Appui au Développement de l'infrastructure globale de l'information en Afrique

Guide de gestion et développement des connexions et interconnexions des réseaux aux nœuds nationaux d'Internet

Préparé par Désiré Karyabwite,
Consultant en gestion de nœud Internet
Genève, juin 2000

BUREAU DE DÉVELOPPEMENT DES TÉLÉCOMMUNICATIONS
Union internationale des télécommunications
UIT

TABLE DES MATIÈRES

1 Introduction

La progression des machines interconnectées en réseau local est considérable. On l'estime à plus de 50% en 1998 et à près de 80% pour l'an 2000 alors qu'en 1991 il y en avait moins de 10% et 40% en 1993. Internet, ensemble de réseaux locaux, se développe si vite que les pays en développement ont du mal à suivre pour pouvoir bénéficier pleinement de cette avancée technologique. Il y a donc un risque de déséquilibre toujours grandissant entre pays industrialisés et pays en développement en matière d'accès à l'information.

Une des missions officielles de l'Union internationale des télécommunications (UIT) est de veiller à ce que le développement des télécommunications profite à toute l'humanité. C'est ainsi que la coopération technique du Bureau de développement des télécommunications de l'UIT (l'UIT/BDT) avec les pays Membres s'appuie principalement sur les technologies de pointe qui facilitent le développement des télécommunications à des coûts relativement intéressants.

Dans un contexte où le secteur des télécommunications connaît une véritable mutation compte tenu de la convergence des technologies des télécommunications, de l'informatique et de l'audiovisuel, le but de ce guide est de faciliter le repérage dans le domaine des réseaux de communication basés sur Internet, une technologie innovante. L'objectif est d'apporter une assistance technique aux opérateurs des télécommunications pour développer leur infrastructure globale de l'information (GII). C'est un domaine tellement complexe qu'il est impossible d'être exhaustif et ce guide n'a pas la prétention de l'être. Cependant, il essaye de proposer une base de travail, un fil conducteur aux ingénieurs chargés de la planification et du développement des réseaux de communications en Afrique.

Le deuxième chapitre présente l'architecture des réseaux ainsi que la transmission des données sur TCP/IP, standard de fait sur le réseau Internet. Le troisième chapitre traite de la planification d'un nœud national d'Internet, les connexions et interconnexions sur Internet. Le quatrième chapitre concerne la gestion, la métrologie et la qualité de service sur Internet. Le cinquième chapitre présente les éléments de planification du développement du réseau Internet par des technologies de pointe pouvant servir à la connexion des ISP (Internet Service Providers) ou d'autres consommateurs. Le sixième chapitre concerne les aspects réglementaires et juridiques relatifs à l'utilisation des technologies de pointe sur Internet. Le septième chapitre propose un plan de formation pour le renforcement des capacités locales nécessaires à un véritable développement d'Internet et sa prise en charge par les responsables locaux. Le chapitre huit conclut ce guide. A titre d'information, un budget prévisionnel pour un projet de montage d'un nœud national Internet ainsi qu'un cahier des charges pouvant servir de base aux opérateurs télécom en Afrique qui veulent se lancer comme opérateur Internet national, sont annexés à ce guide.

2 Architectures des réseaux et transmission des données

2.1 Généralités

Il y a quelques années, l'interconnexion des réseaux locaux se limitait à quelques dizaines de mètres. Avec le développement d'Internet, les réseaux locaux, par l'intermédiaire de passerelles, permettent aux utilisateurs de communiquer avec les réseaux étendus, le réseau téléphonique commuté (RTC) et bien d'autres. Les informations transmises sont de diverses natures, parmi lesquelles des données informatiques, mais aussi du son ou des images. Pour arriver a faire l'interconnexion des différents réseaux, l'usage du protocole IP (Internet Protocol) est obligatoire dans les nœuds qui vont faire le routage des données entre les réseaux. Ainsi, Internet est un réseau à commutation de paquets.

On désigne par «hôtes» les machines terminales, reliées par le réseau, qui sont soit à l'origine, soit destinataires des données transmises, et qui les traitent. Chaque hôte est caractérisé par son adresse sur le réseau.

Le «débit» est la quantité d'informations élémentaires que le réseau peut acheminer pendant une unité de temps. Il est exprimé en bit par seconde ainsi qu'en multiple de cette unité [kbit/s] pour kilobit par seconde, [Mbit/s] pour mégabit par seconde, et [Gbit/s] pour gigabit par seconde.

Les réseaux locaux sont fréquemment appelés «sous-réseaux» pour éviter la confusion avec la couche 3 du modèle OSI. Généralement les réseaux sont classés en fonction de leur étendue, à savoir:

- Les LAN (*Local Area Network*) sont limités à la surface d'un immeuble et ont des débits pouvant atteindre 100 Mbit/s (réseau local). La technologie Gigabit Ethernet (1000 Mbit/s) est la tendance stratégique pour les LAN et les Intranets.
- Les MAN (*Metropolitan Area Network*) sont aux dimensions d'une ville et ont des débits de l'ordre de 2 Mbit/s à 155 Mbit/s (réseau métropolitain).
- Les WAN (*Wide Area Network*) sont de taille nationale ou internationale (réseau étendu). Les systèmes numériques modernes qui constituent l'épine dorsale d'Internet (backbone Internet) ont des débits de 34 Mbit/s, 140 Mbit/s voire 565 Mbit/s ou des multiples de ces débits.

2.2 Le modèle de référence OSI et le protocole TCP/IP

2.2.1 Normalisation

Internet est un monde de systèmes hétérogènes et pour permettre la communication entre systèmes émanant de constructeurs différents, l'ISO (*International Organization for Standardization*), qui regroupe les instances de normalisation, a défini une norme appelée OSI (*Open System Interconnection*) «interconnexion des systèmes ouverts». Cette norme est décomposée en 7 sous-ensembles fonctionnels appelés «couches»:

1 La *couche Physique*: elle est en charge de la transmission de suites de bits au niveau physique d'interconnexion.

2 La *couche Liaison de données* est responsable du contrôle d'erreur, en appliquant le principe «accusé de réception».

3 La *couche Réseau* prend en charge le routage, le contrôle de flux pour éviter des pertes d'unités de données par engorgement de la voie de transmission ainsi que la compatibilité des réseaux à interconnecter si nécessaire.

4 La *couche Transport* est responsable de l'acheminement des informations de bout en bout via le réseau (entre expéditeur et destinataire).

5 La *couche Session* est responsable de la mise en place et du contrôle du dialogue entre les tâches distantes. Elle active et synchronise certains événements, par exemple la duplication d'une base de données en plusieurs points d'un réseau.

6 La *couche Présentation* est responsable de la représentation des données échangées par les applications sur les réseaux interconnectés. Elle traite les problèmes courants d'hétérogénéité, de représentation des données:

   - C'est le cas de certains processus qui codent les nombres entiers en stockant l'octet de poids fort avant l'octet de poids faible (*big-endian*), tandis que d'autres font l'inverse (*little-endian*).
   - C'est le cas de certaines machines qui représentent les caractères sous forme de codes ASCII, d'autres grâce au code EBCDIC.
   - C'est le cas des plates-formes qui ne respectent pas la norme de l'IEEE (*Institute of Electrical and Electronic Engineers*) pour représenter les nombres flottants.

7 La *couche Application :* cette dernière couche a pour fonction de fournir des services aux utilisateurs d'un réseau. C'est à ce niveau qu'on rencontre les programmes de transfert de fichiers, d'émulation de terminal, d'échange de courrier électronique, etc. Les programmes mis en œuvre doivent garantir la sécurité et la confidentialité des échanges de données et garantir l'intégrité des informations et leur sauvegarde en cas d'incident.

Les différentes couches de l'hôte destinataire réalisent un travail symétrique aux couches correspondantes de l'hôte expéditeur. En effet au passage de chaque couche, de la couche 7 (couche Application) à la couche 1 (couche Physique), des informations sont rajoutées (encapsulation) et des unités de données sont découpées (fragmentation). Côté destinataire, quand on repasse de la couche 1 (couche Physique) vers la couche 7 (couche Application), le traitement inverse est effectué.

2.2.2 Protocole TCP/IP standard de fait

2.2.2.1 Présentation

TCP/IP est une famille d'une vingtaine de protocoles (et autant de commandes), dont font partie les protocoles TCP (*Transmission Protocol*) et IP (*Internet Protocol*). En réseau local, moins d'une dizaine d'entre eux sont utilisés. TCP/IP se positionne comme un protocole d'interconnexion de réseaux hétérogènes. A ce titre, il est totalement indépendant des couches basses (*Ethernet, Token Ring, X25*). Il recouvre les couches 3 à 7 du modèle OSI, sans qu'il puisse y avoir de corrélation précise entre les couches de TCP/IP et celles d'OSI sachant que TCP/IP est bien antérieur au modèle OSI.

TCP/IP est aussi bien utilisé sur de petits réseaux locaux qu'à travers les liaisons internationales. C'est le protocole sur lequel s'appuie INTERNET, interconnexion de réseaux locaux TCP/IP à travers le monde entier.

2.2.2.2 Mode de fonctionnement du protocole IP

La couche IP (*Internet Protocol*) a pour but d'acheminer un paquet de données entre une station source et une station destinataire qui peut être située sur le même segment de réseau ou sur des réseaux différents reliés par une ou plusieurs passerelles.

Chaque paquet est une entité qui est absolument indépendante de toutes les autres. IP n'offre qu'un service de type remise de datagrammes, c'est-à-dire d'unités de données en mode non-connecté. Il ne s'occupe pas du contrôle de flux de données.

Les données constituant le paquet à émettre sont fournies par la couche Transport. Deux cas peuvent alors se produire:

- si la station destinataire se trouve sur le même réseau que la station émettrice, le paquet est envoyé directement vers la station destinataire;
- si la station destinataire se trouve sur un autre réseau, IP envoie le paquet vers une passerelle. Cette passerelle se charge d'acheminer le paquet vers la station destinataire, ou vers un sous-réseau, jusqu'à l'acheminement final du paquet. Cette notion d'acheminement d'un paquet au travers des passerelles dans une architecture de réseaux interconnectés est à la base de la formation des adresses Internet. IP procure aux couches de niveau supérieur trois services importants, à savoir:
  - l'acheminement de l'unité de données;
  - la gestion des requêtes de service;
  - le rapport des erreurs de transmission.

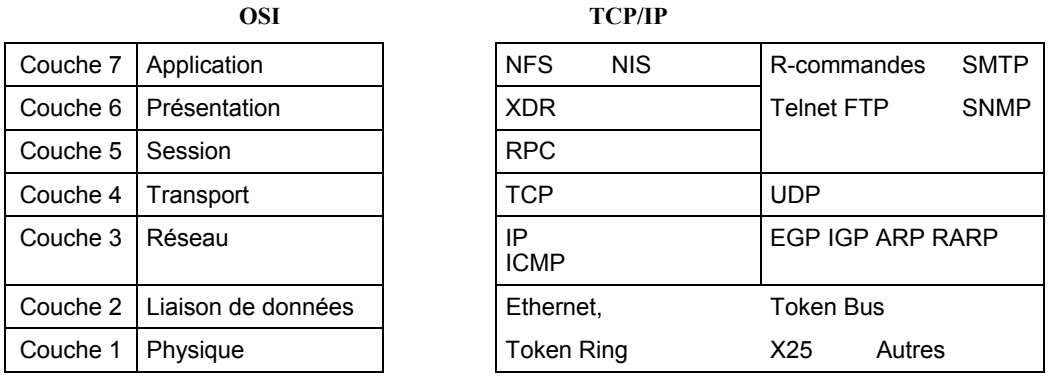

Fig. 2.1 Parallélisme entre le modèle OSI et TCP/IP (Source: Réseaux TCP/IP – Editions WAN & LASER)

2.2.2.3 La formation d'adresses IP

Les adresses IP (dites aussi adresses Internet) ont une longueur fixe de 32 bits, soit 4 octets (1 octet = 8 bits). Ce sont des adresses logiques, à distinguer des adresses physiques (des cartes Ethernet ou Token Ring, par exemple). Elles se composent de deux parties: l'adresse du réseau, et l'adresse de l'hôte sur ce réseau. Une adresse IP doit être unique au monde, c'est pourquoi seul le NIC (*Network Information Center*) attribue les adresses de réseau et la partie «adresse de l'hôte» est laissée à l'appréciation de l'administrateur.

On a l'habitude d'écrire les adresses IP octet par octet, chacun d'entre eux étant séparé du précédent par un point, exemple:156.106.194.24. Il existe principalement trois classes d'adresses Internet:

- *la classe A:* est caractérisée par une adresse réseau sur 8 bits dont le premier bit est à 0. Les adresses de classe A sont du type RRR.HHH.HHH.HHH, où RRR désigne un octet de l'adresse du réseau, et HHH un octet de l'adresse de l'hôte. La partie RRR est comprise entre 1 et 127. Un sous-réseau de classe A n'a que le premier des quatre nombres fixés, c'est-à-dire que toutes les machines de ce sous-réseau auront une adresse qui commence par le même nombre (compris entre 1 et 254). Un sous-réseau de classe A peut donc contenir 254^3 machines;
- *la classe B:* est caractérisée par une adresse réseau sur 16 bits, dont les deux premiers sont 10. Les adresses de classe B sont du type RRR.RRR.HHH.HHH. Leur premier octet est compris entre 128 et 191 inclus. Un sous-réseau de classe B a les deux premiers nombres fixés et peut donc contenir 254^2 machines;
- *la classe C:* est caractérisée par une adresse réseau sur 24 bits dont les trois premiers bits sont à 110. Les adresses de classe C sont du type RRR.RRR.RRR.HHH. Leur premier octet est compris entre 192 et 223. Un sous-réseau de classe C a les trois premiers nombres fixés et peut donc contenir 254 machines.

Pour les 3 classes d'adresses, il est impossible d'avoir tous les bits à 0 ou tous les bits à 1. On distingue en plus:

- les adresses de *classe D*, utilisées par les mécanismes de multicast, c'est-à-dire d'envoi de message à un groupe de machines utilisant un protocole commun (par opposition au *broadcast* qui désigne l'envoi de messages à un groupe de machines utilisant un même réseau);
- les adresses de *classe E,* réservées pour de futures extensions d'IP.

Notons que les adresses 0.0.0.0 et 255.255.255.255 ont une signification particulière. Elles ne peuvent donc pas être attribuées à un hôte. L'adresse 0.0.0.0 est émise par une machine qui ne connaît pas sa propre adresse IP. Certaines versions obsolètes se servent de cette adresse de destination pour émettre en diffusion générale. Une adresse dont tous les bits de la partie hôte sont à 1 correspond à une diffusion générale (*broodcast*) sur le réseau désigné.

NOTE – Deux stations situées sur le même sous-réseau (c'est-à-dire entre lesquelles aucune passerelle n'est intercalée), porteront des adresses IP dont les parties réseau (1, 2 ou 3 premiers octets) seront identiques.

Noter qu'il est possible de découper un réseau disposant d'une seule adresse de classe A, B ou C en différents sous-réseaux interconnectés par des routeurs. Le principe d'adressage de telles configurations est à voir de cas en cas, suivant l'attribution d'adresses IP par pays et l'organisation du NIC (*Network Information Center*). Sur un PC (Windows 95 ou 98), il est très facile de vérifier l'attribution d'une adresse IP: cliquer sur «démarrer», puis «exécuter». Dans la fenêtre qui apparaît, taper «WINIPCFG» comme c'est indiqué sur la Figure 2.2. L'adresse IP de l'hôte apparaît ainsi que l'adresse de la carte, le masque de sous-réseau et l'adresse de la passerelle par défaut (voir Figure 2.2).

2.2.2.4 DNS sur Internet

Pour les ordinateurs qui se connectent momentanément sur Internet via un modem, le fournisseur d'accès leur attribue une adresse «temporaire» qui n'est valable que durant la période de connexion. D'autres ordinateurs sont connectés en permanence sur Internet et ont des adresses IP fixes. Il n'est donc pas facile de s'y retrouver. C'est pourquoi un système de noms symboliques est utilisé pour faciliter la lecture et la mémorisation par des êtres humains. Un mécanisme basé sur l'utilisation de serveurs de noms (*Domain Name Server* – DNS) hiérarchisés, permet de retrouver l'adresse numérique d'une machine à partir de son nom symbolique.

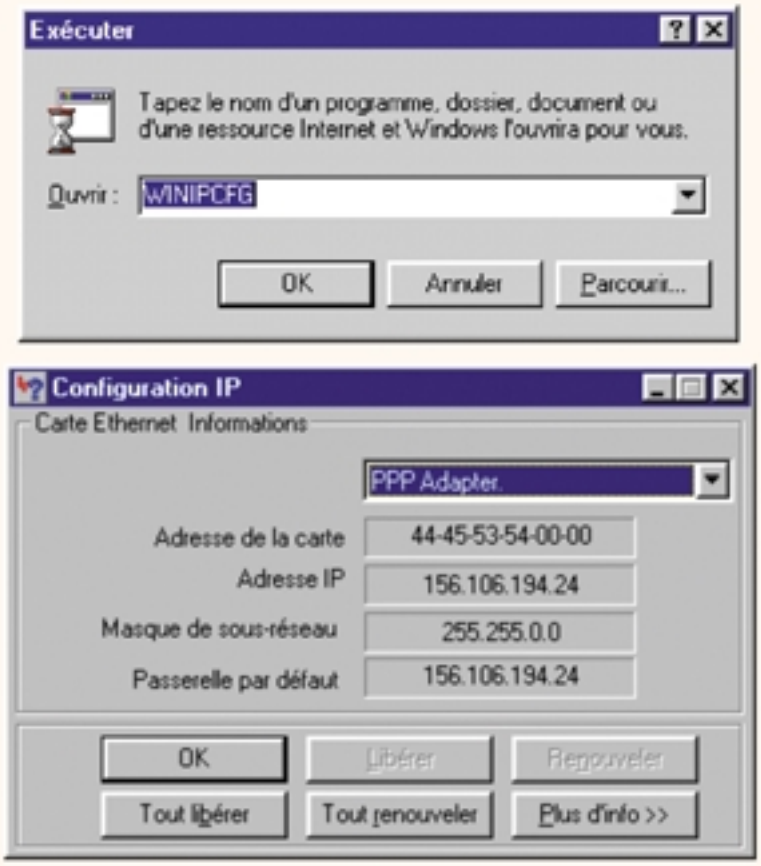

Fig. 2.2 Vérification de l'adresse IP d'un hôte sur un réseau (hôte de l'UIT)

Internet a été subdivisé en domaines (appelés *Top Level Domains*), eux-mêmes subdivisés en sous-domaines qui, à leur tour, peuvent être subdivisés en sous-sous-domaines, et ainsi de suite. Les DNS qui se trouvent au sommet de la hiérarchie (niveau 1) ne connaissent que les DNS de niveau immédiatement inférieur (niveau 2), correspondant à chaque domaine.

Les DNS du deuxième niveau ne connaissent que les DNS racine (niveau 1) et les DNS de niveau 3 se trouvant dans leur domaine (sous-domaines). Ainsi de suite. Le nombre de niveaux peut varier d'un domaine à l'autre. Le nom Internet d'une machine indiquera la succession des noms de sous –...– sous-domaines par lesquels il faut passer, en partant du niveau où la machine est enregistrée et en remontant jusqu'à arriver à un TLD (*Top Level Domain*). Il y a deux catégories de TLD, les TLD nationaux et les TLD génériques.

Principaux domaines (TLD):

- *com:* réseau commercial
- *org:* organisations à but non lucratif
- *gov:* organisations gouvernementales aux Etats-Unis
- *mil:* organisations militaires aux Etats-Unis
- *edu:* organisations éducatives aux Etats-Unis
- *net:* organisations qui ont un très large réseau
- *ml:* Mali
- *rw:* Rwanda, *etc.*

Dès février 1997, quelques nouveaux domaines ont été proposés, il s'agit de:

- *firm:* entreprises et firmes
- *store:* entreprises offrant des marchandises à acheter
- *web:* entités dont les activités sont principalement liées au Web
- *arts:* entités dont les activités sont liées à la culture et aux divertissements
- *rec:* entités dont les activités sont principalement liées aux divertissements
- *info:* entités fournissant des services d'information
- *nom:* nomenclature individuelle ou personnelle

Les TLD sont gérés par un organisme appelé Internet Assigned Number Authority (IANA). IANA est le coordinateur central pour l'attribution de valeurs uniques pour des paramètres tels que adresses Internet, noms de domaines, numéros de protocoles et numéros de ports, pour l'ensemble des protocoles Internet. La gestion d'adresses Internet au sein d'un sous-réseau est décentralisée. Les DNS gèrent des bases de données séparées pour les adresses de courrier électronique et pour les adresses de machines.

Pour accélérer le temps de réponse lors d'une requête, les serveurs DNS tiennent généralement à jour un «cache» contenant les adresses récemment demandées, de façon à ne pas avoir à repasser trop souvent par la hiérarchie de DNS pour trouver à nouveau des adresses souvent demandées. Le grand problème avec ce mécanisme est que si une adresse ne peut pas être trouvée pour une raison quelconque, cette information «négative» est elle aussi stockée dans le cache, même s'il ne s'agissait que d'un problème temporaire. On peut donc se trouver dans l'impossibilité de se connecter à une machine, bien que celle-ci soit à nouveau opérationnelle, car entre-temps, la machine a gardé en mémoire qu'elle n'est pas accessible.

Les DNS fonctionnent dans les deux sens: adresse numérique-adresse symbolique correspondante et vice versa. Par le principe d'alias, il est possible d'avoir plusieurs noms symboliques pour la même adresse numérique.

2.2.2.5 Les protocoles ARP et RARP

Les adresses physiques des hôtes sont stockées en PROM sur les cartes d'interface avec le réseau, tandis que les adresses logiques sont stockées dans des fichiers sur disque. A l'intérieur d'un même réseau physique (ou sous-réseau), deux machines ne peuvent communiquer que si elles connaissent leurs adresses physiques respectives. Les adresses manipulées par les couches hautes sont des adresses logiques, qui s'affranchissent des considérations sur le type d'architecture du réseau (Ethernet, Token Ring, X25, ...). Il est donc nécessaire d'établir un mécanisme de mise en correspondance de ces adresses physiques et logiques.

Pour illustrer cette problématique, prenons le cas d'un réseau Ethernet: l'adresse Ethernet d'un hôte est stockée sur 6 octets, alors que son adresse Internet est stockée sur 4 octets. Comment convertir une adresse logique sur 32 bits en adresse physique sur 48 bits? La résolution de ce problème est confiée au protocole ARP (*Address Resolution Protocol*).

Le cas d'une station sans disque est aussi intéressant: elle connaît son adresse physique, mais pas son adresse logique. Pour faire l'acquisition de son adresse logique, elle aura recours au protocole RARP (*Reverse Address Resolution Protocol*). Le problème de l'acquisition de sa propre adresse logique est situé en amont du problème d'acquisition de l'adresse physique d'un hôte distant. En effet, comment cette station sans disque peut-elle répondre à une demande ARP si elle ne connaît pas son adresse logique? Elle serait incapable de reconnaître que le message ARP lui est adressé. C'est pourquoi elle doit émettre un message RARP dès sa mise sous tension, avant même de charger (via le réseau) son système d'exploitation, ou ses applicatifs.

ARP et RARP sont déclenchés automatiquement par IP, et cela de manière totalement transparente, tant pour le programmeur que pour l'utilisateur.

2.2.2.5.1 Fonctionnement du protocole ARP

Un hôte A veut émettre un message à l'attention d'un hôte B. Or A ne connaît que l'adresse logique de B (c'est-à-dire son adresse IP). A émet un message spécifique, contenant:

- sa propre adresse logique;
- son adresse physique;
- l'adresse logique de B.

Ce message est destiné à tous les hôtes de son réseau (*broadcast*). Seul l'hôte B reconnaît son adresse Internet, et le récupère. Il retourne alors à A (dont il connaît les adresses physique et logique) un message contenant son adresse physique. Et à partir de là, les deux machines peuvent commencer à communiquer. La diffusion générale (*broadcast*) étant un mécanisme très coûteux en ressources du réseau, il n'est évidemment pas question, à chaque échange de message, de procéder de la manière décrite précédemment. Chaque hôte gère un cache, contenant une table de mise en correspondance des adresses logiques et des adresses physiques dont il a récemment fait l'acquisition. Avant de diffuser un message général, le protocole s'assure que l'adresse physique qu'il recherche ne se trouve pas dans le cache.

2.2.2.5.2 Fonctionnement du protocole RARP

L'hôte du réseau qui veut faire l'acquisition de son adresse logique émet un message RARP contenant son adresse physique. Ce message est émis à destination de tous les hôtes du réseau local. Un seul hôte du réseau, configuré dans cette optique, reconnaît le message RARP. Ce serveur d'adresses possède une table de mise en correspondance des adresses physiques des stations sans disque, et de leurs adresses logiques. Il retourne donc un message à la station sans disque, contenant son adresse logique.

Afin d'éviter des problèmes de surcharge du serveur d'adresses, le réseau comporte souvent plusieurs serveurs, tous susceptibles de répondre aux messages RARP. Ce protocole n'est utilisé que par les hôtes du réseau qui n'ont pas d'informations sur leur adresse logique, par exemple des stations sans disque.

2.2.2.6 Le protocole ICMP

Le protocole ICMP (*lnternet Control Message Protocol*) permet d'échanger des messages de tests et de contrôle entre deux hôtes. Il autorise la détection d'éventuels problèmes sur le réseau. Les datagrammes ICMP sont encapsulés dans des datagrammes IP. A chaque message du protocole ICMP est associé un type, qui renseigne sur un événement survenu sur le réseau, par exemple:

- «*Destination injoignable*»: une passerelle a reçu un datagramme qu'elle est incapable d'acheminer (ses tables de routage ne lui donnent pas les informations nécessaires). Elle émet alors un message ICMP de ce type vers l'expéditeur du datagramme. C'est également le même principe si la couche IP du destinataire ne peut délivrer son message à la couche supérieure.
- «*Dépassement de temps*»: prévient l'expéditeur d'un datagramme IP de la destruction de ce datagramme, lorsque le champ temps de vie de l'en-tête est à 0.
- «*Problème de paramétrage*»: émis par un hôte qui ne reconnaît pas l'en-tête IP du datagramme qu'il vient de recevoir. Ce message est émis en cas de destruction du datagramme.
- «*Saturation*»: ce message est émis si une passerelle n'a plus la mémoire suffisante pour continuer à recevoir des datagrammes (saturation du réseau).
- «*Echo*»: ce message est émis par un hôte pour tester l'intégrité de la ligne de communication. L'hôte émetteur s'attend à recevoir une réponse de type «réponse d'écho».
- «*Réponse d'écho*»: message émis par un hôte qui reçoit un message d'écho.

2.2.2.7 Nouveau schéma d'adressage IPv6

La réserve d'adresses IP arrive à épuisement et les diverses estimations prévoient une pénurie pouvant survenir entre 2000 et 2010, vu la progression des connexions sur Internet. L'adressage actuel est donc un problème. Les adresses sous IPv4 sont codées sur 4 octets, soit 32 bits. Les adresses sous IPv6 sont

codifiées sur 16 octets, soit 128 bits donc 2^{128} adresses possibles. IPv6 abandonne le découpage des adresses en classes, au profit d'une organisation plus hiérarchisée comportant: trois types d'adresses Unicast, un format Multicast et un nouveau format Anycast.

- *Adresses Unicast:* ce format d'adresse se rapproche de l'adresse IPv4. Il est fondé sur le prestataire: il contient une adresse prestataire, une adresse client chez le prestataire, une indication du réseau chez le client ainsi qu'une adresse interface.
- *Adresses Multicast:* ce type d'adresse permet comme dans IPv4 d'acheminer en une seule fois des paquets vers plusieurs hôtes appartenant à un même groupe.
- *Adresses Anycast:* ce nouveau format autorise l'affectation de la même adresse physique à plusieurs interfaces sur le réseau. Les paquets envoyés à une adresse Anycast sont dirigés vers l'interface physique la plus proche. La notion de proximité est gérée selon un ratio prenant en compte les coûts de transmission et les performances.

La structure de l'en-tête IPv6 est considérablement simplifiée. Elle ne compte que 8 champs et ceci accélère le traitement des paquets. Nous n'entrerons pas en matière mais nous avons tenu à décrire les principes de base. Pour plus d'information, nous recommandons le livre «IPv6 Théorie et pratique» de Gisèle Cizault chez O'REILLY.

2.2.2.8 Sécurité et authentification

Les applications d'Internet telles que le commerce électronique réclament une confidentialité et une sécurité accrue: les numéros de carte de crédit circulent sur le Net, ainsi que les signatures électroniques, mais aussi les ordres de virement dont l'origine et le contenu doivent être sûrs. IPv4 n'offre aucune solution intégrée et l'on devrait recourir à des surcouches logicielles pour y arriver. IPv6 inclut 2 méthodes de sécurisation directement au niveau de la couche Réseau:

- Une première méthode permet d'interdire à un expéditeur d'adresser des paquets à un destinataire s'il n'a pas établi au préalable une connexion en s'identifiant de manière sécurisée. Le fonctionnement de l'algorithme est laissé à l'initiative des développeurs. Cette méthode permet d'éliminer la plus grande partie des attaques.
- Une deuxième méthode permet de déchiffrer l'échange des données hôtes, réalisant ainsi une sorte de «Tunnel IP», empêchant l'interception et la modification des données transmises.

2.2.2.9 Le protocole IPv6 et la qualité multimédia sur Internet

IPv6 va améliorer sensiblement le principe du «Multicast», l'application type vidéoconférence. Ce principe permet d'envoyer des paquets à plusieurs destinataires en une fois. Plutôt que d'envoyer les mêmes données à chaque destinataire, les données sont envoyées une fois et ce sont les routeurs intermédiaires compatibles IPv6 qui les distribuent. Les Figures 2.3 et 2.4 illustrent le principe de fonctionnement.

2.2.2.10 Le protocole TCP

Le protocole TCP (*Transmission Control Protocol*) a été développé pour assurer des communications fiables entre deux hôtes sur un même réseau physique, ou sur des réseaux différents. TCP assure un transport des données en mode connecté, ordonné, bidirectionnel. Il complète le protocole IP. Le protocole TCP est chargé de couper le flux de données transmis par la couche supérieure en segments, qui constituent les unités de données prises en charge par TCP.

Pour éviter la perte éventuelle d'information entre les hôtes, TCP utilise un mécanisme qui consiste, pour une station désireuse d'envoyer un paquet vers une autre, à l'envoyer à intervalles réguliers jusqu'au moment où elle reçoit un acquittement positif. TCP utilise un numéro de séquence pour identifier chaque segment afin d'éviter les duplications. Néanmoins, un hôte ne délivre pas d'acquittement à chaque segment reçu, car ceci ralentirait excessivement la communication.

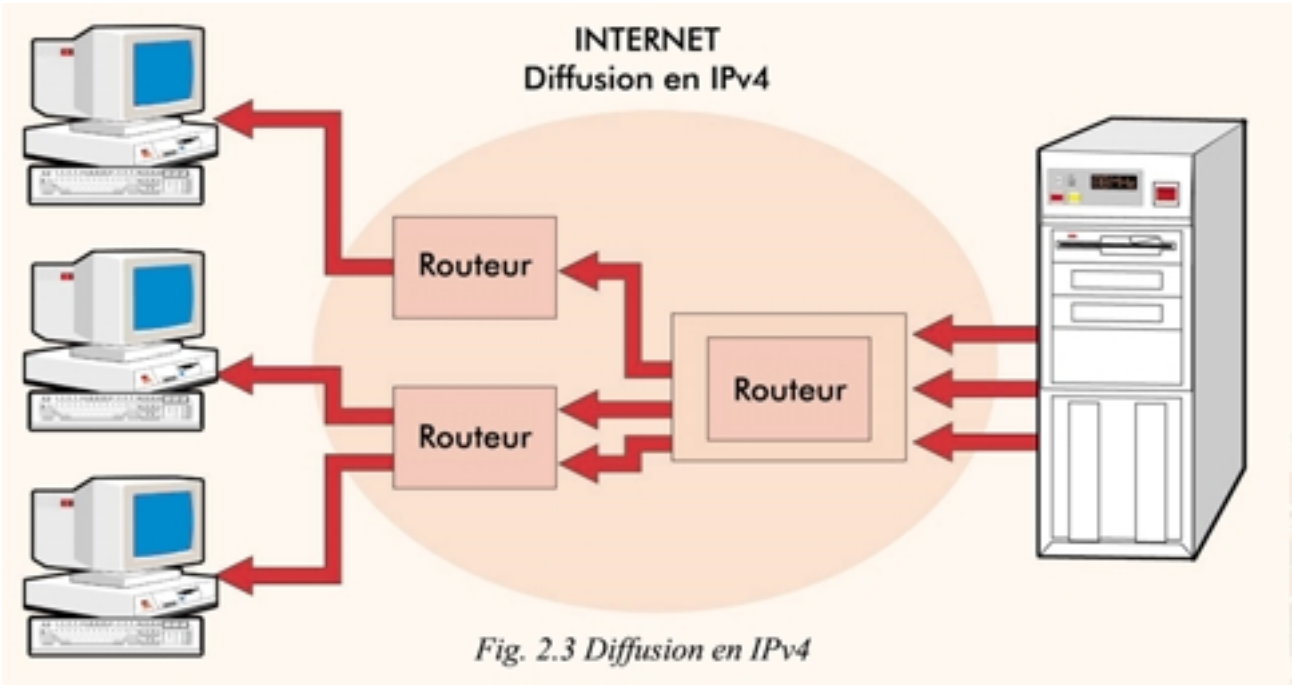

Fig. 2.3 Diffusion en IPv4

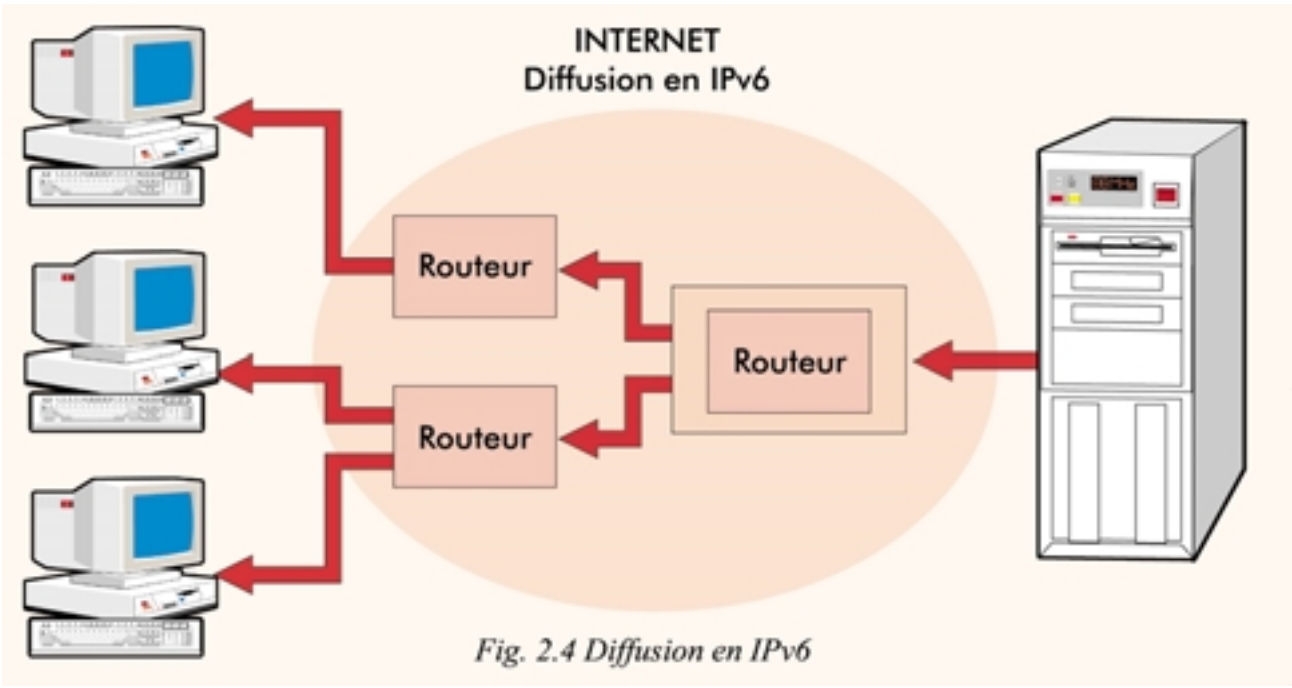

Fig. 2.4 Diffusion en IPv6

2.2.3 Les autres principaux protocoles de la famille de TCP/IP

2.2.3.1 Gateway to Gateway Protocol

GGP (*Gateway to Gateway Protocol*) permet à deux passerelles d'échanger des informations de routage, pour remettre à jour dynamiquement leurs tables de routage. Il ne se conçoit qu'à travers des réseaux longue distance, lorsqu'il y a une multitude de chemins différents pour atteindre le même hôte. Il est totalement inutile en réseau local. Les unités de données GGP sont encapsulées dans des datagrammes IP. Les informations véhiculées par GGP sont des couples d'adresses de réseau et de distance sachant que la distance d'un réseau est exprimée en nombre de passerelles à traverser pour l'atteindre. Une passerelle qui maintient ce type d'information peut alors faire le meilleur choix pour acheminer une unité de données par le trajet le plus court. L'information est propagée de passerelles en passerelles voisines. Pour plus de détails, voir le livre «Réseaux TCP/IP», Editions WAN & LASER.

2.2.3.2 Le protocole BOOTP

Il sert aux stations sans disque à faire l'acquisition de leur adresse IP. C'est une alternative à RARP, et le principe de fonctionnement est le même.

2.2.3.3 Le protocole SMTP

SMTP (*Simple Mail Transiter Protocol*) est le protocole standard d'échange de courrier électronique sur réseau TCP/IP.

2.2.3.4 Le protocole SNMP

Simple Network Management Protocol permet l'acquisition de données sur le fonctionnement du réseau. C'est un protocole d'administration de réseau.

2.2.3.5 Les protocoles XDR et RPC

XDR (*eXternal Data Representation*) est un protocole du niveau de la couche Présentation du modèle OSI. Il permet d'encoder des données de manière standard pour lever tous les problèmes d'hétérogénéité entre les plates-formes.

RPC (*Remote Procedure Call*) offre aux développeurs d'applications un mécanisme permettant de réaliser des appels à des procédures distantes se comportant quasiment comme des appels à des procédures locales. Ces deux protocoles ont été créés par Sun Microsystem en 1986, en vue du développement de NFS (*Network File System*) et NIS (*Network Integration Service*).

2.3 Interconnexion des réseaux de transmission sur Internet

2.3.1 Généralités

Un réseau de transmission permet à tout matériel informatique qui lui est connecté de communiquer directement avec tout autre hôte. Trois grandes catégories de réseaux de transmission peuvent être distinguées: les réseaux à commutation de circuits, les réseaux à commutation de messages, les réseaux à commutation de paquets.

Historiquement les réseaux à commutation de circuits ont été les premiers à apparaître, le réseau téléphonique commuté (RTC) en est le représentant le plus ancien et le plus couramment utilisé pour connecter les abonnés à Internet via la boucle locale. Pour plus de détails, voir le livre «Réseaux TCP/IP», Editions WAN & LASER.

2.3.1.1 Les réseaux à commutation de circuits (RTC)

Un circuit matérialisé est construit entre un émetteur (équipement terminal de traitement de données) et un récepteur (équipement de terminaison de circuit de données). Ce circuit n'appartient qu'aux deux entités qui communiquent. Le circuit doit être établi avant que des informations puissent transiter. Il dure jusqu'au moment où l'une des deux entités interrompt la communication. Si les deux correspondants n'ont plus de données à se transmettre pendant un certain temps, la liaison reste inutilisée, d'où l'idée de concentrer plusieurs communications sur une même liaison pour que le taux d'utilisation des liaisons augmente. Si de nombreuses communications utilisent une même liaison, une file d'attente va se former. Il faut alors prévoir des tampons de mémoire pour retenir les messages, en attendant que la liaison soit disponible.

2.3.1.2 Les réseaux à commutation de messages

Un message est une suite d'informations formant logiquement un tout pour l'expéditeur et le destinataire: par exemple un fichier complet, une ligne tapée sur un terminal, un secteur de disque, etc. Un réseau à commutation de messages est un réseau maillé de nœuds de commutation. Le message est envoyé de nœud de commutation à nœud de commutation jusqu'au destinataire, il ne peut être envoyé au nœud suivant tant qu'il n'est pas complètement et correctement reçu par le nœud précédent. Il faut des tampons aux nœuds intermédiaires pour mémoriser les messages tant que ceux-ci ne sont pas correctement stockés dans le nœud suivant.

Il faut également un système de gestion des transmissions qui acquitte les messages correctement reçus et demande la retransmission des messages erronés. De plus, comme la capacité des mémoires intermédiaires est limitée, il va falloir introduire un contrôle sur le flux des messages pour être sûr qu'il ne va pas y avoir de débordement. Des politiques de routage des messages peuvent être introduites pour aider et sécuriser les transmissions. Par exemple si une liaison tombe en panne, il faut prévoir un autre chemin. Si les messages sont trop longs, du type fichier par exemple, ils peuvent être stockés sur disque aux nœuds intermédiaires. Dans ce cas, le temps de réponse de la transmission augmente énormément.

2.3.1.3 Les réseaux à commutation de paquets

Pour accélérer la vitesse de transmission et rendre beaucoup plus simples les reprises sur erreur, on a vu apparaître le concept de réseau à commutation de paquets. Le paquet est une suite d'informations binaires ne pouvant pas dépasser une longueur fixée à l'avance. Les messages des utilisateurs sont découpés en paquets pour pouvoir être transmis plus facilement. Ces derniers ont couramment une longueur maximale de 1 000 à 2 000 bits (125 à 250 caractères). Les principes sont les mêmes que dans les réseaux à commutation de messages, seulement les blocs d'informations élémentaires sont beaucoup plus courts.

Les paquets sont envoyés indépendamment les uns des autres et les liaisons entre nœuds de commutation les prennent en compte pour les émettre au fur et à mesure de leur arrivée dans le nœud. Les paquets de plusieurs messages peuvent donc être multiplexés temporairement sur une même liaison.

Le rôle des nœuds de commutation est d'aiguiller les paquets vers la bonne porte de sortie qui peut être donnée, par exemple, par une table de routage. On peut remarquer que les liaisons entre commutateurs ne sont pas affectées explicitement à une paire origine-destinataire comme dans la commutation de circuits. Une liaison est utilisée en même temps par l'ensemble des paquets que le routage oblige à transiter par cette même liaison.

Par rapport à la commutation de messages, la gestion de blocs d'informations de petite taille est plus simple surtout au niveau des reprises sur erreur. En revanche, surgit le problème du réassemblage des paquets pour reformer le message original. En particulier si des paquets prennent des routes distinctes et que l'un se perde, il faudra le plus souvent effectuer une reprise sur l'ensemble du message.

2.3.2 Les supports physiques de transmission sur Internet

2.3.2.1 Généralités

Il existe principalement trois types de supports utilisés dans les réseaux, la paire torsadée, le câble coaxial et la fibre optique. Le choix d'un support de transmission adapté est fonction essentiellement du coût et du débit souhaité. Le support peut être utilisé en bande de base, c'est-à-dire que le message occupe toute la largeur de la bande passante du câble, ou en large bande, qui implique que plusieurs messages sont acheminés simultanément, à des fréquences différentes. Le signal véhiculé peut être:

- *numérique (ou digital)*: il s'agit alors d'un signal carré. Une certaine tension électrique (ou une combinaison de tensions électriques) pendant un certain temps code un bit à 1, une autre tension (ou combinaison de tensions) pendant un temps identique représente un bit à 0;
- *analogique*: c'est un signal sinusoïdal. L'information est encodée par la variation de la fréquence du signal, ou par la variation de sa phase, ou par une combinaison des deux.

Notons également que pour des raisons de développement technologique et de coût d'investissements raisonnables, on fait de plus en plus recours aux technologies sans fils pour la transmission des données sur Internet. Nous verrons ces technologies par la suite.

2.3.2.2 La paire torsadée

C'est le support physique le plus simple, il est réalisé à partir de paires de fils électriques, quelquefois blindés. Il permet des transmissions de données informatiques à une vitesse de 100 Mbit/s sur une distance de 100 m.

- Les principaux avantages de ce type de support sont sa simplicité de connexion, et son faible coût.
- Ses inconvénients sont la faiblesse du débit, due à une forte atténuation du signal et à sa sensibilité aux phénomènes de compatibilité électromagnétique, limitée par le recours au blindage. Ce câble est employé notamment par les technologies Token Ring et Ethernet 10 base T, ou 100 base T.

2.3.2.3 Le câble coaxial

Un câble coaxial est constitué de deux conducteurs cylindriques de même axe séparés par un isolant. Le conducteur central est appelé l'âme. C'est un support de plus en plus utilisé qui permet de limiter les perturbations dues aux bruits externes. En cas de perturbations importantes, un blindage s'avère nécessaire.

Il a été démontré que le rapport entre les diamètres des deux conducteurs doit être de 3,6. Les différents câbles sont désignés par les diamètres utilisés en mm. Les deux plus couramment utilisés sont le 9,5/2,6 et le 4,4/1,2.

Le premier (9,5/2,6) autorise un débit de 10 Mbit/s sur un câble d'une longueur de 200 m. Le second (4,4/1,2) permet un débit analogue (10 Mbit/s) sur un câble de 500 m. Les deux bénéficient d'un blindage externe. Ils sont respectivement employés pour mettre en œuvre 1'Ethernet 10 base 5 et l'Ethernet 10 base 2 qui seront décrits au paragraphe 2.3.4.

Pour les mêmes raisons que sur les fils métalliques, plus la distance à parcourir est faible et plus le débit binaire peut être grand. Néanmoins, on ne peut dépasser certaines limites puisque l'atténuation du signal augmente avec la fréquence. Son coût est plus élevé que celui de la paire torsadée. La connexion est moins simple qu'avec la paire torsadée:

- pour le 10 base 2, on utilise une prise en T;
- pour le 10 base 5, on fait recours à une prise dite «vampire» dont un élément perce le câble jusqu'à l'âme.

2.3.2.4 La fibre optique

La fibre optique est une technologie relativement nouvelle, et encore peu répandue. Dans les fils métalliques, on transmet les informations par l'intermédiaire de courant électrique modulé. Avec la fibre optique, on utilise un faisceau lumineux modulé. Il a fallu attendre les années 1960 et l'invention du laser pour que ce type de transmission voie le jour. Ce support permet d'atteindre des débits de l'ordre du Gbit/s sur plusieurs kilomètres. C'est le support le plus cher mais aussi le plus sûr.

2.3.3 Technologies d'accès au support

2.3.3.1 Accès multiple avec écoute de la porteuse CSMA/CD

Cette technique est issue des réseaux radio, elle est applicable sur les réseaux à bus. C'est cette technologie qui est utilisée dans les réseaux de type *Ethernet.* Elle repose sur l'hypothèse que le trafic généré par chaque site l'est sous la forme de rafales de courte durée. Tant que l'on n'approche pas de la saturation, la probabilité pour que deux sites veuillent émettre au même moment est donc faible, et les sites émettent sans autorisation préalable.

Une amélioration tendant à diminuer les risques de collision consiste en ce que chaque site écoute en permanence le réseau quand il n'émet pas, pour savoir si un paquet est en cours de transmission. Il ne lance son émission que si le support est libre. Cette technique s'appelle CSMA (*Carrier Sense Multiple Access*). Les risques de collisions sont toujours possibles, car un paquet peut être émis sans être détecté par une autre station à cause du temps de propagation sur le réseau.

L'autre amélioration consiste à écouter également pendant l'émission pour détecter les collisions. Si une collision est détectée, l'émetteur s'arrête. Cette technique ne diminue pas le nombre de collisions, mais «limite les dégâts» en cas de collision. Avec cette deuxième amélioration, la technique s'appelle CSMA/CD (CD pour *Collision Detection*)*;* c'est la technique utilisée dans les réseaux Ethernet.

Les *avantages* de cette technique sont les suivants:

- premier réseau local à bénéficier d'un consensus de groupes industriels et d'une normalisation, Ethernet est le réseau le plus répandu;
- tant que le nombre de collisions reste faible, la méthode d'accès est performante et rapide.

Les *inconvénients:*

- Les performances du réseau se dégradent rapidement au-delà d'un taux de collisions excédant 5%;
- dans sa version 10 base 5, le médium est un câble spécial coûteux;
- le fonctionnement correct de la méthode d'accès implique un maximum admissible pour le temps de propagation aller-retour d'un signal sur le bus, et par conséquent une longueur maximale du bus. Cette contrainte étant liée au temps de propagation et non à l'affaiblissement des signaux ne peut être levée par l'usage de répéteurs;
- le temps d'attente avant transmission d'un message n'est pas limité. On peut simplement donner une probabilité pour qu'il ne dépasse pas une certaine valeur. Ceci pose des problèmes pour des applications temps réel au niveau industriel et pour la transmission de voix digitalisée.

2.3.3.2 Le bus à jeton (token bus)

Dans ce type de réseau un signal particulier (le jeton) est propagé sur le réseau. Toute station qui reçoit le jeton peut soit le retransmettre immédiatement si elle n'a rien à émettre, soit l'intercepter et envoyer son message, puis réémettre le jeton. Le jeton est un signal spécial, conçu pour pouvoir être reconnu et généré rapidement.

L'intérêt principal des réseaux à jeton sur bus est de concilier la fiabilité propre aux structures en bus passif et la garantie d'un débit minimal, que peut donner la technique jeton, contrairement à la technique CSMA/CD (voir 2.3.3.1). En plus, le bus travaillant en diffusion, l'information est transmise en une seule étape à la station destinataire. Chaque station peut donc «bufferiser» la trame entière sans diminuer les performances, ce qui n'est pas le cas des réseaux en anneau.

2.3.3.3 L'anneau à jeton (token ring)

Dans un anneau, l'information circule de proche en proche jusqu'à ce qu'elle fasse le tour de l'anneau. Pour minimiser l'impact des «bufferisations» dans les stations intermédiaires sur le temps de transfert entre deux stations, la station qui ne veut ni émettre ni recevoir se contente de retransmettre les informations.

Quand une station veut émettre, elle capture le jeton en interrompant la retransmission et insère à sa place l'information à transmettre. Cette information fait le tour du réseau, passant par la station destinataire qui en prend une copie et revient jusqu'à la station émettrice qui l'extrait de l'anneau sur lequel elle réinjecte le jeton. Une procédure d'accusé de réception très simple peut également être implémentée. Ainsi, la station émettrice peut savoir si l'information a bien été reçue.

2.3.4 L'architecture Ethernet

2.3.4.1 Fonctionnement

L'architecture Ethernet est constituée de deux couches fondamentales: la couche Physique et la couche de contrôle. Ces deux couches correspondent respectivement aux couches 1 et 2 du modèle OSI d'interconnexion de systèmes ouverts (voir Figure 2.1). Cette architecture présente comme avantages, la clarté de la spécification observée au niveau de la définition des responsabilités de chaque couche ainsi que la flexibilité qui permet à la couche de contrôle d'être transparente à tout type de connexion physique.

Ethernet utilise la méthode d'accès CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*) (voir 2.3.3.1). Lorsqu'une station désire émettre sur le réseau, elle commence par examiner si le support de communication est occupé ou non. Si une transmission est en cours, la station attend jusqu'à ce que la voie se libère, puis elle effectue sa transmission. Il peut évidemment se produire des collisions en raison du nombre d'équipements qui se partagent le support de communication. `

Lorsqu'une collision se produit, la station émettrice interrompt sa transmission et transmet des bits de bourrage, pour avertir les autres stations du réseau de la collision. La station reprendra sa transmission ultérieurement, en fonction d'un algorithme défini. La détection des collisions se fait par comparaison entre le signal émis par la station et le signal circulant sur le support de communication.

En raison de la vitesse de propagation des signaux, de l'ordre de 200 000 km par seconde, et de l'amplitude réduite à 2,5 km, les retransmissions de trames, même dans les réseaux chargés, ne prennent au maximum que quelques milli-secondes.

2.3.4.2 Les composantes de base d'Ethernet

Ethernet intègre quatre composantes principales: la station hôte; le contrôleur (carte Ethernet); le câble coupleur entre le contrôleur et le système de transmission ainsi que le système de transmission.

2.3.4.2.1 La station hôte

La station consiste généralement en un ordinateur, un serveur de terminaux, ou une imprimante. Mentionnons que les terminaux classiques ne peuvent servir de stations en raison de leur absence d'interface réseau. Toutefois, ils peuvent être reliés à un serveur de terminaux qui remplira les fonctions d'accès au réseau. Dans ce cas, la station abrite le contrôleur.

2.3.4.2.2 Le contrôleur

Le contrôleur offre toutes les fonctions nécessaires à l'accès au support. Ceci inclut la mise en forme des données, la gestion des liaisons, le codage/décodage des informations. Le contrôleur est physiquement installé sur une «carte Ethernet», qui est enfichée dans le bus de la machine hôte.

2.3.4.2.3 Le câble coupleur

Le câble coupleur est à la jonction entre le contrôleur et le système de transmission. Le contrôleur s'occupant des fonctions de communication, cette interface se révèle assez simple. Il s'agit d'un câble (paire torsadée blindée) entre le contrôleur et le module d'émission/réception. Souvent appelé «câble de descente». Sa longueur maximale est de 50 m. Certaines configurations se dispensent purement et simplement de ce câble et relient directement le contrôleur au système de transmission.

2.3.4.2.4 Le système de transmission

Le système de transmission inclut les composantes nécessaires à l'échange de données un module d'émission/ réception appelé *transceiver* (transmetteur). Ce boîtier fournit l'environnement électronique nécessaire pour transmettre et recevoir le signal, ainsi que pour reconnaître la présence d'un signal émis par une autre station. Il doit également détecter les collisions. Ce système est complété par le support de transmission (câble).

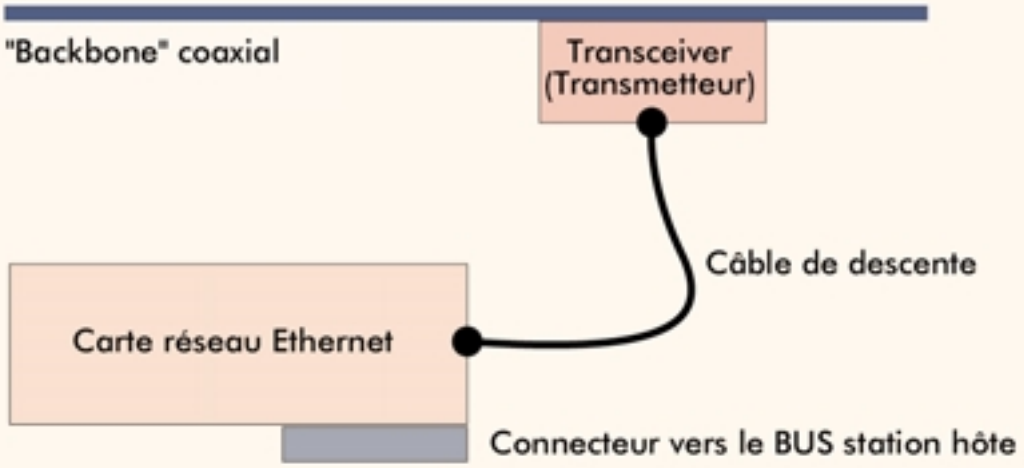

Fig. 2.5 Composants principaux d'un réseau Ethernet

2.3.4.3 Différentes configurations Ethernet

2.3.4.3.1 Ethernet standard

Un réseau Ethernet standard a pour épine dorsale (backbone) le câble coaxial épais, dit 10 base 5, qui permet d'atteindre un débit de 10 Mbit/s en bande de base. Chaque segment a une longueur maximale de 500 m. On peut connecter un hôte tous les 2,5 m, et le câble porte des marques à cet effet. La longueur totale du réseau ne peut excéder 2 500 m (5 segments reliés par 4 répéteurs). La jonction du transmetteur au câble est réalisée sans coupure, par l'intermédiaire de prises vampires. Dans le cas où le réseau Ethernet standard comprend plus de 2 segments reliés en série par des répéteurs, un segment sur deux ne peut pas accueillir d'hôte, il sert uniquement à étendre la portée du réseau. La Figure 2.6 illustre le principe de montage.

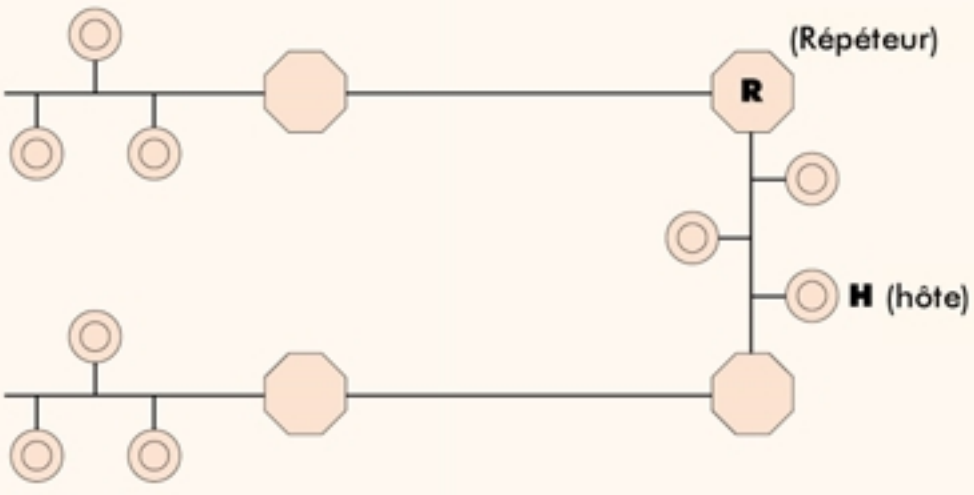

Fig. 2.6 Configuration Ethernet standard avec 5 segments au maximum

2.3.4.3.2 Ethernet fin

L'Ethernet fin (*thin Ethernet*) utilise un câble coaxial fin non blindé 10 base 2 autorisant des débits de 10 Mbit/s en bande de base. Le raccordement des transmetteurs au support s'effectue par une prise BNC en T. Les caractéristiques physiques du câble limitent la longueur des segments à 185 m et la longueur totale du réseau peut atteindre 925 m (soit 5 segments et 4 répéteurs). Deux hôtes en communication ne peuvent être séparés par plus de 4 répéteurs.

2.3.4.3.3 Ethernet 10 base T et Fast Ethernet 100 base T

La topologie de ce type de réseaux est l'étoile. Le support est constitué de segments de paire torsadée d'une longueur maximale de 100 m, qui relient chaque station au HUB (*Host Unit Broadcast*) central. Le débit atteint 10 Mbit/s ou 100 Mbit/s. La technologie 10 base T ou 100 base T est fréquemment utilisée en conjonction avec 10 base 2 ou 10 base 5: une arête principale en câble coaxial relie entre eux un certain nombre de HUB, ce qui permet d'étendre latéralement la portée du réseau. Les connecteurs utilisés sont de type RJ45 (prise téléphonique américaine).

2.3.5 L'architecture Token Ring

2.3.5.1 Généralités

L'architecture Token Ring a été conçue par IBM et reprise par l'IEEE (Institute of Electrical and Electronic Engineers) sous la norme 802.5 (norme ISO 8802.5). La topologie est en anneau et la méthode d'accès est à jeton. On distingue la configuration en Token Ring à 4 Mbit/s et à 16 Mbit/s.

2.3.5.2 Les composantes de l'architecture Token Ring

- La station hôte: comme dans le cas d'Ethernet, il s'agit le plus souvent d'un ordinateur ou d'une imprimante munie d'une interface réseau.
- Le contrôleur qui est hébergé par la carte réseau de l'hôte.
- Le câble coupleur qui relie le contrôleur au MAU (*Multistation Access Unit*). Il est en paire torsadée, blindée (longueur maximale 610 m) ou non blindée (longueur maximale 305 m).
- Le système de transmission qui comprend un MAU permettant de connecter plusieurs stations hôtes en un point de l'anneau. Il joue le rôle d'un HUB entre un ensemble de stations et l'anneau. Il comprend en plus un câble de type paire torsadée, blindée ou non.

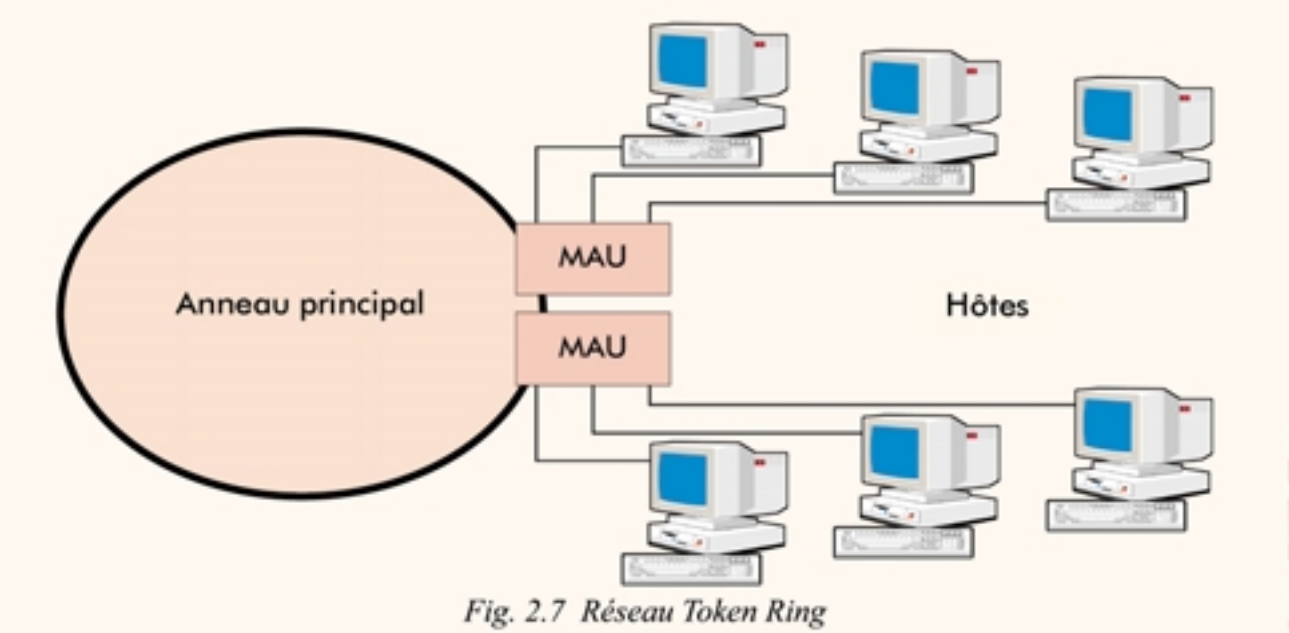

Fig. 2.7 Réseau Token Ring

2.3.6 Autres architectures

2.3.6.1 Généralités

Les architectures citées dans ce paragraphe servent généralement pour interconnecter des sous-réseaux classiques (Ethernet ou Token Ring). En effet, on relie rarement directement des hôtes sur des architectures de ce type, vu leurs coûts élevés, et les interfaces réseaux classiques ne fonctionnent pas à des vitesses aussi élevées, ce qui conduirait à une sous-exploitation de la capacité du support.

2.3.6.2 Ethernet 100 base T

Ethernet 100 base T a un débit de 100 Mbit/s, indifféremment sur de la paire torsadée ou de la fibre optique, déployée en étoile autour d'un HUB. La méthode d'accès utilisée est CSMA/CD.

2.3.6.3 Ethernet 100 base VG ou «AnyLan»

Il véhicule aussi bien des trames Ethernet classiques que des trames Token Ring, sur de la paire torsadée ou de la fibre optique.

2.3.6.4 FDDI (Fiber Distributed Data Interface)

FDDI est constitué d'un double anneau à jeton et en fibre optique, d'une longueur maximale de 100 km, il a un débit de 100 Mbit/s.

2.3.6.5 DQDB (Distributed Queue Dual Bus)

DQDB utilise un double bus en fibre optique à un débit de 155 Mbit/s.

2.3.7 Equipements d'interconnexion des réseaux

2.3.7.1 Généralités

On appelle équipements d'interconnexion les appareils connectés au réseau, mais qui n'en sont pas hôtes. Ils portent une appellation différente selon leur niveau d'intelligence artificielle ou le rôle qu'ils jouent au niveau de l'interconnexion.

2.3.7.2 Le matériel

- *Les répéteurs:* les répéteurs se contentent de réémettre le signal en le réamplifiant. Ils fonctionnent au niveau 1 du modèle OSI.
- *Les ponts:* ils agissent au niveau liaison de données (couche 2) et comportent une certaine logique. Ils permettent notamment d'interconnecter deux réseaux de même architecture physique et de filtrer les trames qui passent d'un réseau à l'autre pour éviter un engorgement inutile.
- *Les routeurs:* ils travaillent au niveau de la couche 3 du modèle OSI, et s'occupent du routage des unités de données. Ils permettent d'interconnecter deux réseaux de types différents. Un routeur transfère des paquets en les analysant au niveau 3 du modèle ISO. Un routeur peut faire office de passerelle «Gateway» entre des réseaux de natures différentes (Ethernet à FDDI, Token Ring à Ethernet, ATM à FDDI). Enfin, dans les cas de grands réseaux fortement maillés, il déterminera le meilleur chemin pour atteindre une adresse considérée (nombre de nœuds à franchir, qualité de la ligne, bande passante, etc.).
- *Les passerelles:* c'est un terme générique qui désigne un équipement de niveau supérieur ou égal à la couche 3. Il autorise l'interconnexion «intelligente» de réseaux hétérogènes.
- *Les HUB (Host Unit Broadcast):* ces équipements (*Host Unit Broadcast*) sont au centre des configurations en étoile et assurent l'interconnexion des différentes branches de l'étoile.
- *Les MAU (Multistation Access Unit):* les MAU (*Multistation Access Unit*) sont des équipements destinés aux topologies en anneau. Ils servent à interconnecter plusieurs hôtes en un point unique de l'anneau (voir Figure 2.7).

3 Conception et déploiement d'un nœud Internet

3.1 Généralités

Selon le rapport de «*US Internet Council*» http//www.usic.org/usic_state_of_net99.htm) du 12 avril 1999, au mois de janvier 1999, il existait plus de 43 millions de serveurs Internet dans le monde (Network Wizards) dont seulement 0,1829 million en Afrique. Il y avait 829 millions de pages Web en 1998 et 1,45 milliard étaient prévues fin 1999 (Internet Data Corporation).

Selon «*Computer Industry Almanach*», fin 1998, 364,4 millions d'ordinateurs personnels étaient utilisés dans le monde. La répartition est estimée à 129 millions (le tiers) aux Etats-Unis; 32,8 millions au Japon; 21,1 millions en Allemagne; 18,25 millions en Grande-Bretagne; 15,35 millions en France.

Toutes ces statistiques nous montrent à quel point le continent Africain est en retard en matière de nouvelles technologies de l'information et la nécessité d'avoir un plan d'action spécial dans chaque pays pour essayer de relever ce défi.

Dans le chapitre 2, nous avons passé en revue les grandes orientations en matière de réseaux, leurs interconnexions et la transmission des données. Dans le chapitre 3, nous nous concentrerons plus sur la conception, la planification et le déploiement d'un nœud d'Internet au niveau national. Nous allons passer en revue les éléments actifs utilisés, et observer pour chaque cas la gestion et l'utilisation des adresses de couche 2 (adresses MAC) et de couche 3 (adresses IP). Cette approche va nous permettre de mieux comprendre le fonctionnement des différents acteurs techniques d'un réseau Internet et par la suite, et suivant les stratégies de chaque opérateur des télécommunications, celui-ci pourra développer son réseau en intégrant un ou plusieurs nœuds d'interconnexion pour un accès au niveau régional ou international.

3.2 Eléments de planification d'un nœud national d'Internet

3.2.1 Généralités

Dans ce paragraphe, nous allons voir les techniques et leur fonctionnement pour pouvoir planifier un nœud Internet au niveau national. Certaines choses déjà vues dans le chapitre précédent seront approfondies pour permettre à toute personne de comprendre le fonctionnement et aux professionnels de se rappeler très vite des notions qui ne leur sont pas étrangères.

3.2.2 Services réseaux et les couches du modèle OSI

Au début des années 1980, les participants de différents comités de standardisation décidèrent de définir un modèle logique décrivant les différents éléments qui permettent à deux systèmes informatiques de communiquer. Près de dix ans après le début des travaux, le modèle OSI (*Open Systems Interconnection*) fut accepté. Ce modèle a pour but de séparer tous les processus et protocoles prenant part à une communication réseau et de les regrouper en sept couches en fonction de leur tâche. Le but de cette standardisation était de définir donc les interfaces entre chaque couche. Ces sept couches et les services y relatifs sont représentés dans le tableau suivant.

Tableau 3.1 – Modèle OSI et les services réseaux (*Sources: FI-6 1998*)

OSI

Couche 7	Application	(FTP, SMTP)
Couche 6	Présentation	
Couche 5	Session	(DNS)
Couche 4	Transport	(TCP, UDP)
Couche 3	Réseau	(IP)
Couche 2	Liaison de données	(Ethernet, Token Ring)
Couche 1	Physique	(coax, paire torsadée, fibre optique)

Chaque couche est responsable de recevoir et transmettre l'information à ses deux couches voisines, indépendamment des autres couches. La Figure 3.1 illustre la relation entre des éléments physiques d'un réseau et le modèle OSI.

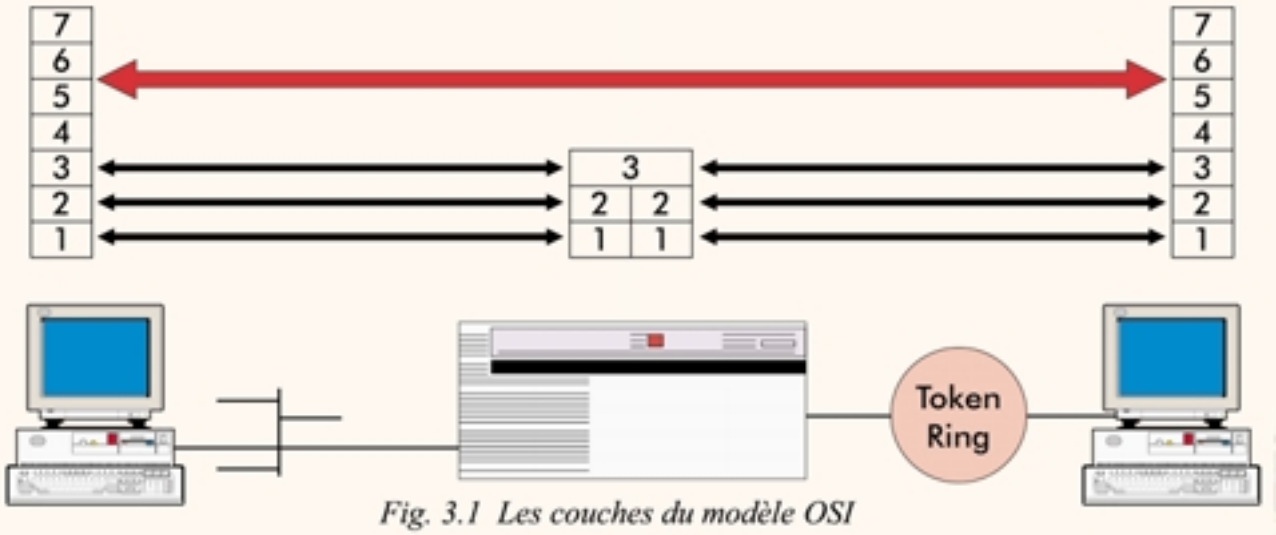

Fig. 3.1 Les couches du modèle OSI

Chaque ordinateur doit implémenter ces sept couches s'il veut communiquer sur le réseau auquel il est connecté. Par contre, les éléments actifs du réseau tels que les routeurs et les switches n'utilisent que les premières couches (1, 2 et 3) du modèle OSI. En règle générale, les deux ou trois premières couches sont présentes sur tous les éléments d'un réseau, alors que les quatre couches supérieures sont résidentes sur les hôtes.

3.2.3 Encapsulation sur Ethernet et TCP/IP

Pour illustrer les principes d'interactions entre les différentes couches du modèle OSI, nous allons voir comment cette conception est mise en œuvre, en regardant de plus près les principes d'adressages utilisés pour envoyer de l'information à travers un réseau.

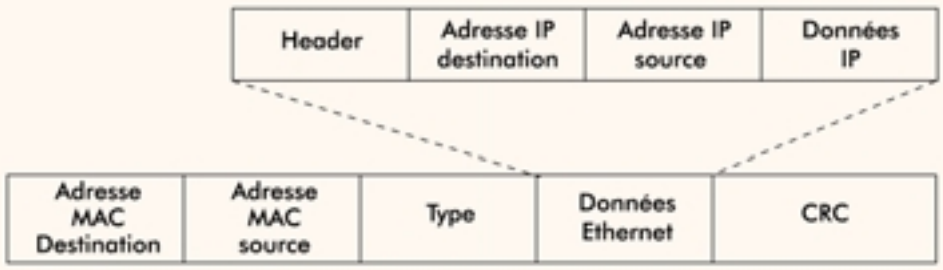

Fig. 3.2 La trame Ethernet

Les protocoles décrits sont Ethernet pour la couche 2 (Liaison de données) et IP pour la couche 3 (Réseau). Pour plus de détails, voir FI-6/1998.

La Figure 3.2 met en évidence les différentes adresses utilisées lors d'une communication entre deux postes. Un message IP envoyé sur un segment Ethernet contient quatre adresses différentes, soit deux (logiques et physiques) pour indiquer la destination du message et deux pour en indiquer la source. Les adresses sources seront utilisées par une station pour identifier et pour répondre à son interlocuteur.

Les adresses utilisées au niveau Ethernet sont dites adresses MAC (*Media Access Control*). Ces adresses sont composées de 6 octets et sont généralement données sous forme hexadécimale (A0-32-B1-98-17-D4). L'adresse MAC est directement gravée sur la carte réseau d'un ordinateur ou sur l'interface d'un routeur (adresse physique). L'adresse MAC est unique dans le monde.

Les adresses IP sont attribuées de manière software par les utilisateurs. Elles se composent de 4 octets et sont généralement représentées sous forme décimale (156.106.194.24) comme on l'a vu plus haut.

Sur un réseau, une station est identifiée par deux adresses distinctes: l'adresse MAC et l'adresse IP. Pour envoyer un paquet, il ne suffit donc pas de connaître l'adresse IP d'une station, il faut en plus lui associer une adresse MAC.

3.2.4 Protocole ARP

Le protocole ARP (*Address Resolution Protocol*) est utilisé pour trouver l'adresse MAC d'une station à partir de son adresse IP. Son principe de fonctionnement est illustré par la Figure 3.3.

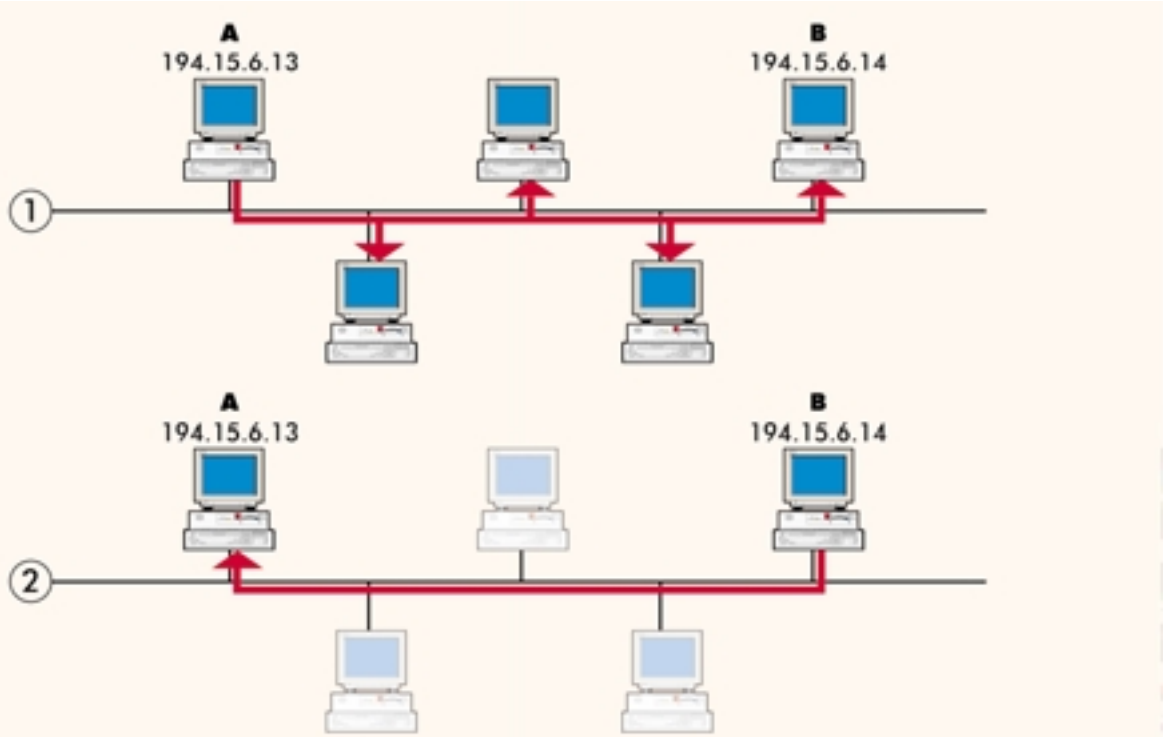

Fig. 3.3 Protocole ARP

La station A désire envoyer un message à la station B, et connaît son adresse IP. Malheureusement, elle ne sait pas à quelle adresse MAC elle doit envoyer sa trame Ethernet. En première étape (1), elle envoie un broadcast Ethernet qui contient l'adresse IP demandée (194.15.6.14). Toutes les stations reçoivent ce message et examinent l'adresse IP demandée. En deuxième étape (2), seule la station B répond à la requête ARP. Elle insère dans la réponse sa propre adresse MAC. La station A peut finalement envoyer des données à la station B en utilisant cette adresse MAC. (*Source: FI-6/1998*)

3.2.5 Le segment Ethernet

Le segment Ethernet est la forme la plus simple de ce que peut être un réseau informatique. Il est physiquement matérialisé par un câble coaxial ou par un concentrateur de câblage ou hub. La Figure 3.4 illustre une communication IP entre deux stations d'un même segment Ethernet.

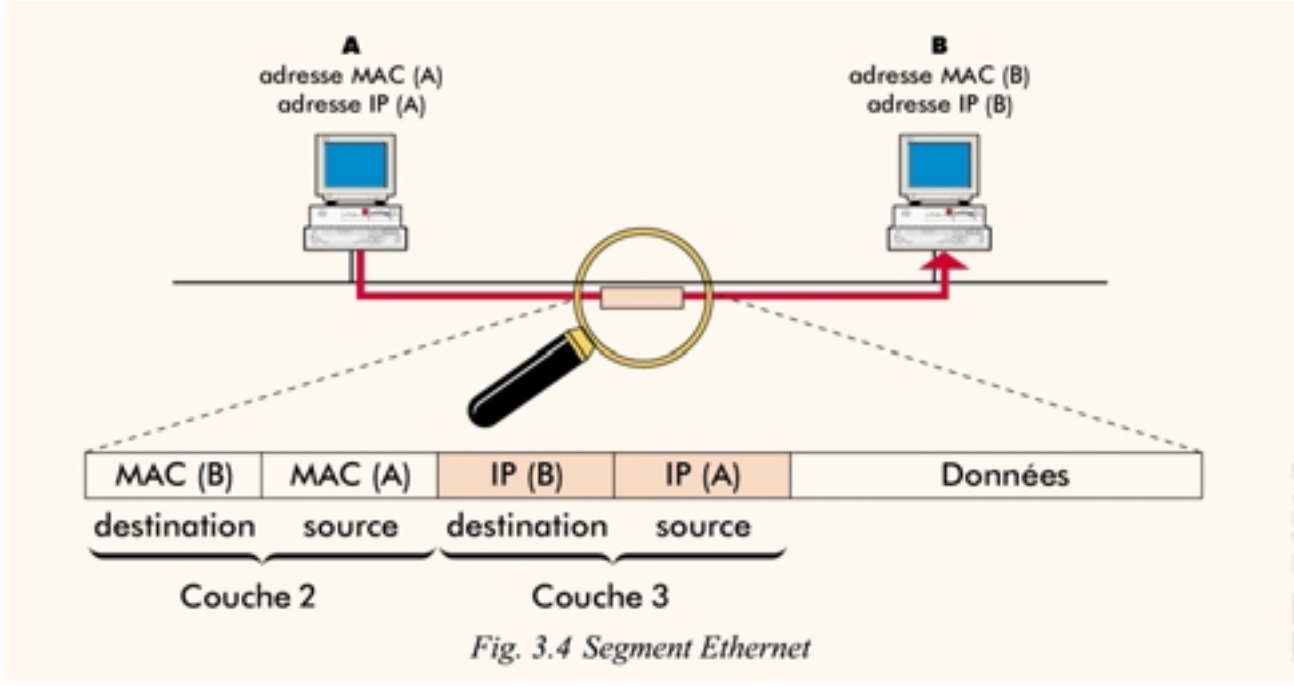

Fig. 3.4 Segment Ethernet

La station A connaissait l'adresse IP de la station B. Elle a ensuite lancé une requête ARP pour découvrir son adresse MAC. La station A dispose alors des deux adresses nécessaires pour envoyer un message à la station B. Tous les paquets envoyés contiendront les quatre adresses de la communication, à savoir l'adresse MAC de destination et l'adresse MAC source pour la couche 2 du modèle OSI, ainsi que l'adresse IP de destination et l'adresse IP source pour la couche 3.

Dans le cas d'un segment Ethernet, les quatre adresses utilisées sont exclusivement celles des deux stations désirant communiquer.

3.2.6 Le routeur

Le partage du support de communication et la limite de taille constituent un grand problème sur les réseaux Ethernet: quel que soit le nombre de stations connectées sur un segment Ethernet, seule une d'entre elles pourra émettre, alors que les autres attendront leur tour. Pour remédier à cette lacune, on utilise le routeur. Le but d'un routeur est d'interconnecter deux segments Ethernet de deux réseaux ou sous-réseaux. La Figure 3.5 illustre le principe de fonctionnement d'une communication entre deux stations séparées par un routeur.

Cet exemple met en valeur l'intervention de l'administrateur réseau dans le processus de communication. En effet, l'adresse IP, le subnet mask et le default Gateway ont été configurés sur les deux machines. Le responsable du réseau a dû choisir des paramètres de couche 3 et assigner des valeurs aux postes. Il a défini deux sous-réseaux de 255 adresses IP, à savoir le sous-réseau 194.100.100.X où se trouve la station A avec 194.100.100.2 comme adresse IP et le sous-réseau 194.100.200.X où se trouve la station B avec 194.100.200.2 comme adresse IP, les deux étant séparés par un routeur.

Le routeur est une passerelle entre ces deux sous-réseaux. Lorsque la station A décide d'envoyer un message à la station B, elle compare la partie réseau de son adresse IP (194.100.100) à celle de destination (194.100.200). Ces deux adresses des deux sous-réseaux n'étant pas les mêmes, elle va envoyer le paquet IP à sa passerelle par défaut, c'est-à-dire au routeur. Elle effectue donc une requête ARP pour découvrir l'adresse MAC du routeur, puis construit la trame Ethernet en utilisant l'adresse MAC du routeur, et l'envoie sur le segment. Le routeur reçoit la trame, en extrait uniquement le message IP, effectue une requête ARP pour trouver l'adresse AC de la station B dont il connaît l'adresse IP par le message de la station A, et envoie la nouvelle trame Ethernet sur le deuxième segment et jusqu'au destinataire B.

Les adresses IP contenues dans le message sont celles de la station source et de la station de destination. Elles ne sont jamais modifiées durant la traversée du réseau. Seules sont modifiées les adresses MAC.

Le routeur est un élément de couche 3, car il choisit la destination du message en lisant les informations contenues au niveau IP. Pour plus de détails, voir FI-6/1998.

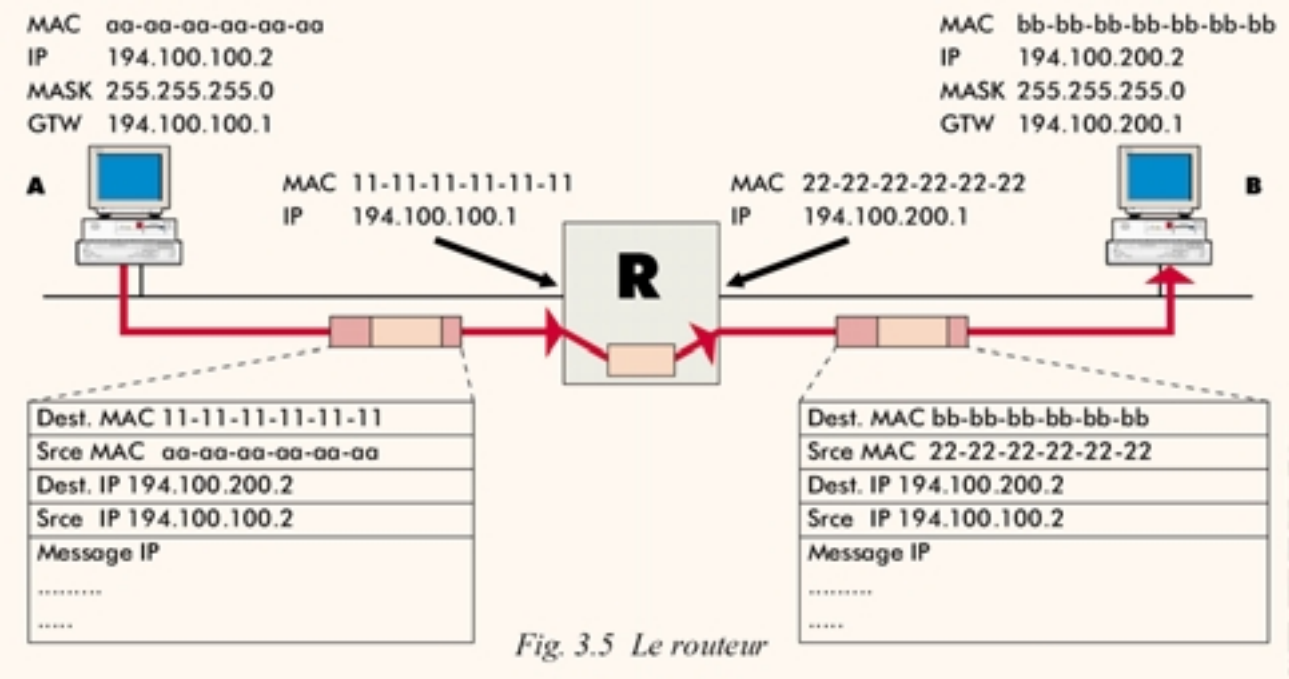

Fig. 3.5 Le routeur

L'avantage du routeur est de séparer les machines au niveau de la couche 2. Le trafic Ethernet interne à l'un des segments ne traversera pas le routeur, c'est-à-dire que les communications ARP entre deux machines qui se trouvent dans le même sous-réseau ne vont pas «polluer» l'autre sous-réseau qui n'est pas concerné. Seule la communication intersegments passera, en s'élevant au niveau de la couche 3.

3.2.7 Le switch

Le switch permet de diviser un segment Ethernet en plusieurs brins distincts et offre ainsi la possibilité à plusieurs stations d'émettre en même temps, tout en restant connectées logiquement au même segment Ethernet. Il construit une table de correspondance adresse-port en lisant les adresses MAC sources, et utilise cette table pour propager les trames reçues. Lorsqu'une trame contient une adresse inconnue ou lorsqu'elle indique une adresse de broadcast, le switch la propage sur tous les ports, afin que toutes les stations puissent la lire. La Figure 3.6 illustre le fonctionnement d'un switch.

Le switch est donc un produit de couche 2, et ne prête aucune attention à l'information transportée dans les trames Ethernet. La présence d'un switch est totalement invisible pour une station. Lorsqu'une station désire envoyer un paquet IP, elle effectuera une requête ARP. Le switch propagera cette requête sur tous les brins (broadcast). La réponse traversera à nouveau le switch, et la communication commencera entre les deux stations. Les quatre adresses utilisées seront à nouveau celles des deux stations concernées. Pour plus de détails, voir FI-6/1998.

Avec un switch, quatre stations ou plus peuvent communiquer simultanément sur le même segment Ethernet. Ainsi, le problème de partage du média et la limite de taille sur les réseaux sont enfin résolus.

3.2.8 Le routing switch ou commutation IP

Le routing switch, ou layer 3 switch ou encore la commutation IP, a été conçu pour offrir les mêmes performances en termes de débit et de temps de latence qu'un switch, mais au niveau 3 du modèle OSI. En d'autres termes, il ne s'agit plus d'extraire le paquet IP et de le router, mais bien de le commuter. La Figure 7 met en évidence les principes de fonctionnement d'un routing switch.

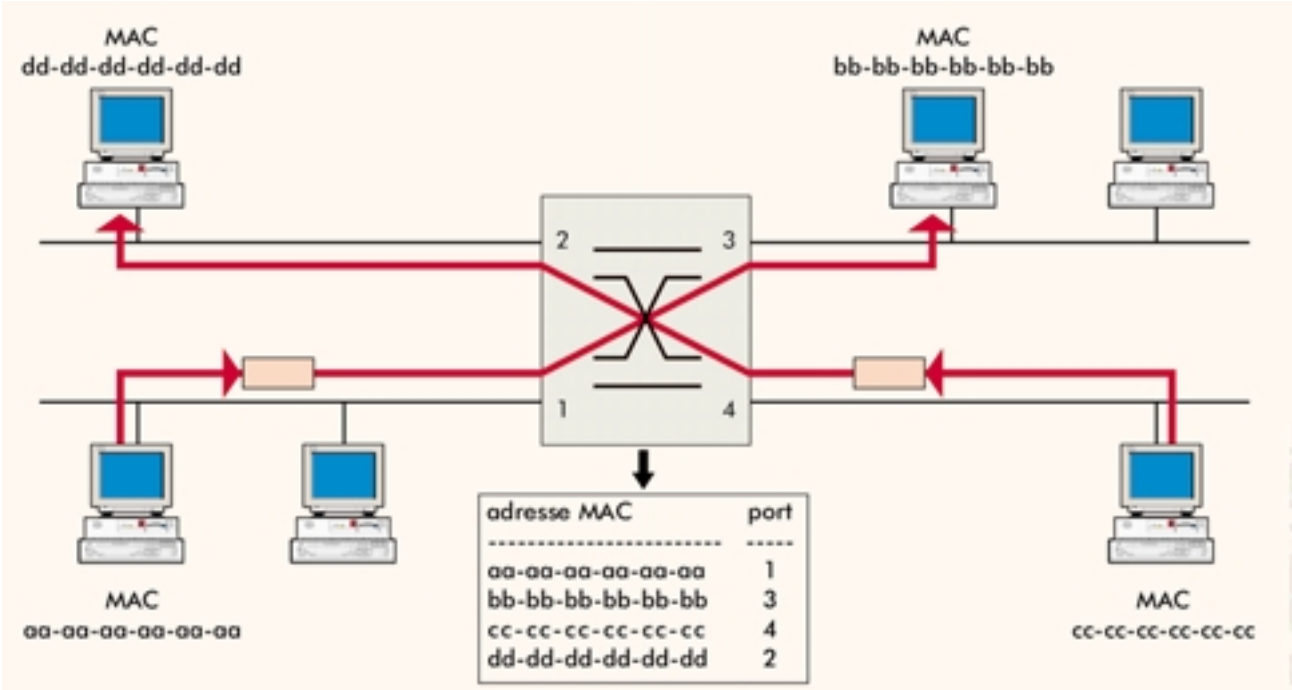

Fig. 3.6 Le switch

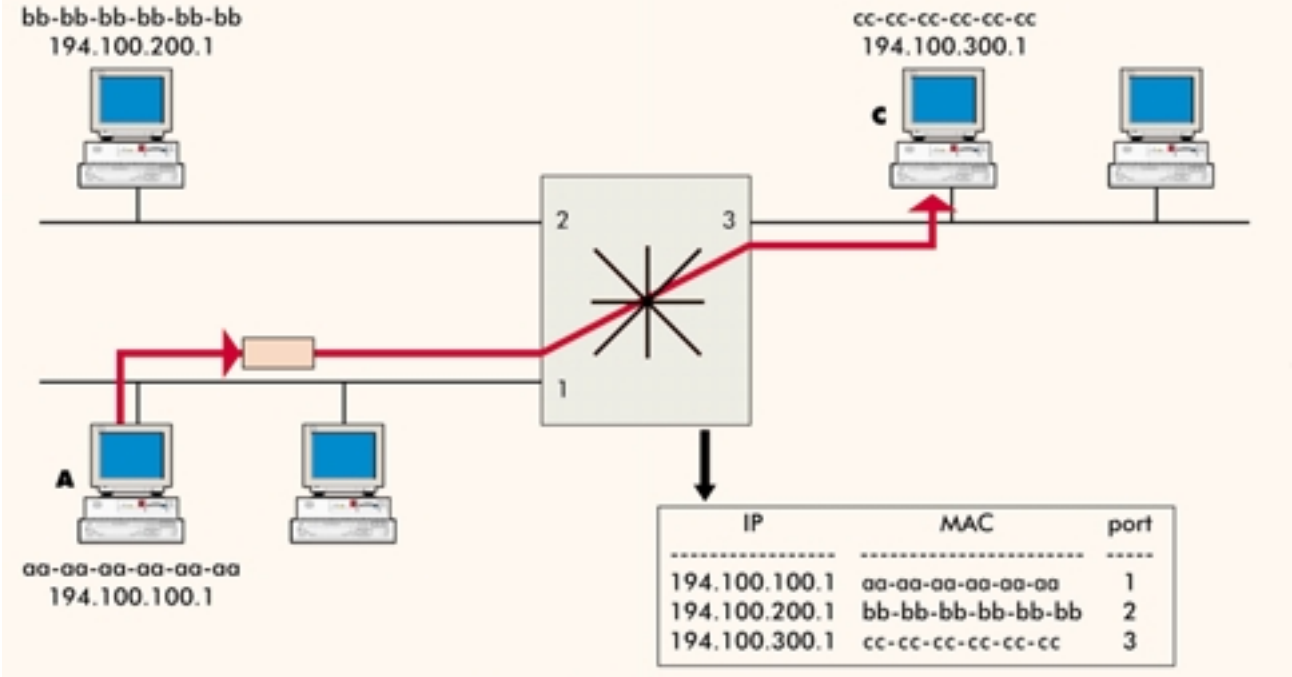

Fig. 3.7 Le routing switch

On a vu au paragraphe 3.2.6 qu'un routeur possède une table de routage faisant correspondre des adresses IP à des ports et au paragraphe 3.2.7 qu'un switch fait correspondre des adresses MAC à des ports. Le routing switch construit et maintient une table qui associe l'adresse IP d'une station, son adresse MAC et le port auquel elle est connectée. La décision de propagation d'une trame est prise en fonction de l'adresse IP de destination.

En nous basant sur la configuration présentée par la Figure 3.5, on se rend compte que le routeur a été remplacé par le routing switch dans la Figure 3.7. Les stations ont reçu comme masque de sous-réseau, la valeur 255.255.255.0, et comme passerelle par défaut, l'adresse de l'interface du routing switch à laquelle elles sont connectées. Le routing switch est donc vu comme le routeur par défaut et assumera cette charge.

Si la station A veut communiquer avec la station C, elle compare les deux adresses IP et envoie une trame à son routeur par défaut, en utilisant l'adresse MAC du routing switch. Lorsque le routing switch reçoit cette trame, il lit l'adresse IP de destination, qui correspond effectivement à la station C. Il cherche alors une correspondance dans la table, et découvre que l'adresse 194.100.300.1 de la station C est atteignable par le port 3, et que l'adresse MAC correspondante est cc-cc-cc-cc-cc-cc-cc.

Le routing switch modifie alors l'adresse MAC de destination de la trame (cette adresse était celle de sa propre interface), et la commute sur le port 3, aussi vite que l'aurait fait un switch de couche 2. Le routing switch prend donc ses décisions de routage en se basant sur les adresses de couche 3, mais fonctionne en utilisant les mêmes principes de commutation qu'un switch Ethernet. (*Source: FI-6/1998*)

3.2.9 Connexion internationale et architecture générale

Le choix de la connexion au backbone de l'opérateur international (MCI, SPRINT, CompuServe, UUNET, AT&T WorldN, Concert Internet Plus, etc.) doit être guidé par la qualité de service et la topologie de son réseau et celui de ses partenaires. Un opérateur au niveau national, voire même régional, a un large choix de la bande passante suivant ses besoins et sa stratégie de développement.

Tableau 3.2 – Bandes passantes typiques

56/64 kbit/s	448/512 kbit/s	6 Mbit/s
112/128 kbit/s	560/640 kbit/s	12 Mbit/s
224/256 kbit/s	672/768 kbit/s	45 Mbit/s
336/384 kbit/s	1 244/1 544 Mbit/s	

Le choix idéal pour la bande passante serait de 1,2/1,5 Mbit/s (uplink/downlink) pour un opérateur qui prévoit un nombre d'abonnés de l'ordre de quelques dizaines de milliers qui utiliseraient le World Wide Web, l'E-mail, les news groups, le FTP, etc.

La Figure 3.8 illustre un schéma de l'architecture générale d'un réseau national Internet maillé, caractérisé par la redondance des équipements. En l'occurrence, nous avons représenté deux nœuds nationaux Internet, avec une possibilité pour l'opérateur national d'Internet de choisir sa connexion chez un ou plusieurs opérateurs internationaux avec une marge de sécurité suffisante.

La topologie représentée dans ce paragraphe constitue un modèle pour une planification à moyen et à long terme. Les ingénieurs chargés de la planification et du développement du réseau l'adapteront en tenant compte du contexte national et régional en intégrant les éléments exposés dans le chapitre 5 de ce guide, «Stratégies et développement du réseau Internet».

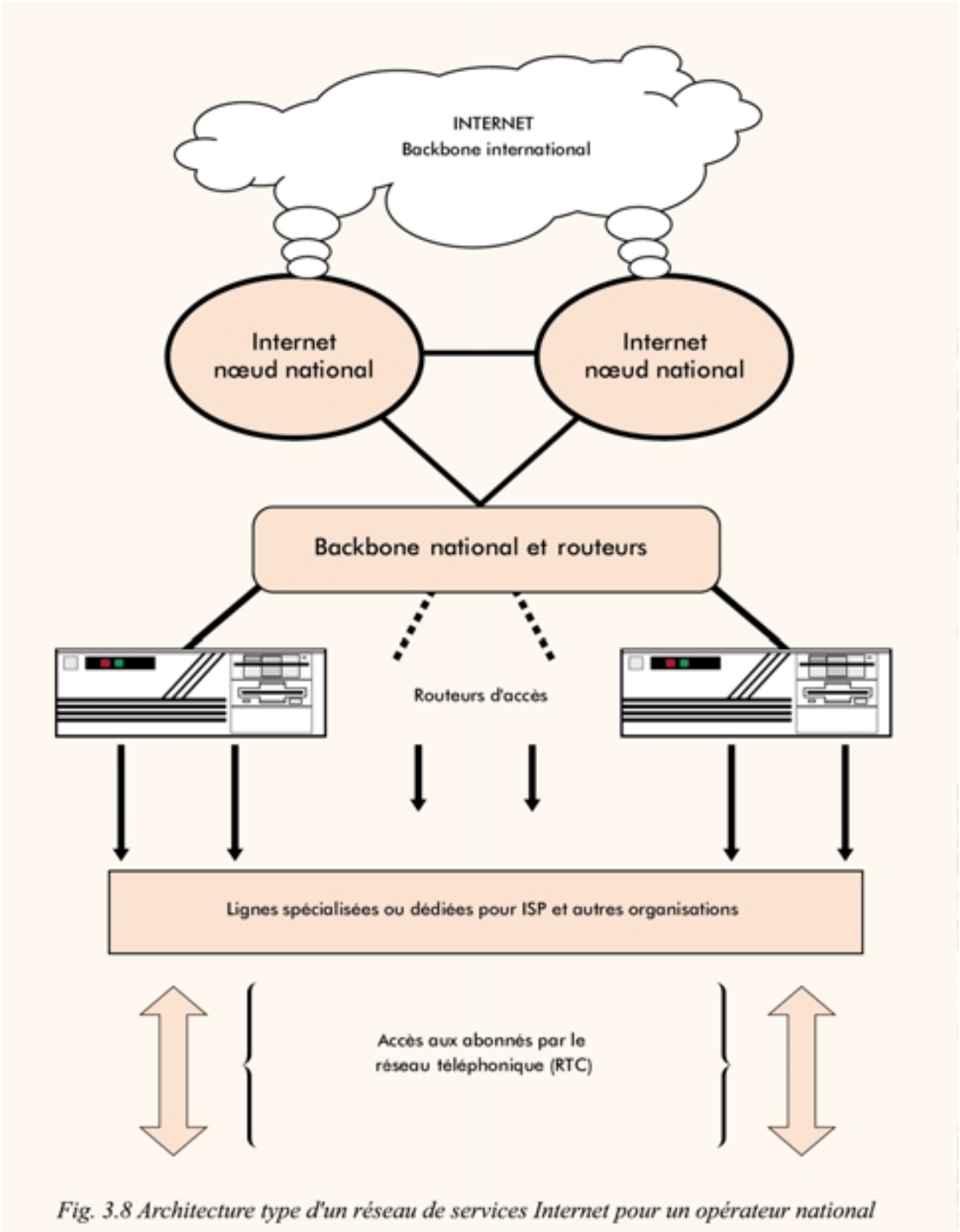

Fig. 3.8 Architecture type d'un réseau de services Internet pour un opérateur national

3.3 Equipements de base d'un nœud national pour Internet

3.3.1 Généralités

Les technologies d'accès dont nous venons de décrire sont très importantes pour le développement d'Internet et particulièrement en Afrique où le retard en connectique se creuse de plus en plus, soit 0,4% de serveurs en Afrique contre 65,6% en Amérique, 24,3% en Europe, 7,3% en Asie et 2,4% en Océanie (*Source: UIT World Telecommunication Indicators Database*). La technologie du routing switch bien qu'elle soit encore jeune devrait être intégrée dans toute stratégie de planification et développement du réseau Internet suivant l'évolution et la topologie du réseau national.

Le domaine où l'on va installer les équipements du nœud national pour Internet doit être très bien protégé, et on doit assurer une sécurité sans faille à tous les niveaux sans oublier les risques liés aux incendies.

3.3.2 Topologie de base d'un nœud national pour Internet

3.3.2.1 Liaison satellite

Avec un satellite en orbite géostationnaire, c'est-à-dire sur l'équateur, à une altitude de 36 000 km, on peut réaliser la transmission de données sur Internet par faisceaux hertziens et 3 satellites suffisent pour couvrir la Terre.

Le transpondeur est un élément essentiel d'un satellite et constitue l'ensemble réception/retransmission du signal (uplink/downlink) installé à bord. Il comprend une antenne de réception, un amplificateur à faible bruit, un filtre, un amplificateur de puissance pour l'émission et une antenne d'émission.

La puissance d'émission du transpondeur dépend de la largeur du faiseau d'émission qui est lui-même dépendant de l'antenne: plus on veut une diffusion large, plus il faut de la puissance. Pour la transmission des données sur un backbone confortable, on peut généralement utiliser des canaux à 2 Mbit/s. Les fréquences uplink et downlink sont différentes et espacées de 3 MHz environ.

On peut avoir une bonne bande passante avec la solution par liaisons satellite qui est la plus adaptée aux pays Africains par manque de développement des liaisons fibre optique qui offrent des temps de propagation plus courts que les liaisons satellite. Les tarifs varient en fonction de l'opérateur, de la bande passante et des relations commerciales déjà établies.

Suivant l'infrastructure et la stratégie de l'opérateur, on peut se connecter au «Backbone» de l'opérateur international de différentes façons. On utilise fréquemment les solutions suivantes:

- Accès satellite point à point ou SCPC (*Single Channel Per Carrier*) à un débit minimal de 128 kbit/s mais d'autres débits sont proposés comme nous l'avons vu dans le paragraphe 3.2.9 (voir Tableau 3.2). Le dimensionnement de l'antenne parabolique est fonction du choix en débit.

- Accès partagé au satellite dit «accès multiple à répartition dans le temps» AMRT ou TDMA (*Time Division Multiple Access* en anglais). Le débit minimal recommandé est de 128 kbit/s.

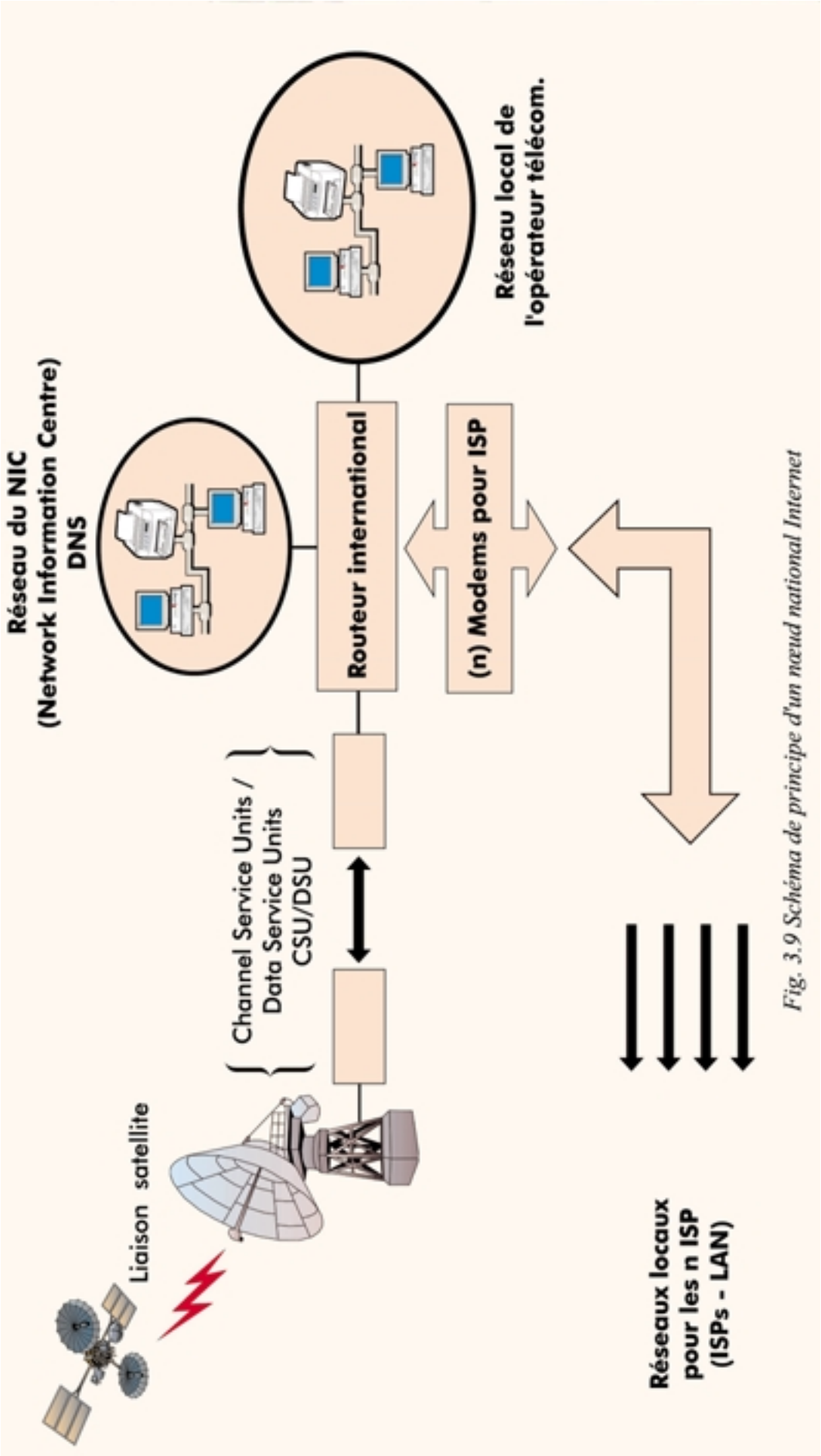

Fig. 3.9 Schéma de principe d'un nœud national Internet

3.3.2.2 Routeur International

Le routeur international est relié à la station terrienne via un adaptateur V35 CSU/DSU (*Channel Service Units/Data Service Units*). Ce routeur doit avoir un port pour connecter le réseau local de l'opérateur télécom, un autre pour la connexion au réseau du NIC (*Network Information Center*) pour le DNS (*Domain Name Server*) et les sauvegardes. Pour connecter les prestataires de services Internet (ISP), il doit avoir également au moins six ports. Lorsque ce routeur reçoit un paquet, il cherche l'adresse du réseau de destination dans la table de routage et l'envoie sur l'interface concernée. Si, dans la table de routage, il n'existe pas cette adresse de destination, il l'envoie vers la route par défaut. L'algorithme de routage implémenté tient compte de tout ou partie des points suivants:

- Optimisation en sélectionnant la meilleure route dans tous les cas. Ceci dépend des Metrics. Par exemple, un algorithme de routage peut utiliser le nombre de Hops et Delay mais peut mettre plus de poids pour le calcul pour le Delay.
- Simplicité et robustesse.
- Rapidité de convergence. La convergence est l'agrément entre tous les routeurs pour déterminer la meilleure route. Lorsqu'un routeur rend ou détecte une route indisponible ou devenant disponible, il informe ses partenaires en distribuant une mise à jour pour les tables de routage.

Pour faciliter le travail du routeur et de l'administration du nœud national d'Internet, on doit diviser le réseau appartenant à une classe d'adresse donnée en sous-réseaux appelés Subnets. Pour limiter le trafic par zone géographique et limiter le taux de «paquets Broadcast», on attribuera alors une partie du champs de l'adresse au numéro du Subnet. Le masque de sous-réseau (ou Subnet Mask) permettra au routeur de déterminer la route des paquets destinés aux machines d'un même sous-réseau. (IPaddr AND Subnet Mask)

Il est possible de forcer une route dans les tables de routage en créant une route spécifique. On parle alors de route statique, par opposition aux routes dynamiques qui sont «apprises» par les protocoles.

La table ARP (*Address Resolution Protocol*) contiendra les paires *adresse IP-Adresse MAC* nécessaires à l'acheminement des paquets sur les segments connectés aux interfaces du routeur. Les paquets issus ou transmis par ce routeur contiendront toujours l'adresse MAC de celui-ci. Les adresses contenues dans la table ARP n'ont pas une durée de vie illimitée. La durée de vie typique est de l'ordre de 240 minutes.

Au niveau de ce routeur, on peut effectuer un filtrage pour certaines adresses, par exemple les adresses MAC ou adresses IP que l'administrateur jugera infréquentable, pour diverses raisons. A titre indicatif, les routeurs le plus souvent utilisés sont de marque Cisco, type Cisco 7513, 7507, 7000, 4500, 2511, 2516, etc.

3.3.2.3 DNS

Parmi les équipements du réseau de l'organisme qui centralise les informations du réseau (le NIC), le DNS (*Domain Name Server*) est très important et nous recommandons, pour cette tâche, un ordinateur avec une configuration minimale de 450 MHz, de 128 Mégas de RAM, 10 Gigas de disque dur, une carte réseau 3COM Etherlink, un lecteur DVD, un lecteur de disquette 3,5 pouces, un écran SVGA de 17 pouces et le système d'exploitation UNIX Solaris 2.x. La même configuration est recommandée pour le secondary DNS server, qui va contenir les données du DNS primaire par redondance. Pour un niveau élevé de sécurité sur les fonctions du DNS, nous recommandons un accès fortement restreint. Il faut éviter toute session Telnet, FTP, HTTP, SMTP, etc., sur la machine.

3.3.2.4 Modems

Pour relier les réseaux des prestataires de services Internet (ISP, *Internet Services Providers*) au nœud national d'Internet, on utilise des modems pour ligne(s) louée(s). Ces lignes ne passent pas par aucun organe de commutation. On parle dans ce cas de lignes spéciales (LS), ligne louée, ligne dédiée ou de ligne point à point. On peut utiliser des amplificateurs logés dans les centraux appartenant à l'opérateur de télécommunication pour atteindre les prestataires de services Internet (ISP) qui seraient éloignés.

Les modems mis en œuvre ont un débit minimal de 64 kbit/s et sont du même type coté nœud national Internet et coté ISP. On a par exemple une paire des modems RAD ASM-20 ou Patton 1090 KiloStream reliés par des connecteurs RJ45.

Un modem (MOdulateur-DEModulateur) est un appareil permettant de transmettre des données sur des lignes destinées au téléphone pour être exploitées par un ordinateur. Un modem dit «intelligent» est capable de s'adapter aux paramètres de l'ordinateur auquel il est connecté et de gérer la transmission sur la ligne cuivre, par exemple pour retransmission en cas d'erreur et la compression des données.

Les modems à basse vitesse (jusqu'à 64 kbit/s) utilisent la transmission dite en «bande de base», ce qui veut dire l'image analogique du signal digital tandis que les modems rapides utilisent les techniques de modulation en quadrature QAM, mais à plus haute fréquence et avec plus de niveaux de modulation que les modems pour ligne commutée à usage privé:

- 64, 128 kbit/s sur 2 fils;
- 256 kbit/s à 2 Mbit/s sur 4 fils.

Tableau 3.3 – Normes et vitesses de transmission

Normes CCITT	Vitesse	Modulation
V21/Bell 103	300 bit/s	FSK
V22/Bell 212a	1 200 bit/s	DPSK
V23	1 200/75 bit/s	DPSK
V22 *bis*	2 400 bit/s	QAM
V32	9 600 bit/s	QAM
V32 *bis*	14 400 bit/s	QAM
V34	28 800 bit/s	QAM
V34+	33 600 bit/s	QAM

3.3.2.5 Alimentation automatique d'énergie électrique

La qualité de l'alimentation en 220 V alternatif des fournisseurs d'énergie électrique n'est pas garantie. Pour cette architecture de base du nœud, il est impératif d'utiliser les onduleurs ou alimentations de secours appelées aussi UPS (*Uninterruptible Power Supply*). Un onduleur pour le routeur international sera nécessaire, un autre pour le DNS et un autre pour le réseau local. Pour les grands réseaux fortement maillés, certains onduleurs équipés d'une interface Ethernet ou Token Ring incluant un agent SNMP sont intégrés au réseau et peuvent être gérés et suivis automatiquement malgré la distance géographique qui les sépare du poste de pilotage du réseau.

3.3.3 Réseau local

Pour le réseau local au niveau de l'opérateur télécom Internet, il faut un routeur qui a au moins deux ports Ethernet dont un qui sert à la connexion au routeur international et un pour relier le réseau Ethernet local protégé par un firewall. Pour les ordinateurs, la configuration minimale recommandée est de 450 MHz, de 128 Mégas de RAM, 512 de Cache, 10 Gigas de disque dur, une carte réseau 3COM Etherlink, un lecteur DVD, un lecteur de disquette 3,5 pouces, un écran SVGA de 17 pouces et le système d'exploitation UNIX Solaris 2.x. On peut utiliser un serveur pour fournir l'E-mail, le World Wide Web, le transfert de fichier. Cependant, pour une meilleure gestion comme on le verra dans la suite, nous recommandons l'utilisation d'une machine par service Internet (Web, E-mail, FTP, News).

Pour l'analyse et la comptabilité pour le trafic, un ordinateur avec une configuration minimale de 450 MHz, de 128 Mégas de RAM, 10 Gigas de disque dur, une carte réseau 3COM Etherlink, un lecteur DVD, un lecteur de disquette 3,5 pouces, un écran SVGA de 17 pouces est suffisant. Le logiciel RADIUS du domaine public peut être utilisé pour l'authentification et la facturation. Pour plus de détails, voir sur Internet à l'adresse suivante: http://www.livingston.com/Forms/radiusform.cgi.

Le serveur de communication doit pouvoir établir 1 000 communications simultanées avec une possibilité d'étendre cette capacité. Il sera modulaire et extensible sans perturbation de service. On peut également accéder à ce réseau via des modems Dial-Up. Le nombre peut varier suivant les besoins et 16 modems, chacun de 33,6 kbit/s V.34 *bis,* montés dans un rack peuvent suffire pour un début ou comme projet pilote.

3.3.4 Prestation des services Internet: solution Netscape SuiteSpot

3.3.4.1 Généralités

Le déploiement de la solution Netscape SuiteSpot sur le LAN (réseau local de l'opérateur télécom national) permet de fournir tous les services Internet comme un ISP traditionnel. Cette solution est simple pour les personnes qui ont une bonne expérience sur Solaris 2.x. L'administration générale du système est très pratique pour les services Internet comme c'est illustré sur la Figure 3.10.

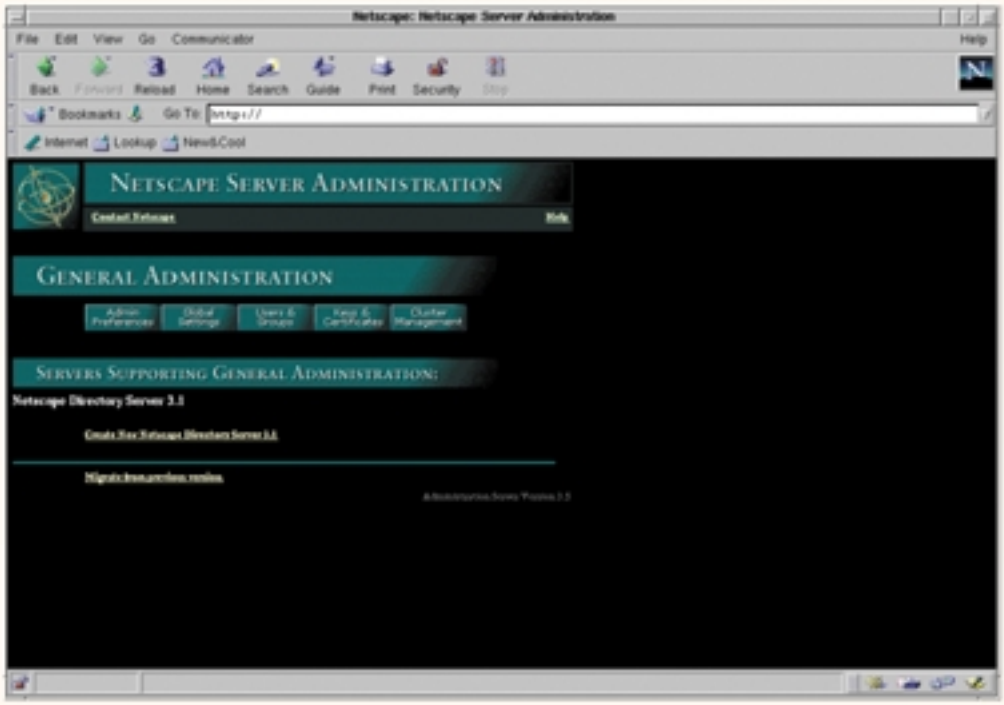

Fig. 3.10 Interface d'administration de Netscape Server

Pour une meilleure gestion et un bon fonctionnement, il est recommandé dans la mesure du possible de réserver pour chaque serveur une machine dédiée. La solution de Microsoft avec «Internet Information Server 4.0» est également intéressante et présente des caractéristiques adaptées. Certains de ses composants, comme Microsoft Certificate Server, peuvent remplacer valablement leurs équivalents de la solution Netscape SuiteSpot. Le choix de la présentation de la solution Netscape SuiteSpot a été dicté par l'actualité: Sun Microsystems, AOL et Netscape ont mis leurs efforts en commun pour dominer le marché des produits Internet. On voit donc très mal comment on peut éviter ce produit sur Internet.

3.3.4.2 Netscape Directory Server

Netscape Directory Server est nécessaire pour constituer un annuaire distribué LDAP (*Lightweight Directory Access Protocol*) qui peut être utilisé pour la messagerie électronique par exemple. A l'installation, l'application se décompose en deux serveurs distincts, dont le serveur Netscape Directory lui-même et un serveur HTTP dit «serveur d'administration» qui sert à l'installation et à la configuration d'autres serveurs de la famille Netscape SuiteSpot.

3.3.4.3 Netscape Certificate Server

Netscape Certificate Server permet de transférer des informations confidentielles et sensibles sur Internet concernant par exemple les applications du commerce électronique. Pour protéger le contenu des transactions de tout détournement ou de toute surveillance, on utilise le cryptage. Les certificats délivrés par Netscape Certificate Server sont conformes à la norme x.509v3, ils sont utilisés par SSL (*Secure Sockets Layer*), une implémentation sécurisée de la couche Transport de TCP/IP du modèle OSI. Ces certificats contiennent comme informations l'identification du propriétaire contenant le nom, l'organisme, l'adresse, etc. Ils contiennent également la clé publique du propriétaire, la période de validité, un numéro de série.

N'importe qui peut faire circuler les informations cryptées sur le réseau Internet. Certains pays ont une réglementation claire, c'est ainsi qu'en France, le cryptage est interdit. Aux Etats-Unis d'Amérique, il est interdit d'exporter des produits cryptés. Avec le développement du commerce électronique, certaines informations sont extrêmement sensibles. D'autres informations, comme celles des institutions gouvernementales, sont d'une importance capitale qu'il faut recourir à la cryptologie.

Les pare-feu (*Firewall*) ne suffisent pas pour garantir la sécurité des données circulant à travers le réseau, destinées au serveur Web ou émises par lui. La technologie du cryptage (ou chiffrement) des données empêche les pirates de lire ou de falsifier les données. Dans l'environnement du Web, le protocole Secure HTTP sert à sécuriser les applications HTTP, tandis que le protocole SSL (*Secure Sockets Layer*) utilise le cryptage pour sécuriser les sessions IP. Les Figures 3.11 et 3.12 représentent les algorithmes de cryptage les plus utilisés.

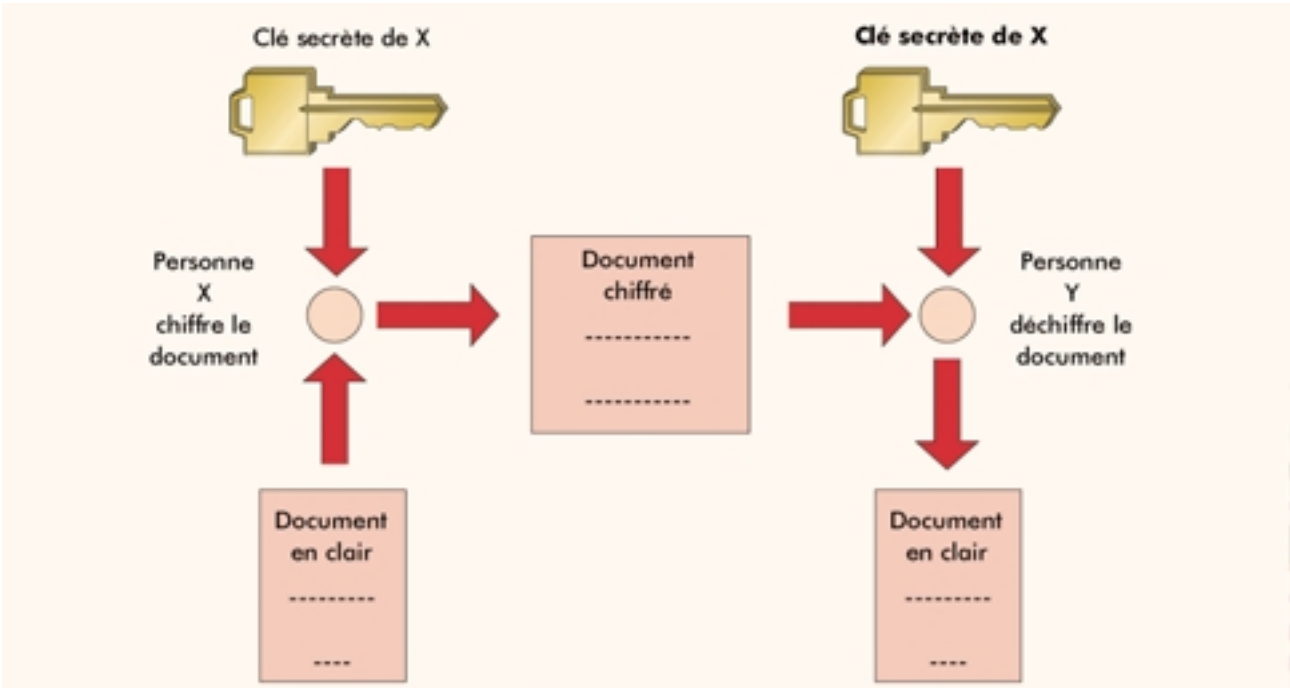

Fig. 3.11 Schéma de principe, cryptage par les algorithmes symétriques

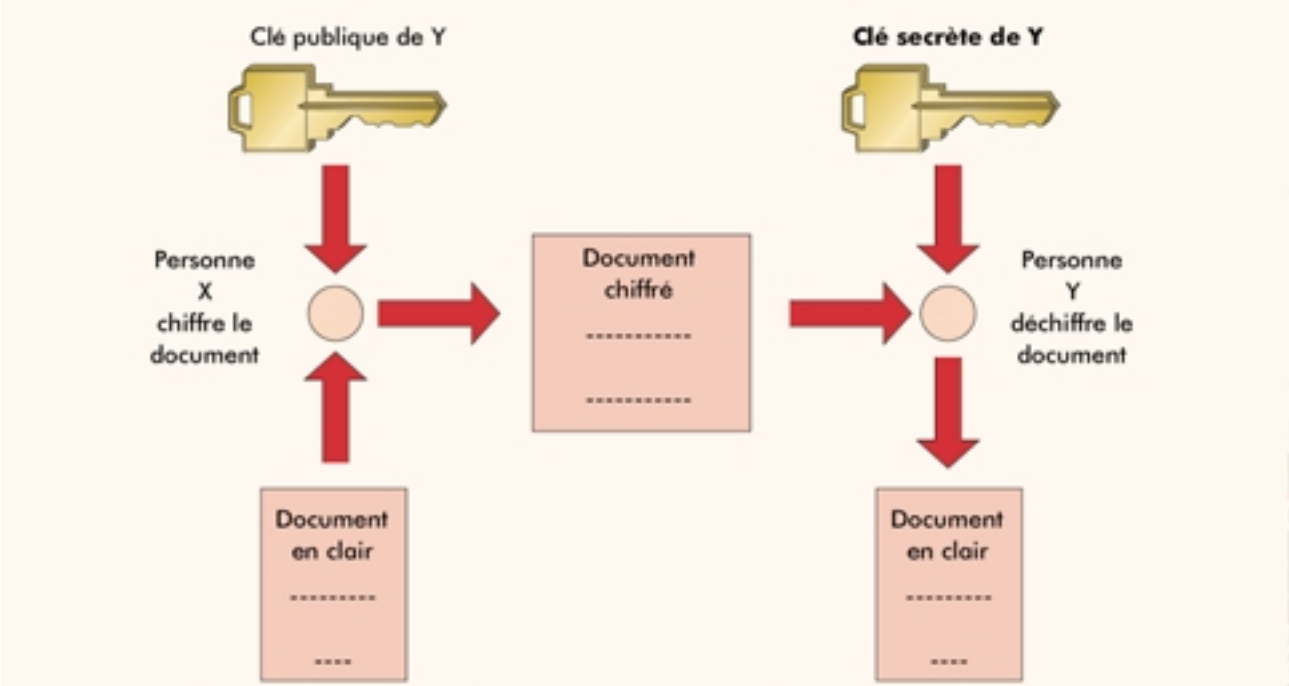

Fig. 3.12 Schéma de principe, cryptage par les algorithmes asymétriques

La plupart des techniques de cryptage utilisent la norme DES (*Data Encryption Standard*). Cet algorithme fut développé en 1975 par IBM. Le principe de base consiste en une clé secrète pour la personne qui code le message et le destinataire décode le message avec la même clé qui a servi pour le codage. Les algorithmes qui utilisent ce principe appartiennent à la famille des algorithmes dits symétriques.

Le problème des algorithmes symétriques est qu'il faut transmettre la clé secrète au destinataire du message codé. La question qui se pose est de comment transmettre cette clé secrète avec sécurité?

Ce problème a été résolu avec l'apparition des algorithmes asymétriques, basés sur l'utilisation de deux clés différentes: l'une est publique et permet le chiffrement, l'autre est secrète et permet de déchiffrer les messages. Chaque utilisateur dispose donc à la fois d'une clé publique (connue de tous, elle peut être disponible dans des annuaires) et d'une clé secrète qui lui est propre. Si un utilisateur veut coder un message, il utilise la clé publique du destinataire et envoie les informations. Celui-ci reçoit le message et le décode grâce à sa clé secrète. Ce concept est appliqué dans l'algorithme RSA (acronyme des noms des concepteurs *Ronald Rivest Adi Shamir* et *Len Adleman*) de Data Security Inc. (http://www.rsa.com/).

Bien que ce système soit plus simple à utiliser qu'un logiciel fondé sur l'algorithme symétrique, il présente néanmoins un inconvénient car, rien n'interdit à un pirate d'entrer sur un annuaire des clés publiques et de substituer sa propre clé publique à celle d'un utilisateur. Lorsqu'un émetteur voudra chiffrer un message avec la clé publique de Y, il utilisera en fait la clé du pirate et celui-ci pourra alors intercepter le message en question et le déchiffrer avec sa propre clé secrète. Il pourra éventuellement le modifier, le chiffrer avec la clé publique de Y (qu'il aurait subtilisée au préalable) et le renvoyer vers le véritable destinataire Y. Celui-ci croira que le message reçu est authentique, alors qu'il aura été falsifié juste avant.

Des mécanismes d'authentification très performants ont donc été développés. Lorsqu'un émetteur désire envoyer un message, il lance au préalable un programme dit de hachage qui, à l'aide de sa clé privée, va créer une image numérique des informations.

Une fois le message transmis et reçu par le destinataire, celui-ci peut déchiffrer cette image grâce à la clé publique de l'émetteur. Si le message a été falsifié entre-temps, les deux documents ne correspondront pas. Si la clé publique a été falsifiée, elle ne pourra pas décoder l'image transmise.

3.3.4.4 Netscape Enterprise Server

A son installation, Netscape Enterprise Server se décompose en trois applications dont le serveur d'administration, le serveur HTTP et le moteur de recherche intégré (ou moteur d'indexation). La version la plus répandue du protocole HTTP est la version 1.0. Il est à noter que cette version présente quelques problèmes qui peuvent provoquer des confusions même chez les ingénieurs les plus expérimentés. C'est le cas de l'utilisation du standard MIME qui est suffisamment proche de celle de HTTP tout en étant suffisamment différente. La fermeture de la connexion après chaque document provoque la perte des informations de congestion et l'ouverture de plusieurs connexions simultanées accélère l'affichage d'un document mais congestionne le serveur avec des ouvertures simultanées. La version 1.1 de HTTP va corriger ces défauts que nous n'avons pas pu énumérer tous ici, elle va améliorer les performances tout en restant compatible avec la version 1.0.

3.3.4.5 Netscape Messaging Server

Netscape Messaging Server utilise la même version du serveur d'administration qu'Enterprise Server, il n'est donc pas nécessaire d'installer deux fois ce dernier. Ce serveur de messagerie utilise deux répertoires pour conserver les fichiers, à savoir /var/spool/mailbox pour les mails reçus par les utilisateurs et /var/spool/postoffice pour les mails en instance (départ) et les fichiers de configuration. Le courrier adressé au postmaster est retransmis à un utilisateur chargé de le gérer. Le courrier adressé aux utilisateurs locaux de la machine sur laquelle tourne le serveur est conservé comme d'habitude sous /var/mail. Il n'y a pas de numéro de port à préciser lors de l'installation, car il est impossible de modifier le port par défaut (le port 25) utilisé pour le protocole SMTP, puisque le serveur de messagerie fait partie d'un ensemble de serveurs qui s'attendent à le trouver à ce port.

3.3.4.6 Netscape Collabra Server

Internet favorise le travail de groupe et Netscape Collabra Server est l'outil nécessaire pour gérer les forums (News) et pour faciliter le travail du modérateur. Les forums sont fondés sur le protocole NNTP (*Network News Transfer Protocol*), qui est à la fois un protocole distribué d'échange d'information entre serveurs, et le protocole client-serveur utilisé pour la consultation des articles. Collabra Server utilise la même version du serveur d'administration qu'Enterprise Server. Le numéro de port par défaut pour le protocole NNTP est 119. Il peut être changé, mais c'est un risque, surtout si ce serveur doit s'intégrer dans une chaîne de serveurs.

3.3.4.7 Netscape Proxy Server

Netscape Proxy Server est un serveur proxy comme tant d'autres. Il s'exécute principalement sur un système firewall qui fournit un accès contrôlé et une protection par rapport au monde extérieur. Dans une telle topologie, les browsers doivent être configurés de telle sorte qu'ils utilisent le serveur proxy pour gérer leurs requêtes. Du point de vue du serveur cible, toutes les requêtes reçues sont perçues comme provenant du serveur proxy, et non du client (utilisateur) d'origine.

Comme les requêtes des clients sont dans ce cas acheminées via le serveur proxy, il est logique de mettre en œuvre le cache sur le même serveur. Le principe de fonctionnement est très simple. Une machine est configurée pour recevoir les requêtes qui proviennent de l'intérieur du réseau national et qui demandent des informations sur le Web à l'extérieur du domaine. Cette machine examine si le document a été demandé précédemment. Si le document demandé se trouve déjà sur la machine cache, une mini-requête est envoyée vers le serveur où il est censé résider, pour savoir s'il a été modifié entre-temps. En cas de modification, on va rechercher ce document et c'est cette nouvelle version qui sera gardée à son tour sur la machine cache; sinon c'est la page stockée sur la machine cache qui est envoyée au client Web. Si c'est la première fois que cette page est demandée, la requête est envoyée à l'extérieur, on se retrouve dans le cas classique; mais le document est stocké sur la machine cache en vue d'éventuelles requêtes ultérieures.

On peut avoir une architecture en cascade «parent-enfant» en recommadant à tous les prestataires de services Internet et d'autres institutions d'adopter la même stratégie. Dans ce cas, les requêtes n'ayant pas pu être satisfaites par un cache le seront par des caches voisins. Le gain sur le trafic extérieur à chaque réseau et sous-réseau est très important et des économies importantes seront effectuées. Et la qualité de service va s'améliorer.

Il est très important de ne pas confondre le cache dont il est question ici avec les possibilités qu'offrent les navigateurs comme Internet Explorer et Netscape d'utiliser un cache au niveau local sur la machine: ce cache est sur le disque et il est configuré avec Nestcape 4.xx comme suit: Allez sur «Edition» et choisissez «Préférences». Sous «Avancé», cliquez sur «Serveur proxy» puis sur «Configuration automatique du proxy» ou configuration manuelle du proxy. Avec Internet Explorer 4.xx, il faut aller sur «Affichage (View)» et choisir «Options Internet» puis cliquer sur connexion. Remplir les champs et cliquer ensuite sur le bouton «Avancé» et remplir les champs selon la manière prévue par l'opérateur local. Les fichiers de type scripts (cgi-bin) ne sont pas stockés. Les documents demandés par le protocole FTP depuis une page Web sont stockés. La gestion de l'espace cache se fait selon le principe suivant: c'est le document dont l'accès est le plus ancien qui disparaît le premier.

D'autres solutions alternatives à Netscape Proxy Server existent comme Squid. Pour plus de détails, consulter la home page de Squid à l'URL http://www.nlanr.net/Squid/. La version commerciale du cache Harvest peut également être utilisée. La Figure 3.13 illustre le principe de fonctionnement d'un serveur proxy.

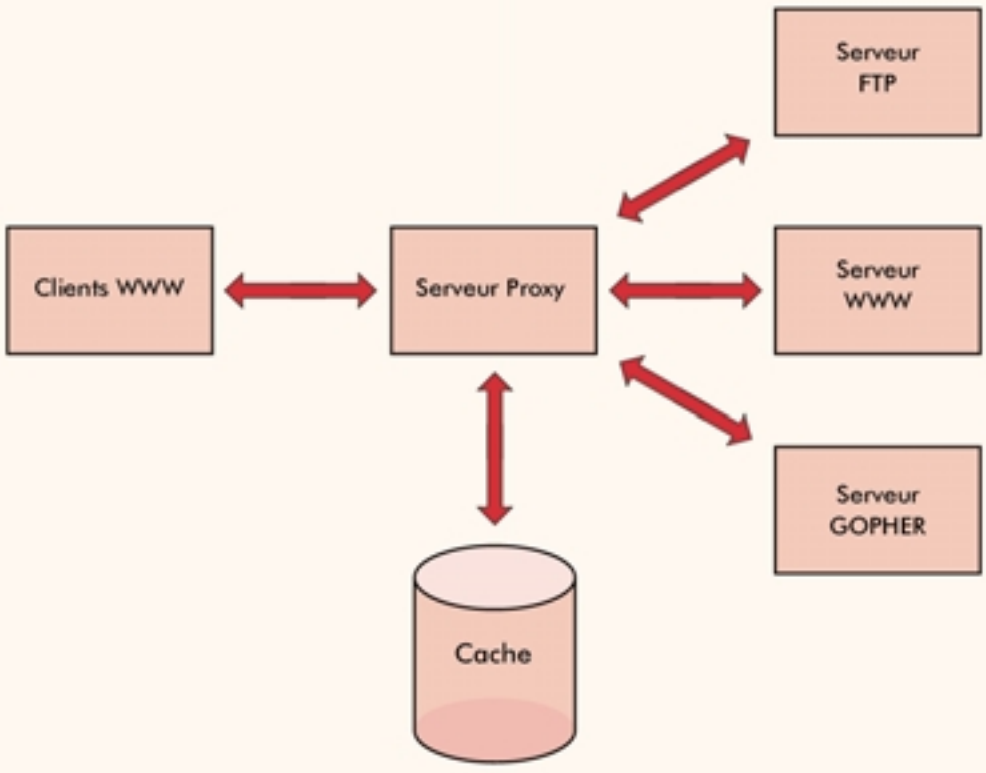

Fig. 3.13 Schéma de principe d'un serveur Proxy

4 Ingénierie des services Internet et maintenance

4.1 Généralités

Avec le développement du commerce électronique, de la télémédecine, du télé-enseignement et les applications en temps réel sur Internet (Bourse électronique ou les enchères électroniques), l'Afrique a une chance à saisir pour son développement général en concentrant toutes les énergies et les capacités humaines nécessaires pour développer Internet, l'invention de ce siècle.

Internet ne peut pas se développer en Afrique si les exigences de qualité de service (*QoS: Quality of Service*) ne sont pas prises en compte dans toutes les étapes d'un tel projet. Les exigences nécessaires pour une recherche de la qualité totale doivent être menées et mises en avant par l'organe de gestion.

L'ingénierie des services Internet s'occupe en général de mesurer, analyser le trafic, contrôler les congestions sur le réseau d'un opérateur. Le trafic sur Internet va être l'enjeu du 21e siècle et tout le monde est concerné. Il est donc important de bien le gérer, car les enjeux économiques seront immenses, quand on sait qu'en 1998, le tarif était d'environ 100 $US/Gbyte pour le trafic entrant (*Source: SWITCH-Internet*). L'ingénierie des services Internet permettra la planification, de détecter les problèmes et d'établir des qualités de service différentes sur Internet et, par conséquent, de facturer différemment les services demandant une qualité supérieure.

4.2 Gestion des réseaux et qualité de service Internet

4.2.1 Généralités

La gestion technique du réseau Internet est basée essentiellement sur le protocole SNMP (*Simple Network Management Protocol*) et à la gestion par WWW ainsi que sur un savoir-faire dans le domaine de hautes technologies.

La gestion des appareils de réseau est assurée essentiellement par un ensemble réduit d'ordinateurs installés au nœud national d'Internet qui pilote plusieurs hubs, routeurs, bridges et autres switches, ainsi que l'accès par les modems pour lignes commutées.

4.2.2 Principaux moyens de gestion

Il existe plusieurs plates-formes de gestion dont OpenView, produit du constructeur HP. OPTIVITY de Bay Networks permet de gérer les hubs, switches de ce constructeur, ainsi que les routeurs Cisco qui dominent le marché d'Internet. D'autres plates-formes de management UNIX comme SunNet Manager, ISM (*Integrated System Management*) de Bull et SystemView d'IBM gèrent aussi le matériel de réseau. INTERCONNECT MANAGER de Hewlett-Packard gère les hubs HP et WEBMANAGE de Tribelink assure la gestion des modems 28,8 kbit/s (PPP).

Au sein de chaque agent SNMP, il y aura une base d'information MIB (*Management Information Base*) du câblage des sites et des équipements raccordés au nœud national d'Internet.

Le RMON (*Remote Monitoring*) permet d'accéder aux mesures d'une sonde qui collecte les paquets pour en faire des statistiques. On a ainsi la possibilité de voir la collection des mesures à la demande de la station de management. Certains processeurs de management de hub font office de sonde RMON.

4.2.3 Autres moyens de gestion intégrés au système

Une détection de défaillances n'est possible et efficace que quand les informations collectées sont claires, classées et accessibles aux personnes habilitées à le faire. Certains outils de diagnostic sont intégrés au système UNIX et d'autres sont gratuits et disponibles sur Internet (voir RFC 1147). La détection des défaillances peut se faire essentiellement par:

ifconfig: Détection des mauvaises adresses IP, des masques de sous-réseau incorrects ainsi que des adresses de diffusion erronées. Cet outil fait partie du sytème UNIX.

arp: Détecte les systèmes connectés au réseau local qui sont configurés avec l'adresse IP incorrecte. Il fournit les informations concernant la conversion des adresses Ethernet/IP. Arp fait partie intégrante d'UNIX.

netstat: Sert à afficher des statistiques détaillées à chaque interface réseau. Il fournit diverses informations.

ping: Permet d'envoyer répétitivement des paquets à un nœud du réseau selon le protocole ICMP. Celui-ci renvoie un paquet en écho et indique si le système peut atteindre un hôte à distance. Ping affiche aussi les statistiques concernant la perte de paquets et la durée de la transmission.

nslookup: Fournit les informations concernant le service noms DNS. Il joue le même rôle que dig.

traceroute: Indique sur quelle voie les paquets ont été acheminés entre deux systèmes distants par ICMP. On mesure ainsi le taux de succès des échanges TRACEROUTE qui donne une trace du chemin parcouru par le paquet, ainsi que les temps de transit pour chaque nœud du parcours.

etherfind: Cet outil analyse les différents paquets transmis entre les hôtes d'un réseau. Etherfind est un analyseur de protocole TCP/IP qui examine les paquets jusqu'à leurs en-têtes.

4.2.4 Principaux indicateurs de gestion

Un administrateur réseau doit construire l'historique de son réseau. En comprenant le passé, il pourra être capable de prédire le futur, dans une certaine mesure. Construire un profil de référence du réseau, c'est mesurer et enregistrer l'état opérationnel de son réseau sur une période donnée et les mesures effectuées serviront ensuite de base de comparaison. Ainsi, l'administrateur réseau pourra définir «les conditions normales» d'exploitation du réseau en se basant sur l'inventaire de son réseau et établir par exemple un premier profil sur une semaine, repérer «les périodes critiques», «les périodes d'utilisation importante», «les erreurs», etc. Il déterminera ce qui est acceptable ou inacceptable, compte tenu du contexte national.

Un profil de charge correctement défini doit permettre ensuite de repérer les changements significatifs dans le comportement du réseau lors de l'analyse quotidienne des résultats, ainsi que de prévoir le comportement sous une charge donnée ou anticiper des problèmes créés par l'introduction de nouveaux services.

Les indicateurs les plus pertinents pour gérer et analyser le trafic sur un réseau sont les suivants:

- *l'utilisation du réseau:* charge (en entrée, en sortie), pics d'utilisation;
- *les nœuds du réseau:* les dix machines les plus consommatrices. L'expérience montre que 10% seulement des nœuds d'un réseau engendre 90% du trafic. Il convient ensuite d'affiner l'étude de ces machines (quelles applications? combien d'utilisateurs? etc.);
- *bande passante ou débit maximal:* taux de transfert maximal pouvant être maintenu entre deux points terminaux;
- *les applications ou services:* identifier les cinq ou six services qui consomment la quasi-totalité de la bande passante (Web, News, sauvegardes);
- *les statistiques d'erreurs:* collisions, perte de paquets;
- *le délai de transit par paquet:* entre deux points distants est la caractéristique principale de la QoS. Le délai est le temps écoulé entre l'envoi d'un paquet par un émetteur et sa réception par le destinataire. Le délai tient compte du délai de propagation le long du chemin et du délai de transmission induit par la mise en file d'attente des paquets dans les systèmes intermédiaires;

- *gigue:* variation du délai de bout en bout;
- *disponibilité:* taux moyen d'erreurs d'une liaison.

Pour plus de détails concernant la qualité de service Internet, nous conseillons les documents suivants: «*Quality of Service: delivering QoS on the Internet and in Corporate Networks*» de Paul Ferguson et Geoff Huston, Wiley Computer Publishing, 1998 et «*Quality of Service: Fact, Fiction or Compromise?*» de Paul Ferguson et Geoff Huston, INET 98, juillet 1998.

4.2.5 Simple Network Management Protocol

Le protocole SNMP (*Simple Network Management Protocol*) définit le dialogue entre une station de contrôle et un nœud du réseau. Il permet de connaître l'état d'un appareil sur le réseau (hub, switch, routeur, etc.) et de gérer les événements exceptionnels. Il permet également la mesure du trafic et des erreurs à distance. Il facilite la configuration d'appareils à distance. La station de management peut être un PC, un Mac ou une station UNIX.

Le logiciel HP OpenView du constructeur Hewlett Packard est basé sur les requêtes utilisant le protocole SNMP (*Simple Network Management Protocol*) pour permettre la gestion des nœuds d'un réseau. La représentation est graphique et l'utilisateur a le choix de dessiner lui-même le plan de son réseau en plaçant uniquement les icônes des appareils qu'il juge utile de gérer ou d'utiliser l'option Auto-discovery qui va interroger tous les subnets d'un LAN et dessiner une carte des objets répondant à SNMP.

HP (*OpenView*) permet la représentation par icônes des différents éléments actifs d'un réseau qui répondent aux requêtes SNMP. OpenView est organisé en une série de «Maps et Submaps» qui constituent une hiérarchie de cartes du réseau Internet jusqu'au poste de travail de l'utilisateur. HP (*OpenView*) est constitué d'une plate-forme gérant la partie standard de SNMP et installée sous UNIX, Windows 95 ou Windows NT. Pour pouvoir représenter des nœuds spécifiques (routeurs, switchs, hubs, etc.) et leurs particularités de fonctionnement, ainsi que leur aspect graphique, on utilise la partie étendue de la MIB (*Management Information Base*), base de données du câblage des sites et des équipements raccordés au réseau.

Deux produits, Interconnect Manager de HP et Optivity de Bay Networks utilisent cette même plate-forme HP (*OpenView*) pour gérer leurs produits spécifiques.

Le logiciel de gestion de réseau OPTIVITY est un programme de gestion des appareils de BayNetworks. Optivity est construit sur une plate-forme SNMP HP (*OpenView*). Il permet, outre la gestion d'événements exceptionnels, d'effectuer des mesures de trafic et d'erreurs du réseau. Un des avantages de ce produit est l'usage des graphes qui mesurent le trafic traversant la totalité d'un hub ou d'un port en particulier. De même, on peut procéder à des mesures d'erreurs qui permettent d'identifier le nœud du réseau qui est à l'origine des perturbations. Un autre aspect intéressant de ce produit est la possibilité d'action à distance sur un équipement. On peut établir une connexion Telnet pour configurer un bridge, un serveur de terminaux ou un routeur, en sélectionnant l'icône de l'appareil considéré. On peut effectuer un Ping sur n'importe quel nœud du réseau qui répond au protocole ICMP. Il est possible également de couper un port d'un hub depuis la station de management pour isoler un nœud.

La fonction *Set Threshold* permet de définir des seuils de trafic ou d'erreurs qui auront pour effet, s'ils sont atteints, d'envoyer un message à la station de management et, si on le désire, une fonction automatique sera activée par le processeur du hub, comme la partition d'un port qui a dépassé le niveau d'erreurs défini.

En installant le programme Carbon Copy sur la station OPTIVITY, ainsi qu'un modem sur une ligne téléphonique, il est possible de prendre à distance le contrôle de la station de gestion avec un ordinateur portable connecté à un autre modem. La tendance dans le domaine de la gestion des réseaux est l'utilisation des logiciels de gestion par le Web.

4.3 Métrologie et analyse du trafic Internet

4.3.1 Généralités

En général et pour des raisons principalement économiques, aucune exploitation des services Internet ne peut être rentable sans réaliser des mesures et une analyse de trafic fiables. La métrologie entre en force dans le domaine Internet et plusieurs produits sur le marché, certains du domaine public, permettent de mesurer et d'analyser le trafic.

C'est ainsi que le logiciel NNSTAT installé sur une station UNIX permet de mesurer le trafic entrant (payant) et sortant du réseau. On capturera ainsi les paires d'adresses source/destination au niveau IP, ce qui permet de quantifier le trafic de chaque partenaire connecté au nœud national d'Internet (trafic entrant vers tel hôpital, vers les institutions universitaires et gouvernementales, etc.).

Ce logiciel est du domaine public et peut être téléchargé par FTP à partir du site:
ftp://gatekeeper.dec.com/pub/DEC/net/NNstat_3.3beta.tar.Z

Le logiciel Optivity de Bay Networks utilise la plate-forme HP OpenView pour gérer leurs produits spécifiques mais aussi pour effectuer des mesures de trafic et d'erreurs du réseau. D'autres logiciels comme IP Trafic (http://www.urec.cnrs.fr/IPtrafic/), NetraMet (*Network traffic Meter*) ou MRTG (*The Multi Router Traffic Grapher*) (http://www.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg.html) peuvent également être utilisés.

4.3.2 Principe de fonctionnement

Les fabricants des routeurs mettent à disposition de leurs clients des systèmes comme Netflow de Cisco. La collecte des informations sur le trafic est réalisée à partir des tables de flux établies par le routeur principal qui relie le réseau national aux sites externes. Cette technique permet d'assurer la véracité de la mesure de trafic pour des couples adresse-source/adresse-destination par type et port IP. Comme seules les adresses IP sont connues, il faut constituer une correspondance entre les noms des institutions et les adresses IP respectives pour réaliser les graphiques.

Les informations sont d'abord collectées de manière continue et formatées dans un fichier qui contient tout ce qu'il faut pour établir des statistiques détaillées. Ces informations servent à enrichir une base de données. Un traitement permet ensuite de générer toutes les images du trafic afin qu'elles soient disponibles en temps voulu avec un accès instantané.

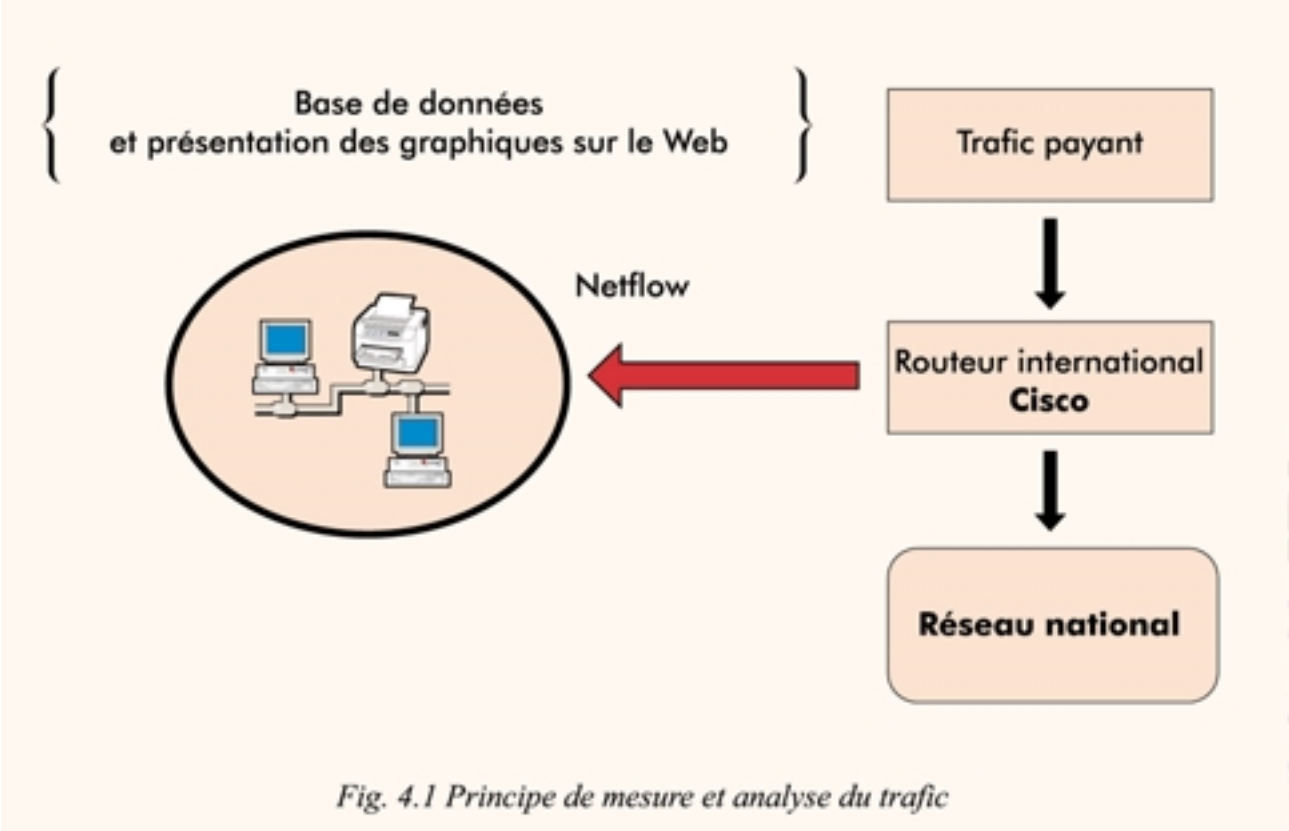

Fig. 4.1 Principe de mesure et analyse du trafic

Sur la Figure 4.2, nous avons les différentes composantes du trafic typique d'une grande institution (*Source: SWITCH-Internet*).

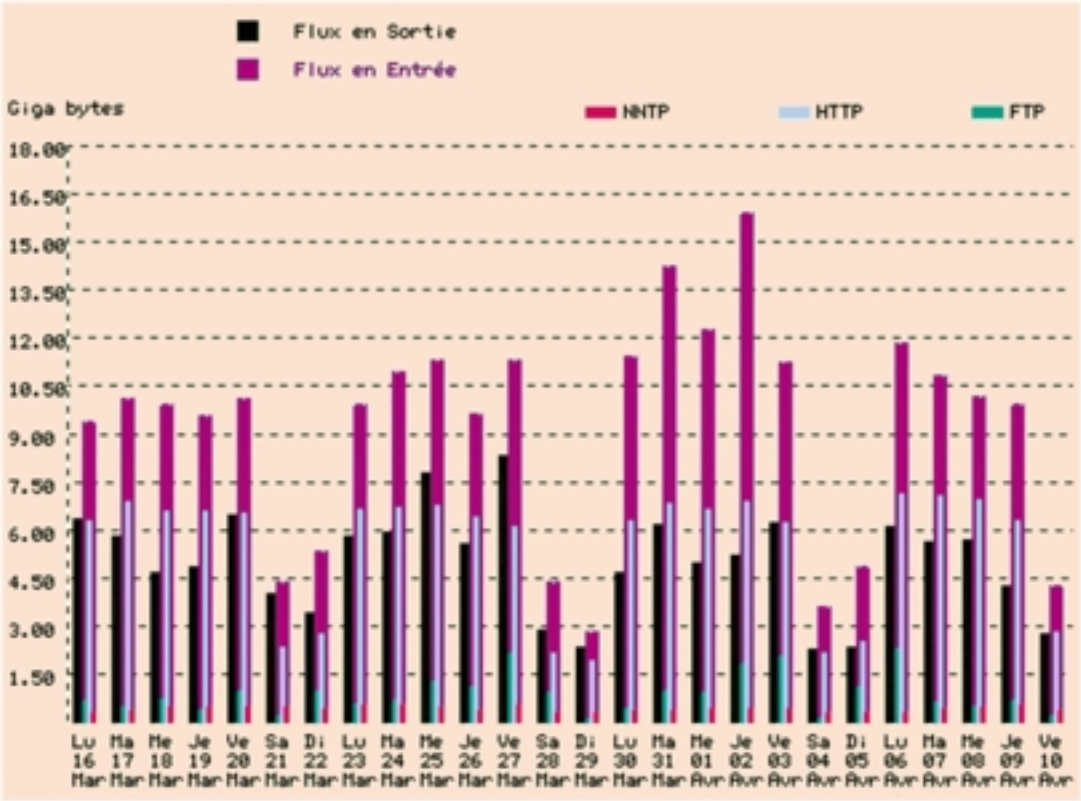

Fig. 4.2 Composantes d'une analyse du trafic Internet

4.4 Sécurité du système

4.4.1 Généralités

La plupart du temps, les risques en matière de gestion de réseau et traitement de l'information sont de trois sortes à savoir: les accès non autorisés, la divulgation d'informations et le service non assuré par un mauvais fonctionnement du système. Il est donc impératif d'évaluer les risques et d'analyser le niveau de confidentialité des informations que l'on traite et que l'on veut faire passer sur Internet. Les effractions sont d'une extrême gravité puisqu'elles entraîneraient la perte de confiance et de la sécurité. Il faut noter que les organismes gouvernementaux, les universités, les banques sont les plus visés par les intrus.

4.4.2 Audit et sécurité des réseaux

Les principaux fournisseurs de logiciels d'audit sont: CISCO, BULL, CHECKPOINT, DIGITAL, ISS, MATRANET, SECURITY DYNAMICS, SOLSOFT. Parmi les logiciels d'audit, il en existe qui sont gratuits comme:

- COPS qui permet de faire un audit sécurité sur un système UNIX. Pour installer la version 1.04 de COPS, voir à l'adresse: http://www.urec.cnrs.fr/securite/outils/cops/cops-1.04.tar.Z sur Internet.
- CRACK qui permet de détecter le degré de sécurité des mots de passe sur un système UNIX. Ce logiciel est disponible sur Internet.

- SATAN qui permet de détecter les problèmes de sécurité, les plus connus, liés aux services offerts sur un réseau de machines UNIX. Pour l'installer, consulter le site: http://www.urec.cnrs.fr/securite/outils/satan/satan-1.1.1.tar.Z sur Internet.

- TCP_WRAPPERS qui permet de limiter, enregistrer, les accès aux services offerts sur un réseau de machines UNIX.

- TRIPWIRE qui permet de vérifier sur un système UNIX si des fichiers ont été modifiés, endommagés ou altérés. Pour l'installer, consulter le: http://www.urec.cnrs.fr/securite/outils/tripwire/tripwire-1.2.tar.Z.

4.4.3 Lutte contre les virus

Les virus informatiques représentent un véritable danger pour les entreprises car leurs données très importantes peuvent être définitivement perdues. Il existe plusieurs sortes de virus et on ne peut pas les identifier tous, car ce n'est pas l'objet de ce guide, mais à titre d'information générale, il existe des virus de boot, les virus de fichiers, les vers, les «cheval de Troie» et les bombes logiques ainsi que les virus macro. La lutte de ces virus doit se faire au niveau de l'installation des antivirus sur les serveurs et sur les stations clientes. Les plus connus sont les modules antivirus NLM, spécifiques aux serveurs Netware. Cependant d'autres produits sont également disponibles pour les serveurs Windows NT et UNIX.

4.4.4 Les sauvegardes

La fiabilité de plus en plus grande du matériel, notamment des disques durs, n'est pas une excuse valable pour justifier l'absence d'une sauvegarde (backup) car une mauvaise manipulation de l'utilisateur (effacement, formatage) peut arriver. Les pertes sur les données utilisateur sont complètement irréversibles et nécessitent impérativement plusieurs sauvegardes sérieusement ignifugées. La sauvegarde peut faire gagner plusieurs jours par machine et la qualité de service en dépend. Il faut toujours distinguer les sauvegardes concernant le système et les applications des sauvegardes des données utilisateur.

4.4.5 Les onduleurs

La qualité de l'alimentation en 220 V alternatif des fournisseurs d'énergie électrique n'est pas garantie à cause des résistances, moteurs et appareils connectés qui consomment l'énergie d'une façon aléatoire.

Pour alimenter les systèmes informatiques, il est impératif d'utiliser les onduleurs ou alimentations de secours appelées aussi UPS (*Uninterruptible Power Supply*). Pour les grands réseaux, certains onduleurs peuvent être équipés d'une interface Ethernet ou Token Ring incluant un agent SNMP. L'ensemble des opérations s'effectuant alors à partir d'une station d'administration, quelle que soit sa position géographique, exactement comme pour les hub, routeur, etc. Comme pour ces derniers, une MIB standard pour onduleur a été définie d'un commun accord par les principaux fabricants. Il est important pour des raisons de compatibilité, de veiller à ce que le logiciel fourni avec l'interface SNMP s'insère dans la plate-forme de gestion des autres équipements du réseau, comme par exemple dans HP OpenView de Hewlett Packard, dans NetView d'IBM, etc.

5 Stratégies et développement du réseau Internet

5.1 Généralités

Le secteur des télécommunications connaît une véritable révolution. Avec Internet, les stratégies des opérateurs s'adaptent à cette nouvelle donne. Les grands constructeurs de réseaux vont redéfinir le cœur du secteur de l'information: les réseaux de données et téléphoniques vont converger par le biais d'Internet. On optimise les réseaux IP qui prennent en charge des applications contenant de la voix, de la vidéo et des données en simplifiant le fonctionnement des réseaux et en réduisant les coûts tout en offrant un avantage

compétitif de taille. Les responsables africains du secteur des télécommunications de notre époque doivent faire face à une augmentation systématique de la charge de leur réseau. L'émergence d'Intranet, les nouvelles applications ou simplement l'augmentation du nombre de postes les obligent à mettre en place de nouvelles solutions capables de répondre aux attentes des utilisateurs. Heureusement, les constructeurs ont anticipé ces changements et proposent des produits adaptés à chaque situation.

Les opérateurs de télécommunications en Afrique essayent de relever le défi, et des projets de développement d'Internet prennent de plus en plus de l'importance en fonction des contraintes dans chaque pays. Dans ce chapitre, nous allons voir les différentes technologies à intégrer dans un plan stratégique pour le développement du réseau Internet en Afrique.

5.2 Réseaux unifiés et téléphonie IP

5.2.1 Généralités

Les nouvelles technologies permettent d'effectuer des appels internationaux à partir d'un ordinateur individuel à destination de n'importe quel téléphone dans le monde. Tout en restant tranquillement assis derrière un ordinateur, on peut appeler un correspondant qui est à l'autre bout du monde et ceci en bénéficiant d'un tarif téléphonique incroyablement bas. Cette réalité ne peut pas être négligée dans la planification du développement d'Internet dans chaque pays.

5.2.2 Principe de fonctionnement

Les prestataires de téléphonie sur Internet permettent aux clients équipés d'un PC avec carte-son d'effectuer des appels à partir de leur ordinateur et de communiquer via Internet avec les standards téléphoniques. Le standard relaye ensuite l'appel à sa destination finale instantanément et automatiquement, c'est-à-dire à n'importe quel téléphone. La communication se fait donc en temps réel, de manière ininterrompue et en duplex intégral entre les deux correspondants.

5.2.3 La commutation IP et les réseaux unifés

Le routing switch, ou layer 3 switch ou encore le switch de couche 3 constitue la dernière innovation technologique et offre toutes les fonctionnalités d'un routeur, additionnées aux performances d'un switch. Cette innovation est appelée aussi «commutation IP». Sa facilité d'intégration dans les réseaux existants en fait le candidat idéal à la succession des routeurs, mais aussi l'élément incontournable dans le déploiement de backbones basés sur la technologie Ethernet. Il sera l'un des principaux acteurs des réseaux de demain, les «Unified Networks».

Les Unified Networks (réseaux unifiés) intègrent les transmissions par commutation, routage, optiques, filaires, sans fil et IP dans un ensemble exhaustif de produits fonctionnant entre eux et qui offrent un niveau de prévisibilité, de contrôle et de sécurité que seuls certains réseaux privés dédiés garantissaient jusqu'alors.

En rassemblant la voix, la vidéo et les données dans un seul réseau unifié, les opérateurs de télécommunications en Afrique, les fournisseurs de services Internet et les entreprises seront en mesure de proposer à leurs clients des applications multimédias et un service de haut niveau à travers le monde, tout en réalisant des économies importantes dans le coût total d'un réseau et en gagnant une position plus compétitive sur le marché.

5.3 ATM et développement de Backbone

5.3.1 Généralités

Les récentes percées technologiques dans les domaines de l'informatique, de l'audiovisuel et des télécommunications permettent de véhiculer et de traiter un volume considérable d'informations. Les structures économiques, les modes d'organisation et de production, l'accès à la connaissance, les loisirs et les méthodes de travail vont subir de profondes mutations. Les enjeux économiques et sociaux qui en résulteront auront

certainement des répercussions au niveau planétaire. Les opérateurs de télécommunications en Afrique intégreront dans leurs stratégies de développement cette nouvelle donne. Les infrastructures de télécommunications modernes, leurs applications, les aspects sociaux, les droits de propriétés intellectuelles, les sociétés des médias, la sécurité de l'information sont autant de défis qu'il conviendra de relever sur la base d'une approche commune entre gouvernements.

L'édification de la société africaine de l'information est tributaire de la mise en œuvre des autoroutes de l'information. Principal maillon dans la chaîne de l'information, les réseaux à haut débit deviennent incontournables grâce à deux percées technologiques fondamentales: la transmission optique et l'ATM (*Asynchronous Transfer Mode*).

5.3.2 Backbone en mode de transfert asynchrone (ATM)

ATM (*Asynchronous Transfer Mode*) fut choisi par l'organe central de normalisation du monde des télécoms (l'UIT) vers la fin des années 1980. ATM est l'héritier direct de Frame Relay, dont il diffère par l'emploi de paquets de petite et même taille (appelés cellules ATM) avec des débits allant de 1,544 mégabits à 1,2 gigabits par seconde. Les cellules comprennent 48 octets d'informations.

Les fonctions de routage de cellules sont implantées en hardware, contrairement à la plupart des routeurs IP ou des commutateurs X25 ou Frame Relay. Dans le cas d'ATM, on parle aussi de commutateur plutôt que de routeur de cellules.

ATM ajoute aux technologies qui l'ont précédé la possibilité de garantir la capacité et la qualité des services par connexion. Ainsi, on peut établir une connexion entre deux systèmes ATM et spécifier par exemple qu'on souhaite pour cette connexion un débit garanti de 3 Mbit/s, un délai maximal de 100 ms, une variation de délai inférieure à 5 ms, et un taux de pertes de cellules inférieur au taux donné. De telles garanties sont nécessaires pour pouvoir transporter sur ATM les circuits numériques (2 Mbit/s, 34 Mbit/s) qui forment les services essentiels des opérateurs de télécom. Elles sont aussi utiles pour établir des connexions multimédias, par exemple pour transporter des flux audio ou vidéo.

De plus, la technique ATM permet d'allouer dynamiquement le débit de transfert sur les réseaux au débit effectif de la source d'information. Cette propriété lui confère l'avantage de mieux utiliser les capacités de transmission et par voie de conséquence de réduire les coûts de transport de l'information.

Par le biais de l'ATM, l'information pourra être recherchée, triée, partagée et transmise rapidement, facilement et ce, à des coûts raisonnables. De nouvelles perspectives de développement seront ainsi offertes pour la recherche, la santé, l'éducation, les services financiers et administratifs et le secteur de l'industrie.

L'introduction de la technique ATM doit intervenir par étapes successives couvrant progressivement les besoins du marché national et régional en fonction de l'innovation technologique et des coûts de production.

Des liaisons satellite en ATM peuvent être implémentées et un commutateur ATM doit être installé dans une ville ainsi que des multiplexeurs de réseau dans d'autres villes de chaque pays, voire même dans des pays voisins. Ainsi, l'opérateur Internet pourra connecter les ISP et ses principaux clients aux différents multiplexeurs disponibles. Ce backbone en ATM peut offrir des connexions avec un débit de 34 Mbit/s voire même 155 Mbit/s sur Ethernet.

Cette stratégie est adaptée au développement des projets régionaux dans une perspective d'intégration dans des projets de grande envergure comme Oygen, Africa One et les autres.

5.3.3 Mode de connexion au Backbone ATM

Pour connecter les partenaires (autres opérateurs Internet), ISP ou principaux clients sur ATM, on peut utiliser un accès 34 Mbit/s, SMDS (Switched Multimegabit Data Service) avec serveur de connexions. Un DSU (Data Service Unit marque Digital Link par exemple) doit être installé sur chaque site. Une interface HSSI (High-Speed Serial Interface) permettra la connexion à un routeur Cisco 7000. Le routeur sera connecté sur l'épine dorsale FDDI du client donnant ainsi l'accès à l'ATM. Il est également possible de connecter les machines utilisées par les opérateurs Internet directement sur des sous-réseaux FDDI pour profiter pleinement de la bande passante offerte.

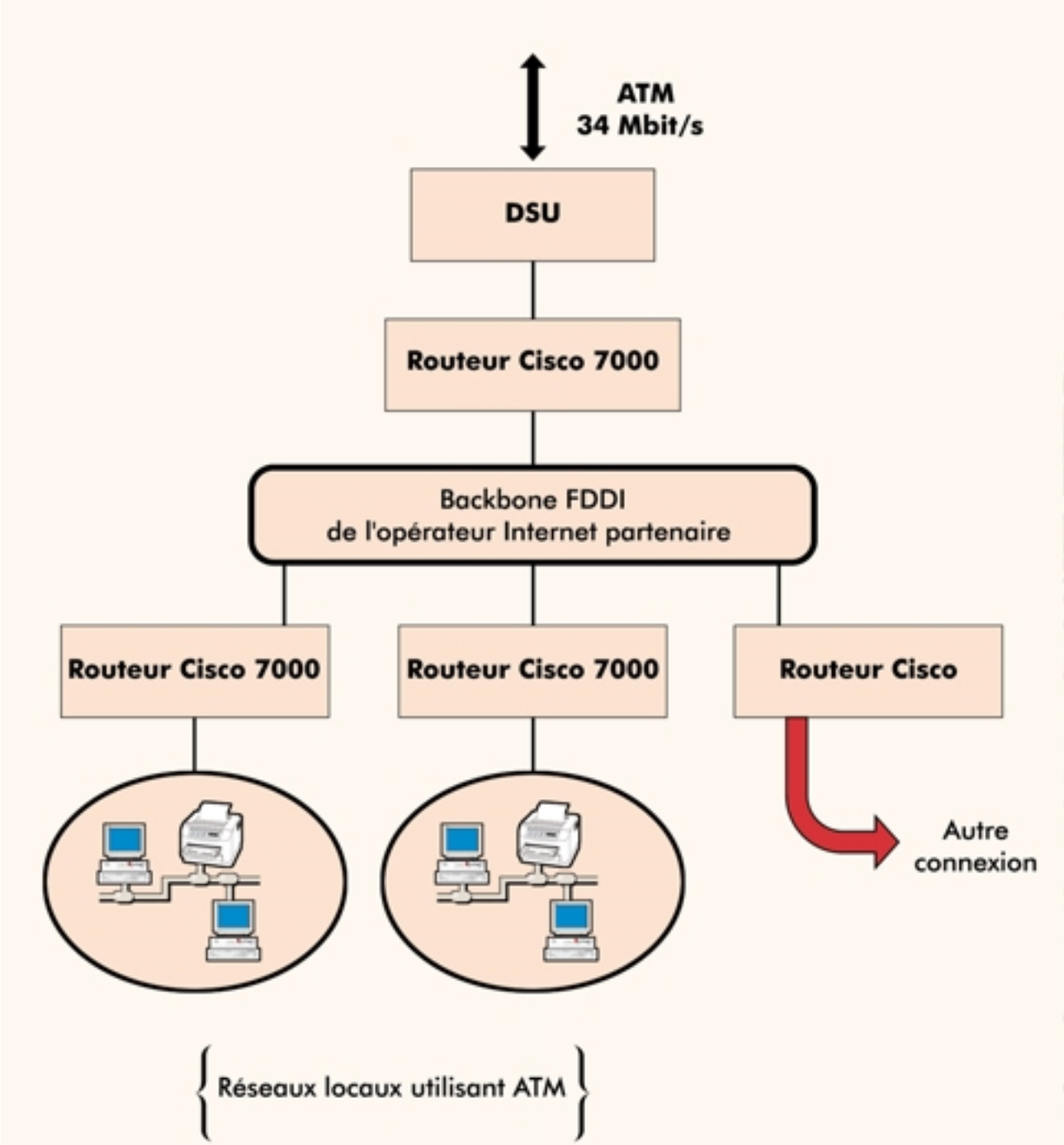

Fig. 5.1 Schéma de principe, connexion au backbone ATM

5.3.4 Communications IP sur ATM

La mise en œuvre d'ATM requiert le portage des protocoles réseau (tels que IP et autres), sinon, un ordinateur connecté par ATM ne pourrait parler qu'à un autre ordinateur ATM. Comme on le sait, IP permet d'interconnecter des réseaux tels qu'Ethernet et Token Ring. Il est donc relativement simple d'ajouter ATM à cette liste, ce qui fut fait par l'IETF (Internet Engineering Task Force) dans une série de RFC (*Requests For Comments*, nom cryptique donné aux documents officiels de l'IETF).

La solution classique est un modèle qui fonctionne de la façon suivante (voir Figure 5.2). Les ordinateurs ont des adresses IP (A1, A2) et des adresses ATM (a1, a2). Au démarrage, l'ordinateur 1 établit une connexion ATM avec le serveur d'adresses. Ce dernier peut être implanté dans un routeur ou dans un ordinateur connecté au même réseau ATM et son adresse ATM est donc bien connue. Le serveur d'adresses apprend par ce moyen que l'adresse IP A1 est accessible par l'adresse ATM a1. L'ordinateur 1 désire envoyer des données à l'ordinateur 2 en utilisant le protocole IP. L'ordinateur 1 connaît donc l'adresse IP de l'ordinateur 2. Il lui faut maintenant déterminer l'adresse ATM de l'ordinateur 2, ce qu'il obtient en le demandant au serveur d'adresses, par la connexion ATM déjà établie (1).

L'ordinateur 1 peut alors établir une connexion vers l'ordinateur 2, si ce n'est déjà fait, et l'utiliser pour envoyer les données (2). Le rôle du serveur d'adresses est de compenser l'absence de propriété de diffusion (broadcast) d'un réseau ATM. Rappelons que, sur un réseau Ethernet, Token Ring ou FDDI, la résolution d'adresse se fait en diffusant la demande à tout le réseau, ce qui est simple à réaliser dans les réseaux à support partagé.

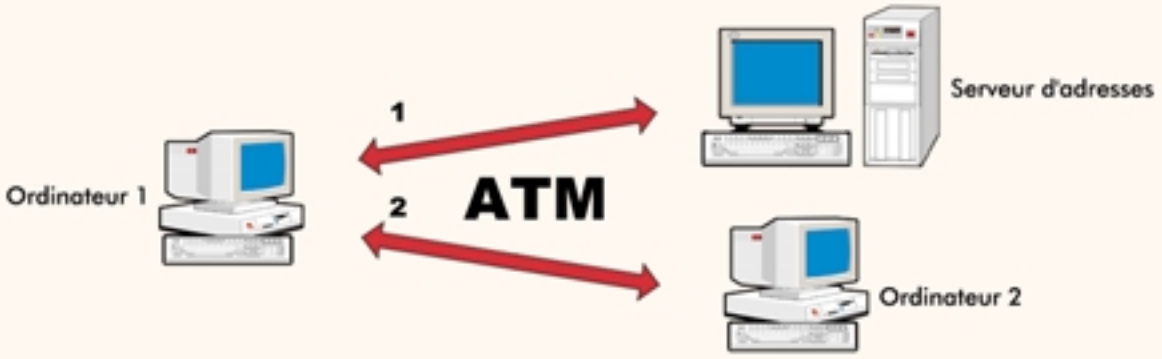

Fig. 5.2 Schéma de principe, communication IP sur ATM

Le scénario présenté à la Figure 5.2 ne s'applique que si les ordinateurs 1 et 2 sont définis comme appartenant au même réseau logique. Sinon l'utilisation d'un routeur est indispensable entre les ordinateurs 1 et 2 pour communiquer.

Le modèle classique utilise donc ATM comme un Ethernet (d'où son nom), et ne permet pas en général d'utiliser ATM de bout en bout. Une solution à ce problème est en élaboration NHRP (*Next Hop Resolution Protocol*). Cette solution autoriserait des systèmes appartenant à des réseaux logiques différents à établir des connexions ATM directes entre eux.

5.3.5 ATM de bout en bout ou RSVP?

Le transport de flux vidéo sur Internet est possible mais la qualité est variable, imprévisible, insuffisante pour des utilisateurs aux exigences habituelles.

Un des points importants qu'apporte ATM est la réservation de ressources, rendue possible parce qu'ATM utilise des connexions. La garantie de ressources est nécessaire pour transporter des flux tels que la vidéo ou l'audio avec une qualité commerciale. Pour offrir des garanties de ressources, une solution est d'utiliser ATM de bout en bout pour des problèmes spécifiques car, contrairement à IP, ATM n'est pas une technologie d'interconnexion.

Avec cette nécessité pour le multimédia sur Internet d'avoir un IP avec réservation, la solution de l'IETF est RSVP (*Resource reSerVation Protocol*). Contrairement à ATM, RSVP est un protocole d'accompagnement d'IP, et ne demande pas de nouvelle carte d'interface de communication sur les ordinateurs. Cependant, pour fonctionner correctement, RSVP demande que les routeurs soient modifiés pour effectuer toutes les tâches liées à la réservation, tâches pour lesquelles les équipements actuels n'ont pas été conçus.

ATM est la technologie de choix pour les réseaux publics offrant de la bande passante tarifée (à cause, entre autres, de son aspect orienté connexion); par contre, la communication de bout en bout demande un protocole tel que RSVP, indépendant de la carte d'interface de communication. Cependant ATM va s'implanter dans les

réseaux locaux, soit directement, soit comme technologie d'interconnexion entre commutateurs (*switched Ethernet, switched Token Ring*), ainsi, les réseaux publics offriront des services large bande en utilisant une base ATM. Par contre, RSVP risque bien de s'imposer dans tous les cas où l'hétérogénéité est la règle. En particulier, on verra RSVP implanté même sur ATM, pour permettre à des systèmes ATM d'utiliser des communications à réservation de ressources avec des systèmes non-ATM. Pour plus de détails, voir FI-9/1995.

5.4 Développement du réseau en fibre optique

5.4.1 Généralités

Lorsque le backbone (l'épine dorsale) du réseau national (voire même régional) est en ATM avec des points principaux souvent appelés PoP (*Point of Presence*), les différents sites peuvent y être raccordés par fibre optique que l'on peut poser sur les lignes à haute tension, à des débits de 34 voire même de 155 Mbit/s. Au-dessus de ces débits, une technologie de multiplexage synchrone SDH (Synchronous Digital Hierarchy) peut être utilisée pour permettre le transport de canaux allant de 155 Mbit/s jusqu'à 10 Gbit/s en multipoints sur fibre optique. Pour plus de détails, il faudrait consulter plusieurs Recommandations (G.780, G.783 à G.785) de l'UIT (Union internationale des télécommunications, ITU en anglais).

5.4.2 Principe de conversion de signaux électriques en signaux optiques

Le transceiver Ethernet optique a pour fonction de convertir des impulsions électriques en signaux optiques véhiculés au cœur de la fibre optique. A l'intérieur des deux transceivers partenaires, les signaux électriques sont traduits en impulsions optiques par une LED (*Light Emitting Diode*) et lus par un phototransistor ou une photodiode. Une fibre optique est utilisée pour chaque direction de la transmission. Les émetteurs utilisés sont de trois types: les LED (*Light Emitting Diode*) qui fonctionnent dans le rouge visible (850 nM); les diodes à infrarouge qui émettent dans l'invisible à 1 300 nM et les lasers, utilisés pour la fibre monomode, dont la longueur d'onde peut être de 1 300 ou 1 550 nM.

5.4.3 Types de fibres optiques

On utilise trois types de fibres optiques, à savoir la fibre à saut d'indice 200/380 qui est constituée d'un cœur et d'une gaine optique en verre de différents indices de réfraction. A cause d'une section importante du cœur, cette fibre provoque une grande dispersion des signaux qui la traversent, ce qui génère une déformation du signal reçu. La fibre à gradient d'indice a un cœur constitué de couches de verre successives ayant un indice de réfraction proche, ce qui provoque une égalisation des temps de propagation, ce qui a pour conséquence la réduction de la dispersion nodale. La bande passante est typiquement de 200-1 500 MHz par km. La fibre monomode quant à elle a le cœur si fin que le chemin de propagation des différents modes est pratiquement direct. La dispersion nodale est quasiment nulle. La bande passante transmise est supérieure à 10 GHz/km. Cette fibre est utilisée essentiellement pour les sites éloignés.

5.4.4 Liaisons et qualité des transmissions par fibre optique

La fibre optique est utilisée pour renforcer principalement le backbone et les réseaux nécessitant un niveau de sécurité élevé. Elle offre une très bonne résistance aux écoutes privées et aux attaques actives telles que l'injection d'un signal étranger visant à brouiller et tromper les utilisateurs de réseaux au niveau des terminaux et des transmissions. La fibre optique ne rayonnant pas du tout, on est obligé de la couper avec une scie en diamant pour établir un branchement en dérivation, ce qui n'est pas à la portée des premiers venus.

Les modems reliés aux fibres optiques sont équipés de détecteurs de disparition ou d'atténuation du signal suite à un branchement pirate. Sur une longue distance, un répéteur à laser régénère le signal tous les 40 km environ, un module optoélectronique revitalise les impulsions lumineuses affaiblies. Pour améliorer les débits, il est conseillé de remplacer ces répéteurs et d'utiliser des amplificateurs 100% optiques qui multiplient par 100 leur débit.

Après avoir installé une liaison en fibre optique, il convient de mesurer la perte induite par la fibre elle-même et par les connexions effectuées. Le Power meter constitué d'une paire calibrée d'émetteur-récepteur de lumière, permet de mesurer la totalité de la perte de la ligne en [dB]. On mesurera la perte à la longueur d'onde utilisée en exploitation (850 ou 1 300 nM).

Le réflectomètre est un appareil qui envoie une impulsion optique dans la fibre. Un écran permet de visualiser l'allure du signal réfléchi dans le verre. On peut ainsi mesurer avec précision la longueur de la liaison et les pertes engendrées à chaque connexion. En outre, cet appareil est très utile pour localiser les coupures éventuelles de la fibre et pour identifier la connexion qui est la cause d'une trop grande perte optique. Le Power meter ne donne que la perte globale de la liaison; le réflectomètre indique où se trouve la connexion défectueuse.

5.5 Connexions par liaisons laser pour les sites Internet

5.5.1 Généralités

Lorsqu'on n'a pas la possibilité d'établir une liaison par fibre optique ou ligne téléphonique dédiée, on peut installer une liaison par laser, pour autant que les deux sites à relier soient distants de moins d'un kilomètre et qu'il n'y ait pas d'obstacle au faisceau. On trouve des lasers qui se comportent comme une paire de répéteurs à 10 Mbit/s et même des lasers à 155 Mbit/s pour ATM.

5.5.2 Caractéristiques des liaisons laser

L'alignement des faisceaux est difficile à réaliser et demande beaucoup de savoir-faire. L'avantage indéniable de ces liaisons est la mobilité des systèmes et leurs prix intéressants. En cas de déménagement, on peut récupérer une paire de lasers contrairement aux câbles en fibres installés sous les routes et ponts par exemple. L'expérience a montré en Europe que le laser ne souffre ni du brouillard, ni des grosses chutes de neige. Il faut installer les lasers hors d'atteinte des bricoleurs et éviter les obstacles au laser. Cette solution est bonne pour les cas difficiles entre bâtiments éloignés d'une organisation. Elle est fiable, mais moins sûre qu'une liaison en cuivre ou en fibre.

5.6 Technologies de pointe et l'accès à Internet

5.6.1 Généralités

Actuellement, la plupart des réseaux de télécommunication en Afrique, infrastructures en cuivre du téléphone datant des années 1970, ne sont pas adaptés au développement d'Internet. Les coûts d'investissement très élevés, le manque de personnel qualifié et un habitat dispersé sont les principales causes qui risquent de freiner le développement du réseau Internet en Afrique. Heureusement, l'introduction dans les réseaux existants des technologies de pointe et l'usage des technologies alternatives constituent un atout pour bâtir une infrastructure globale de l'information (GII) en Afrique.

5.6.2 ADSL

5.6.2.1 Généralités

ADSL (Asymmetric Digital Subscriber Line) est la nouvelle technologie de transmission de données avec une performance qui se situe entre les liaisons numériques de type RNIS (réseau numérique à intégration de services) et les liaisons haut débit du câble. Les technologies qui permettent cette astuce sont appelées «xDSL» et sont toutes dérivées de la technologie DSL utilisée dans le cadre de liaisons numériques RNIS (le type de codage utilisé est le même). Le terme xDSL se décompose en quatre groupes: ADSL, HDSL, SDSL et VDSL. A chacun de ces sous-groupes correspondent une utilisation et des caractéristiques particulières.

Aujourd'hui, l'ADSL est la technologie la plus au point et commercialement prête. Les expérimentations en cours en France, au Canada, aux USA et ailleurs prouvent que le système ADSL permet déjà de transmettre des informations à 8 Mbit/s sur 3 km. Cette technologie est une alternative à un investissement dans de coûteux équipements câblés en utilisant les ressources du fil de cuivre qui ne sont pas encore exploitées et pourtant installées depuis les années 1970.

En réalité, les possibilités des fils de cuivre ne sont pas utilisées à l'optimum car le réseau téléphonique a d'abord été conçu pour transporter de la voix. La bande passante utilisée par les équipements de communication classiques est bridée à 3,3 kHz. Or, les caractéristiques physiques des lignes d'abonné permettent en réalité de supporter la transmission de signaux à des fréquences de l'ordre de 1 MHz. En

modifiant les équipements au niveau du central téléphonique et chez l'utilisateur, il est apparu donc possible d'optimiser l'utilisation de ces lignes. En fonction de la distance séparant l'abonné de son central téléphonique, les paires de cuivre peuvent supporter des débits de 1,5 Mbit/s (5,5 km), 2 Mbit/s (4,9 km), 6,3 Mbit/s (915 m) et 51,8 Mbit/s (305 m). Pour plus de détails, voir la norme ADSL actuelle (T1.413).

5.6.2.2 Principe de fonctionnement de l'ADSL

Les câbles reliant les centraux téléphoniques aux utilisateurs possèdent tous une bande passante d'environ 1 MHz. Les communications téléphoniques n'utilisent que 4 kHz. On constate donc qu'il reste une bande passante de 996 kHz qui est inutilisée. Les modems ADSL ont été conçus pour utiliser l'entièreté de la bande passante disponible sur les câbles tout en permettant l'utilisation normale du téléphone.

Avec cette technique, la bande passante est divisée en trois parties. Le haut de la bande (1 MHz) est réservé au canal descendant (central/abonné) à debit élevé (8 Mbit/s). En milieu de bande (entre 300 et 700 kHz), se trouve un canal bidirectionnel à débit moyen utilisé pour émettre les données. Le troisième canal est réservé soit à la téléphonie analogique classique (entre 0 et 4 kHz) soit au RNIS (entre 0 et 80 kHz). Ce dernier sera toujours opérationnel en cas de panne du modem. Cette approche «multicanaux» permet en outre aux utilisateurs d'accéder au WWW ou tout autre serveur tout en téléphonant ou envoyant un fax par exemple.

De plus, la plupart des modems ADSL se mettent sur une prise Ethernet, ce qui permet de les partager en réseau. Cette asymétrie, qui réserve pour le flux «central vers abonné» une bande passante supérieure au flux «abonné vers central», est tout à fait adaptée à la consultation de documents multimédia de type vidéo ou son en direct. Avec cette technologie, on peut transformer Internet en canal télévisé.

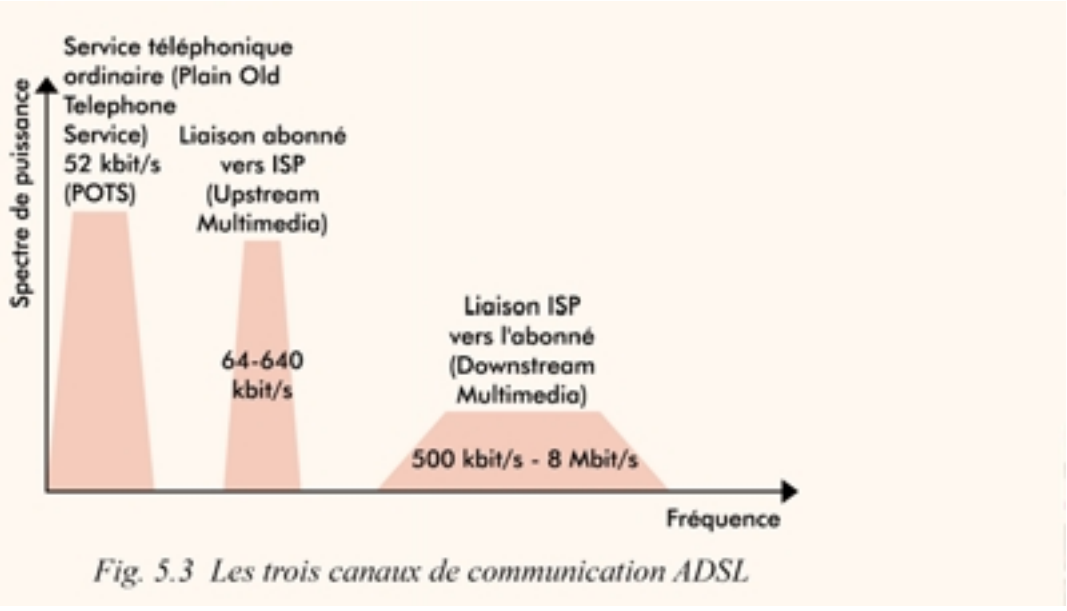

Fig. 5.3 Les trois canaux de communication ADSL

5.6.2.3 Le modem ADSL

Un des avantages d'ADSL est qu'il ne nécessite pas d'aménagements coûteux et encombrants pour les utilisateurs de la technologie. A la Figure 5.4 nous avons quelques exemples de modem, dont celui de chez Motorola; autres fabricants: Alcatel-Bell, Orckit, Amati, Ericsson, Hayes, 3COM. Le modem doit se trouver à chaque extrémité de la ligne.

Les principaux problèmes qui freinent le développement rapide de cette technologie sont le prix des modems et les performances des systèmes qui dépendent du profil et de l'état de la ligne de cuivre. Celle-ci n'étant pas constituée d'un seul câble continu, mais de plusieurs tronçons reliés entre eux, c'est au moment du passage à ce point de jonction que le signal transmis peut se dégrader et réduire la vitesse de transmission. En plus, deux lignes téléphoniques installées trop proches l'une de l'autre ont tendance à se parasiter.

Fig. 5.4 Quelques modems ADSL

5.6.2.4 L'adaptateur d'accès

L'adaptateur d'accès est un bâti contenant les cartes de terminaison de ligne ADSL, les coupleurs POTS et l'interface avec le backbone.

Fig. 5.5 Armoire d'accès ADSL

5.6.2.5 Les coupleurs POTS

Le coupleur POTS est conçu à partir de plusieurs filtres spécialisés (filtres passe-bande) assurant la séparation du signal téléphonique analogique en bande de base et du signal numérique modulé. On utilise soit un coupleur passif, soit un coupleur actif en fonction des caractéristiques d'impédance de la boucle locale et des exigences spécifiques du pays.

Dans le cas d'un coupleur actif, le modem est équipé d'un relais pour assurer que le coupleur soit court-circuité en cas de panne de l'alimentation locale. Ceci garantit la disponibilité du service téléphonique de base en toutes circonstances. Le coupleur POTS peut, soit être séparé, soit être intégré dans le modem et l'adaptateur d'accès.

5.6.3 Internet par satellite

5.6.3.1 Généralités

Plusieurs sociétés, comme Netsat, Matra Grolier Network ou Pandemonium Group proposent des liaisons satellitaires aux fournisseurs d'accès et aux entreprises.

Un opérateur télécom ou groupe d'opérateurs Internet en Afrique peuvent disposer d'un segment spatial de 34 Mbit/s au-dessus de l'Atlantique Nord, et avoir un accord de réciprocité avec MCI (Etats-Unis) par exemple sur sa boucle optique de 155 Mbit/s, et installer deux ou plusiers stations d'émission/réception dans les pays et aux endroits prévus, reliant à Internet les fournisseurs d'accès.

INTELSAT avec BT, COMSAT, EMBRATEL, France Télécom et d'autres opérateurs vont distribuer Internet pour la prestation de services de diffusion multipoint par satellite. Par ce système, les contenus Internet les plus fréquemment consultés sont mis en cache dans un endroit pour stockage des données, en vue d'une multidiffusion jusqu'aux prestataires de services Internet dans le monde entier qui, à leur tour, les stockent en cache pour les besoins nationaux et locaux. Dans cette solution, l'opérateur Internet a le choix d'adopter la technologie «Push» ou «Pul» (*Source: INTELSAT*).

5.6.3.2 Internet par réseaux satellites VSAT

Le VSAT (Very Small Aperture Terminal), antenne parabolique de petit diamètre, permet de mettre en place un réseau de télécommunications via des satellites utilisables pour Internet sans passer par la boucle locale. Les antennes sont en communication avec le hub (connexion au LAN ou réseau local) par l'intermédiaire d'un satellite. Cette solution permet de mettre en place des liaisons de communications interactives. Cependant, elle n'est viable que pour des grandes organisations ayant de nombreux sites dispersés au nombre de 50 minimum (*Source: Salgues, 1997*). C'est une solution qui est donc adaptée à un opérateur qui veut étendre ses services Internet sur un territoire assez large. L'inconvénient est le temps moyen de propagation qui est relativement long et qui constitue une gêne pour la téléphonie (écho) et pour la transmission de données (ralentissement au niveau de protocole).

5.6.4 Boucle locale radio

5.6.4.1 Généralités

Les liaisons dédiées ou liaisons spécialisées sont souvent coûteuses. Les opérateurs de télécommunication pour développer Internet trouveront une technologie alternative et compétitive en faisant recours à la technologie «boucle locale radio». Ces liens radio s'appuient sur les très hautes fréquences. Le dispositif retenu permet d'obtenir un débit allant jusqu'à 2 Mbit/s. un certain nombre de conditions techniques doivent être réunies pour en bénéficier. Un grand inconvénient est la sensibilité aux perturbations surtout en cas d'orage où les liaisons peuvent être interrompues.

5.6.4.2 Principe de fonctionnement

Pour utiliser ce genre de technologies, les utilisateurs des liaisons spécialisées (LS), le plus souvent les ISP (Internet Services Provider), universités, écoles, hôpitaux, entreprises et administrations, doivent être à moins de 7 km du point d'accès de l'opérateur et disposer d'une vue directe de son toit vers le pylône. L'installation technique chez le client est assez simple. Sur le toit de l'un ou l'autre des clients cités ci-dessus, une antenne est installée et reliée au boîtier «émetteur/routeur» de son réseau.

Le dispositif est plus conséquent chez l'opérateur. Sur son toit, un mât est installé, couplé d'un hauban haut d'environ 18 m, sur lequel est placée une cinquantaine d'antennes. Le mât est relié à la liaison spécialisée par deux liens sécurisés à 100 Mbit/s. Ces derniers sont eux-mêmes connectés à une baie «d'émetteurs/ récepteurs» hertziens qui aboutissent à un routeur spécifiquement développé pour gérer les connexions radio.

Le coût de l'investissement peut aller jusqu'à 250 000 $ US. Pour le client, la note est fonction de la taille du faisceau (bande passante) et du volume d'informations tranférées, par mois. Trois tailles de faisceau sont souvent proposées, à savoir 512 kbit/s, 1 Mbit/s et 2 Mbit/s. A titre d'exemple, avec un faisceau de 2 Mbit/s et un trafic mensuel de 15 Go, le client est taxé environ 10 000 FF par mois en France.

L'accès hertzien s'adresse aux ISP et entreprises (ou institutions) qui souhaitent une connexion permanente avec un besoin de bande passante supérieure à 128 kbit/s. Un avantage particulier de cette technologie est une gestion simplifiée. Par exemple, une simple programmation logicielle suffit pour augmenter la bande passante. La seule contrainte pour une utilisation efficace est la visibilité entre les deux antennes.

5.6.5 Technologie MMDS ou Microwave Multipoint Distribution System

5.6.5.1 Généralités

Il est rare de trouver en Afrique le câble pour la télévision qui serait utilisable pour Internet à haut débit. Une alternative intéressante et moins coûteuse est l'utilisation de la transmission numérique sur MMDS (*Microwave Multipoint Distribution System* ou diffusion multiplexée sur canal micro-ondes) considéré comme le câble du milieu rural. MMDS est un procédé de diffusion de programmes de télévision analogique ou numérique par micro-ondes, ou hyperfréquences. On peut utiliser la modulation d'amplitude ou mieux la modulation de fréquence, utilisée par les satellites de télévision directe. Cet accès sans fil au réseau local peut être utilisé pour Internet. Une autre possibilité existe, il s'agit des systèmes de la norme européenne DECT (*Digital European Cordless Telephone* ou télécommunications numériques sans fil européennes).

5.6.5.2 MMDS, alternative au câble de télévision

L'opérateur peut capter par des paraboles en tête de réseau, des programmes de télévision sélectionnés en provenance des divers satellites, et les redistribuer ensuite au moyen d'un émetteur hypercâble. Il suffit ensuite d'équiper les usagers (individuellement ou collectivement) d'une mini-antenne active de 10 cm (à moins de 30 km de l'émetteur, la portée atteignant 100 km pour une antenne de 28 cm), et d'un récepteur de TV par satellite. Pas de travaux de génie civil, pas de ligne à tirer, des délais d'installation réduits, un environnement préservé grâce à la petite taille des récepteurs. Inventé pour la télévision, le MMDS semble une alternative intéressante au câble en Afrique.

La législation dans chaque pays devra intégrer cette alternative qui n'est autorisée dans certains pays européens que pour l'extension d'un réseau câblé en campagne, ou le transport en fin de réseau câblé, de l'artère principale (câble) aux foyers. Le MMDS constitue également une alternative pour la transmission de données multimédia à haut débit également utilisable pour l'accès Internet.

5.6.5.3 Accès à Internet par MMDS

En s'inspirant du cas du Mexique où le seul réseau de Mexico dessert environ 400 000 abonnés, en Afrique on peut également utiliser la technologie MMDS pour se connecter à Internet. Pour utiliser MMDS afin de se connecter à Internet, on installe à côté de l'émetteur un IRS (*Internet Radio Server*), micro-ordinateur raccordé au réseau local du provider Internet qui transformera le signal au standard MPEG-2/DVB, pour émission via l'antenne hypercâble (architecture de MDS-France). L'abonné à Internet est obligé de s'équiper, en plus de son antenne, d'une carte PC qui intègre un récepteur satellite (permettant de recevoir les données à 2, 4, 8 ou 15 Mbit/s), d'un navigateur standard, et d'un modem RTC, GSM ou d'un adaptateur RNIS pour la voie de retour. Actuellement, la solution la plus répandue est le MMDS en mode unidirectionnel et le dialogue de l'internaute vers le serveur doit s'effectuer par un chemin différent. Un nouveau système bidirectionnel à 2 Mbit/s vient d'être mis sur le marché.

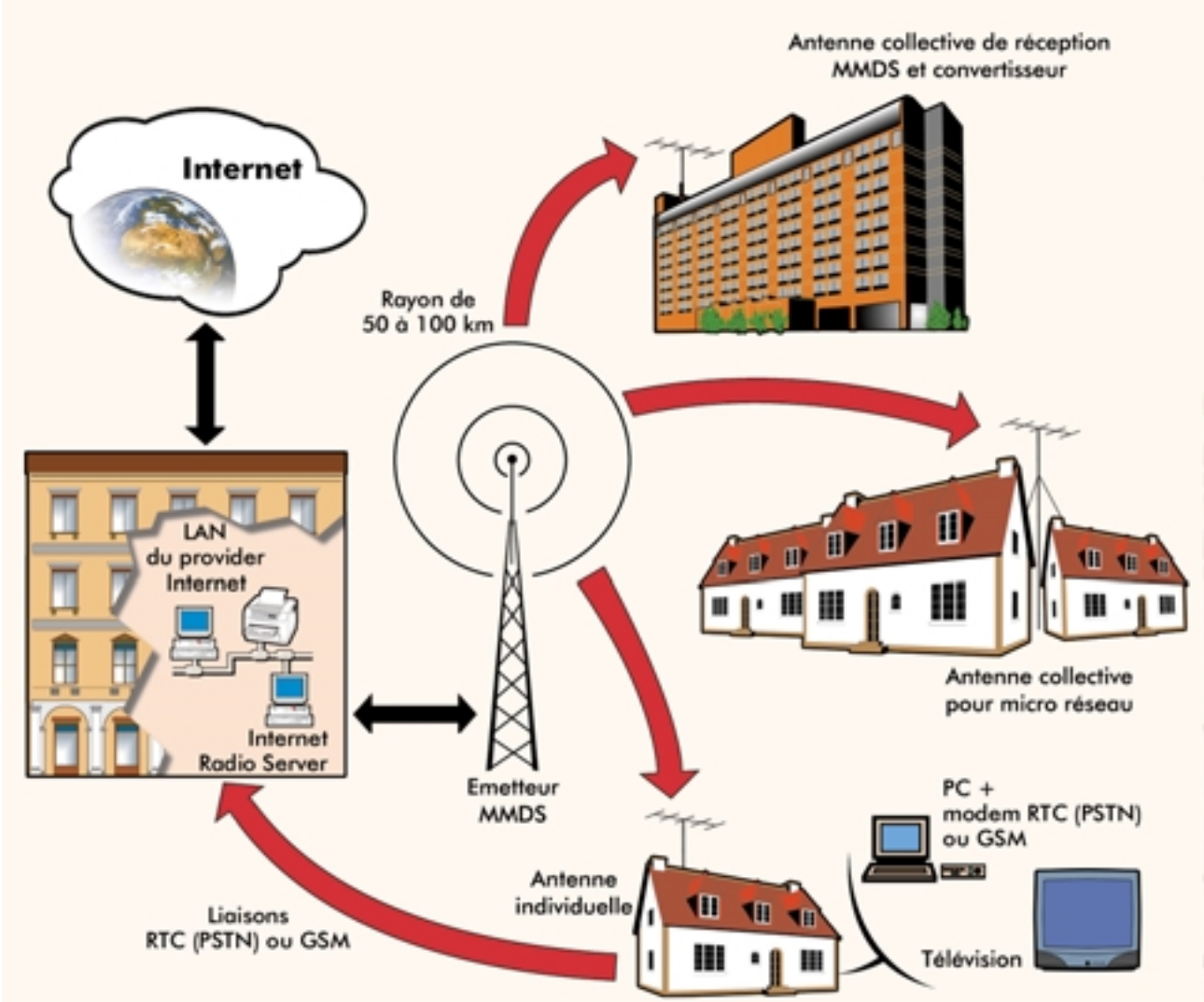

Fig. 5.6 Accès Internet par MMDS - Unidirectionnel

6 Aspects réglementaires et juridiques

6.1 Généralités

Le développement du secteur des télécommunications connaît une véritable mutation compte tenu de la convergence des technologies des télécommunications, de l'audiovisuel et de l'informatique. Plusieurs aspects réglementaires et juridiques doivent suivre cette évolution technologique. Dans ce paragraphe, nous allons relever quelques aspects que nous jugeons importants et à chaque administration des télécommunications de les adapter à son contexte national. La Figure 6.1 illustre l'état de l'art en technologies Internet.

6.2 Protection des nouvelles technologies

6.2.1 Généralités

Plusieurs technologies nouvelles se développent. Elles seront introduites surtout au niveau de la boucle locale, partie terminale du réseau de communication, qui dessert chaque abonné comme on vient de le voir dans le chapitre précédent, ainsi qu'au niveau de la sécurité de l'information et du réseau. Ceci va favoriser la baisse des coûts et développera la vente des services Internet. Il est donc important d'intégrer dans la régulation des télécommunications dans les pays africains, l'évolution nécessaire des conditions réglementaires permettant d'introduire les nouvelles technologies de boucle locale, l'usage de la cryptologie et des communications vocales sur Internet.

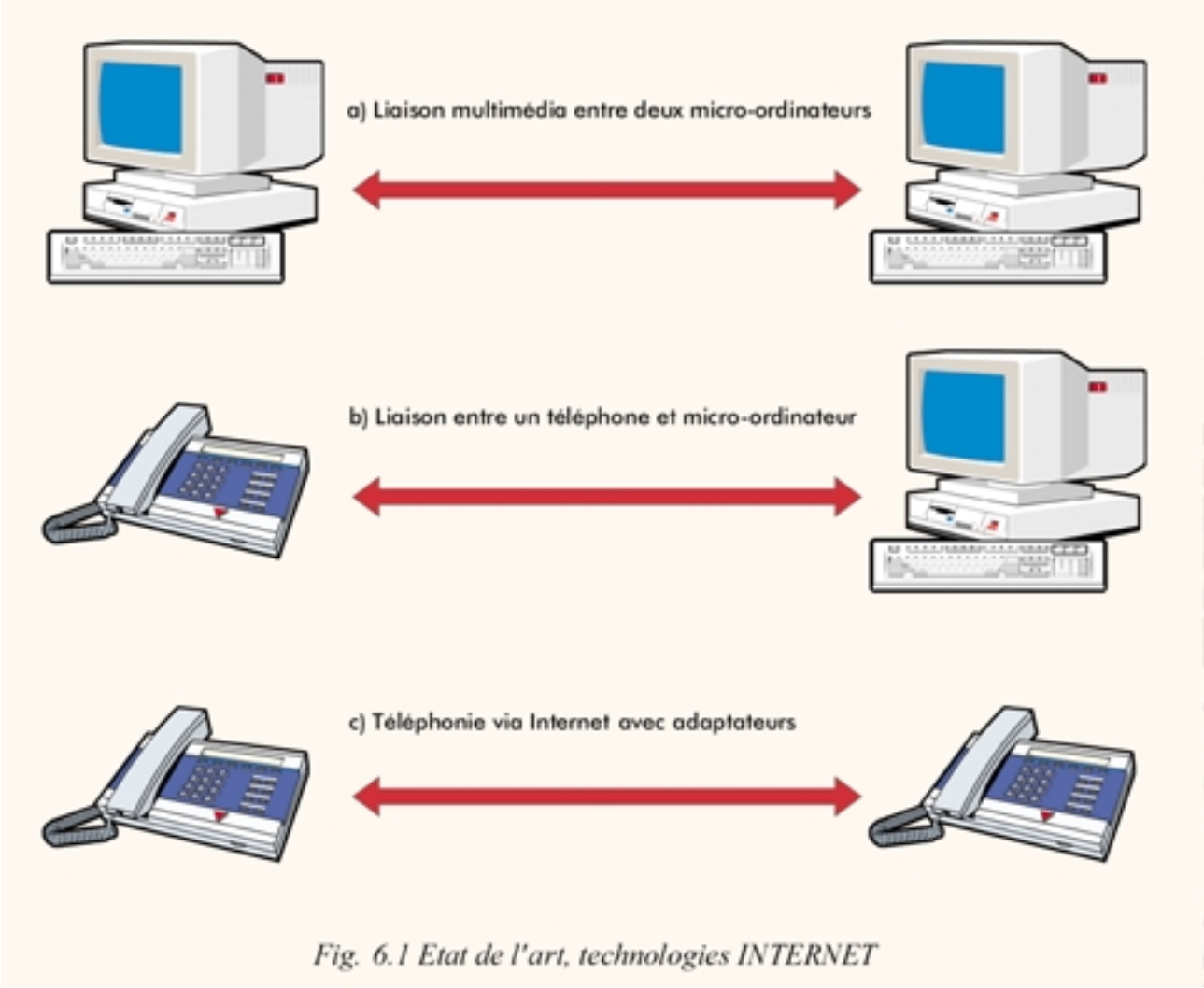

Fig. 6.1 Etat de l'art, technologies INTERNET

6.2.2 Cryptologie

Un moyen de cryptologie peut être sous une forme matérielle ou logicielle. La cryptologie est utilisée pour satisfaire les fonctions technologiques suivantes:

– *Fonction d'intégrité des données:* (la non-altération accidentelle ou frauduleuse de l'information).
– *Fonction d'authentification:* (signature numérique – authentification des partenaires et authentification de l'origine des informations).
– *Fonction de confidentialité:* (protection de l'information).

Un cadre juridique réglementant l'usage de la cryptologie dans le cadre des communications sur Internet doit progressivement s'adapter à l'usage de cette technologie car incontournable pour la plupart des applications sur Internet. La cryptologie est primordiale pour le commerce électronique. Les propositions qui suivent tiennent compte à la fois du développement des technologies de l'information et de la sécurité d'un Etat et de ses citoyens.

Ainsi, pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure d'un Etat, tout en permettant la protection des informations et le développement des communications et des transactions sécurisées sur Internet, les mesures suivantes sont très importantes et méritent une attention particulière dans chaque pays africain:

- *L'importation et l'exportation des systèmes de cryptologie:* La fourniture ou l'importation dans un pays et l'exportation tant d'un moyen que d'une prestation de cryptologie sont soumises à autorisation préalable de l'organe national de réglementation des télécommunications, lorsqu'ils assurent des fonctions de confidentialité. L'autorisation peut être subordonnée à l'obligation pour le fournisseur de communiquer l'identité de l'acquéreur.

- *Liberté pour l'usager d'utiliser la cryptologie:* L'utilisation d'un moyen ou d'une prestation de cryptologie est libre pour un usager si le moyen ou la prestation de cryptologie ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis (ou pour des fonctions de signature numérique) ou encore si le moyen ou la prestation assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées par l'organe national responsable pour la sécurité nationale.

- *Autorisation à l'usager d'utiliser la Cryptologie:* L'utilisation d'un moyen ou d'une prestation de cryptologie est Soumise à autorisation de l'organe national responsable dans les autres cas.

6.2.3 Fonction de confidentialité

Actuellement pour la plupart des pays africains, l'organisme chargé de gérer pour le compte d'autrui les conventions secrètes de moyens ou prestations de cryptologie permettant d'assurer des fonctions de confidentialité reste le ministère de tutelle même si la libéralisation du secteur des télécommunications est une réalité.

La liberté d'utiliser des moyens de cryptologie pour rendre confidentiel un message devrait être totale, à condition que les prestations de confidentialité employées soient gérées par un tiers de confiance. Le tiers de confiance est donc un organisme agréé qui gère des clés de chiffrement pour le compte de l'utilisateur. Ce dernier passe un contrat avec le tiers de confiance qui lui transmet régulièrement les clés à utiliser pour chiffrer son information. Dans la licence du tiers de confiance figure une clause par laquelle celui-ci doit, en vertu de la loi, remettre les clés de chiffrement aux autorités habilitées en cas de nécessité.

Le tiers de confiance doit être clairement désigné dans chaque pays. Ainsi, l'utilisateur peut-il s'appuyer sur un professionnel de la cryptologie qui lui garantit un service de haute qualité, tandis que l'Etat peut, en cas de besoin, accéder au contenu de l'information pour des raisons majeures relatives à la sécurité nationale.

6.2.4 Responsabilités des professionnels de la cryptologie

Les organismes qui exerceront cette fonction doivent être préalablement agréés par l'autorité compétente. Ils sont assujettis au secret professionnel dans l'exercice de leurs activités agréées. Ils sont tenus de conserver les conventions secrètes qu'ils gèrent. Dans le cadre de l'application de la loi relative au secret des correspondances émises par la voie des télécommunications ainsi que dans le cadre des enquêtes menées suivant le code de procédure pénale, ils doivent les remettre aux autorités judiciaires ou aux autorités habilitées, ou les mettre en œuvre selon leur demande. Ils doivent exercer leurs activités agréées sur le territoire national.

Les dispositions libérales qui intéressent l'utilisateur font porter le poids de la réglementation sur les professionnels de la cryptologie. Les autres prestataires de services Internet (PSI) doivent informer les pouvoirs publics des produits qu'ils mettent sur le marché, produits spécialement conçus pour cet usage et pour lesquels ils ont reçu une autorisation de fourniture. Ils doivent aussi demander un agrément s'ils veulent devenir tiers de confiance et sont tenus à un strict respect des règles auxquelles ils ont souscrit. Des dispositions pénales particulières sont prévues s'ils ne s'y conformaient pas.

6.2.5 Infractions et dispositions pénales

- Sans préjudice de l'application du code des douanes, le fait de fournir, d'importer ou d'exporter un moyen ou une prestation de cryptologie sans avoir obtenu l'autorisation préalable des autorités ou en dehors des conditions de l'autorisation délivrée est puni par la loi (emprisonnement et amende: la durée et le montant seront définis par les autorités compétentes).

- Le fait de gérer, pour le compte d'autrui, des conventions secrètes de moyens ou de prestations de cryptologie permettant d'assurer des fonctions de confidentialité sans avoir obtenu l'autorisation ou en dehors des conditions de cet agrément est puni par la loi (emprisonnement et amende: la durée et le montant seront définis par les autorités compétentes).

- Le fait de fournir, d'importer, d'exporter ou d'utiliser un moyen ou une prestation de cryptologie en vue de faciliter la préparation ou la commission d'un crime ou d'un délit est puni par la loi (emprisonnement et amende: la durée et le montant seront définis par les autorités compétentes).
- La tentative des infractions prévues ci-dessus est punie des mêmes peines.
- Est puni par la loi le fait de refuser de fournir les informations ou documents ou de faire obstacle au déroulement des enquêtes des autorités (emprisonnement et amende: la durée et le montant seront définis par les autorités compétentes).

6.2.6 Définition et normes

Les organismes de normalisation tels que l'UIT-T, l'ISO pour l'international et l'AFNOR pour la France ont fixé le vocabulaire de la cryptologie. Le texte de référence est l'ISO 7498-2 de septembre 1990.

authentification	processus appliqué par l'expéditeur et le destinataire pour garantir l'intégrité des données et fournir l'authentification de l'origine des données (ISO 8730);
authentification de l'origine des données	confirmation que la source des données reçues est celle revendiquée (ISO 8730);
algorithme d'authentification	algorithme utilisé conjointement à une clé d'authentification et un ou plusieurs éléments d'authentification à des fins d'authentification (ISO 8730);
élément d'authentification	élément de message que l'on désire protéger par l'authentification (ISO 8730);
intégité des données	capacité qu'ont des données de ne pas pouvoir être altérées ou détruites d'une manière frauduleuse (ISO 8730);
chiffrement	transformation cryptographique de données en vue de produire un texte chiffré (ISO 8730);
cryptogramme	informations chiffrées (ISO 8732);
déchiffrement	l'inverse du chiffrement réversible correspondant (ISO 8730);
chiffre	discipline qui englobe tous principes, moyens et toutes méthodes destinés à la transformation de données afin de cacher leur contenu, d'empêcher leur modification et leur utilisation frauduleuse (ISO 8732); NOTE – Le chiffre définit les méthodes de chiffrement et déchiffrement. L'attaque d'un principe, de moyens ou de méthodes cryptographiques est appelée cryptanalyse.
clés	séries de symboles commandant les opérations de chiffrement et de déchiffrement (ISO 7498-2:1989);
gestion des clés	production, stockage, distribution, suppression, archivage et application de clés conformément à la politique de sécurité (ISO 7498-2:1989);
politique de sécurité	ensemble des critères permettant de fournir des services de sécurité (ISO 7498-2:1989).

6.3 La téléphonie sur Internet

6.3.1 Généralités

L'apparition de services toujours plus performants, la volonté des fournisseurs d'accès à Internet de commercialiser des offres de services vocaux et l'attrait financier des utilisateurs pour ces offres laissent présager d'importantes perspectives de développement pour ce type de services. Suivant la législation en vigueur dans chaque pays et les programmes de libéralisation du secteur des télécommunications, l'Etat détient ou non le monopole de l'exploitation du téléphone public. Suite au développement des technologies de l'information et relativement aux différents accords entre les Etats et les différents prestataires de services Internet (PSI), il est important de définir le statut à donner aux communications vocales sur Internet, pour éviter des interprétations et des confusions qu'elles peuvent engendrer lorsqu'on décide de les exploiter.

6.3.2 Définition

La définition de la téléphonie vocale est sujette à certaines interprétations suivant les aspects techniques ou fonctionnels. Pour l'article 1 de la Directive 90/388/CE, on entend par «service de téléphonie vocale», l'exploitation commerciale pour le public du transport direct et de la commutation de la voix en temps réel au départ et à destination des points de terminaison du réseau public commuté, permettant à tout utilisateur d'utiliser l'équipement connecté à un tel point de terminaison pour communiquer avec un autre point de terminaison. Elle précise ailleurs qu'il importe que le service offre «la possibilité de joindre automatiquement n'importe quel abonné au téléphone» pour pouvoir être qualifié de téléphonie vocale.

Certaines autorités, dont les autorités françaises, contestent et à juste titre cette interprétation restrictive de la définition, qui ne mentionne que des communications avec «un autre point de terminaison». Elles estiment qu'il n'est pas nécessaire que tous les points de terminaison du réseau public commuté puissent être joints pour que le service soit qualifié de service téléphonique public. Selon cette définition, les services restreints et les opérateurs qui n'offrent que des services de communications internationales ressortent bien du régime de la téléphonie vocale.

6.3.3 Evolution des communications vocales sur Internet

De manière générale, en matière de communication vocale sur Internet, on peut en distinguer deux cas:

- *Les communications vocales de première génération:* Ces communications concernent certains utilisateurs, qui se sont dotés par eux-mêmes d'un logiciel transformant la voix en données et vice versa et qui sont en mesure, à partir de leur ordinateur, d'échanger une conversation avec un autre utilisateur d'Internet connecté au même moment et qui dispose d'équipements et logiciels de conversion compatibles sans une intervention spéciale du fournisseur d'accès.
- *Les communications vocales de seconde génération*: Ces communications impliquent une intervention active du prestataire d'accès. Il met en place, sur son serveur, les logiciels permettant la transformation de la voix en données et vice versa, ainsi que les interfaces permettant de joindre n'importe quel abonné sur le réseau téléphonique commuté (RTC). L'utilisateur peut alors, à partir de son ordinateur ou de son poste téléphonique, selon le service proposé, appeler son fournisseur d'accès à Internet, qui achemine la communication via Internet. Techniquement, ces systèmes IP doivent être compatibles avec le protocole de signalisation SS7 et conformes aux normes relatives aux Recommandations H.323 et H.248 de l'UIT-T.

6.3.4 Exploitation commerciale de la téléphonie sur Internet

Les services de «seconde génération» sont disponibles à titre expérimental, dans plusieurs pays, et sont une réalité aux Etats-Unis. Ils sont susceptibles de poser à court terme un problème de concurrence réel pour les communications longue distance à tout opérateur du téléphone classique, si tous les prestataires de services Internet se mettaient également à les exploiter.

L'intérêt des utilisateurs, la nécessité de maintenir un cadre réglementaire cohérent, équilibré et non discriminatoire, la nécessité d'assurer des conditions de concurrence loyale entre les différents acteurs, ainsi que la nécessité d'assurer la fourniture du service universel et un financement pérenne de celui-ci, tout en encourageant l'innovation, nous ont amené à formuler les propositions suivantes:

- Les administrations devraient considérer que les communications vocales de seconde génération font partie des services réservés soumis aux licences d'exploitation dans le cadre de la libéralisation des télécommunications. Les droits et obligations attachés, notamment en termes d'interconnexion et de contribution au financement du service universel, seront exigés aux exploitants de ces services.
- Les communications vocales sur Internet de «première génération», ne sont pas considérées comme de la téléphonie vocale, ce qui implique notamment que leur fourniture est libéralisée, et qu'elles ne peuvent faire l'objet ni d'une licence individuelle ni d'une contribution au financement du service universel.

Toutefois, l'évolution des technologies et du marché pourrait remettre en cause ces propositions à tout moment.

7 Renforcement des capacités locales

7.1 Généralités

Le développement de la Société africaine de l'information passe par le renforcement des capacités locales. En matière d'administration de systèmes informatiques tels que la gestion de nœuds nationaux d'Internet, il est indispensable d'être bien formé sur l'administration de systèmes UNIX et Windows NT, les plus utilisés sur Internet et de suivre régulièrement des séminaires de formation sur les nouvelles technologies de l'information.

7.2 Système d'exploitation UNIX

Une formation de base sur le système UNIX Solaris 2.x est nécessaire pour avoir une connaissance d'ensemble et ainsi pouvoir exploiter au maximum le potentiel des applications Internet (TCP/IP et l'administration des réseaux). Nous recommandons aux opérateurs télécom en Afrique de former des ingénieurs à l'administration UNIX. Cette formation peut être organisée dans les centres de formation nationaux bien équipés. Cette formation peut être répartie en 10 chapitres comme suit:

1 Généralités
2 Arborescence
3 Les périphériques
4 Le système de fichiers
5 Démarrage et arrêt du système
6 Messagerie et communication
7 Gestion des processus
8 Gestion des utilisateurs
9 Gestion des impressions
10 Sécurité sous UNIX

7.3 TCP/IP en environnement NT

Face à une progression très rapides des réseaux locaux en environnement NT et l'importance grandissante que prend Microsoft sur le marché Internet, il est également important de renforcer les connaissances des responsables locaux à la gestion et administration des réseaux TCP/IP en environnement NT dans le but de pouvoir exploiter au maximum les potentialités de Internet Information Server dans le cadre de la gestion de Internet, des Intranet et Extranet. Cette formation peut être répartie en 15 chapitres comme suit:

1 Adressage Internet.
2 Adressage de sous-réseaux.
3 Routage sous TCP/IP.
4 Installation et configuration d'un routeur Windows NT server.

5 Le service DHCP.

6 Résolution d'adresses ARP.

7 NetBios sur TCP/IP.

8 Le service serveur WINS

9 Le service des noms de domaines.

10 Le protocole SNMP.

11 Commandes et utilitaires TCP/IP.

12 Le protocole IP.

13 Le protocole ICMP.

14 Le protocole UDP.

15 Le protocole TCP.

7.4 Netscape SuiteSpot

Dans le contexte de la fusion des grandes sociétés leaders sur le marché d'Internet où Netscape, AOL et Sun Microsystems ont uni leurs efforts pour dominer ce marché, il nous semble important et vital pour les opérateurs télécom en Afrique de mettre un accent particulier et former les responsables locaux à la configuration et administration de serveur Internet basée sur la solution Netscape SuiteSpot. Cette formation peut être subdivisée en plusieurs parties relatives aux notions suivantes:

- Procédures réseaux et architecture des services Internet.
- Directory Server v 3.11 installation, administration, gestion db.
- Certificate Server v 1.0.1 installation, configuration, démarrage, synchro LDAP.
- Enterprise Server v 3.5.1 installation, configuration, directory server gateway.
- Messaging Server v 3.5 installation, configuration.
- Collabra Server v 3.51 installation, configuration.
- Proxy Server v 3.5 installation, configuration.

7.5 Internet Information Server

La solution Internet Information Server n'est pas à négliger car elle apporte également tous les outils indispensables à la création, au déploiement des applications, à l'administration et à l'analyse quotidienne des activités sur les sites Web. Une formation complète garantissant un réel succès devrait être basée sur les notions suivantes:

- L'installation et la configuration de IIS (Internet Information Server 4.0).
- La configuration et la gestion de l'accès aux ressources.
- L'intégration et l'interactivité.
- Le fonctionnement des applications.
- Le contrôle et l'optimisation.
- La résolution des problèmes.

7.6 Métrologie et gestion de la qualité

La qualité de service (QoS) dans Internet est encore un vaste chantier. La méthode utilisée jusqu'à présent consiste à fournir des réseaux surdimensionnés et comme Internet croît tous les jours, cette méthode ne peut plus s'appliquer indéfiniment. La culture de la qualité de service est très importante pour pouvoir exploiter convenablement les services Internet. En Afrique, l'ingénierie des services risque de connaître un

retard faute des capacités locales pour gérer les performances d'un réseau et assurer un service de bonne qualité. Il est donc nécessaire et urgent de former les ingénieurs pour implémenter la qualité de service dans Internet et sous forme de services différenciés, ainsi que l'architecture «Integrated Services» développée par l'IETF (*Internet Engineering Task Force*). Les logiciels et les principaux points qui peuvent être l'objet d'une formation ou de séminaires sont les suivants:

- Logiciel «NNSTAT» ftp://gatekeeper.dec.com/pub/DEC/net/NNstat_3.3beta.tar.Z.
- Le logiciel *Optivity* de Bay Networks.
- IP Trafic (http://www.urec.cnrs.fr/IPtrafic/).
- NetraMet (Network traffic Meter).
- MRTG (The Multi Router Traffic Grapher) (http://www.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg.html).
- Généralités sur la qualité de service.
- Critères de base de la qualité de service dans Internet.
- Implémenter la QoS dans Internet.
- Modèle «Integrated Services » de l'IETF.
- Mesurer la QoS.
- Routage, ATM et QoS.

8 Conclusion

Internet et les autoroutes de l'information véhiculent à la fois le son, les images et les données. Selon la société californienne RateXchange, spécialisée dans la négociation de minutes de téléphone et de bande passante sur le Web, 40% du trafic sera constitué en 2004 par des données, contre 18% en 1998. En revanche, aujourd'hui 78% du trafic représente le transport de la voix, ce trafic chutera à 30% en 2004. Internet est donc incontournable pour la vie économique moderne.

Internet est vital pour le développement de l'Afrique. La tâche est immense et les efforts que doit déployer l'UIT/BDT pour développer cette technologie en Afrique sont attendus par tous les pays Membres de l'Union et couvrent plusieurs domaines: la connectique, la gestion technique, l'administration des systèmes, l'ingénierie des services et la métrologie, sans oublier le renforcement des capacités locales et les centres d'excellence pour le montage d'ordinateurs dans chaque pays, comme base de l'industrie moderne des télécommunications du XXIe siècle.

Des plans d'actions au travers de la mise en œuvre d'une infrastructure de réseau basée sur les tous récents progrès technologiques sont à encourager. Il faut aller au-delà de la technologie Internet classique et dépasser la dépendance vis-à-vis du trafic téléphonique habituel. Des efforts particuliers devront être consentis pour l'élargissement du public visé à travers la mise en place de boucles locales et la fourniture de prestations diversifiées et innovatrices répondant aux attentes de la clientèle.

L'UIT assiste ses Membres à promouvoir en Afrique les autoroutes de l'information et doter ce continent d'une infrastructure de télécommunications lui permettant de relever le défi universel sans précédent qu'est Internet.

9 Bibliographie

[1] KARYABWITE, Désiré, UIT/MAL/R.126, *Gestion technique du nœud et stratégie de développement d'Internet au Mali,* Société des télécommunications du Mali*,* SOTELMA, 1998.

[2] KARYABWITE, Désiré, UIT/COI/185, *Propositions et formation pour l'amélioration du système d'information de gestion des télécommunications aux Comores*, SNPT, 1997.

[3] KARYABWITE, Désiré, UIT/MAG/186, *Propositions et formation pour l'amélioration du système d'information de gestion des télécommunications à Madagascar*, TELMA, 1997.

[4] KARYABWITE, Désiré, *Management des technologies, Internet pour les PME de hautes technologies*, EPFL, 1996.

[5] UIT Guide du passage à l'An 2000, 1999.

[6] Recommandation UIT-T H.233, *Système de confidentialité pour les services audiovisuels*, 1995.

[7] Recommandation UIT-T H.234, *Système de gestion de clés de chiffrement et d'authentification pour les systèmes audiovisuels*, novembre 1994.

[8] *Challenges to the Network Internet for Development*, UIT, 1999.

[9] *Réseaux TCP/IP*, Editions Wan & Laser, 1997.

[10] HUNT, Craig, O'Reilly & Associates Inc., chez Addison Wesley.

[11] Du BOIS, Robert, *Structure et applications des émetteurs et des récepteurs*, PPR-1995.

[12] BOUYER, Gérard, *Transmissions et réseaux de données*, chez DUNOD, 1995.

[13] VIALLE, Pierre, *Stratégies des opérateurs de télécoms*, chez HERMÈS,1998.

[14] BOISSEAU, Marc, *Les communications par satellite*, chez HERMÈS, 1991.

[15] PERRICHON, J.-M., *Les réseaux sans fil*, chez MASSON*,* 1994.

[16] SERVIN, Claude, *Télécoms de la transmission à l'architecture de réseaux*, InterEditions, 1998.

[17] Netsurf, numéro 34.

[18] Site de la bourse pour les minutes de télécommunications: www.Pulver.com.

[19] Authentification et analyse de trafic: logiciel RADIUS (http://www.livingston.com/Forms/radiusform.cgi, ou http://www.merit.edu/aaa/).

[20] Sécurité et FireWall (http://www.tis.com/docs/products/fwtk/).

[21] Livres sur Internet (http://www.ora.com/).

[22] CIZAULT, Gisèle, *IPv6 Théorie et pratique,* chez O'REILLY.

[23] Le BOUDEC, J.Y., FI-9/1995.

[24] FERGUSON, Paul, HUSTON, Geoff, *Quality of Service: Delivering QoS on the Internet and in Corporate Networks,* Wiley Computer Publishing, 1998.

[25] Articles sur la QoS: http://www.wiley.com/compbooks/ferguson/.

[26] FERGUSON, Paul, HUSTON, Geoff, *Quality of Service: Fact, Fiction or Compromise?,* INET 98.

Annexe I

Budget prévisionnel

Equipement pour un nœud national Internet	
Routeurs (2 Cisco 4000)	US$ 20 000
Concentrateur (Synoptics) et routeurs pour ISP (5 Cisco 2511)	15 000
PC pour serveur public WWW (Pentium)	7 000
PC pour le développement de WWW (Pentium)	7 000
PC pour le contrôle du réseau et de la compatibilité	7 000
Poste de travail pour la gestion du système de sécurité	20 000
Système de backup	3 000
Logiciels	11 000
Frêt	10 000
Sous-total	100 000
Equipement pour la formation	
Routeur	5 000
PC pour serveur WWW (Pentium)	7 000
PC pour le contrôle de la compatibilité	7 000
Serveur terminal (avec 16 modems)	10 000
Logiciels	4 000
Frêt	7 000
Sous-total	40 000
Ingénierie, formation et appui technique	
Bases pour UNIX	15 000
Configuration et installation d'Internet	15 000
A déterminer (bourses de stage, experts, etc.)	50 000
Sous-total	80 000
Liaison avec le satellite international	
Une année	60 000
Sous-total	60 000
Imprévus	
Imprévus	20 000
TOTAL	300 000

Les chiffres indiqués en dollars et les marques des équipements ne sont donnés qu'à titre indicatif car les prix et les performances des équipements changent suivant les fabricants et le moment du passage effectif de la commande. Nous nous sommes inspirés des chiffres avancés par l'USAID pour le projet Leland concernant le montage d'un nœud national Internet élémentaire avec un débit confortable. Ce budget prévisionnel est une base de travail à adapter suivant les circonstances dans chaque pays.

Annexe II

Cahier des charges

Opérateur Internet – Installation et développement d'un nœud national Internet

II.1 Généralités

Ce cahier des charges est basé sur les technologies exposées dans ce Guide. Il est à l'usage de chaque pays africain qui souhaiterait obtenir des offres pour la fourniture et l'installation d'accès à Internet.

Pour le développement d'Internet, un nœud national peut suffire pour commencer mais très vite une nécessité d'un deuxième et voire même un troisième se fera sentir suivant l'étendue du territoire à couvrir, le backbone nécessaire et le niveau de qualité de service à atteindre.

La connexion vers Internet sera réalisée via une station terrienne et des liaisons filaires, en faisceau hertzien ou en fibres optiques pour constituer un système global de connexion.

Il est demandé à chaque soumissionnaire d'utiliser un débit élevé, une connexion backbone dédiée, le débit minimal étant de 128 kbit/s. Le but ultime d'un projet Internet est de fournir une extension du «Backbone» dans le pays et de permettre à l'opérateur national de fournir les services courants d'Internet (WWW, E-mail, FTP) aux ISP (*Internet Services Providers*) et aux autres abonnés.

II.2 Spécification du nœud national d'Internet

La conception du nœud national d'Internet devra permettre à l'opérateur national, aux ISP locaux et entreprises utilisatrices d'être facilement connectés via les liaisons spécialisées classiques ou en utilisant l'une ou l'autre des technologies de pointe.

Il sera également pris en compte les liaisons à haut débit. L'architecture du nœud doit respecter les standards agréés. Les critères principaux du choix du nœud seraient les suivants:

- Le nœud devra être facilement adaptable de telle sorte que la capacité puisse être étendue sans interruption totale des services.
- La clarification des solutions d'interconnexion future en cas d'extension du réseau suivant l'étendue du territoire.
- Le nœud devra être compatible avec les infrastructures de télécommunications locales et l'architecture proposée devra être facilement extensible.
- La redondance.
- La qualité des équipements et leurs spécifications techniques et normes.
- Le nœud devra être d'une maintenance aisée.
- Le nœud comportera des aiguillages redondants.
- Système de sécurité de communication, et les équipements associés permettant le contrôle.
- Fonction de supervision et possibilité de mener des actions correctives.
- La qualité des mesures et l'analyse du trafic.
- La clarté et la simplicité de la documentation fournie.
- La convivialité d'exploitation du système.

II.3 Equipements

II.3.1 Liaison satellite

La liaison satellite doit être clairement dimensionnée. La puissance d'émission du transpondeur dépend de la largeur du faiseau d'émission qui est lui-même dépendant de l'antenne. Plus on veut une diffusion large, plus il faut de puissance.

Les principales informations suivantes sont obligatoires:

- La compagnie à qui appartient le satellite.
- Le nom de l'opérateur International pour l'accès à Internet ainsi que la carte de son Backbone au niveau mondial.
- La vitesse de transmission (débit) et puissance.
- Les fréquences uplink et downlink.
- Les caractéristiques techniques de l'antenne et nature de polarisation.

II.3.2 Routeurs

Les routeurs proposés doivent pouvoir faire office de passerelle «Gateway» entre des réseaux de natures différentes (Ethernet à FDDI, Token Ring à Ethernet, ATM à FDDI). Prévoir que dans le cas où le réseau deviendrait maillé, de déterminer le meilleur chemin pour atteindre une adresse considérée (nombre de nœuds à franchir, qualité de la ligne, bande passante, etc.).

Les routeurs livrés devraient donc être configurés pour accepter la connectivité vers le réseau de l'opérateur international et vers d'autres réseaux locaux (à préciser suivant le pays). La configuration devant être facilement modifiable pour la croissance future.

Il faudra préciser les fonctionalités de l'algorithme de routage: s'il tient compte de tout ou partie des points suivants:

- *Optimisation* en sélectionnant la meilleure route dans tous les cas (ceci dépend des Metrics. Par exemple, un algorithme de routage peut utiliser le nombre de Hops et Delay mais peut mettre plus de poids pour le calcul pour le Delay).
- *Simplicité et robustesse*.
- *Rapidité de convergence* (la convergence est l'agrément entre tous les routeurs pour déterminer la meilleure route).

Le nombre de ports doit être suffisant pour l'interconnexion vers:

- La station terrienne.
- Un nombre suffisant d'ISP par lignes spéciales (LS).
- D'autres réseaux locaux (LAN de l'opérateur télécom, universités, hôpitaux).

En résumé, les routeurs devront avoir les caractéristiques suivantes:

- Les routeurs fonctionnent principalement au niveau 3 du modèle OSI.
- Peuvent faire office de Bridge pour certains protocoles.
- Permettront de diviser une classe d'adresse en Subnets, limitant ainsi le trafic et le taux de Broadcast.
- Peuvent filtrer des adresses <adresse IP – adresse MAC>.
- Déterminent le meilleur chemin en fonction de la bande passante de la ligne et du nombre de nœuds Hops à franchir.
- Maintiennent et transmettent aux nœuds suivants leurs tables de routage.

- Collectionnent les paires <Adresse IP – Adresse MAC> dans une table ARP.
- Font office de serveur de temps NTP. [Les routeurs peuvent faire office de serveur de temps en diffusant (Broadcast) dans les divers sous-réseaux l'heure exacte obtenue par une horloge selon le protocole NTP (*Network Time Protocol*)].
- Conforme au passade à l'an 2000.

Le nombre des routeurs est à préciser suivant les besoins de chaque pays. Ils utiliseront les protocoles standards de TCP/IP: IP; ICMP; ARP; RARP; IDP; RIP. Ils seront obligatoirement compatibles (SNMP) pour leur gestion.

II.3.3 DNS

Les soumissionnaires devront fournir les équipements du réseau local de l'organisme qui centralise les informations (le NIC), principalement pour le DNS (Domain Name Server). Ils préciseront le nombre et les caractéristiques des ordinateurs nécessaires, la configuration minimale étant la suivante: pour chaque ordinateur 450 MHz (ou supérieur), 128 Mégas de RAM, 10 Gigas de disque dur (ou mieux), une carte réseau 3COM Etherlink, un lecteur DVD, un lecteur de disquette 3,5 pouces, un écran SVGA de 17 pouces et le système d'exploitation UNIX Solaris 2.x. La même configuration peut être adoptée pour d'autres serveurs, par exemple le Secondary DNS server.

II.3.4 Autres équipements d'interconnexion

Les soumissionnaires devront fournir la liste d'équipements qu'ils jugent nécessaires pour la solution qu'ils proposent, à savoir les répéteurs, les ponts, les routeurs, les passerelles, les HUB (*Host Unit Broadcast*), les MAU (*Multistation Access Unit*). Les soumissionnaires préciseront les modems en mode asynchrone et les modems en mode synchrone (ISP).

II.3.5 Ordinateurs

Les ordinateurs utilisés dans le système de sécurité et de gestion seront des stations avec des imprimantes associées. La capacité des mémoires sera dimensionnée pour permettre d'exécuter toutes les fonctions sans dégradation des services avec une grande qualité de réponse.

II.4 Prestation nationale des services Internet

Afin de pouvoir développer la prestation de services Internet (grands comptes et particuliers), le LAN de l'opérateur national doit être configuré pour: un système de FireWall doit protéger les services Internet que fournit l'opérateur sauf les services publics comme le WWW.

Pour une meilleure gestion technique et un bon fonctionnement de tous les services Internet, il est conseillé dans la mesure du possible de réserver une machine dédiée pour chaque serveur correspondant au service Internet donné (en prévoyant donc l'extension du système et la facilité pour une maintenance aisée).

Les soumissionnaires devront préciser la configuration des machines, la topologie proposée (Ethernet standard, Ethernet fin, Ethernet 10 base T ou Fast Ethernet 100 base T) et les logiciels serveurs pour les principaux services Internet suivants:

- Le WWW.
- La messagerie électronique.
- Le FTP (transfert de fichiers).

- Les Forums ou News.
- Les accès sécurisés (authentification et certificats).
- Proxy.

Le serveur de communication établira au moins quelques centaines de communications simultanées avec une possibilité de l'étendre à 1 000. Il sera modulaire et extensible sans perturbation des services.

Les serveurs et les machines devront fonctionner sur le système UNIX Solaris 2.x ou sur Windows NT.

II.5 Gestion technique, sécurité et analyse du trafic

Les soumissionnaires devront fournir un système d'audit et sécurité du système, lutte contre les virus, un système de sauvegardes et la sécurité d'alimentation électrique en utilisant les onduleurs ou UPS (*Uninterruptible Power Supply*). La gestion et administration du réseau sera basée sur le protocole SNMP. Chaque soumissionnaire précisera le nombre d'ordinateurs et leurs caractéristiques techniques nécessaires pour la gestion des appareils de réseau. Il précisera le nombre de hubs, de routeurs, de bridges et autres switches qu'il peut gérer.

Les moyens de gestion du réseau seront clairement désignés ainsi que les plates-formes de gestion, par exemple, le produit HP OpenView, SunNet Manager ou Netview d'IBM, etc. Le système devra également avoir les moyens élémentaires de gestion comme: PING qui permet d'envoyer répétitivement des paquets à un nœud du réseau selon le protocole ICMP, TRACEROUTE qui, par ICMP, donne une trace du chemin parcouru par le paquet, ainsi que les temps de transit pour chaque nœud du parcours, etc.

Les mesures, l'analyse du trafic doivent être effectuées d'une façon conviviale. La base de données sur les informations du réseau doit être clairement définie et intégrée au système de gestion du réseau.

Parmi les opérations souhaitées, on peut citer (la liste n'étant pas exhaustive):

- *La gestion des défauts:* la détection, la localisation et la correction des perturbations du réseau.
- *La gestion de la configuration:* l'accès aux paramètres de configuration (adresses IP) ainsi que leurs modifications aisées.
- *La gestion des clients et base de données y relative:* la poursuite et les données nécessaires de création pour permettre la facturation des clients.
- *La gestion de la maintenance:* les poursuites d'exploitation du réseau lors de l'établissement ou de la modification, soit à l'utilisation, à l'identification, à l'adressage et à la maintenance du hardware ou logiciel.
- *Les performances de gestion:* les performances du réseau basées sur les objectifs liés au niveau de l'utilisation.
- *Système de protection par FireWall et fiabilité:* filtrage, protection du réseau contre les accès et utilisations non autorisés.
- *Prévision de la capacité:* les changements de la capacité et de la croissance basés sur les données d'utilisation du réseau, les performances et l'entrée de l'usager.
- *Secours à distance*.
- *Gestion des processus par le Web; gestion des ISP*.