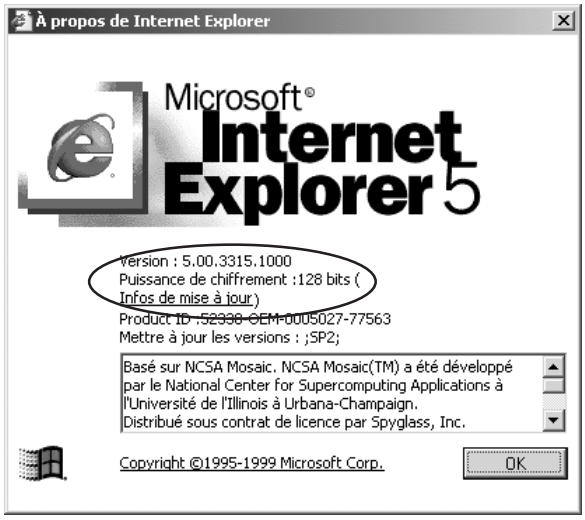

Figure 5.20 Description des clés de cryptage utilisées par Internet Explorer.

Figure 5.21 Identification d'une connexion sécurisée par cryptage.

c) Sécurisation d'un serveur web par authentification

➤ Mise en place d'une autorité de certification privée (*Certificat Root CA*)

Le service nécessaire est *Certificate Server*. Il peut être installé sous Windows 2000 Server à partir de la fenêtre « ajout/suppression de programmes », comme le montre la figure 5.22.

Une fois le service installé, Windows 2000 ajoute automatiquement l'autorité de certification *Root CA* à la liste sous le nom du serveur sur lequel il est installé. La liste des autorités de certification est accessible par le menu « outils » du navigateur *Internet Explorer* en sélectionnant l'option « options Internet ». Dans la fenêtre, sélectionner l'onglet « contenu » et cliquer sur « certificats ». La liste des autorités de certification se trouve dans l'onglet « autorités principales de confiance ». Il faut ensuite que le serveur web demande un certificat à l'autorité de certification créée.

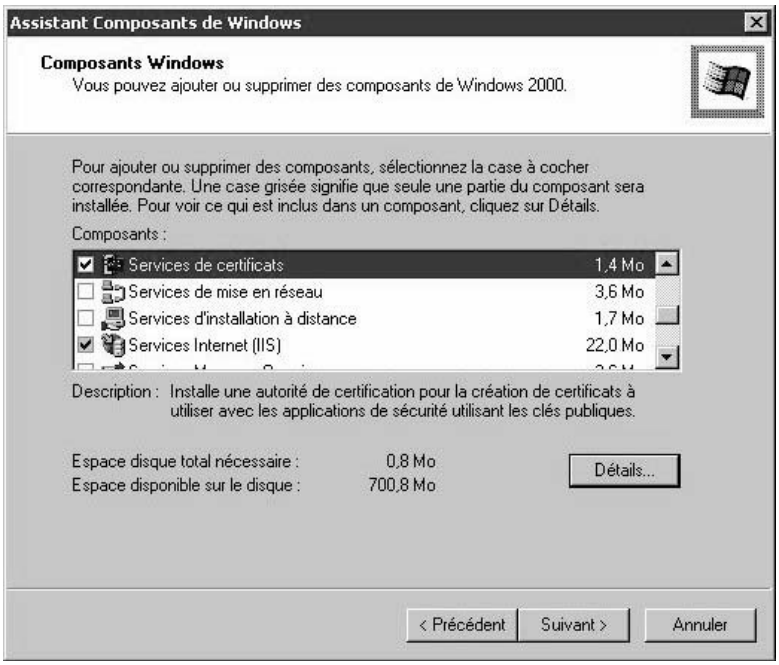

Figure 5.22 Installation du service « Certificate Server ».

Cette opération comprend quatre phases :

1. Création d'une demande de certificat.
2. Envoi de la demande au serveur de l'autorité de certification.
3. Téléchargement du certificat créé.
4. Installation sur le serveur du certificat téléchargé.

La procédure est détaillée dans l'étude de cas 2 en fin de chapitre.

➤ Mise en place d'une sécurisation par authentification sur le client

Des serveurs sécurisés demandent au client qui se connecte de fournir un certificat. Un client peut obtenir un certificat personnel auprès d'organismes de certification. Des organismes proposent des certificats gratuits ou des certificats de test à durée limitée. Parmi ceux-ci, Certplus (*http://www.certplus.com*) le CNRS (*http://igc.services.cnrs.fr/CNRS-Standard/certificats.html*) et Certinomis (*http://www.certinomis.com*), filiale du groupe La Poste. L'obtention d'un certificat se fait en trois phases :

1. Demande de certificat à l'autorité de certification.
2. Envoi d'un avis de retrait du certificat par l'autorité de certification.
3. Installation du certificat sur le poste du client.

La procédure est détaillée dans l'étude de cas 2 en fin de chapitre.

Résumé

1. Choix d'un serveur http

➢ dans l'architecture matérielle d'un serveur, le nombre de processeurs, la capacité de la mémoire et sa rapidité seront plus importants que sa capacité graphique ou multimédia ;
➢ la sécurité du stockage des données est également un point important ;
➢ la technologie RAID (*Redondant Array of Inexpensive Disks*) répartit les données d'un fichier sur plusieurs disques.

2. Configuration d'un serveur Apache

➢ la configuration utilise le fichier texte **httpd.conf** qui sera modifié à l'aide d'un éditeur ;
➢ la 1re modification consiste à donner un nom au serveur par la directive **« ServerName »** ;
➢ il est necessaire de faire correspondre le nom donné au serveur et référencé par DNS avec le nom déclaré pour la directive ServerName ;
➢ il faut placer la page d'accueil dans le répertoire par défaut ;
➢ l'accès à un répertoire est contrôlé par deux fichiers « .htaccess » et « .htpasswd » ;
➢ pour le reste, le fichier httpd.conf est organisé en deux parties : la première concerne les ressources du serveur et leur localisation ; la deuxième permet le contrôle des accès aux différents répertoires du serveur http.

3.Configuration d'un serveur IIS

➢ l'installation des services Internet se fait par ajout/suppression de composant Windows ;
➢ la première étape consiste à attribuer un nom et une adresse IP au site web (« propriétés », « site web ») ;
➢ il faut ensuite indiquer le répertoire où se trouvent la page d'accueil et les fichiers par défaut (« propriétés », « répertoire de base » et « documents »).

4. Sécurisation d'un serveur http

➢ la sécurité peut s'obtenir par l'obscurité, par l'hôte ou par le réseau ;
➢ les cinq questions de la sécurisation des échanges sont : la confidentialité, l'authentification, le contrôle d'accès, l'intégrité et la non-répudiation ;
➢ un serveur Apache ou IIS sous Linux ou Windows est sécurisé au niveau des ressources en utilisant les droits des utilisateurs, groupes et éventuellement domaines de Windows ;
➢ un serveur Apache sous Linux peut être sécurisé au niveau protocole, par filtrage d'adresses IP ou de port avec l'outil « ipchains » ;
➢ le pare-feu, placé entre le réseau local et Internet, filtre les paquets entrant et sortant à partir d'une liste de règles ;

➢ les paquets qui ne sont pas autorisés à traverser le pare-feu par l'une des règles sont rejetés ;
➢ les pare-feu spécialisés (exemple CISCO PIX506) se configurent à partir d'un ordinateur connecté par le réseau, par un port USB ou une liaison série ;
➢ la sécurisation d'un serveur passe par le cryptage des données transmises et/ou l'authentification du serveur et/ou du client ;
➢ le cryptage des données est assuré par le protocole SSL ;
➢ avant la transmission, serveur et station échangent la clé de cryptage et testent la transmission cryptée ;
➢ les certificats autorisent l'authentification du serveur et/ou du client ;
➢ les certificats peuvent être autogénérés ou générés par une autorité de certification ;
➢ le client reçoit la clé et le certificat du serveur et demande un certificat à l'autorité de certification pour vérifier la validité de la clé ;
➢ le service de certification doit être installé sur Windows 2000 Server (fenêtre « ajout/suppression de programmes ») pour créer une demande de certificat ;
➢ l'autorité de certification crée le certificat à réception de la demande envoyée par le serveur ;
➢ client et serveur téléchargent le certificat auprès de l'autorité et l'installent sur leur ordinateur.

QCM

Une version électronique et interactive est disponible sur le site *www.dunod.com*.

1. Choisir un serveur http

Q1. Quelles caractéristiques sont importantes dans un serveur ?
a) le nombre de processeurs *b) la capacité mémoire*
c) la qualité de l'écran *d) la carte graphique*
e) le stockage *f) la sauvegarde*

Q2. La technique RAID permet le stockage d'un fichier (plusieurs réponses) :
a) sur plusieurs disques *b) sur plusieurs partitions*
c) en deux exemplaires *d) avec des contrôles d'erreur*

2. Configuration d'un serveur Apache

Q3. La configuration d'un serveur Apache se fait dans le fichier :
a) autoexec.bat *b) config.htm* *c) config.sys*
d) httpd.conf *e) .htaccess* *f) .htpasswd*

Q4. Le contrôle d'accès à un répertoire d'un serveur Apache utilise les fichiers :
a) autoexec.bat *b) config.htm* *c) config.sys*
d) httpd.conf *e) access.conf* *f) passwd.conf*

3. Configuration d'un serveur IIS

Q5. La configuration d'un serveur web IIS utilise :
a) le fichier autoexec.bat *b) le fichier config.sys*
c) le gestionnaire des services Internet *d) le navigateur web*

Q6. Parmi les paramètres intervenant dans la configuration du serveur IIS se trouvent :
a) le nom du fichier par défaut *b) l'adresse IP du serveur*
c) le type de réseau utilisé *d) l'emplacement du fichier httpd.conf*

4. Sécurisation d'un serveur http

Q7. Les attaques de sites web consistent à :
a) trouver un point d'entrée sur le serveur
b) utiliser un ordinateur sans autorisation
c) modifier la configuration d'une station

Q8. Quels problèmes résout le cryptage des transmissions de données ?
a) la confidentialité *b) l'authentification* *c) le contrôle d'accès*
d) l'intégrité *e) la non-répudiation*

Q9. Sur un serveur Apache, l'outil logiciel « ipchains » sert à paramétrer :
a) la configuration réseau *b) la mise à jour du site web*
c) l'arborescence des pages du site *d) le filtrage de paquets*

Q10. Sur un serveur IIS, le contrôle de l'accès aux pages web utilise :
a) le fichier httpd.conf *b) le fichier config.sys*
c) le fichier .htaccess *d) les règles du pare-feu*
e) les règles de Windows *f) le fichier .htpasswd*

Q11. Dans une entreprise utilisant un seul pare-feu, son efficacité sera maximale placé :
a) entre le serveur de compte et le serveur web
b) entre l'accès Internet et le serveur de compte
c) entre l'accès Internet et le routeur d'accès au réseau local
d) entre les stations du service financier et le serveur web

Q12. Le pare-feu filtre les paquets (plusieurs réponses) :
a) entrant sur le réseau local *b) circulant sur le réseau local*
c) sortant du réseau local *d) changeant de sous-réseau*

Q13. Le rejet d'un paquet par un pare-feu se fait par consultation :
a) de la destination du paquet *b) de l'URL transportée*
c) de l'application de destination *d) du nom de la station source*

Q14. Le protocole SSL est un protocole de niveau :
a) physique *b) liaison* *c) réseau*
d) transport *e) session* *f) application*

Q15. Pour une transmission sécurisée de données, un certificat autorise :
a) la confidentialité *b) l'authentification* *c) le contrôle d'accès*
d) l'intégrité *e) la non-répudiation*

Q16. Pour une transmission cryptée de données, une autorité de certification sert :
a) à créer la clé de cryptage *b) de point de transit des données*
c) à donner le droit d'utilisation de la clé
d) à contrôler la validité de la clé

Q17. Avant l'envoi d'une demande à une autorité de certification, le serveur doit :
a) créer la clé de cryptage *b) envoyer la clé au client*
c) installer la clé sur le serveur *d) demander une clé de cryptage au client*

Exercices

➤ (*) : facile(**) : moyen(***) : difficile

Corrigés à la fin du livre et sur le site *www.dunod.com*.

5.1 (*) Le service SMTP est l'un des plus attaqués sur Internet. Nous allons étudier la mise en place d'un Firewall pour protéger un serveur de courrier interne représenté figure 5.23.

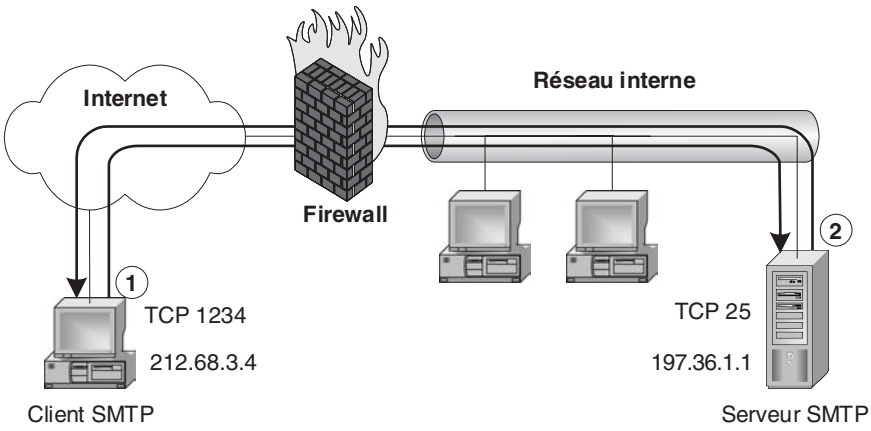

Figure 5.23

Dans un premier temps, le routeur qui fait office de Firewall est configuré suivant le tableau 5.4.

Tableau 5.4

Règle	Direction	@ source	@dest.	Protocole	Port dest.	Action
A	Entrant	Externe	Interne	TCP	25	Permission
B	Sortant	Interne	Externe	TCP	>1023	Permission
C	Sortant	Interne	Externe	TCP	25	Permission
D	Entrant	Externe	Interne	TCP	>1023	Permission
E	Toutes	Toutes	Toutes	Tous	Tous	Refus

a) Quelles sont les connexions autorisées par les règles A à E ?

b) Les connexions décrites par la figure 5.23 sont-elles autorisées ? Écrire les deux connexions dans le tableau 5.5 en précisant à quelle règle générale elles se rapportent (règles A à E).

Tableau 5.5

Connexion	Direction	@ source	@dest.	Protocole	Port dest.	Règle
1						
2						

c) Comment peut-on modifier le tableau de départ pour qu'un agresseur externe ne puisse ouvrir une connexion sur le serveur SMTP en se faisant passer pour une station du réseau local (station interne) ?

5.2 (**) **Configuration du firewall**

Une entreprise dispose de 20 postes, d'un serveur de messagerie, d'un serveur Intranet d'un serveur web et d'un serveur de stockage. Les employés utilisent le mail et doivent accéder à Internet. L'entreprise souhaite protéger son réseau interne.

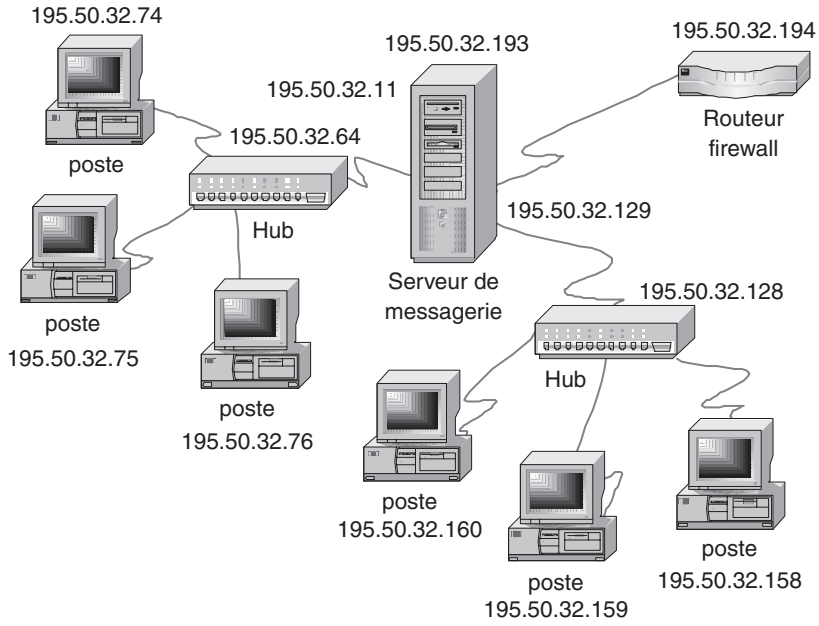

Figure 5.24

Règles de sécurité :

– Règle 1 : les clients extérieurs ne doivent pouvoir utiliser le réseau interne que pour envoyer un message aux employés.

– Règle 2 : les employés doivent pouvoir utiliser l'intégralité du réseau interne.

– Règle 3 : les employés doivent accéder à Internet.

Tableau 5.6 Règles de filtrage.

Source	Destination	Service	Action	Track	Install	On
any	mailsrv	smtp	accept	short	log	Gateways
localnet	any	any	accept	short	log	Gateways
any	any	any	reject	long	log	gateways

La première ligne correspond à la règle 1.

La deuxième ligne correspond aux règles 2 et 3.

Tous les autres accès sont interdits (les paquets sont comparés aux règles dans l'ordre du tableau de configuration). La troisième ligne permet de mémoriser dans le journal les tentatives d'accès illicites.

Un serveur Intranet est connecté sur le réseau. Il doit être accessible de tous les postes du réseau, mais inaccessible de l'extérieur. Quelles modifications apporter à la configuration du firewall ?

Tableau 5.7

Source	Destination	Service	Action	Track	Install	On
any	mailsrv	smtp	accept	short	log	Gateways
localnet	any	any	accept	short	log	Gateways
any	any	any	reject	long	log	gateways

5.3 (*) Vous avez décidé de faire de votre ordinateur un serveur http sous IIS.

a) Préparez les répertoires destinés à recevoir les pages web.

b) Relevez sur votre ordinateur les paramètres qui vous seront nécessaires pour la configuration du serveur.

Exercices pratiques

5.4 Serveur Apache

Vous devez administrer un serveur Apache sous Linux. Vous disposez pour cela d'une distribution de Linux opérationnelle sur un serveur avec le programme httpd installé. Vous devez disposer également d'un ordinateur client muni d'un navigateur ou à défaut, utiliser comme client le navigateur du serveur.

a) Vérifiez que le programme httpd est bien installé et opérationnel : commande */etc/rc.d/init.d/httpd status* pour connaître l'état du serveur et éventuellement commande */etc/rc.d/init.d/httpd start* pour le démarrer.

b) Comment modifier le fichier de configuration *httpd.conf* pour donner au serveur Apache un nom DNS ? Quel service doit être mis en œuvre pour pouvoir utiliser ce nom à partir d'un navigateur ? En l'absence de ce service quelle adresse peut-on mettre ?

c) Comment modifier le fichier *httpd.conf* pour donner un numéro de port non standard, différent de 80, au service HTTP ? Tester sur le client. Quel URL avez-vous utilisé ?

d) Quel est le compte par défaut utilisé sur le serveur pour la connexion ?

e) Comment limiter le temps pendant lequel le serveur doit attendre la transmission d'une requête, après l'établissement d'une connexion par un client ?

f) Comment mettre en œuvre le serveur de proxy et paramétrer le cache ?

g) La directive *TypesConfig* spécifie le fichier contenant la table des correspondances des extensions de fichier pour les types de données MIME. En l'absence de cette directive, le fichier par défaut est /etc/mime.types ou */etc/httpd/conf/apache-mimes.types*. Quelles sont les extensions vidéo reconnues ?

h) Créer un nouvel utilisateur ainsi qu'une page html personnelle dans le sous-répertoire approprié de l'utilisateur.

i) Vérifier les droits sur ce sous-répertoire pour que tout le monde puisse lire. Tester cette page à partir d'un navigateur. Quelle URL avez-vous utilisée ?

j) La fabrication d'un mot de passe se fait par le programme *htpasswd* qui prend la syntaxe suivante :

htpasswd [-c] passwordfile username

Avec l'option -c le fichier est créé ; sans l'option -c le fichier est complété par la nouvelle entrée.

passwordfile est le nom du fichier contenant les utilisateurs et les mots de passe (par exemple users.http).

username est le nom de l'utilisateur.

k) Tester, à partir du navigateur client, une protection d'accès pour le répertoire personnel créé précédemment.

5.5 Firewall sous Linux

Ce travail doit être réalisé par deux personnes. Lancer une connexion Telnet sur la machine de votre voisin. Vérifier avec les outils dont vous disposez, les ports utilisés sur la machine locale et sur la machine distante.

a) Créer un script Ipchains avec les règles suivantes :

- interdire par défaut tous les ports en input (par facilité autoriser les output et forward) ;
- autoriser la machine de votre voisin à se connecter sur le port telnet ;
- autoriser votre machine à faire du telnet sur les machines extérieures ;
- autoriser les "pings" sur votre machine ;
- autoriser votre machine à pinguer toutes les machines extérieures ;
- autoriser dns avec UDP (nécessaire pour naviguer) ;
- autoriser dns avec TCP (idem) ;
- autoriser la navigation sauf sur le serveur web local.

b) Tester toutes les règles.

5.6 Partage sécurisé de connexion Internet sous Linux

Créer un script Ipchains permettant d'effectuer un partage de connexion Internet pour un réseau privé d'adresse 192.168.0.0. L'adresse du routeur coupe-feu sera 192.168.0.1 côté privé et attribué dynamiquement côté Internet.

a) Que devez-vous modifier dans le fichier de configuration réseau */etc/sysconfig/network* ?

b) Comment devez-vous configurer les stations du réseau privé ?

Étude de cas 1 : Contrôle d'accès aux répertoires d'un site web

L'exemple montre la procédure permettant de contrôler l'accès aux pages situées dans chacun des répertoires « admin » et « informatique » du site « serviut » (figure 5.4). L'arborescence du site est représentée figure 5.25.

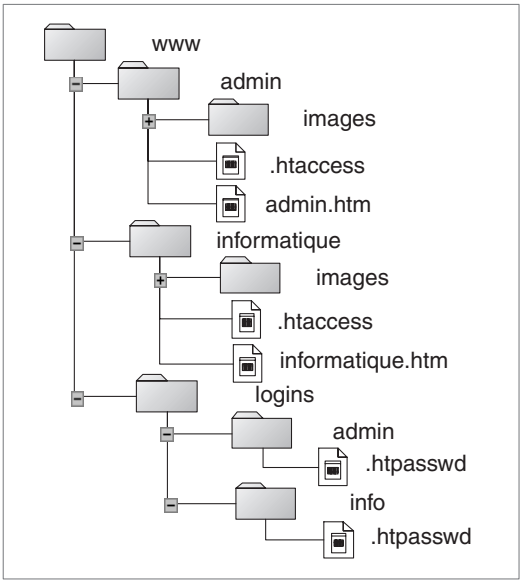

Figure 5.25 Arborescence du site « serviut ».

Les fichiers de contrôle « .htaccess » sont placés dans le répertoire à contrôler. Pour le répertoire « admin », le fichier est :

```
AuthUserFile  c:\programmes\easyphp1-7\www\logins\admin\.htpasswd
AuthGroupFile  /dev/null
AuthName   "accès protégé"
AuthType  Basic
<LIMIT GET POST>
Require valid-user
</LIMIT>
```

Ce fichier est un fichier texte. Il peut être créé avec un simple éditeur de texte. Dans le cas où le bloc-note de windows est utilisé, le fichier sauvegardé aura une extension « .txt ». Il faudra renommer le fichier sous Dos en utilisant la commande « rename ».

Reste à créer le fichier « .htpasswd » situé dans le répertoire « logins » sous-répertoire « admin ». La création de ce fichier se fera par la commande Dos « htpasswd » se trouvant dans le répertoire apache\bin. Sous Windows, le

codage par défaut du mot de passe utilise le format MD5. Dans l'exemple de la figure 5.26, pour clarifier l'exemple, le codage du mot de passe est interdit.

Figure 5.26 Création d'un mot de passe d'accès à un répertoire.

Le fichier ainsi créé contient : `admin:web`

L'ajout de comptes et de mots de passe s'obtient en renouvelant la commande et en omettant le paramètre « -c ». Il suffit d'opérer de la même manière pour le répertoire « informatique ».

Étude de cas 2 : Mise en place d'un certificat d'authentification

L'étude montre les procédures permettant de créer un certificat d'authentification sur un serveur, de le transmettre à une autorité pour certification, et de le télécharger par un client pour l'installer sur son poste. L'autorité de certification utilisée est Certinomis (site web : *http://www.certinomis.com*). La première étape consiste à obtenir un certificat auprès de l'autorité de certification.

1. Création d'une demande de certificat

La création d'une demande de certificat utilise un assistant de certificat disponible dans « services Internet », menu « propriétés » en sélectionnant l'onglet « sécurité du répertoire » et le bouton « certificat de serveur » (figure 5.27).

L'assistant propose de créer un certificat, d'attribuer un certificat existant ou d'importer un certificat. Il demande d'attribuer un nom au certificat, de définir la longueur de la clé de cryptage, le nom du serveur demandeur, ainsi que le répertoire de stockage du certificat. Le certificat est alors créé et stocké en fichier texte dans le répertoire spécifié (figure 5.28).

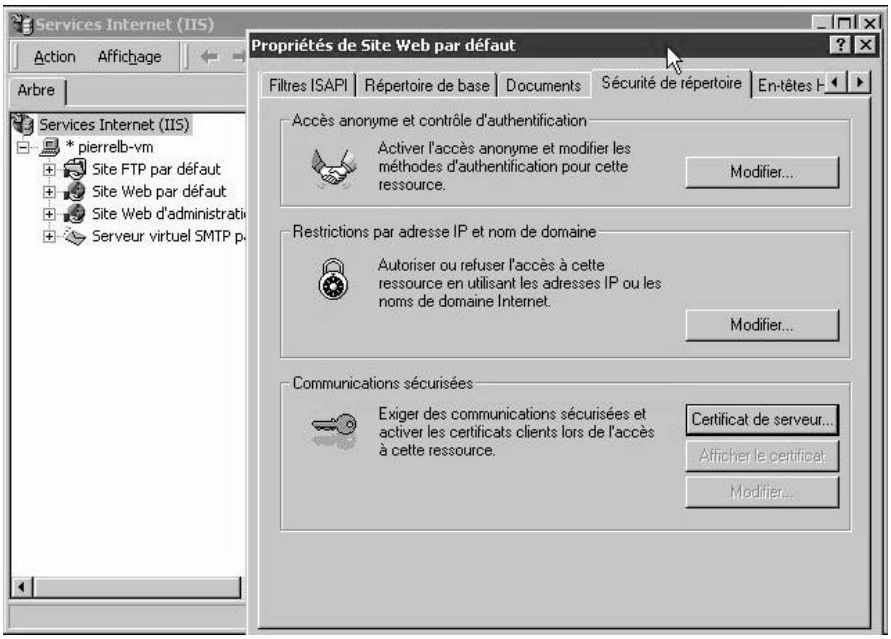

Figure 5.27 Assistant de création d'une demande de certificat.

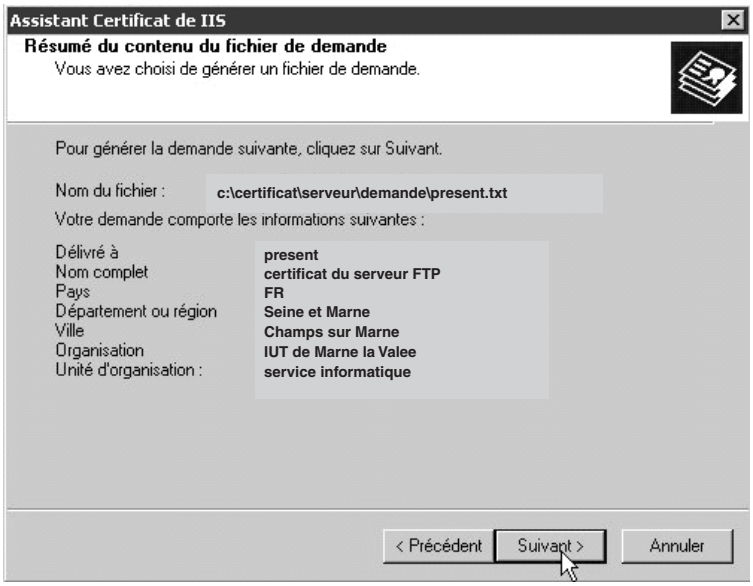

Figure 5.28 Demande de certificat.

Dans le cas d'une autorité de certification privée, la demande de certification doit être soumise à l'autorité locale *Root CA*.

2. Envoi de la demande de certificat

La page d'accueil du serveur de l'autorité de certification propose de remplir un formulaire contenant entre autre l'adresse électronique. Pour l'obtention d'un certificat de test, seule l'adresse électronique est utilisée pour vérifier l'identité du demandeur (figure 5.29).

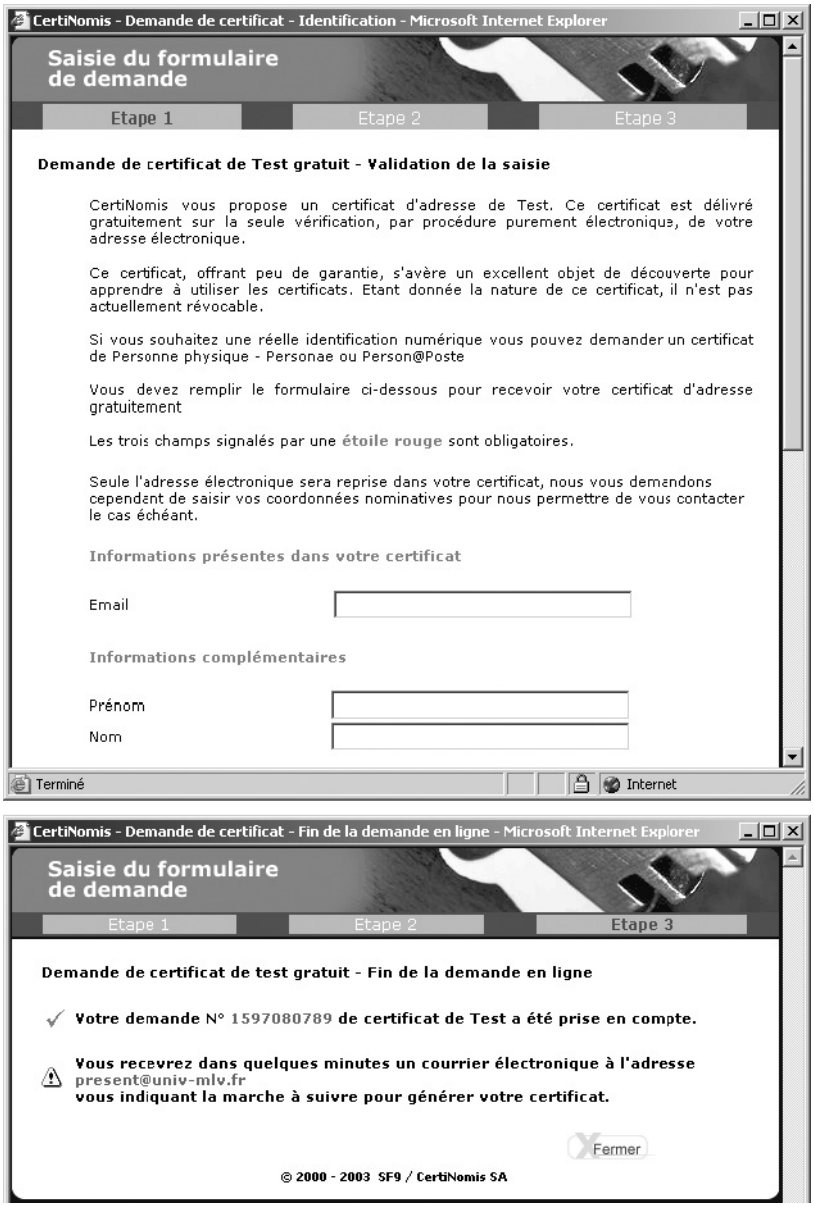

Figure 5.29 Page d'accueil d'un serveur d'une autorité de certification.

Dans le cas d'une création de certificat, il faudra recopier (par un copier/coller) le contenu de la demande de certificat créé précédemment dans le formulaire proposé par le serveur (sans oublier les champs ------- BEGIN NEW CERTIFICATE REQUEST et ---- END NEW CERTIFICATE REQUEST).

Le serveur de l'autorité de certification va alors créer votre certificat. Il vous fournit un identifiant et vous envoie un code d'accès par courrier électronique à l'adresse fournie dans le formulaire.

3. Téléchargement du certificat

Il faut que le demandeur du certificat se connecte au serveur de l'autorité de certification en utilisant le code d'accès reçu par courrier électronique, sélectionne le certificat en attente et le télécharge (figure 5.30).

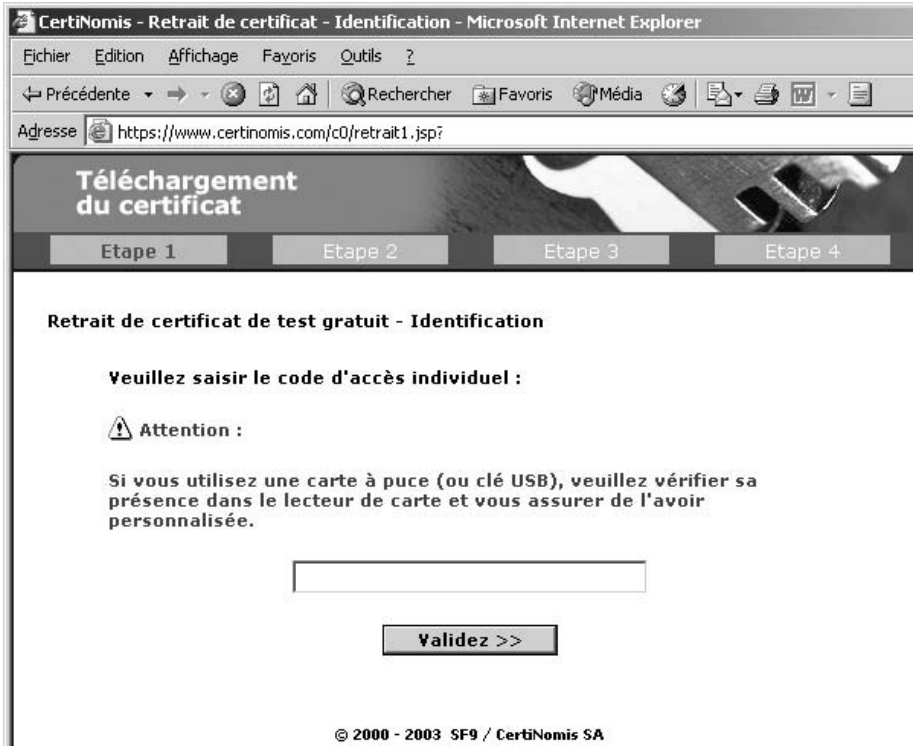

Figure 5.30 Page d'accueil du serveur de l'autorité de certification Root CA.

4. Installation du certificat

Il existe 2 méthodes :

– copier le certificat directement sur un répertoire du serveur web, puis double-cliquer dessus ;

– utiliser l'assistant d'installation de certificat disponible dans « services Internet », menu « propriétés » en sélectionnant l'onglet « sécurité du répertoire » et le bouton « certificat de serveur ».

Après avoir sélectionné l'option « traiter la demande en attente et installer le certificat », l'assistant demande le chemin du répertoire où se trouve le certificat reçu de l'autorité de certification. Le certificat est ensuite installé.

Dans l'onglet « sécurité du répertoire » du menu « propriétés », deux boutons ont fait leur apparition dans le cadre « communications sécurisées ». Ils permettent de visualiser ou modifier les certificats installés (figure 5.31).

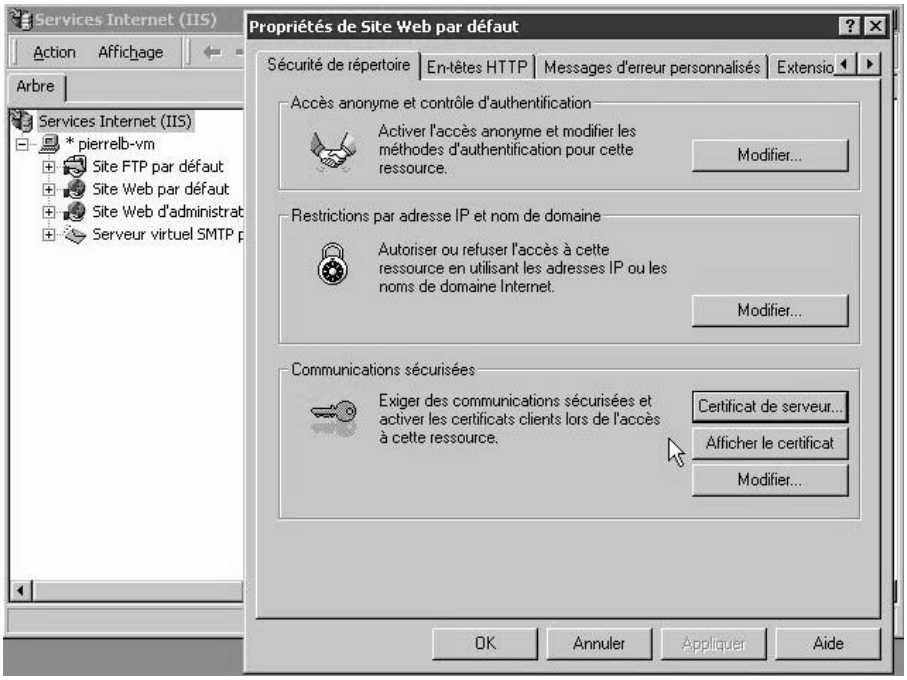

Figure 5.31 Boutons de visualisation/modification des certificats installés.

Il faut encore configurer l'accès au serveur pour imposer une communication sécurisée par authentification. L'accès au menu de configuration se fait en cliquant sur le bouton « modifier » du cadre « communications sécurisées » de la fenêtre (figure 5.31).

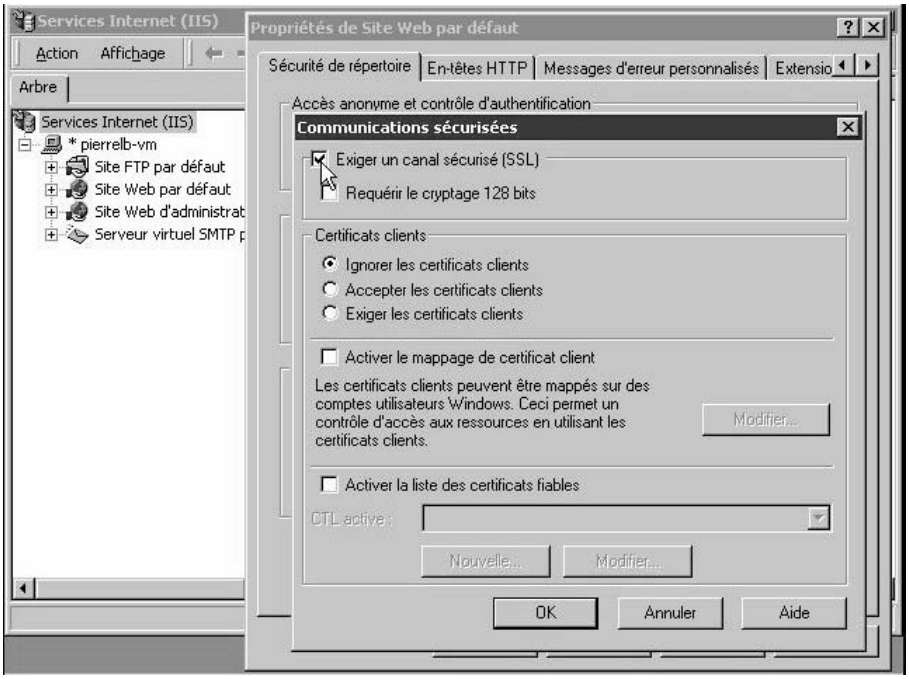

Figure 5.32 Menu de configuration d'une communication sécurisée avec le serveur web.

Le menu permet d'activer le cryptage, d'exiger ou non le certificat du client, et dans l'affirmative, de les relier ou non aux comptes clients gérés par Windows, leur donnant ainsi automatiquement les droits d'accès aux ressources configurés dans Windows (figure 5.32).

Le serveur n'est plus accessible que par une URL « https:// ».

Mise en place d'une sécurisation par authentification sur le client

Des serveurs sécurisés demandent au client qui se connecte de fournir un certificat. Un client peut obtenir un certificat personnel auprès d'organismes de certification. Des organismes proposent des certificats gratuits ou des certificats de test à durée limitée. Parmi ceux-ci, le CNRS (*http://igc.services.cnrs.fr/CNRS-Standard/certificats.html*) et Certinomis (*http://www.certinomis.com*), filiale du groupe La Poste. L'obtention d'un certificat se fait en trois phases :

1. Demande de certificat

Le site présente un formulaire à remplir. Les informations indispensables qui serviront à l'établissement du certificat sont le nom, le prénom et l'adresse e-mail. Une fois le formulaire rempli et vérifié, la demande est enregistrée par le serveur du site qui informe que le certificat sera envoyé par e-mail.

2. Envoi de l'avis de retrait

Un message électronique informe le client qu'il peut télécharger son certificat. Cet avis (figure 5.33) contient l'adresse de retrait et un code d'accès.

```
De: Autorite CertiNomis [autorite@certinomis.com]
Envoyé: dimanche 7 septembre 2003 21:04
À: dominique present
Objet: Certinomis de test gratuit ID 1597080789

Cher client,

votre demande de certificat de test gratuit a été acceptée.
Vous pouvez maintenant charger votre certificat à l'adresse
suivante :

https://www.certinomis.com/c0/retrait1.jsp

(veillez à bien copier l'intégralité de cette adresse dans le
même navigateur depuis lequel vous avez effectué votre demande)

Votre code de retrait est:
Vous devez le copier et le coller dans la boîte de dialogue
de l'URL précitée.

Merci de votre fidélité,
Meilleures salutations.

"CertiNomis est une filiale de la Poste: http://www.certinomis.com"
```

Figure 5.33 Avis de retrait du certificat client.

3. Installation du certificat

Deux méthodes sont possibles :

– installation automatique ;

– téléchargement du certificat au format texte et copie dans l'éditeur de certificat.

La seconde méthode est plus délicate car elle laisse place à des erreurs de copie.

Quelle que soit la méthode, il faut se connecter à l'adresse indiquée par le mail. La page d'accueil demande le code d'accès autorisant le retrait du certificat.

Une fois l'accès autorisé, il suffit de valider le chargement du certificat (figure 5.34).

Figure 5.34 Chargement et installation du certificat.

Le certificat est installé automatiquement. Son contenu peut être affiché (menu « outils », option « options Internet », onglet « contenu », bouton « certificats », sélectionner le certificat et cliquer sur le bouton « affichage »). La figure 5.35 montre le contenu du certificat obtenu.

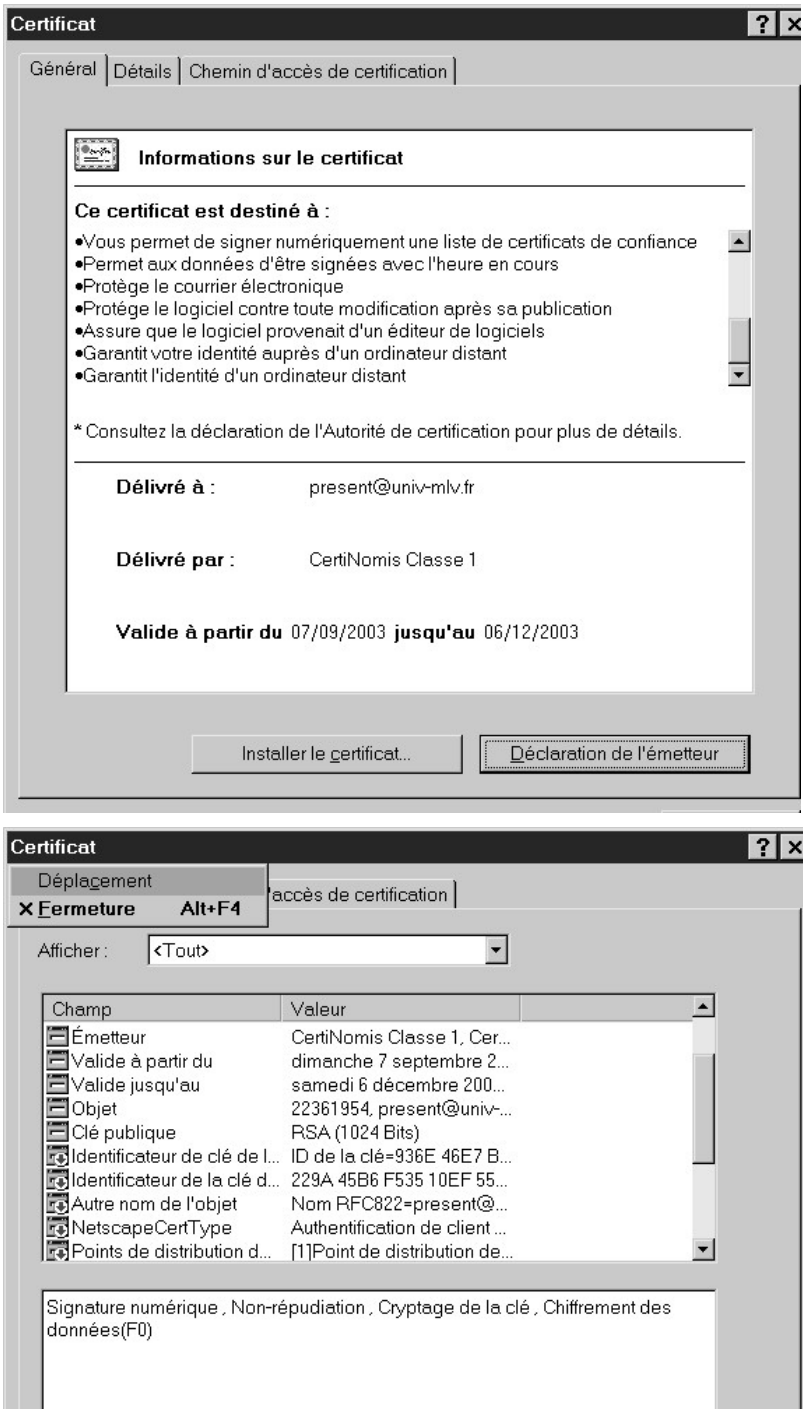

Figure 5.35 Contenu du certificat « client ».

Chapitre **6**

Corrigés des QCM et des exercices

CHAPITRE 1

QCM

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
b)	*b) ; c)*	*c)*	*c) ; d)*	*b)*	*c)*	*a)*	*b)*

CHAPITRE 2

QCM

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
a) ; c) ; d)	a)	b)	a)	c)	d)	b)	c)	a) ; d)
Q10	**Q11**	**Q12**	**Q13**	**Q14**	**Q15**	**Q16**	**Q17**	**Q18**
b)	b)	d)	b) ; d)	b)	c)	c) ; e)	a) ; b)	a)

Exercices

2.1 a) Le taux de surbooking est 120*56/2 000 = 3,36.

b) Sur une ligne à 2 Mb/s, il est possible de faire passer simultanément 35 communications à 56 Kb/s. Il faudra donc 35 modems au prestataire de service.

2.2 a) La LS doit permettre un débit de 3*512 + 0,6*2*512 + 0,6*12*128 = 3 Mb/s.

b) Avec 3 lignes à 2 Mb/s, le FAI pourra connecter 3*2 000/0,6/128 = 78 prestataires à 128 Kb/s.

2.3 a) Le débit moyen par connexion est de 20*60/60 = 20 Ko/s, soit 160 Kb/s. Le nombre de clients Netissimo 1 pouvant être connectés sera 500/160 = 3 clients.

b) Chaque lien 2 Mb/s peut supporter 3 clients Netissimo 1. Pour 10 clients il faudra donc 4 liens.

c) Pour 4 liens à 2 Mb/s, il faut compter annuellement : 25 % des frais de raccordement + l'abonnement annuel aux liens + l'abonnement annuel au débit souscrit de 8 Mb/s, soit un coût annuel de 2,4 M€/an.

d) Pour des abonnements à 25 €/mois il faudra 8 000 clients pour amortir ce coût.

2.4 a) Pour un modem à 56 Kb/s, le Ko/s sur le RTC coûte 2,14 €/mois, sur le câble 0,61 €/mois et 1,87 €/mois sur l'ADSL.

b) Le câble est plus économique, mais le débit n'est pas garanti. Il s'agit donc d'un coût minimum. Sur le RTC, il faudra au moins 25 heures pour transférer les 600 Mo de données. Il faudra donc ajouter le coût des 5 heures de communication supplémentaire au coût de l'abonnement. Ce mode de transmission est peu adapté à un tel volume de transfert.

CHAPITRE 3

QCM

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
c)	*c)*	*d)*	*b)*	*c)*	*c)*	*a) ; d)*	*a) ; b)*	*a)*
Q10	**Q11**	**Q12**	**Q13**	**Q14**	**Q15**	**Q16**	**Q17**	**Q18**
b) ; c)	*a)*	*b)*	*b)*	*a)*	*b)*	*d)*	*a) ; b) ; c)*	*d)*
Q19	**Q20**	**Q21**	**Q22**	**Q23**	**Q24**	**Q25**	**Q26**	**Q27**
a) ; b)	*a) ; c)*	*b) ; c)*	*b) ; d)*	*c)*	*b)*	*b)*	*e)*	*a)*
Q28	**Q29**							
c)	*d)*							

Exercices

3.1 La classe C autorise 2 097 150 réseaux ((223 – 191)*256*256 – 2), auxquels il faut enlever les adresses de la plage 192.168.0.0 à 192.168.255.0, soit 256 réseaux de 254 machines correspondant à des adresses privées. La classe C peut donc offrir 2 032 126 adresses de réseaux routables sur Internet.

3.2 Le nombre d'adresses se situe entre 256 et 512. Une classe C n'est pas suffisante. Il faut attribuer une adresse de classe B, en utilisant que le bit de poids faible du second octet pour l'adressage sur le réseau local. L'adresse de réseau (et donc le masque de réseau) utilisera 8 + 8 + 7 = 23 bits. L'adresse affectée à l'entreprise pourra avoir la forme suivante : 191.55.24/23 et le masque de réseau sera 255.255.254.0.

3.3 a) L'entreprise a besoin de 34 adresses, ce qui nécessite 6 bits d'adressage Elle se verra attribuer une sous-classe de la classe C telle que 192.55.55.0/26.

b) Les 110 postes clients peuvent être adressés sur la plage d'adresses privées 10.0.10.20 à 10.0.10.129. La plage d'adresses publiques utilisée peut être 192.55.55.1 à 192.55.55.34.

3.4 Tableau de routage du routeur R1 :

Réseau client	Routeur voisin	Distance
A	R3	2
B	R3	2
C	=	1
Internet A	R4	5
Internet B	R3	3
Internet C	R6	2

3.5 a) Modifications de la table de routage de R3 :

Réseau client	Routeur voisin	Distance
B	R2	4

b) Table de routage du routeur R2 :

Réseau client	Routeur voisin	Distance
A	R3	4
B	=	1
C	R1	6
Internet A	R4	2
Internet B	R3	5
Internet C	R3	7

3.6 Les chemins possibles et leur coût sont : R1-R3-R5 = 4 ; R1-R2-R3-R5 = 11 ; R1-R4-R2-R3-R5 = 11 ; R1-R6-R3-R5 = 7. Le chemin le plus court est donc R1-R3-R5.

3.7 a) Les chemins possibles sont : R1-R2-R3-R5 = 11 ; R1-R4-R2-R3-R5 = 11 ; R1-R6-R3-R5 = 7. Le chemin le plus court est donc R1-R6-R3-R5.

b) Il faut augmenter le coût de la liaison R1-R6 à une valeur supérieure à 5.

3.8 a) Les chemins possibles entre les réseaux A et B sont :

R3-R5-R4-R1-R2 = 42 ; R3-R5-R6-R7-R1-R2 = 52 ; R3-R5-R4-R7-R1-R2 = 52 ; R3-R5-R6-R7-R4-R1-R2 = 62. Le plus court chemin est R3-R5-R4-R1-R2.

b) La valeur du chemin R4-R5 doit être supérieure à 20. Le chemin R3-R5-R6-R7-R1-R2 devient le plus court.

3.9 a) La somme des débits moyens et des débits crêtes sur le lien R1-R2 est de 8 Mb/s. La demande de connexion ferait passer le débit total à plus de 10 Mb/s. La liaison n'est donc pas possible.

b) La somme des débits sur le lien R1-R4 est de 9 Mb/s. Il ne pourra accepter la connexion demandée. Par contre, le lien R1-R7 dispose de 6 Mb/s de bande passante libre. Les liens R7-R6 ; R6-R5 et R5-R3 disposent respectivement de 43,4 Mb/s ; 42,1 Mb/s et 4,9 Mb/s de bande passante libre. Ce chemin est donc possible pour la liaison entre le poste du réseau B et le serveur vidéo du réseau A.

CHAPITRE 4

QCM

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
b)	*c)*	*c)*	*d)*	*a)*	*b)*	*d)*	*a)*	*a)*
Q10	**Q11**	**Q12**	**Q13**	**Q14**	**Q15**	**Q16**	**Q17**	**Q18**
c)	*b)*	*a)*	*c)*	*c)*	*a)*	*b)*	*a)*	*c)*
Q19	**Q20**	**Q21**	**Q22**					
c)	*a)*	*a)*	*c) ; d); f)*					

Exercices

4.1 Chemin emprunté par le message :

Client émetteur : Jean-Luc Blanc ; serveur d'émission : vega.masson.fr ; serveur de destination : univ-mlv.fr ; BAL du destinataire : present.

4.2 a) Adresse de la liste : profs-*src@univ-nlt.fr* ; adresse du serveur de liste : univ-tln.fr

b) Chemin suivi par le message entre l'émetteur et le serveur de liste :

Client émetteur : présent ; serveur d'émission : univ-mlv.fr ; serveur de destination : mail.univ-nlt.fr BAL de destination : profs-src

Chemin suivi par le message entre le serveur de liste et le destinataire :

Serveur émetteur : mail.univ-nlt.fr ; serveur de destination : univ-mlv.fr ; BAL du destinataire : present

4.3 a) Une passerelle de messagerie pourra être placée entre le serveur de messagerie mail.iut.fr et Internet. Le serveur de messagerie étudiant mail2.iut.fr sera connecté à la passerelle.

b) Les étudiants pourront garder leur adresse. La distribution sera assurée par la passerelle. Celle-ci fera la transposition entre l'adresse initiale « *etudiant »@mail.iut.fr* » et l'adresse de la BAL de cet étudiant à « etudiant »@mail2.iut.fr

4.4 a) Si la liste est ouverte, il faudra envoyer les deux messages suivants :

Destinataire *sympa@iut.univ-mlv.fr* Objet : SUSCRIBE administratifs.src maud aile

Destinataire *sympa@iut.univ-mlv.fr* Objet : SIGNOFF administratifs.src jean tasse

Si la liste est fermée, le propriétaire de la liste enverra les deux messages suivants :

Destinataire *sympa@iut.univ-mlv.fr* Objet : ADD administratifs.src maud aile

Destinataire *sympa@iut.univ-mlv.fr* Objet : DEL administratifs.src jean tasse

b) Pour vérifier que les modifications ont bien été faites, il faut demander la liste des abonnés de la liste par le message :

Destinataire *sympa@iut.univ-mlv.fr* Objet : REVIEW administratifs.src

4.5 Le répertoire de base (home directory) est le répertoire public ftp /pub. L'URL d'accès au fichier sera donc : *ftp://univ-mlv.fr/maitrise/newprog.c*

4.6 Sur un serveur FTP, la connexion anonyme permet de rendre accessible à tout le monde des fichiers en téléchargement. Cette solution est largement utilisée par les professionnels qui veulent mettre à disposition de leurs clients des mises à jour des logiciels qu'ils commercialisent. L'inconvénient est qu'il n'est pas possible de vérifier de façon fiable les clients qui se sont connectés. La connexion non-anonyme permet de limiter l'accès à certains fichiers à une liste de personnes autorisées. Une application courante est faite par les professionnels qui ne veulent permettre l'accès de leurs fichiers qu'à certains clients tels que leurs revendeurs ou des développeurs particuliers. Sur un site web, les pages sont accessibles à tout le monde par défaut. Il est pourtant possible de rendre certaines pages accessibles après identification par un compte et un mot de passe (voir chapitre 5, *Les serveurs HTTP : configuration et sécurisation*).

4.7 Sur un poste client, la messagerie n'a besoin de se connecter qu'au serveur de messagerie. Il faudra également qu'il puisse se connecter au serveur de comptes. Les règles à éditer dans le pare-feu personnel seront :

Protocole	Adresse source	Adresse dest.	Port	Règle
SMTP	locale	195.50.50.2	25	autorisé
SMTP	195.50.50.2	locale	>1024	autorisé
POP3	locale	195.50.50.2	110	autorisé
POP3	195.50.50.2	locale	>1024	autorisé
ICMP	10.50.0.2	locale		autorisé
ICMP	locale	10.50.0.2		autorisé
tous	toutes	toutes	tous	interdit

L'explorateur Windows doit dialoguer avec les postes et serveurs du réseau local uniquement. Il utilise le protocole UDP. Les règles de filtrage à insérer dans le tableau précédent juste avant la dernière règle seront :

Protocole	Adresse source	Adresse dest.	Port	Règle
UDP	locale	10.50.0.0/120	>1024	autorisé
UDP	10.50.0.0/120	locale	>1024	autorisé

CHAPITRE 5

QCM

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
a) ; b) ; e) ; f)	*a) ; c)*	*d)*	*d) e)*	*c)*	*a) ; b)*	*a)*	*a)*	*d)*
Q10	**Q11**	**Q12**	**Q13**	**Q14**	**Q15**	**Q16**	**Q17**	
e)	*c)*	*a) ; c)*	*a) ; c)*	*d)*	*b)*	*d)*	*a)*	

Exercices

5.1 a) A et B autorisent les connexions SMTP entrantes (courrier entrant, serveur interne) ; C et D autorisent les connexions SMTP sortantes (courrier sortant, serveur externe) ; E s'applique dans tous les autres cas et interdit tous les paquets non autorisés.

b) Oui, les paquets ① sont autorisés par la règle A ; les paquets ②, sont autorisés par la règle B.

Connexion	Direction	@ source	@dest.	Protocole	Port dest.	Règle
1	Entrant	212.168.3.4	197.36.1.1	TCP	25	A
2	Sortant	197.36.1.1	212.168.3.4	TCP	1234	B

c) Il faut rajouter un colonne pour prendre en compte le test du bit ACK des segments TCP (voir paragraphe 3.4.2). Les paquets entrants ne seront acceptés qu'avec un bit ACK à 1, donc pour une connexion TCP initiée de l'intérieur (voir figure 3.10).

5.2 L'ajout d'un serveur Intranet nécessite l'ajout des règles suivantes :

source	destination	service	action	track	install	On
any	mailsrv	smtp	accept	short	log	Gateways
localnet	any	any	accept	short	log	Gateways
localnet	localnet	http	accept	short	log	
any	localnet	http	deny	short	log	gateways
any	any	any	reject	long	log	gateways

5.3 a) Vous devez créer le répertoire qui servira de répertoire de base. Ce répertoire recevra le fichier constituant la page d'accueil de votre serveur.

b) Il vous faut :
- définir un nom pour le serveur ;
- relever l'adresse IP de votre poste.

Annexe

Protocoles et couches OSI

SIGLES UTILISÉS

AAL	ATM Adaptation Layer
ARP	Address Resolution Protocol
ATM	Asynchronous Transfert Mode
CHAP	Challenge Handshake Protocol
BGP	Border Gateway Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EGP	External Gateway Protocol
FTP	File Transfert Protocol
HDLC	High Level Data Link Control
HTTP	Hyper Text Transfert Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPX	Internet Packet eXchange
ISDN	Integrated Services Digital Network
LAPB	Link Acces Protocol Balanced
LAPD	Link Acces Protocol on D Channel
LPP	Lightweight Presentation Protocol
NCP	Netware Core Protocol
NDS	Netware Directory Services
NFS	Network File System

NLSP	Netware Link Services Protocol
NNTP	Network News Transfert Protocol
OSPF	Open Shortest Path First Protocol
PAD	Packet Assembly Disassembly
PAP	Password Autentification Protocol
PPP	Point to Point Protocol
RARP	Reverse ARP
RIP	Routing Information Protocol
RNIS	Réseau Numérique à Intégration de Services
SAP	Service Advertising Protocol
SDH	Synchronous Digital Herarchy
SLIP	Serial Line IP
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNAP	Sub Network Access Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPX	Sequenced Packet eXchange
STP	Shielded Twisted Pair
TAXI	Tranparent Asynchronous eXchange Protocol
TCP	Transmission Control Protocol
TELNET	Telnet Terminal virtuel
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
XDR	eXternal Data Representation

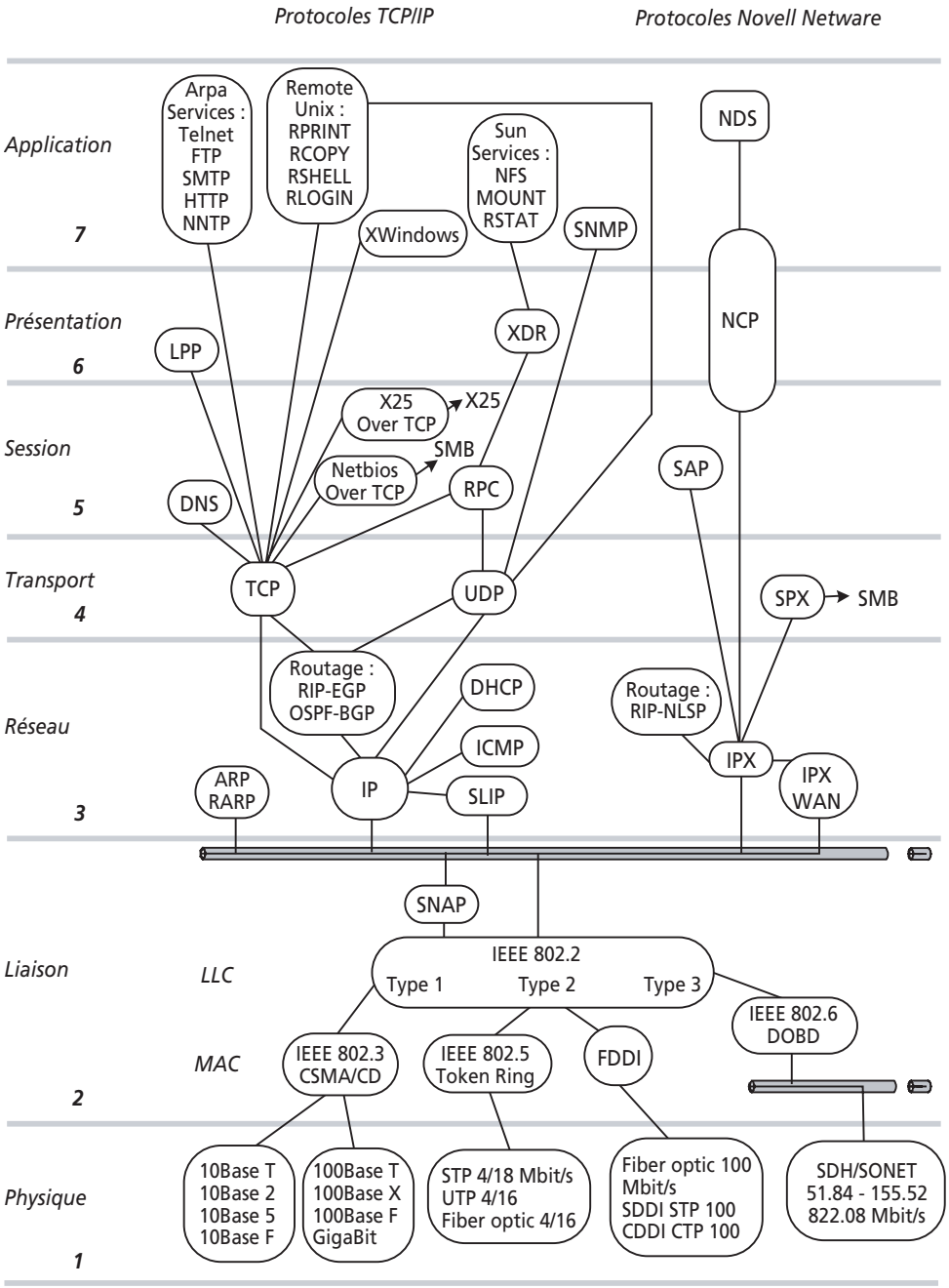
Protocoles TCP/IP
Protocoles Novell Netware
Application
7
Présentation
6
Session
5
Transport
4
Réseau
3
Liaison
LLC
MAC
2
Physique
1
Arpa Services : Telnet FTP SMTP HTTP NNTP
Remote Unix : RPRINT RCOPY RSHELL RLOGIN
XWindows
Sun Services : NFS MOUNT RSTAT
SNMP
NDS
NCP
XDR
LPP
X25 Over TCP
X25
SMB
Netbios Over TCP
RPC
SAP
DNS
TCP
UDP
SPX
SMB
Routage : RIP-EGP OSPF-BGP
DHCP
ICMP
Routage : RIP-NLSP
IPX
IPX WAN
ARP RARP
IP
SLIP
SNAP
IEEE 802.2
Type 1
Type 2
Type 3
IEEE 802.6 DOBD
IEEE 802.3 CSMA/CD
IEEE 802.5 Token Ring
FDDI
10Base T 10Base 2 10Base 5 10Base F
100Base T 100Base X 100Base F GigaBit
STP 4/18 Mbit/s UTP 4/16 Fiber optic 4/16
Fiber optic 100 Mbit/s SDDI STP 100 CDDI CTP 100
SDH/SONET 51.84 - 155.52 822.08 Mbit/s

Figure A.1

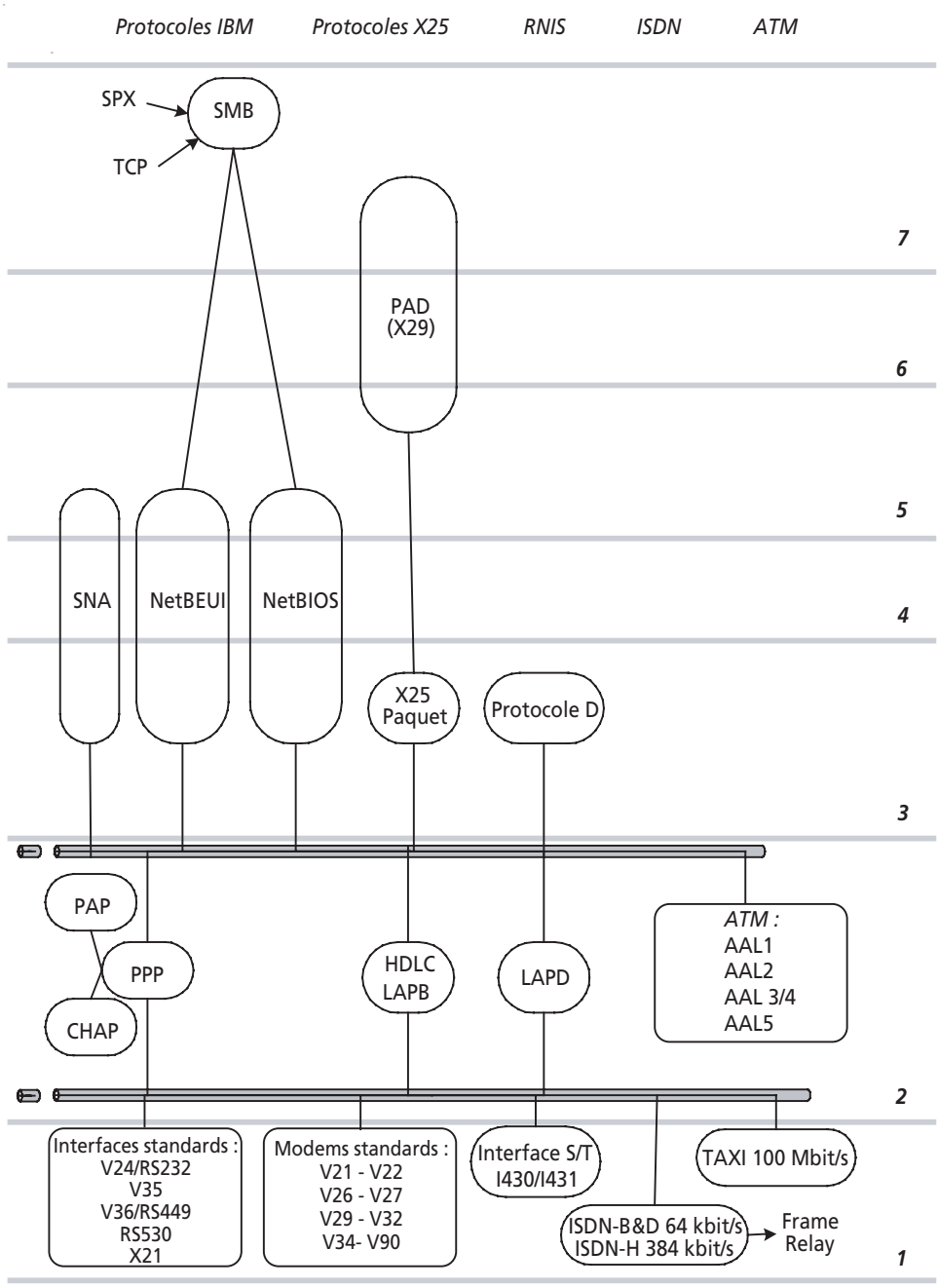
Protocoles IBM
Protocoles X25
RNIS
ISDN
ATM
SPX
TCP
SMB
PAD (X29)
7
6
5
4
3
2
1
SNA
NetBEUI
NetBIOS
X25 Paquet
Protocole D
PAP
PPP
CHAP
HDLC LAPB
LAPD
ATM :
AAL1
AAL2
AAL 3/4
AAL5
Interfaces standards :
V24/RS232
V35
V36/RS449
RS530
X21
Modems standards :
V21 - V22
V26 - V27
V29 - V32
V34- V90
Interface S/T
I430/I431
TAXI 100 Mbit/s
ISDN-B&D 64 kbit/s
ISDN-H 384 kbit/s
Frame Relay

Figure A.2

Bibliographie

CONSTRUCTEURS D'ÉQUIPEMENTS

http://www.cisco.com
http://www.3com.com/
http://www.nortelnetworks.com
http://www.modcomp.com
http://www.olitec.com

PROTOCOLES ET NORMES

http://www.protocols.com
http://www.atmforum.org
http://www.alcatel.com/telecom/mbd/keytech/
http://www.itu.int/ITU-T/index.html
http://hermes.ulaval.ca
http://www.info.univ-angers.fr/pub/pn/reseaux.html
http://dept-info.labri.u-bordeaux.fr
http://www.hsc.fr/ressources/veille/
http://www.x400.org/
http://iut.univ-mlv.fr/etudiants/etudiants.php

OPÉRATEURS DE TÉLÉCOMMUNICATION

http://www.globaltt.com/fr/faraway.html
http://www.entreprises.francetelecom.com/

http://www.netstorming.fr/
http://www.cegetel-entreprises.fr/
http://www.cegetel.fr/
http://www.nortelnetworks.com/index.html
http://www.teleglobe.com
http://www.transfix.fr/frame/telecom/telecommunication.htm

PRESTATAIRES, OPÉRATEURS INTERNET

http://www.aic.fr/
http://www.uunet.com
http://www.eunet.com
http://www.oleane.fr
http://www.mediareseaux.com/

Index