Pujolle

LES RÉSEAUX

Édition 2011

EYROLLES

LES RÉSEAUX

Édition 2011

CHEZ LE MÊME ÉDITEUR

Du même auteur

G. Pujolle. – **Cours réseaux et télécoms**.
N°12415, 3e édition, 2008, 544 pages.

L. Ouakil, G. Pujolle. – **Téléphonie sur IP**.
N°12359, 2e édition, 2008, 466 pages.

D. Males, G. Pujolle. – **Wi-Fi par la pratique**.
N°11409, 2e édition, 2004, 420 pages.

Autres ouvrages sur les réseaux

L. Levier, C. Llorens. – **Tableaux de bord de la sécurité réseau**.
N°12821, 3e édition, 2010, 562 pages.

PH. Sultan. – **Asterisk**. *La téléphonie d'entreprise libre*.
N°12434, 2009, 298 pages.

M. Lucas, M. Derche. – **Le petit manuel des routeurs Cisco**.
N°12602, 2009, 162 pages.

J. Gabès, N. Makarévitch. – **Nagios 3 pour la supervision et la métrologie**.
N°12473, 2009, 482 pages.

P. N. M. Hansteen. – **Le livre de Packet Filter**.
N°12516, 2009, 190 pages.

R. Bergoin, C. Bourg. – **Mémento Cisco**. *IOS – Configuration générale*.
N°12347, 2008, 14 pages.

S. Borderes. – **Authentification réseau avec Radius**.
N°12007, 2006, 300 pages.

J. Steinberg, T. Speed, adapté par B. Sonntag. – **SSL VPN**. *Accès web et extranets sécurisés*.
N°11933, 2006, 220 pages.

B. Boutherin, B. Delaunay. – **Sécuriser un réseau Linux**.
N°11960, 3e édition, 2007, 250 pages.

X. Carcelle. – **Réseaux CPL par la pratique**.
N°11930, 2006, 382 pages.

J. Nozick. – **Guide du câblage universel**.
Logements et bureaux - Nouvelle norme NF C 15-100 - Prises universelles RJ 45.
N°11758, 2e édition, 2006, 110 pages.

LES RÉSEAUX

Édition 2011

Guy Pujolle

Avec la collaboration de Olivier Salvatori
et la contribution de Jacques Nozick

EYROLLES

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Historique des éditions successives de l'ouvrage

1re édition (ISBN : 978-2-212-08840-3) – juin 1995

2e édition (ISBN : 978-2-212-08967-7) – juillet 1997

Réédition en semi-poche (ISBN-13 : 978-2-212-09108-3) – juillet 1999

3e édition (ISBN : 978-2-212-09119-9) – mars 2000

Réédition en semi-poche (ISBN-13 : 978-2-212-11121-7) – juillet 2002

4e édition (ISBN : 978-2-212-11086-9) – juillet 2002

Réédition en semi-poche (ISBN-13 : 978-2-212-11525-3) – juillet 2004

5e édition (ISBN : 978-2-212-11437-9) – septembre 2004

Réédition en semi-poche (ISBN-13 : 978-2-212-11987-9) – septembre 2006

6e édition (ISBN : 978-2-212-11757-8) – septembre 2007

7e édition (ISBN : 978-2-212-12878-9) – novembre 2010

Préface à la 7e édition

Les réseaux composent la structure de base du septième continent qui se forme sous nos yeux. Par l'immense séisme que ce continent supplémentaire engendre en ce début de siècle, la planète entre dans une ère nouvelle. Ce continent est celui de la communication. Constitué de réseaux se parcourant à la vitesse de la lumière, il représente une rupture analogue à l'apparition de l'écriture ou à la grande révolution industrielle.

Ces réseaux, qui innervent aujourd'hui complètement la planète, s'appuient sur la fibre optique, les ondes hertziennes et divers équipements qui permettent d'atteindre de très hauts débits. Internet incarne pour le moment la principale architecture de ces communications.

Les réseaux forment un domaine tellement complexe qu'il est impossible d'en rendre compte de façon exhaustive, et ce livre pas plus que les autres, n'en a la prétention. Simplement, il vise à faire comprendre, de manière à la fois technique et pédagogique, les fondements des réseaux en en dressant un panorama aussi complet que possible.

Les refontes apportées à cette septième édition sont importantes. Premièrement, elle a été réduite de plus d'un tiers afin de ne garder que les éléments de base, en renvoyant tous les suppléments en annexe. Deuxièmement, elle a révisé profondément les principaux chapitres et en a introduit de nouveaux, comme les réseaux hertziens de 4e génération, l'Internet des choses, la virtualisation, etc. Les annexes de l'ouvrage sont disponibles sur le Web. Elles représentent un volume d'informations aussi important que le livre lui-même.

Au total, c'est plus d'un quart du livre qui est totalement neuf et un autre bon quart qui a été fortement remanié. L'autre moitié provient de la 6e édition, tout en étant également améliorée.

Nous recommandons au lecteur d'effectuer la lecture des trente-deux chapitres qui composent l'ouvrage en continuité. Sa construction en huit parties permet aussi de le parcourir par centre d'intérêt.

Il est important de noter une innovation importante : les références bibliographiques, les annexes et toutes sortes d'informations qui viendraient à enrichir le contenu de l'ouvrage sont désormais accessibles sur la page Web dédiée du site Web d'Eyrolles, à l'adresse *www.eyrolles.com*. L'avantage de cette solution est de permettre la mise à jour en continu des références bibliographiques, qui jouent un rôle important dans un monde très vivant.

De même, si certaines annexes n'ont que peu de raisons de changer, de nouvelles annexes devraient apparaître régulièrement pour informer les lecteurs des grandes directions du monde des réseaux.

Cette septième édition n'aurait pu exister sans les six premières et sans l'aide précieuse, depuis 1995, de collègues et de plusieurs générations d'étudiants. Je suis heureux de remercier ici un grand nombre d'entre eux ayant terminé leur thèse depuis plus ou moins longtemps pour leur aide précieuse sur des sujets arides et des collègues plus expérimentés pour leurs apports de qualité.

Table des matières

CHAPITRE 4

Partie II

Partie III

Partie V

Annexes

Appendices

Première partie

Les éléments de base des réseaux

Les réseaux ont pour fonction de transporter des informations afin de réaliser des services pouvant se trouver n'importe où sur le globe. Une série d'équipements matériels et de processus logiciels sont mis en œuvre pour assurer ce transport, depuis les câbles terrestres ou les ondes radio dans lesquels circulent les données jusqu'aux protocoles et règles permettant de les traiter.

Cette première partie de l'ouvrage rappelle les principes de fonctionnement des réseaux et présente en détail les matériels, les logiciels et les architectures protocolaires sur lesquels ils se fondent.

1

Introduction aux réseaux

Les réseaux sont nés du besoin de transporter des données d'un ordinateur à un autre ordinateur. Ces données étant mises sous la forme de fichiers, l'application de base des réseaux est donc le transfert de fichiers. Un peu plus tard, le « transactionnel » est apparu pour permettre à un utilisateur de réaliser des transactions avec un ordinateur distant, par exemple réserver une place d'avion. La session correspond à l'ensemble des transactions d'un même utilisateur pour réaliser une tâche donnée.

Avec l'apparition du Web, le service transactionnel s'est diversifié afin de permettre la recherche d'information par le biais de liens. Ces applications s'appellent client-serveur, c'est-à-dire qu'un client s'adresse à un serveur pour obtenir de l'information.

L'étape suivante des réseaux a été caractérisée par le pair-à-pair, ou P2P (*peer-to-peer*). Dans cette application, tous les éléments connectés au réseau sont équivalents et peuvent être distribués dans le réseau. Les applications pair à pair sont bien connues, en particulier de ceux qui recherchent des fichiers audio ou vidéo sur Internet. Les applications sous-jacentes sont en fait très nombreuses, allant de la téléphonie à la recherche d'informations diverses et variées.

Sans que cela supprime les applications de transfert de fichiers, qu'elles soient client-serveur ou pair à pair, le nouveau service Internet en vogue au début des années 2010 est le *Cloud*, ou « nuage ». Jusqu'à l'arrivée des Clouds, le réseau Internet avait pour objectif de transporter des données pour réaliser un service à distance. Les entreprises permettaient aux itinérants de se connecter à leurs serveurs par le biais d'Internet. Elles possédaient tous les serveurs nécessaires à cela, comme la messagerie électronique, les applications métier ou les serveurs d'archivage, ainsi que la puissance de calcul nécessaire. Aujourd'hui, il est possible de réaliser dans le Cloud ce qui se faisait auparavant dans l'entreprise : calcul, stockage, application métier, messagerie, téléphonie, etc. Les avantages sont nombreux : le client peut accéder à ces services de n'importe où ; ils peuvent être sécurisés par de la redondance ; on peut ajouter instantanément de nouveaux

services, de la puissance de calcul, de l'espace de stockage, etc., au fur et à mesure des besoins, en ne payant que ce qui est utilisé.

Cette nouvelle génération met en œuvre le concept de virtualisation, par lequel les ressources dont l'entreprise ou le particulier à besoin peuvent se trouver n'importe où, voire se déplacer en fonction du coût des serveurs.

Avant de détailler plus avant dans ces nouvelles générations de réseaux, nous allons rappeler quelques éléments clés de l'évolution des réseaux et des architectures actuelles.

Transfert, commutation et routage

Les réseaux modernes sont apparus au cours des années 1960 à la faveur d'une technologie totalement nouvelle permettant de transporter de l'information d'une machine à une autre. Ces machines étaient des ordinateurs de première génération, guère plus puissants qu'un petit assistant personnel actuel. Les réseaux de téléphonie existaient quant à eux depuis longtemps. Ils utilisaient la technologie dite de *commutation de circuits* et le support de lignes physiques reliant l'ensemble des téléphones par le biais de commutateurs. Lors d'une communication, ces lignes physiques ne pouvaient être utilisées que par les deux utilisateurs en contact. Le signal qui y transitait était de type analogique.

La première révolution des réseaux a été apportée par la technologie numérique des codecs (codeur-décodeur), qui permettaient de transformer les signaux analogiques en signaux numériques, c'est-à-dire une suite de 0 et de 1. Le fait de traduire tout type d'information sous forme de 0 et de 1 permettait d'unifier les réseaux. Dans cette génération, la commutation de circuits était toujours fortement utilisée. Les circuits étant devenus numériques, la question s'est posée de faire passer simultanément sur un même circuit plusieurs flots, correspondant à des applications différentes. C'est ainsi qu'on a pu, par exemple, avoir 1 octet (8 bits) de téléphonie, suivi de 2 bits de transfert de fichiers puis de 8 bits d'application vidéo. Cette solution ne s'est toutefois quasiment pas développée et a laissé la place au transfert de paquets.

Le transfert de paquets a permis de prendre en compte la forte irrégularité du débit de la communication entre deux ordinateurs, alternant les périodes de débit important et les périodes de silence, résultant du fait que, par exemple, un ordinateur doit attendre la réponse d'un autre ordinateur.

Dans la commutation de circuits, le circuit reste inutilisé pendant les périodes de silence, induisant un important gaspillage des ressources. À l'inverse, le transfert de paquets n'utilise les ressources du réseau que lors de l'émission effective des paquets. L'idée s'est donc fait jour de constituer des blocs d'information de longueur variable et de les envoyer de nœud de transfert en nœud de transfert jusqu'à atteindre la destination. Les ressources d'une liaison entre deux nœuds ne sont de la sorte utilisées que pendant le transfert des paquets. Les différents paquets provenant d'un même utilisateur et d'une même application forment un *flot*. Une fois les paquets de ce flot parvenus à destination, il est possible d'utiliser la même liaison et les ressources du réseau pour le passage d'autres paquets, provenant d'autres flots.

Parmi les nombreuses solutions de transfert de paquets qui ont été proposées, deux ont résisté au temps, le routage de paquets et la commutation de paquets. Dans le routage

de paquets, les paquets sont aiguillés par chaque nœud de transfert en fonction de leur destination. La route choisie peut être différente selon l'état du réseau, de telle sorte que deux paquets d'un même flot peuvent suivre une route différente. Des *tables de routage* sont implémentées dans ces nœuds afin d'optimiser le transport des paquets en fonction de l'état du réseau.

Issue du monde des télécommunications, la commutation de paquets consiste à mettre en place, avant d'envoyer le moindre paquet, un chemin entre les entités en communication, chemin que tous les paquets d'un même flot doivent emprunter. Ce chemin est appelé *circuit virtuel* parce les paquets d'autres communications peuvent utiliser les mêmes ressources. Il n'y a donc pas de ressource réservée.

Chacune de ces techniques présente des avantages et des inconvénients. Le routage est une technique souple. Dans la mesure où chaque paquet transporte l'adresse du destinataire, la route peut varier sans difficulté, et le paquet n'est jamais perdu. En revanche, il est très difficile d'y assurer une qualité de service, c'est-à-dire de garantir que le service de transport sera capable de respecter une performance déterminée. Avec la commutation de paquets, la qualité de service est plus facilement assurée, puisque tous les paquets suivent un même chemin et qu'il est possible de réserver des ressources ou de déterminer par calcul si un flot donné a la possibilité de traverser le réseau sans encombre.

La principale faiblesse de la commutation de paquets réside dans la mise en place du chemin que vont suivre les différents paquets d'un flot. Ce chemin est ouvert par une procédure spécifique, appelée *signalisation :* on signale au réseau l'ouverture d'un chemin, lequel doit en outre être « marqué » afin que les paquets du flot puissent le suivre. Cette signalisation exige d'importantes ressources, ce qui rend les réseaux à commutation de paquets sensiblement plus chers que les réseaux à routage de paquets.

La figure 1.1 illustre ces deux branches du transfert de paquets, le routage et la commutation, ainsi que les principales techniques qu'elles utilisent.

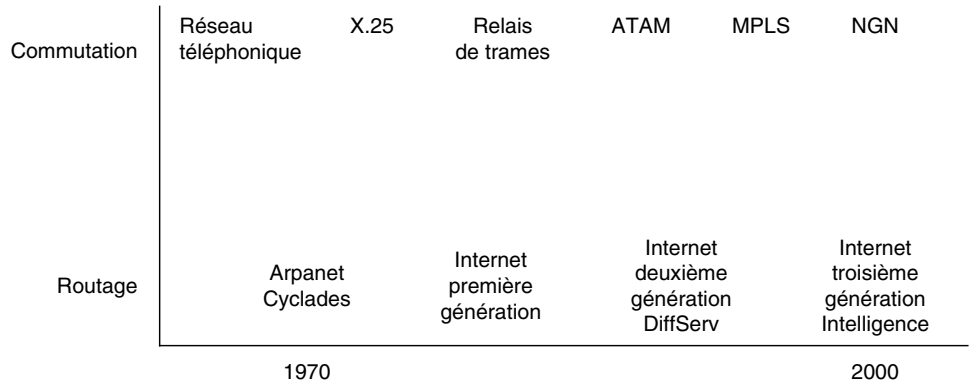


Figure 1.1

Les deux branches du transfert de paquets

Ces deux catégories de réseaux se sont développées en parallèle. Au départ, il n'y avait que peu de concurrence entre ces deux catégories qui s'adressaient à des mondes différents. Avec le temps, les techniques de routage, liées à Internet, se sont étendues au transport d'applications synchrones telles que la téléphonie et la vidéo. En parallèle, la commutation de paquets prenait en charge la téléphonie et la télévision. Aujourd'hui, tous deux sont en concurrence pour le transport des applications multimédias. Leurs avantages et inconvénients auraient plutôt tendance à faire choisir la commutation de paquets par les opérateurs et les très grandes entreprises et le routage par les petites et moyennes entreprises.

Les techniques de routage n'ont que peu changé. Le protocole IP (Internet Protocol) en constitue le principal déploiement : le paquet IP contenant l'adresse complète du destinataire est routé dans des nœuds de transfert appelés routeurs.

À l'inverse, les protocoles liés à la commutation ont beaucoup évolué. La première grande norme de commutation, X.25, a vu le jour dans les années 1980. Cette solution exigeait des opérations importantes pour effectuer la commutation : le chemin était tracé dans le réseau par un ensemble d'indices, appelés *références*, constituant autant de « pierres blanches » sur le chemin. Ces références étant placées dans le paquet lui-même, leur récupération exigeait au départ des efforts importants. Une simplification de ce système de signalisation a été apportée par le relais de trames puis par la technique ATM (Asynchronous Transfer Mode).

Avant d'aller plus loin, il nous faut avancer un peu plus en détail dans la notion de paquet. Un paquet n'est pas un bloc de données que l'on peut envoyer tel quel sur une ligne de communication. Par exemple, si l'on envoie deux paquets collés l'un à l'autre, le récepteur est incapable de distinguer la fin du premier paquet et le début du second. Pour permettre cette opération de reconnaissance, il faut encapsuler chaque paquet dans une trame. La trame possède une succession spécifique d'éléments binaires permettant de reconnaître son début et sa fin. Pour transporter un paquet IP, on peut l'encapsuler dans une trame PPP (Point-to-Point Protocol) ; pour transporter un paquet X.25, on l'encapsule dans une trame LAP-B.

Dans les générations de réseaux suivantes, l'adresse complète du destinataire, ou la référence, est reportée dans la trame afin d'en simplifier la récupération : il n'est de la sorte plus nécessaire de décapsuler la trame pour récupérer le paquet et les informations qu'il contient. Cette solution, mise en œuvre notamment dans le relais de trames et l'ATM, simplifie énormément le travail effectué dans les nœuds de transfert.

Les réseaux avec et sans fil

L'apparition de la technologie paquet dans les réseaux de mobiles et les réseaux sans fil date du début des années 2000 avec l'UMTS (Universal Mobile Telecommunications System). La génération d'avant, le GSM (Global System for Mobile Communications), était fondée sur le circuit. Les réseaux de mobiles permettent la communication tout en se déplaçant. Dans les réseaux sans fil, la communication se fait par le biais d'une antenne, et l'utilisateur doit rester connecté à la même antenne. Les premiers réseaux hertziens

avaient des débits très limités, mais ils ont vite atteint des performances quasiment identiques à celles des réseaux terrestres, du moins sur les paires métalliques.

Les réseaux hertziens sont regroupés en deux catégories, l'une provenant des industriels des télécommunications – et donc de la commutation –, avec une signalisation importante et une forte complexité pour prendre en charge tous les problèmes de la communication, l'autre provenant d'Internet – et donc du routage –, avec beaucoup moins de complexité mais une qualité globale inférieure.

La quatrième génération de réseaux sans fil est devenue complètement compatible avec Internet. Elle atteint des débits identiques à ceux des modems ADSL. Il y a donc uniformisation des mondes filaires et sans fil, de telle sorte qu'un même réseau cœur, le réseau de fibre optique central, permet d'interconnecter un terminal fixe aussi bien qu'un terminal mobile. Cette convergence, que nous décrirons plus en détail dans la suite de ce livre, par le biais d'un réseau cœur unique est appelé NGN (Next Generation Network).

Ces réseaux filaires ou sans fil sont multimédias. Une application multimédia utilise en même temps l'image animée, la parole, le graphisme et des assistances diverses.

Les caractéristiques de cette convergence sont les suivantes :

- Débits très importants dans le réseau cœur, notamment du fait de l'augmentation de la puissance des machines terminales et du débit de chaque client vers le réseau cœur.
- La qualité de service pour réaliser les contraintes de chaque application.
- La sécurisation du transport.
- La gestion de la mobilité et du raccordement à plusieurs réseaux simultanément (multihoming).
- La virtualisation de toutes les ressources du réseau pour réaliser des Clouds.

Le transfert de paquets

La technique utilisée pour le transport des données sous forme numérique, c'est-à-dire sous forme de 0 et de 1, que l'on a adoptée depuis la fin des années 1960 s'appelle le transfert de paquets.

Toutes les informations à transporter sont découpées en paquets pour être acheminées d'une extrémité à une autre du réseau. Cette technique est illustrée à la figure 1.2. L'équipement terminal A souhaite envoyer un message à B. Le message est découpé en trois paquets, qui sont émis de l'équipement terminal vers le premier nœud du réseau, lequel les envoie à un deuxième nœud, et ainsi de suite, jusqu'à ce qu'ils arrivent à l'équipement terminal B.

Le paquet peut provenir de différentes sources. À la figure 1.2, nous supposons que la source est un message préparé par l'émetteur, tel qu'une page de texte éditée au moyen d'un traitement de texte. Le terme message est en fait beaucoup plus vaste et recoupe toutes les formes sous lesquelles de l'information peut se présenter. Cela va d'une page Web à un flot de parole téléphonique représentant une conversation.

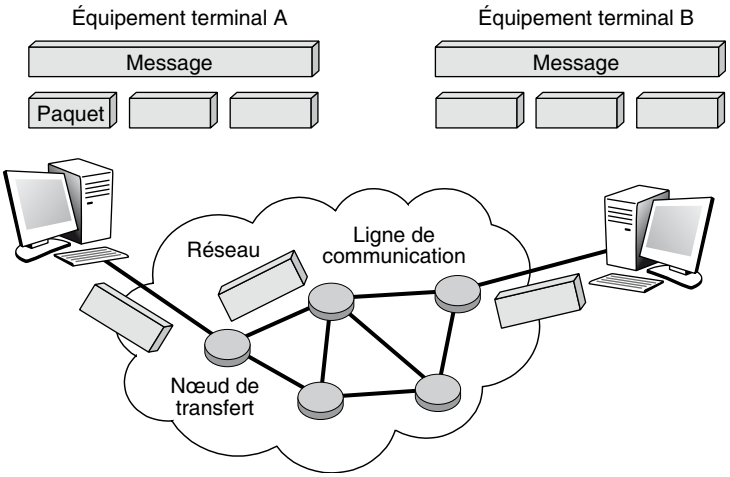


Figure 1.2
Le transfert de paquets

Dans la parole téléphonique, l'information est regroupée pour être placée dans un paquet, comme illustré à la figure 1.3. Le combiné téléphonique contient un équipement qui transforme la parole analogique en une suite d'éléments binaires. Ces bits remplissent petit à petit le paquet. Dès que celui-ci est plein, il est émis vers le destinataire. Une fois le paquet arrivé à la station terminale, le processus inverse s'effectue, restituant les bits régulièrement à partir du paquet pour reconstituer la parole téléphonique.

Le réseau de transfert est composé de nœuds, appelés nœuds de transfert, reliés entre eux par des lignes de communication, sur lesquelles sont émis les éléments binaires constituant les paquets. Le travail d'un nœud de transfert consiste à recevoir des paquets et à déterminer vers quel nœud suivant ces derniers doivent être acheminés.

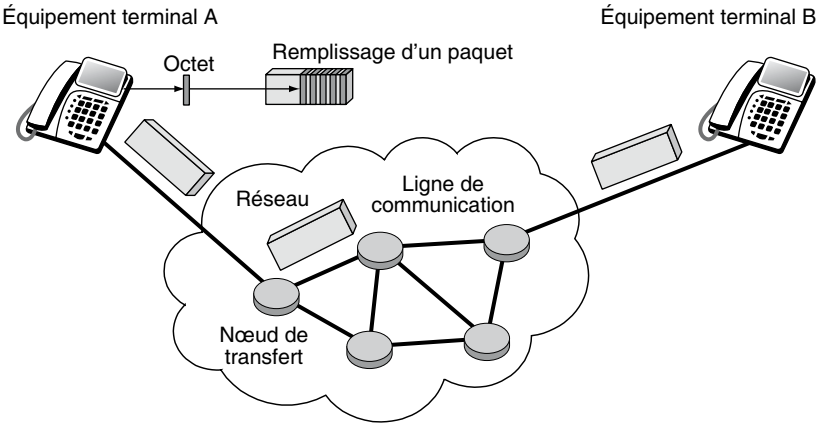


Figure 1.3
Flot de paquets téléphoniques

Le paquet forme donc l'entité de base, transférée de nœud en nœud jusqu'à atteindre le récepteur. Suivant les cas, ce paquet peut être regroupé avec d'autres paquets pour reconstituer l'information transmise. L'action consistant à remplir un paquet avec des octets s'appelle la mise en paquet, ou encore la paquétisation, et l'action inverse, consistant à retrouver un flot d'octets à partir d'un paquet, la dépaquétisation.

L'architecture d'un réseau est définie principalement par la façon dont les paquets sont transmis d'une extrémité à une autre du réseau. De nombreuses possibilités existent pour cela, comme celles consistant à faire passer les paquets toujours par la même route ou, au contraire, à les faire transiter par des routes distinctes de façon à minimiser les délais de traversée.

Le modèle de référence

Pour identifier correctement toutes les composantes nécessaires à la bonne marche d'un réseau à transfert de paquets, un modèle de référence a été mis au point. Ce modèle définit une partition de l'architecture en sept niveaux, prenant en charge l'ensemble des fonctions nécessaires au transport et à la gestion des paquets. Ces sept couches de protocoles ne sont pas toutes indispensables, notamment aux réseaux sans visée généraliste. Chaque niveau, ou couche, offre un service au niveau supérieur et utilise les services du niveau inférieur.

Pour offrir ces services, les couches disposent de protocoles, qui appliquent les algorithmes nécessaires à la bonne marche des opérations, comme l'illustre la figure 1.4. Nous supposons ici que l'architecture protocolaire est découpée en sept niveaux, ce qui est le cas du modèle de référence.

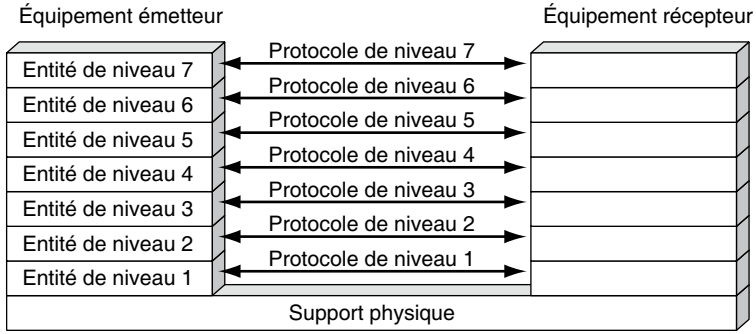


Figure 1.4

Architecture protocolaire d'un réseau à sept niveaux

La couche 3, ou couche réseau, représente le niveau paquet, qui définit les algorithmes nécessaires pour que les entités de cette couche, les paquets, soient acheminées correctement de l'émetteur au récepteur. La couche 7 correspond au niveau application. Le rôle du protocole de la couche 7 est de transporter correctement l'entité de niveau application, le message utilisateur, de l'équipement émetteur à l'équipement récepteur.

La couche 2, ou couche liaison, représente le niveau trame. Elle permet de transférer le paquet sur une ligne physique. En effet, un paquet ne contenant pas de délimiteur, le récepteur ne peut en déterminer la fin ni identifier le commencement du paquet suivant. Pour transporter un paquet, il faut donc le mettre dans une trame, qui, elle, comporte des délimiteurs. On peut aussi encapsuler un paquet dans un autre paquet, lui-même encapsulé dans une trame.

Dans cet ouvrage, nous distinguons les mots « paquet » et « trame » de façon à bien différencier les entités qui ne sont pas transportables directement, comme le paquet IP, et les entités transportables directement par la couche physique, comme les trames Ethernet ou ATM.

La structure en couches de l'architecture protocolaire des réseaux simplifie considérablement leur compréhension globale et facilite leur mise en œuvre. Il est possible de remplacer une couche par une autre de même niveau sans avoir à toucher aux autres couches. On peut, par exemple, remplacer la couche 3 par une couche 3 prime (3') sans modifier les couches 1, 2, 4, 5, 6 ou 7. On ne modifie de la sorte qu'une partie de l'architecture, la couche 3, sans toucher au reste. Les interfaces entre les couches doivent être respectées pour réaliser ces substitutions : l'interface de la couche 3' avec les couches 2 et 4 doit garantir que les couches 2 et 4 n'ont pas à être modifiées.

L'architecture illustrée à la figure 1.4 sert de référence à toutes les architectures réseau, d'où son nom de modèle de référence. Une autre architecture protocolaire, l'architecture TCP/IP (Transmission Control Protocol/Internet Protocol), a été définie un peu avant le modèle de référence par le ministère américain de la Défense. Son rôle premier était d'uniformiser l'interface extérieure des différents réseaux utilisés par le département d'État américain de façon à les interconnecter facilement. C'est cette architecture TCP/IP qui a été adoptée pour le réseau Internet, ce qui lui a offert une diffusion massive.

Une autre architecture provenant de l'utilisation de la trame plutôt que du paquet a été proposée par l'UIT-T (Union internationale des télécommunications-standardisation du secteur télécommunications), pour les applications utilisant à la fois les données, la téléphonie et l'image. Provenant principalement du monde des télécommunications, cette architecture est bien adaptée au transport de flux continus, comme la parole téléphonique. C'est la trame ATM (Asynchronous Transfer Mode) qui représente le mieux cette architecture. Cependant, cette architecture est en forte perte de vitesse, la trame ATM étant progressivement remplacée par la trame Ethernet.

Commutation et routage

Sous le concept de transfert de paquets, deux grandes techniques se disputent la suprématie : la commutation de paquets et le routage de paquets. Dans le routage, les paquets d'un même client peuvent prendre des routes différentes, tandis que, dans la commutation, tous les paquets d'un même client suivent un chemin déterminé à l'avance. De nombreuses variantes de ces techniques ont été proposées, comme nous le verrons dans la suite de l'ouvrage.

Certaines applications, comme la parole téléphonique, posent des problèmes spécifiques de transport lorsqu'elles sont acheminées sous forme de paquets. La difficulté réside dans

la récupération du synchronisme, le flot de parole devant être reconstitué au récepteur avec des contraintes temporelles fortes.

En supposant qu'une conversation téléphonique entre deux individus accepte un retard de 150 ms, il n'est possible de resynchroniser les octets à la sortie que si le temps total de paquétisation-dépaquétisation et de traversée du réseau est inférieur à 150 ms. Des fonctions intelligentes implémentées dans les terminaux informatiques permettent cette resynchronisation. Si un terminal ne dispose pas d'une telle intelligence, la reconstruction du flux synchrone est quasiment impossible après la traversée d'un réseau à transfert de paquets un tant soit peu complexe. Les réseaux de type Internet ont du mal à prendre en compte ces contraintes.

Les réseaux informatiques

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo est généralisée dans les réseaux informatiques, même si cela ne va pas sans difficulté.

On distingue généralement cinq catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau :

- Les réseaux personnels, ou PAN (Personal Area Network), qui interconnectent sur quelques mètres des équipements personnels tels que téléphone mobile, portables, organiseurs, etc., d'un même utilisateur.
- Les réseaux locaux, ou LAN (Local Area Network), qui correspondent par leur taille aux réseaux intra-entreprise. Ils servent au transport de toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par seconde.
- Les réseaux métropolitains, ou MAN (Metropolitan Area Network), qui permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux des différentes entreprises pour leur donner la possibilité de dialoguer avec l'extérieur.
- Les réseaux régionaux, ou RAN (Regional Area Network), ont pour objectif de couvrir une large surface géographique. Dans le cas des réseaux sans fil, les RAN peuvent avoir une cinquantaine de kilomètres de rayon, ce qui permet, à partir d'une seule antenne, de connecter un très grand nombre d'utilisateurs. Cette solution devrait profiter du dividende numérique, c'est-à-dire des bandes de fréquences de la télévision analogique, qui seront libérées après le passage au tout-numérique, fin 2011 en France. Les réseaux RAN sont introduits plus en détail au chapitre 9.

- Les réseaux étendus, ou WAN (Wide Area Network), sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise en ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellite, mais seulement pour des applications particulières à débit faible.

La figure 1.5 illustre sommairement ces grandes catégories de réseaux informatiques.

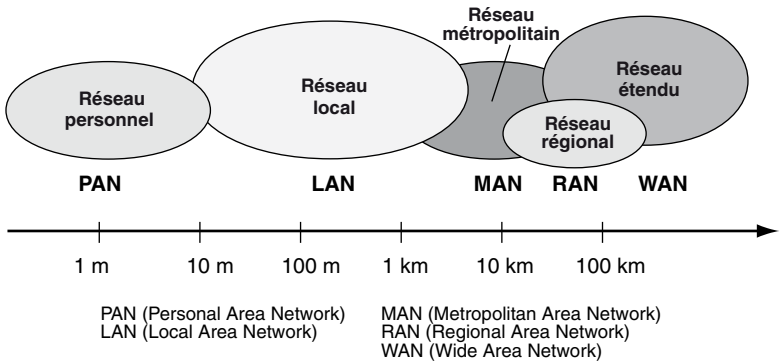


Figure 1.5

Les grandes catégories de réseaux informatiques

Les techniques utilisées par les réseaux informatiques proviennent toutes du transfert de paquets IP (Internet Protocol) généralement encapsulés dans des trames Ethernet. Ces techniques sont étudiées tout au long de l'ouvrage.

Une caractéristique essentielle des réseaux informatiques, qui les différencie des autres catégories de réseaux que nous présentons dans la suite de ce chapitre, est la gestion et le contrôle du réseau, qui sont effectués en grande partie par les équipements terminaux. Par exemple, pour qu'il n'y ait pas d'embouteillage de paquets dans le réseau, l'équipement terminal doit se réguler lui-même de façon à ne pas inonder le réseau de paquets. Pour se réguler, l'équipement terminal mesure le temps de réponse aller-retour. Si ce temps de réponse grandit trop, le terminal ralentit son débit. Cette fonctionnalité est rendue possible par l'intelligence qui se trouve dans les machines terminales commercialisées par l'industrie informatique.

Généralement beaucoup plus simple, l'intérieur du réseau est constitué de nœuds de transfert élémentaires et de lignes de communication. Le coût du réseau est surtout supporté par les équipements terminaux, qui possèdent toute la puissance nécessaire pour réaliser, contrôler et maintenir les communications.

Les réseaux informatiques forment un environnement asynchrone. Les données arrivent au récepteur à des instants qui ne sont pas définis à l'avance, et les paquets peuvent mettre un temps plus ou moins long pour parvenir à leur destinataire en fonction de la saturation du réseau. Cette caractéristique explique la difficulté de faire passer de la parole

téléphonique dans ce type de réseau, puisque cette application fortement synchrone nécessite de remettre au combiné téléphonique des octets à des instants précis. Nous détaillons dans la suite de l'ouvrage les moyens de retrouver cette synchronisation dans un réseau asynchrone.

Aujourd'hui, le principal réseau informatique est Internet. Le réseau Internet transporte des paquets dits IP (Internet Protocol). Plutôt que de parler de réseau Internet, nous préférons parler de réseau IP, qui marque une plus grande généralité. Les réseaux IP sont des réseaux qui transportent des paquets IP d'une machine terminale à une autre. En un certain sens, Internet est un réseau IP particulier. D'autres réseaux, comme les réseaux intranet, transportent également des paquets IP, mais avec des caractéristiques différentes d'Internet.

Les réseaux de télécommunications

Les opérateurs et les industriels des télécommunications ont une vision des réseaux différente de celle des informaticiens. Leur application de base, la parole téléphonique, impose de sévères contraintes, telles que la synchronisation aux extrémités ou le temps de traversée du réseau, qui doit être limité. À l'inverse des réseaux informatiques, qui partent d'un environnement asynchrone et doivent l'adapter pour accepter des applications synchrones, les réseaux de télécommunications sont fondés par essence sur le passage d'applications fortement synchrones.

La parole est une application temps réel, qui exige que les signaux soient remis au récepteur à des instants précis dans le temps. On dit que cette application est isochrone pour bien préciser cette demande de forte synchronisation.

La solution qui a été utilisée quasiment depuis les débuts des télécommunications pour résoudre le problème de la synchronisation est la commutation de circuits. Cette technique consiste à mettre en place entre l'émetteur et le récepteur un circuit physique n'appartenant qu'aux deux utilisateurs en relation. La synchronisation correspond à la remise d'un octet à intervalle régulier. Un équipement appelé codec (codeur-décodeur) transforme la parole en octet à l'émetteur et fait la démarche inverse au récepteur. Le codec doit recevoir les échantillons d'un octet à des instants précis. La perte d'un échantillon de temps en temps n'est pas catastrophique, puisqu'il suffit de remplacer l'octet manquant par le précédent. En revanche, si ce processus de perte se répète fréquemment, la qualité de la parole se détériore.

Les réseaux de télécommunications orientés vers le transport de la parole téléphonique sont relativement simples et n'ont pas besoin d'une architecture complexe. Ils utilisent des commutateurs de circuits, ou autocommutateurs. Il y a une trentaine d'années, lorsqu'on a commencé à imaginer des réseaux intégrant la téléphonie et l'informatique, la seule solution proposée se fondait sur des circuits, un circuit pour la parole téléphonique et un autre pour faire circuler les paquets de données.

Des recherches menées au début des années 1980 ont conduit les industriels et les opérateurs des télécommunications à adopter le transfert de paquets, mais en l'adaptant au

transport intégré de l'information (parole téléphonique plus données informatiques). Appelée Asynchronous Transfer Mode (ATM), ou mode de transfert asynchrone, cette technique est un transfert de paquets très particulier, dans lequel tous les paquets ont une longueur à la fois fixe et très petite. En fait, ce paquet dont la longueur est constante est une trame. Il est simple d'y retrouver le début et la fin des paquets puisqu'il suffit de compter le nombre d'octets. Avec l'adoption, en 1988, du transfert de trames ATM, le monde des télécommunications a connu une véritable révolution.

La technique ATM n'a cependant pu résister à l'arrivée massive d'Internet et de son paquet IP. Toutes les machines terminales provenant du monde informatique ayant adopté l'interface IP, le problème du transfert des paquets est devenu celui des paquets IP. Le monde des télécommunications admet, depuis le début des années 2000, que les réseaux doivent posséder des interfaces IP. Ce qui fait encore débat, c'est la façon de transporter les paquets IP d'un terminal à un autre. Le monde des télécommunications propose, comme nous l'examinons en détail dans la suite de l'ouvrage, d'encapsuler le paquet IP dans une trame puis de transporter cette trame et de la décapsuler à l'arrivée pour retrouver le paquet IP.

La figure 1.6 illustre le cas général où le paquet IP est encapsulé dans une trame, classiquement la trame Ethernet, laquelle est transportée dans le réseau de transfert. Le cas de l'encapsulation dans un réseau ATM demande une étape supplémentaire, consistant à découper le paquet IP, puisque la trame ATM est beaucoup plus petite que le paquet IP.

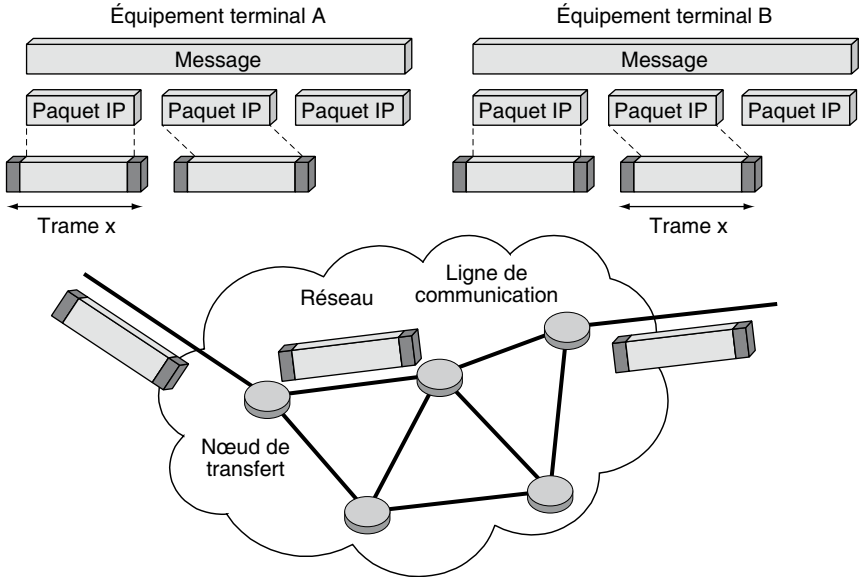


Figure 1.6

Encapsulation du paquet IP dans une trame

En résumé, les réseaux de télécommunications sont passés d'une technologie circuit à une technologie paquet. Malgré le succès du transfert ATM, optimisé pour le multimédia, l'utilisation du paquet IP et de son encapsulation dans une trame Ethernet sont devenues incontournables. Une question en suspens réside dans la façon de transporter le paquet IP pour assurer une qualité de service.

Les réseaux des câblo-opérateurs

Les opérateurs vidéo et les câblo-opérateurs ont pour mission de mettre en place des réseaux câblés et hertziens chargés de transmettre les images de télévision par la voie terrestre ou hertzienne. Cette infrastructure de communication fait transiter des canaux vidéo vers l'utilisateur final. L'amortissement du câblage ou des relais hertziens passe par la mise à disposition des utilisateurs de nombreux canaux de télévision.

Les opérateurs hertziens assurent depuis de longues années la diffusion de canaux de télévision. Leur réseau était essentiellement analogique jusqu'au début des années 2000. Sa numérisation est en cours, aussi bien par satellite que par le biais de relais numériques terrestres pour la TNT (télévision numérique terrestre).

Il existe une grande variété de qualités d'images vidéo, depuis les images saccadées et de faible définition jusqu'aux images animées de très bonne qualité. La classification des applications vidéo, effectuée suivant le niveau de qualité des images, est généralement la suivante :

- Visioconférence. D'une définition relativement faible, sa fonction est de montrer le visage du correspondant. Pour gagner en débit, on diminue le nombre d'image par seconde. La visioconférence se transporte aisément sur un canal numérique à 128 Kbit/s au moyen d'une compression simple à réaliser. On peut abaisser le débit jusqu'à 64 Kbit/s, voire moins, au prix d'une qualité dégradée.
- Télévision. Correspond à un canal de 4 ou 5 MHz de bande passante en analogique. La numérisation de ce canal permet d'obtenir un débit de plus de 200 Mbit/s. Grâce à la compression, on peut faire descendre ce débit à 2 Mbit/s, pratiquement sans perte de qualité, voire à quelques centaines de kilobits par seconde avec une compression poussée, mais au prix d'une qualité parfois dégradée. De plus, à de tels débits, les erreurs en ligne deviennent gênantes, car elles perturbent l'image au moment de la décompression. Un compromis est à trouver entre une forte compression et un taux d'erreur de 10^{-9}, qui ne détruit qu'une infime fraction de l'image et ne gêne pas sa vision. Le standard pour la transmission d'un canal de télévision numérique est aujourd'hui MPEG-2.

  Les améliorations incessantes apportées aux codecs devraient permettre dans quelques années de faire passer un canal de télévision sur une bande encore plus restreinte, tout en y ajoutant de nouvelles fonctionnalités.
- Télévision haute définition. Demande des transmissions à plus de 500 Mbit/s si aucune compression n'est effectuée. Après compression, on peut descendre à une valeur de l'ordre de 10 Mbit/s.

- Télévision 3D. Cette nouvelle génération requiert des débits encore plus importants puisqu'elle consiste à transporter plusieurs images pour en obtenir une seule qui donne l'impression d'être en trois dimension. Après compression, on peut descendre à une valeur de l'ordre de 20 Mbit/s.
- Vidéoconférence. Proche du cinéma, la qualité vidéoconférence requiert des débits considérables de plusieurs dizaines de mégabits par seconde. Compte tenu de ces débits, ce type de canal ne devrait se répandre qu'avec l'arrivée du câblage en fibre optique jusqu'au domicile et dans toutes les entreprises. Un cas particulier, qui semble se développer dans les années 2010, concerne les murs de présence : il s'agit de projeter sur un mur une vidéoconférence de haute qualité avec un son stéréophonique et une transmission en temps réel.

Les câblo-opérateurs se préoccupent en premier lieu de diffuser des images animées de type TV. Les structures de câblage mises en place pour cela permettent de diffuser chez l'utilisateur de nombreux canaux de télévision, qui se comptent aujourd'hui par centaines.

Les applications vidéo vont de la télésurveillance à la vidéo à la demande, ou VoD (Video on Demand), en passant par la messagerie vidéo et le « Home Media Center » domestique pour la diffusion vidéo généralisée à l'échelle d'une maison.

Les réseaux câblés utilisés par les diffuseurs sur la partie terminale du réseau de distribution sont appelés CATV (Community Antenna TeleVision). Le CATV utilise un câble coaxial de 75 Ω, dont la largeur de bande dépasse 1 GHz. On l'utilise aussi comme câble d'antenne de télévision. Il s'agit d'un support unidirectionnel, qui implique d'envoyer le signal vers un centre, lequel le rediffuse à toutes les stations connectées, contrairement à ce qui se passe, par exemple, dans le réseau Ethernet, où le signal est diffusé dans les deux sens du support physique.

Dans un réseau CATV, la diffusion des chaînes de télévision s'effectue facilement du centre vers la périphérie. Pour ajouter des canaux dans le sens inverse, du client vers la tête de réseau, des accès Internet par exemple, on divise la bande passante en deux : une partie pour aller vers la tête de réseau, l'autre desservant les utilisateurs. On parle en ce cas de bande montante et de bande descendante.

Depuis que le prix de revient de la fibre optique et des connecteurs associés est devenu concurrentiel, on l'utilise de plus en plus à la place du câble coaxial. La bande passante de la fibre optique est beaucoup plus importante et permet d'augmenter très fortement le débit des accès Internet.

Les réseaux câblés ont été exploités pendant longtemps en analogique et non en numérique. Les débits sont aujourd'hui suffisants pour y faire transiter des applications multimédias. Cependant, comme nous le verrons, la principale difficulté est de faire transiter plusieurs milliers de canaux montants du terminal vers le réseau sur un canal partagé d'une capacité limitée. Mille clients émettant potentiellement à 1 Mbit/s représentent un débit total de 1 Gbit/s, ce qui est généralement nettement plus que la bande disponible sur la partie montante. Il faut donc très souvent une technique de partage du canal pour arbitrer les accès montants des utilisateurs.

Dans certains pays, comme les États-Unis, les foyers constituent pour les câblo-opérateurs une porte d'entrée simple vers l'utilisateur final. Le câblage, qui est une des clés de la diffusion généralisée de l'information, a été durant de nombreuses années l'objet de toutes les convoitises des opérateurs de télécommunications. Le succès des techniques *x*DSL, utilisant le câblage téléphonique, a toutefois limité l'impact des réseaux câblés. Le déploiement de la fibre optique, de la TNT et des réseaux de mobiles 4G pourraient réduire grandement l'intérêt de ces réseaux.

La principale technique utilisée par les câblo-opérateurs pour transporter les canaux de télévision est le multiplexage en fréquence, qui consiste en une partition de la bande passante en sous-bandes. Chaque sous-bande transporte un canal de télévision. Cette solution est illustrée à la figure 1.7.

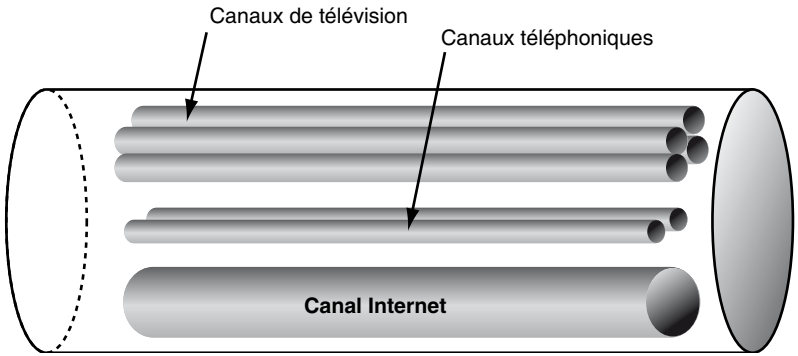


Figure 1 .7
Multiplexage en fréquence dans le CATV

Le multiplexage en fréquence d'un grand nombre de sous-bandes présente l'inconvénient de requérir autant de types de récepteurs que de canaux à accéder. Il faut un décodeur pour la télévision, un modem câble pour Internet et un accès téléphonique pour la parole numérique. Les techniques de multiplexage temporel, dans lesquelles le temps est découpé en petites tranches affectées régulièrement aux utilisateurs, sont beaucoup plus puissantes, puisqu'un même émetteur-récepteur permet de recevoir tous les canaux.

En conclusion, la technique employée par les câblo-opérateurs permet une intégration dans le CATV d'un grand nombre d'applications utilisant des sous-bandes différentes, adaptées à différents types de transmissions. Son principal inconvénient vient du multiplexage en fréquence, qui conduit les câblo-opérateurs à utiliser un grand nombre de bandes en parallèle. Ces bandes peuvent être considérées comme des canaux de communication indépendants les uns des autres, de telle sorte qu'il n'y a pas d'intégration des flux : un client peut utiliser en parallèle un canal de télévision, un canal d'accès Internet et un canal pour la téléphonie. Le canal de télévision est connecté à un câblo-opérateur, le canal d'accès Internet à un opérateur Internet et le canal de téléphonie à un opérateur téléphonique. L'intégration de ces différents réseaux chez un même opérateur est aujourd'hui une réalité que nous étudions tout au long de ce livre.

L'intégration des réseaux

Les sections précédentes ont introduit brièvement les trois grandes catégories de réseaux, informatique, de télécommunications et des câblo-opérateurs, qui se proposent de transporter les données informatiques, la parole téléphonique et la vidéo. Chacun de ces réseaux essaie aujourd'hui de prendre en charge les trois médias simultanément pour tendre vers un réseau intégré. Cette section détaille les caractéristiques d'une telle intégration des réseaux dans un réseau multimédia, ainsi que les contraintes qu'il doit supporter.

Le monde des télécommunications a adopté diverses solutions pour doter ses réseaux de commutation de solutions permettant d'obtenir une qualité de service satisfaisante. La première solution a consisté à utiliser des chemins associés à une classe de service. Les paquets suivant ce chemin étaient traités en priorité dans le commutateur. Cette solution a ensuite évolué vers l'ingénierie de trafic. Au moment de l'ouverture du chemin, le paquet de signalisation note, dans chaque commutateur, les caractéristiques du trafic ayant été négociées entre le client et l'opérateur du réseau. Cette négociation donne naissance à un SLA (Service Level Agreement) que nous retrouverons au chapitre 26. Grâce à ces informations, les nœuds peuvent décider de laisser passer ou non un paquet de signalisation souhaitant ouvrir un chemin. Il est donc relativement simple de négocier une qualité de service correspondant aux différentes applications des réseaux multimédias.

Les réseaux de routage ont bien plus de difficulté à garantir cette qualité de service puisqu'il ne peut y avoir de réservation de ressources et qu'il n'est pas possible de déterminer à l'avance les routeurs par lesquels doivent passer les paquets d'un même flot. Une première solution à ce problème consiste à surdimensionner le réseau pour que les paquets s'écoulent de façon fluide. Si cette solution était acceptable entre 2000 et 2005 grâce à l'importante capacité de transport développée lors de la « bulle Internet » des années 1999-2000, ce n'est plus tout à fait le cas aujourd'hui.

Une nouvelle solution a été proposée consistant à introduire une classification des clients et à ne surdimensionner que les clients de plus haute priorité. Cela suppose de discriminer ces clients, soit par le paiement d'un abonnement plus élevé, soit en restreignant le nombre de clients de l'application considérée. La téléphonie sur IP fonctionne grâce à cette solution. Seuls les paquets IP sortant de téléphones IP se voient affecter la priorité la plus haute. En calculant le nombre maximal de voies téléphoniques pouvant s'écouler sur chaque liaison, on peut en déduire la capacité de la ligne pour qu'elle soit vue comme surdimensionnée.

Conclusion

Ce chapitre a introduit les premiers concepts des réseaux. La convergence de ces réseaux provenant de différents horizons, comme l'informatique, les télécommunications et la vidéo, vers un réseau unique est maintenant achevée.

Nous avons également introduit le passage des réseaux transportant les informations sous forme analogique aux réseaux transportant les informations sous forme numérique. Les

réseaux numériques se sont développés en proposant plusieurs options, le routage et la commutation, et en utilisant aussi bien des supports physiques terrestres que des transmissions radio.

Aujourd'hui, les réseaux analogiques ont quasiment disparu, sauf pour des applications très spécifiques, comme la téléphonie pour la communication entre un contrôleur aérien et un avion, pour des raisons de fiabilité et de disponibilité. Mais même dans ce cas, le passage au numérique s'effectuera dans quelques années. Les raisons en sont le coût des équipements et la réutilisation simple des composants numériques qui n'utilisent que les deux valeurs, 0 et 1.

Les difficultés à résoudre pour la marche parfaite des réseaux hertziens et terrestres sont notamment la mise à niveau de la sécurité, la gestion du réseau global, le contrôle de la mobilité et l'introduction d'une virtualisation complète.

Cet ouvrage détaille de façon graduelle toutes les solutions envisagées et examine les éléments nécessaires à la construction d'un réseau de bout en bout.

2

Architecture des réseaux

Le transport des données d'une extrémité à une autre d'un réseau nécessite un support physique ou hertzien de communication. Pour que les données arrivent correctement au destinataire, avec la qualité de service, ou QoS (Quality of Service), exigée, il faut en outre une architecture logicielle chargée du contrôle des paquets dans le réseau.

L'architecture TCP/IP d'Internet a aujourd'hui supplanté complètement les autres architectures. Cependant, l'architecture OSI (Open Systems Interconnection) provenant de la normalisation de l'ISO (International Standardization Organization) demeure le modèle de référence et la numérotation de ces couches reste le standard pour s'y retrouver. Nous utiliserons dans la suite de cet ouvrage, les couches OSI et plus régulièrement les couches provenant du modèle TCP/IP.

Le présent chapitre détaille ces deux architectures, en commençant par celle introduite par l'ISO il y a une trentaine d'année et qui constitue toujours le modèle de référence pour décrire les éléments nécessaires à la réalisation d'une architecture réseau. Nous examinons ensuite les architectures dites *crosslayer*, qui regroupent toutes les fonctionnalités dans une seule couche.

Le modèle de référence

Les concepts architecturaux utilisés pour décrire le modèle de référence à sept couches proposé par l'ISO sont décrits dans la norme ISO 7498-1. La figure 2.1 illustre cette architecture.

Une couche correspond à un ensemble de protocoles destinés à réaliser le service qui lui est associé. On parle également de niveau qui fait référence dans ce cas à l'entité traitée dans la couche (élément binaire, trame, paquet, message, connexion, syntaxe, sémantique). On numérote les couches et les niveaux de 1 à 7 pour les référencer facilement.

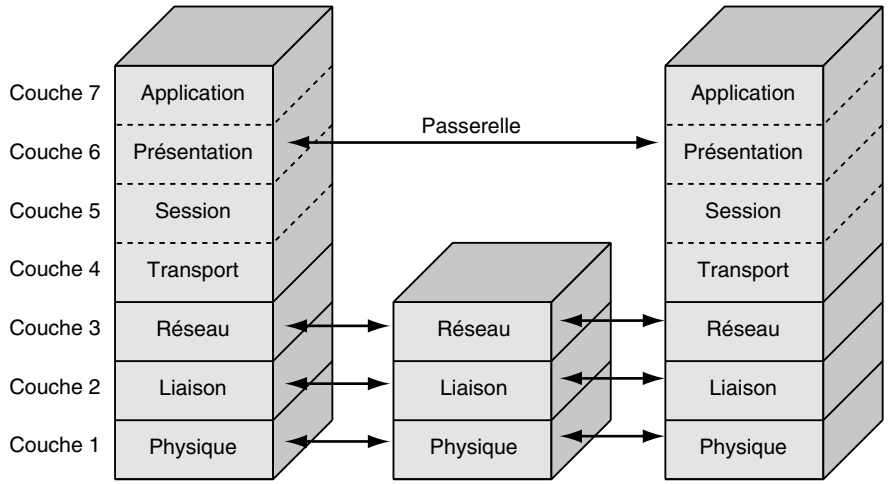


Figure 2.1
L'architecture OSI

Les éléments des réseaux qui prennent en charge les paquets sont appelés des nœuds, ou encore des nœuds de transfert, car ils transfèrent des paquets d'une ligne d'entrée vers une ligne de sortie. Ces nœuds de transfert peuvent être des routeurs ou des commutateurs. Routeurs et commutateurs font l'objet d'un débat continuel, car ils symbolisent deux manières opposées d'acheminer l'information à l'intérieur d'un réseau maillé. Les deux solutions présentent bien sûr des avantages et des inconvénients, notamment souplesse pour le routage et puissance pour la commutation.

La technique de transfert ATM utilise une commutation, tandis qu'Internet préfère le routage. Ethernet peut utiliser le routage, mais il est également possible de commuter les trames Ethernet. La première solution est plutôt orientée entreprise tandis que la seconde est destinée aux opérateurs de télécommunications.

Dans ce chapitre, le mot paquet désigne l'entité à commuter ou à router. Il peut aussi bien s'agir d'une trame que d'un paquet en fonction du niveau auquel s'effectue le transfert.

Les couches du modèle de référence

Le modèle de référence OSI comporte sept niveaux protocolaires plus un médium physique. Le médium physique, que l'on appelle parfois le niveau 0, correspond au support physique de communication chargé d'acheminer les éléments binaires d'un point à un autre jusqu'au récepteur final. Ce médium physique peut prendre diverses formes, allant du câble métallique aux signaux hertziens, en passant par la fibre optique et l'infrarouge.

La couche 1 (physique), ou niveau élément binaire

La couche physique contient les règles et procédures à mettre en œuvre pour acheminer les éléments binaires sur le médium physique. On trouve dans la couche physique les

équipements réseau qui traitent l'élément binaire, comme les modems, concentrateurs, ponts, hubs, etc.

Les différentes topologies de support physique affectent le comportement de la couche physique. Dans les entreprises, les plans de câblage ont une importance parfois déterminante pour le reste de l'architecture. La couche physique nécessite de surcroît un matériel fiable, et il faut parfois dupliquer ou mailler le réseau pour obtenir des taux de défaillance acceptables.

La couche 2 (liaison), ou niveau trame

La trame est l'entité transportée sur les lignes physiques. Elle contient un certain nombre d'octets transportés simultanément. Le rôle du niveau trame consiste à envoyer un ensemble d'éléments binaires sur une ligne physique de telle façon qu'ils puissent être récupérés correctement par le récepteur. Sa première fonction est de reconnaître, lors de l'arrivée des éléments binaires, les débuts et fins de trame. C'est là, aujourd'hui, le rôle principal de cette couche, qui a été fortement modifiée depuis son introduction dans le modèle de référence.

Au départ, elle avait pour fonction de corriger les erreurs susceptibles de se produire sur le support physique, de sorte que le taux d'erreur résiduelle reste négligeable. En effet, s'il est impossible de corriger toutes les erreurs, le taux d'erreur non détectée doit rester négligeable. Le seuil à partir duquel on peut considérer le taux d'erreur comme négligeable est dépendant de l'application et ne constitue pas une valeur intrinsèque.

Appréciation du taux d'erreur

Pour une communication téléphonique, un taux d'erreur d'un bit en erreur pour mille bits émis ne pose pas de problème, l'oreille étant incapable de déceler ces erreurs. En revanche, lors du passage d'une valeur sur un compte bancaire, une erreur en moyenne sur 1 000 bits peut devenir catastrophique. Dans ce cas, il faut descendre à un taux d'erreur de 10^{18} bits, c'est-à-dire d'une erreur en moyenne tous les 10^{-18} bits émis, ce qui représente, sur une liaison à 1 Gbit/s, une erreur en moyenne tous les deux cents jours ou, à la vitesse de 1 Mbit/s, une erreur tous les cinq cents ans. On peut en conclure qu'un même support physique peut être acceptable pour certaines applications et pas pour d'autres.

La solution préconisée aujourd'hui pour traiter les erreurs est d'effectuer la correction d'erreur non plus au niveau trame, mais au niveau application. Pour chaque application, on peut déterminer un taux d'erreur limite entre l'acceptable et l'inacceptable. Comme les médias physiques sont de plus en plus performants, il est généralement inutile de mettre en œuvre des algorithmes complexes de correction d'erreur. En fait, seules les applications pour lesquelles un taux d'erreur donné peut devenir inacceptable doivent mettre en place des mécanismes de reprise sur erreur.

La couche 2 comporte également les règles nécessaires au partage d'un même support physique entre plusieurs stations, par exemple lorsque la distance entre les utilisateurs est faible. La vitesse du signal électrique étant de 200 m/ms, si un utilisateur demande 20 ms pour envoyer son bloc d'information et que le réseau ait une longueur de quelques

centaines de mètres, il doit être seul à transmettre, faute de quoi une collision des signaux se produit. Une telle discipline d'accès est nécessaire dans les réseaux partagés, mais aussi dans les réseaux locaux et certains réseaux métropolitains.

Beaucoup de normes et de recommandations concernent la couche 2, dite aussi niveau liaison. Provenant de l'ISO, la norme HDLC (High-level Data Link Control) a été la première vraie norme à codifier les procédures de communication entre ordinateurs. Nous la détaillons à l'annexe F.

L'ISO a mis au point un ensemble de normes additionnelles de niveau trame concernant les réseaux locaux, les méthodes d'accès et les protocoles de liaison. Tous ces mécanismes effectués au niveau trame sont détaillés au chapitre 14.

La couche 3 (réseau), ou niveau paquet

La couche 3, ou niveau paquet, est appelée couche réseau dans le modèle de référence parce que l'échange de paquets de bout en bout donne naissance à un réseau. Le niveau paquet doit permettre d'acheminer correctement les paquets d'information jusqu'à l'utilisateur final. Pour aller de l'émetteur au récepteur, il faut passer par des nœuds de transfert intermédiaires ou par des passerelles, qui interconnectent deux ou plusieurs réseaux.

Un paquet n'est pas une entité transportable sur une ligne physique, car si l'on émet les bits directement sur le support, il n'est pas possible de détecter la limite entre deux paquets arrivant au récepteur. Il y a donc obligation d'encapsuler les paquets dans des trames pour permettre leur transport d'un nœud vers un autre nœud.

Le niveau paquet nécessite trois fonctionnalités principales : le contrôle de flux, le routage et l'adressage :

- Contrôle de flux. Évite les embouteillages de paquets dans le réseau. Les retards provenant des surcharges de certaines parties du réseau peuvent en effet rendre le temps de réponse inacceptable pour l'utilisateur. Si le contrôle de flux échoue, un contrôle de congestion fait normalement revenir le trafic à une valeur acceptable par le réseau.
- Routage et commutation. Permettent d'acheminer les paquets d'information vers leur destination au travers du maillage des nœuds de transfert. Dans la commutation les paquets suivent toujours la même route, alors que dans le routage ce chemin peut changer. Le routage ne remplace pas le contrôle de flux mais peut être vu comme une de ses composantes, dont il faut tenir compte pour optimiser le temps de réponse. Les techniques de routage peuvent être centralisées ou distribuées, suivant l'option choisie par le gestionnaire du réseau : soit les tables de routage sont conçues par un nœud central, soit elles sont créées par chaque nœud, avec les problèmes de cohérence que cela pose.
- Adressage. La dernière grande fonction de la couche réseau consiste à gérer les adresses des équipements terminaux. Pour cela, il faut ajouter des adresses complètes dans les différents paquets, pour ce qui concerne le routage, ou dans le paquet de signalisation qui ouvre la route, pour la commutation. Les adresses forment un vaste ensemble, qui doit regrouper toutes les machines terminales du monde. L'ISO a dû prévoir une norme d'adressage susceptible de répertorier l'ensemble des équipements terminaux. Dans le monde TCP/IP, un adressage par réseau a été choisi.

Pour mettre en place et développer les fonctionnalités de la couche réseau, il est possible de choisir entre deux grandes méthodes d'accès :

- Le mode avec connexion, dans lequel l'émetteur et le récepteur se mettent d'accord sur un comportement commun et négocient les paramètres et les valeurs à mettre en œuvre.
- Le mode sans connexion, qui n'impose pas de contrainte à l'émetteur par rapport au récepteur.

Le mode avec connexion concerne les techniques de commutation dans lesquels un chemin doit être mis en place. Avec l'aide de la signalisation, la connexion est mise en place avant que débute le transfert des trames. Les modes ATM et Ethernet commuté font partie de cette catégorie. Le protocole IP travaille en mode sans connexion : le transfert des paquets démarrent immédiatement sans que les deux extrémités se mettent d'accord sur les caractéristiques de la communication.

La couche 4 (transport), ou niveau message

Le niveau message prend en charge le transport du message de l'utilisateur d'une extrémité à une autre du réseau. Ce niveau est aussi appelé couche transport pour bien indiquer qu'il s'agit de transporter les données de l'utilisateur. Il représente le quatrième niveau de l'architecture, d'où son autre nom de couche 4.

Le service de transport doit optimiser l'utilisation des infrastructures sous-jacentes en vue d'un bon rapport qualité/prix. La couche 4 optimise les ressources du réseau de communication en gérant un contrôle de flux ou un multiplexage des messages de niveau message sur une connexion réseau. Cette couche de transport est l'ultime niveau qui s'occupe de l'acheminement de l'information. Elle permet de compléter le travail accompli par les couches précédentes. C'est grâce à elle que l'utilisateur obtient la qualité de service susceptible de le satisfaire. Le protocole de niveau message à mettre en œuvre à ce niveau dépend du service rendu par les trois premières couches et de la demande de l'utilisateur.

La couche 4 aujourd'hui la plus utilisée provient de l'architecture du monde Internet et plus exactement de la norme TCP (Transmission Control Protocol). Comme nous le verrons, une autre norme, UDP (User Datagram Protocol), peut aussi être utilisée. Nous examinons ces normes en détail au chapitre 8.

La couche 5 (session), ou niveau connexion

Le rôle de la couche session est de fournir aux entités de présentation les moyens nécessaires à l'organisation et à la synchronisation de leur dialogue. À cet effet, la couche 5 fournit les services permettant l'établissement d'une connexion, son maintien et sa libération, ainsi que ceux permettant de contrôler les interactions entre les entités de présentation.

Ce niveau est aussi le premier de l'architecture réseau à se situer hors de la communication proprement dite. Comme son nom l'indique, la couche session a pour fonction d'ouvrir et de fermer des sessions entre utilisateurs. Il est inutile d'émettre de l'information s'il n'y a

personne à l'autre extrémité pour récupérer ce qui a été envoyé. Il faut donc s'assurer que l'utilisateur que l'on veut atteindre, ou du moins son représentant, qui peut être une boîte aux lettres électronique, par exemple, est présent.

La couche 5 comporte des fonctionnalités rendant possibles l'ouverture, la fermeture et le maintien de la connexion. Les mises en correspondance des connexions de session et des connexions de transport sont effectuées une à une.

De nombreuses autres possibilités peuvent être ajoutées aux commandes de base, appelées primitives, indispensables à la mise en place de la session. La pose de points de resynchronisation, par exemple, est recommandée. Ils permettent, en cas de problème, de disposer d'un point précis, sur lequel il y a accord entre les deux parties communicantes, à partir duquel l'échange peut redémarrer. La gestion des interruptions et des reprises de session est également une fonctionnalité souvent implémentée.

Pour ouvrir une connexion avec une machine distante, la couche session doit posséder un langage qui soit intelligible par l'autre extrémité. C'est pourquoi, avant d'ouvrir une connexion, il est obligatoire de passer par le niveau présentation, qui garantit l'unicité du langage, et le niveau application, qui permet de travailler sur des paramètres définis d'une façon homogène.

La normalisation du niveau session comprend les normes suivantes :

- ISO 8326, ou CCITT X.215, qui définit le service orienté connexion devant être rendu par la couche session. Un additif propose un service sans connexion.
- ISO 8327, ou CCITT X.225, qui spécifie le protocole de session orienté connexion.
- ISO 9548, qui définit un protocole de session en mode sans connexion.

La couche 6 (présentation), ou niveau syntaxe

La couche présentation se charge de la syntaxe des informations que les entités d'application se communiquent. Deux aspects complémentaires sont définis dans la norme :

- La représentation des données transférées entre entités d'application.
- La représentation de la structure de données à laquelle les entités se réfèrent au cours de leur communication et la représentation de l'ensemble des actions effectuées sur cette structure de données.

En d'autres termes, la couche présentation s'intéresse à la syntaxe tandis que la couche application se charge de la sémantique. La couche présentation joue un rôle important dans un environnement hétérogène. C'est un intermédiaire indispensable pour une compréhension commune de la syntaxe des documents transportés sur le réseau. Les différentes machines connectées n'ayant pas la même syntaxe pour exprimer les applications qui s'y effectuent, si on les interconnecte directement, les données de l'une ne peuvent généralement pas être comprises de l'autre. La couche 6 procure un langage syntaxique commun à l'ensemble des utilisateurs connectés.

Si Z est le langage commun, et si une machine X veut parler à une machine Y, elles utilisent des traducteurs X-Z et Y-Z pour discuter entre elles. C'est notamment le cas lorsque les machines X et Y ne suivent pas la norme. Si toutes les machines terminales possèdent en natif un langage syntaxique commun, les traductions deviennent inutiles.

La syntaxe abstraite ASN.1 (Abstract Syntax Notation 1) normalisée par l'ISO est le langage de base de la couche présentation. Fondée sur la syntaxe X.409 du CCITT (Consultative Committee for International Telegraph and Telephone), ASN.1 est une syntaxe suffisamment complexe pour prendre facilement en compte les grandes classes d'applications, comme la messagerie électronique, le transfert de fichiers, le transactionnel, etc.

La normalisation de la couche présentation comprend les normes suivantes :

- ISO 8824, ou CCITT X.208, qui définit la syntaxe ASN.1.
- CCITT X.216 et X.226, qui définissent le service et le protocole de la couche session.

La couche 7 (application), ou niveau sémantique

La couche application est la dernière du modèle de référence. Elle fournit aux processus applicatifs le moyen d'accéder à l'environnement réseau. Ces processus échangent leurs informations de type sémantique par l'intermédiaire des entités d'application.

De très nombreuses normes ont été définies pour cette couche. En ce qui concerne la définition de la couche même, c'est la norme ISO 9545, ou CCITT X.207, qui décrit sa structure.

La couche application contient toutes les fonctions impliquant des communications entre systèmes, en particulier si elles ne sont pas réalisées par les niveaux inférieurs. Il s'occupe essentiellement de la sémantique, contrairement à la couche présentation, qui prend en charge la syntaxe.

L'architecture TCP/IP

Dans les années 1970, le département de la Défense américain, ou DOD (Department Of Defense), décide, devant le foisonnement de machines utilisant des protocoles de communication différents et incompatibles, de définir sa propre architecture. Cette architecture, dite TCP/IP, est à la source du réseau Internet. Elle est aussi adoptée par de nombreux réseaux privés, appelés intranets.

Les deux principaux protocoles définis dans cette architecture sont les suivants :

- IP (Internet Protocol), de niveau réseau, qui assure un service sans connexion.
- TCP (Transmission Control Protocol), de niveau transport, qui fournit un service fiable avec connexion.

TCP/IP définit une architecture en couches qui inclut également, sans qu'elle soit définie explicitement, une interface d'accès au réseau. En effet, de nombreux sous-réseaux distincts peuvent être pris en compte dans l'architecture TCP/IP, de type aussi bien local qu'étendu.

Cette architecture est illustrée à la figure 2.2. Il faut noter dans cette figure l'apparition d'un autre protocole de niveau message (couche 4), UDP (User Datagram Protocol). Ce protocole utilise un mode sans connexion, qui permet d'envoyer des messages sans l'autorisation du destinataire.

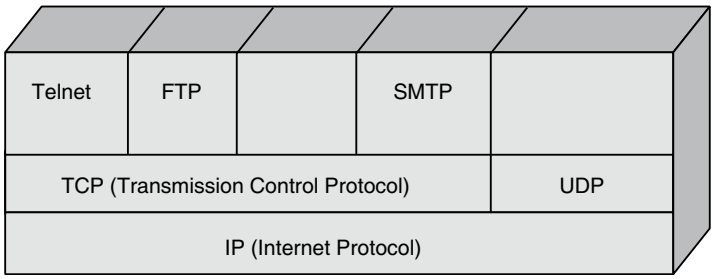


Figure 2.2
Architecture TCP/IP

Cette architecture a pour socle le protocole IP, qui correspond au niveau paquet (couche 3) de l'architecture du modèle de référence. En réalité, il ne correspond que partiellement à ce niveau. Le protocole IP a été conçu comme protocole d'interconnexion, définissant un bloc de données d'un format bien défini et contenant une adresse, mais sans autre fonctionnalité. Son rôle était de transporter ce bloc de données dans un paquet selon n'importe quelle autre technique de transfert de paquets. Cela vaut pour la première génération du protocole IP, appelée IPv4, qui est encore massivement utilisée aujourd'hui. La deuxième version du protocole IP, IPv6, joue réellement un rôle de niveau paquet, avec de nouvelles fonctionnalités permettant de transporter les paquets d'une extrémité du réseau à une autre avec une certaine sécurité.

Les paquets IP sont indépendants les uns des autres et sont routés individuellement dans le réseau par le biais de routeurs. La qualité de service proposée par le protocole IP est très faible, sans détection de paquets perdus ni de possibilité de reprise sur erreur.

Le protocole TCP regroupe les fonctionnalités de niveau message (couche 4) du modèle de référence. C'est un protocole assez complexe, qui comporte de nombreuses options permettant de résoudre tous les problèmes de perte de paquet dans les niveaux inférieurs. En particulier, un fragment perdu peut être récupéré par retransmission sur le flot d'octets. Le protocole TCP est en mode avec connexion, contrairement à UDP. Ce dernier protocole UDP se positionne aussi au niveau transport mais dans un mode sans connexion et n'offre pratiquement aucune fonctionnalité. Il ne peut prendre en compte que des applications qui demandent peu de service de la part de la couche transport.

Les protocoles situés au-dessus de TCP et d'UDP sont de type applicatif et proviennent en grande partie du monde UNIX.

Toute la puissance de cette architecture repose sur la souplesse de sa mise en œuvre au-dessus de n'importe quel réseau existant. Soi, par exemple, X et Y, respectivement un réseau local et un réseau étendu à commutation de cellules ou de paquets. Le protocole IP est implémenté sur toutes les machines connectées à ces deux réseaux. Pour qu'il soit possible de passer d'un réseau à l'autre, un routeur, dont le rôle est de décapsuler le paquet arrivant du réseau X et de récupérer le paquet IP, est mis en place. Après traitement, essentiellement du routage, le paquet IP est encapsulé dans le paquet du réseau Y. Le rôle du routeur est, comme son nom l'indique, de router le paquet vers la bonne destination.

L'architecture d'interconnexion du réseau Internet est illustrée à la figure 2.3.

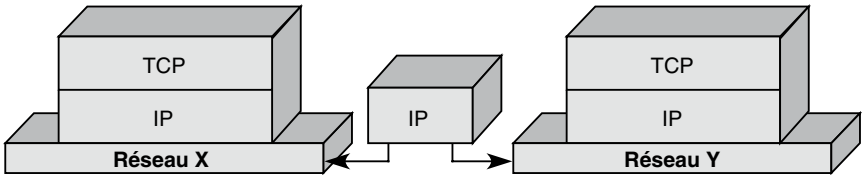


Figure 2.3
Architecture d'interconnexion du réseau Internet

La souplesse de cette architecture peut parfois être un défaut, dans le sens où l'optimisation globale du réseau est effectuée sous-réseau par sous-réseau, c'est-à-dire qu'elle est obtenue par une succession d'optimisations locales.

Une particularité importante de l'architecture TCP/IP est que l'intelligence et le contrôle du réseau se trouvent en presque totalité dans la machine terminale et non pas dans le réseau, en tout cas pour IPv4. C'est le protocole TCP qui se charge d'envoyer plus ou moins de paquets dans le réseau en fonction de l'occupation de celui-ci. L'intelligence de contrôle se trouve dans le PC extrémité, et plus précisément dans le logiciel TCP. La fenêtre de contrôle de TCP augmente ou diminue le trafic suivant la vitesse requise pour faire un aller-retour. Le coût de l'infrastructure est extrêmement bas puisque nombre de logiciels, et donc l'essentiel de l'intelligence, se trouvent dans les machines terminales. Le service rendu par ce réseau de réseaux est de type best-effort, ce qui signifie que le réseau fait de son mieux pour écouler le trafic.

Le protocole IPv6 apporte une nouvelle dimension, puisqu'il introduit des fonctionnalités inédites qui rendent les nœuds du réseau plus intelligents. Les routeurs de nouvelle génération possèdent des algorithmes de gestion de la qualité de service en vue d'assurer un transport capable de satisfaire à des contraintes temporelles ou de perte de paquets. Cependant, le protocole IPv4 a bien réagi aux nouveautés apportées par IPv6, en modifiant certains champs pour proposer les mêmes améliorations.

Dans la version classique d'IPv4, chaque nouveau client n'est pas traité différemment de ceux qui sont déjà connectés, et les ressources sont distribuées équitablement entre tous les utilisateurs. Les politiques d'allocation de ressources des opérateurs de télécommunications sont totalement différentes, un client possédant déjà une certaine qualité de service ne devant pas être pénalisé par l'arrivée d'un nouveau client. Comme nous le verrons, la solution aujourd'hui préconisée dans l'environnement Internet est de favoriser, dans la mesure du possible, les clients ayant des exigences de temps réel, et ce par des protocoles adaptés.

Les applications disponibles au-dessus de l'environnement TCP/IP sont nombreuses et variées. Elles incluent la messagerie électronique (SMTP), le transfert de fichiers (FTP), les bases de données distribuées avec le World-Wide Web (WWW) et bien d'autres.

Les architectures de niveau 1 (élément binaire)

Les architectures de niveau 1 se présentent comme illustré à la figure 2.4.

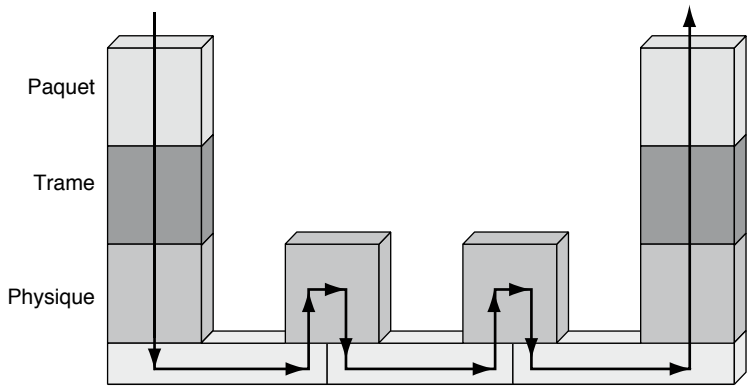


Figure 2.4

Architecture de niveau 1

Le paquet, que nous supposons toujours de type IP dans la suite du chapitre, puisque cela représente presque 100 % des cas, est encapsulé dans une trame, laquelle est émise sur le support physique. Les nœuds intermédiaires ne s'occupent que de modifier le type de support physique, sans remonter au niveau de la trame. C'est la même trame que l'on retrouve à l'autre extrémité du réseau en décapsulant le paquet.

Les réseaux de niveau physique sont évidemment les plus rapides, puisqu'il n'y a pas à récupérer la trame ou le paquet dans les nœuds intermédiaires.

Les architectures de niveau 2(trame)

Une trame peut être définie comme une suite d'éléments binaires qui possède en elle-même un moyen de reconnaissance du début et de la fin du bloc transporté. Par exemple, la norme de niveau 2 Ethernet comporte une suite parfaitement définie permettant la reconnaissance du début et de la fin de la trame. De même, la trame ATM comporte un moyen physique de reconnaissance du début et de la fin. Le protocole PPP (Point-to-Point Protocol) commence et termine par la zone 01111110 qui détermine les débuts et fins. On donne à ces trois exemples le nom de transfert de niveau trame, ou de niveau 2. Ethernet et ATM sont des commutations tandis que PPP est un transfert de niveau 2 entre deux machines.

Une architecture de niveau 2 se présente sous la forme illustrée à la figure 2.5.

Dans cette architecture, on met le paquet IP dans une trame. Les nœuds de transfert intermédiaires rassemblent les bits pour récupérer la trame. Les adresses, ou références, se trouvent dans la trame de façon que le nœud puisse les router ou les commuter. En

générale, il s'agit d'une commutation Ethernet ou ATM. On regroupe les label-switching dans cet ensemble et l'on verra avec MPLS (MultiProtcol Label-Switching) une généralisation de la commutation de niveau 2.

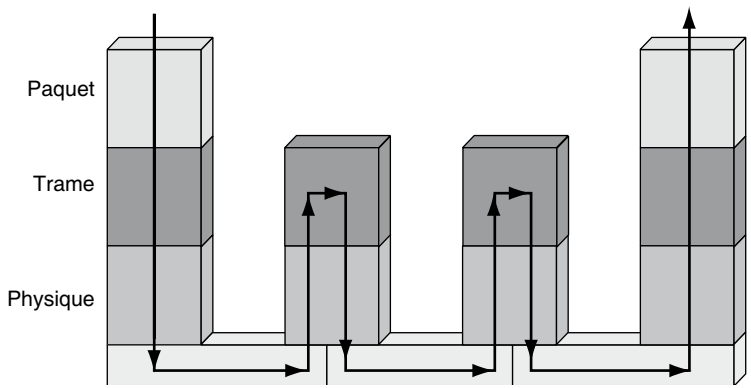


Figure 2.5

Architecture de niveau 2

Il est possible de trouver une commutation de niveau 2 hétérogène, indiquant que la structure de la trame dans un nœud intermédiaire peut-être modifiée. Par exemple, une trame ATM peut-être remplacée par une trame Ethernet. Cela indique que le commutateur décapsule la trame pour récupérer le paquet mais qu'il ne s'en sert pas. Il le réencapsule immédiatement dans une nouvelle trame. Nous trouvons ce genre de technique dans MPLS également.

Les architectures de niveau 3 (paquet)

Une architecture de niveau 3 demande que le niveau de l'entité examinée par le nœud soit un paquet. C'est la solution préconisée par Internet. À chaque nœud, on regroupe les bits pour reformer la trame, puis on décapsule la trame pour retrouver le paquet. On examine ensuite les zones du paquet pour retrouver les zones de contrôle contenant les informations de routage.

Une fois la porte de sortie déterminée, il faut de nouveau encapsuler le paquet dans une trame puis envoyer les éléments binaires sur le support physique. C'est une architecture assez lourde, puisqu'il faut faire beaucoup de travail pour remonter jusqu'au niveau paquet. On comprend qu'elle ait pu être adoptée par Internet, dont le but était d'avoir une structure de données unique, comprise de tous les PC. Cette structure unique est encapsulée dans des trames, qui peuvent être différentes à chaque liaison.

Une architecture de niveau 3 se présente sous la forme illustrée à la figure 2.6.

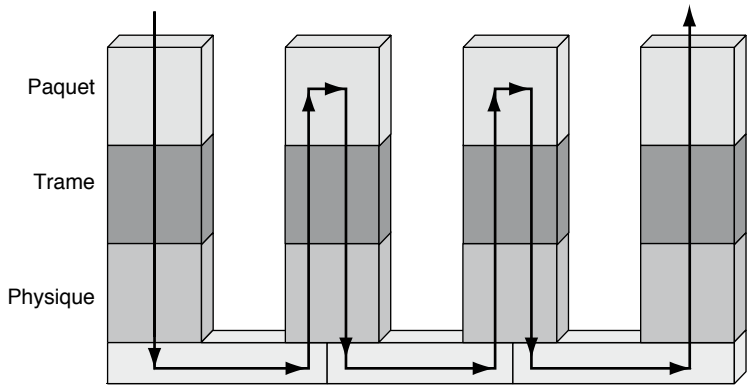


Figure 2.6
Architecture de niveau 3

Les architectures hybrides

Il est envisageable d'avoir des structures hybrides de deux types :

- Chaque nœud de transfert possède un niveau 2 ou un niveau 3.
- Chaque nœud possède à la fois les niveaux 2 et 3.

Dans le premier cas, certains nœuds commutent la trame de niveau 2, mais d'autres nœuds remontent jusqu'au niveau 3 pour aller rechercher l'adresse IP et router sur l'adresse IP du destinataire. Dans le second cas, le nœud reçoit une trame et recherche s'il peut trouver une référence pour commuter, sinon il décapsule la trame pour retrouver le paquet IP et le router. Les nœuds sont alors des routeurs-commutateurs, que l'on trouve dans certains réseaux d'entreprise parce qu'ils permettent d'optimiser le mode de fonctionnement du réseau en fonction des critères des flots. Pour un flot constitué d'un seul paquet, il est plus simple de router. En revanche, dès que le flot est long, il est plus performant de commuter les paquets de l'utilisateur.

Les architectures « crosslayer »

L'architecture en couches a pour avantage de simplifier la compréhension des architectures et de permettre de savoir où se trouvent certaines fonctionnalités. Cependant, cette solution ne permet pas de contrôler le réseau de façon optimale.

Prenons comme exemple le contrôle d'un flot de paquets provenant d'une application de vidéo. Les algorithmes de contrôle ont intérêt à connaître l'application définie dans le niveau 7 qui est en train d'être véhiculée pour savoir si une perte de paquet est importante ou non, si le taux d'erreur du niveau 2 est acceptable ou non, si le support physique permet de redémarrer sur une coupure d'une liaison, etc. En fait, un protocole de contrôle a souvent besoin de connaître des éléments se trouvant dans les différentes couches.

Les architectures *crosslayer* ont pour objectif de rassembler toutes les couches en une seule afin que des algorithmes puissent rechercher les bonnes informations directement au bon endroit.

De nombreuses architectures ont été proposées, mais il semble que l'on s'oriente vers des architectures dites autonomiques (*autonomic*) pour gérer le *crosslayer.* Dans ces architectures, les nœuds sont à la fois autonomes et capables de réagir instantanément. La fonction *crosslayer* est réalisée au travers d'un plan de connaissance qui rassemble les informations nécessaires de tous les niveaux. L'architecture en couches est conservée, mais les connaissances nécessaires au *crosslayer* sont mises en commun dans une couche particulière.

Les techniques de transfert

Il existe cinq grandes techniques de transfert : la commutation de circuits, le transfert de messages, le routage de paquets, la commutation de trames et la commutation de cellules. Il ne reste aujourd'hui plus que deux grandes techniques qui dominent le marché, le routage de paquets et la commutation de trames. Il faut bien noter que d'autres solutions sont tout à fait possible, comme le routage de trames ou la commutation de paquets. Dans le routage de trames, il faudrait une adresse complète dans la trame, et dans la commutation de paquets, une référence dans le paquet (ce qui était le cas de la norme X.25, que nous décrivons en détail à l'annexe F).

Historiquement, les réseaux à commutation de circuits ont été les premiers à voir le jour. Le réseau téléphonique en est un exemple. Les commutations de messages et le routage de paquets sont venus ensuite pour optimiser l'utilisation des lignes de communication dans les environnements informatiques. Enfin, la commutation de trames et la commutation de cellules, ont été mises au point pour augmenter les débits sur les lignes. Nous allons introduire ces différentes solutions avant de les détailler aux chapitres 13 à 17.

La commutation de circuits

Dans la commutation de circuits, un circuit matérialisé est construit entre l'émetteur et le récepteur. Ce circuit n'appartient qu'aux deux équipements terminaux qui communiquent entre eux. La figure 2.7 illustre un circuit traversant trois autocommutateurs, qui sont les équipements capables de mettre bout à bout des segments de circuits pour former un seul circuit de bout en bout. Un excellent exemple de commutation de circuits est le réseau téléphonique. Pour transporter des données sur un circuit, il faut se servir d'un modem (*voir le chapitre 3*).

Le circuit doit d'abord être établi pour que des informations puissent transiter. Le circuit dure jusqu'au moment où l'un des deux abonnés interrompt la communication. Si les deux correspondants n'ont plus de données à se transmettre pendant un certain temps, le circuit reste inutilisé, et les différentes liaisons entre autocommutateurs réalisant le circuit sont inemployées. Pour augmenter le taux d'utilisation des liaisons, on a cherché à concentrer sur une même liaison plusieurs communications.

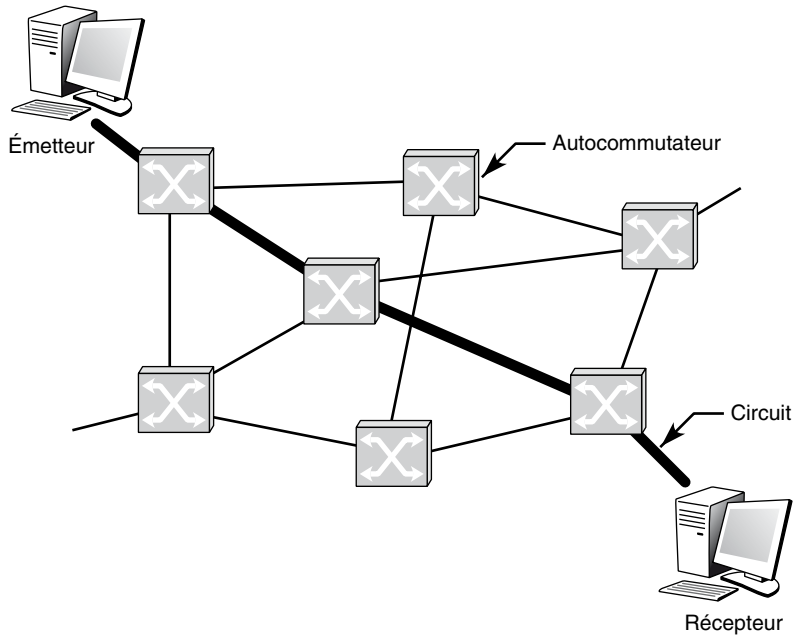


Figure 2.7
Réseau à commutation de circuits

Lorsque de nombreuses communications utilisent une même liaison, une file d'attente se forme, et il est nécessaire de prévoir des zones de mémoire pour retenir les données en attendant que la liaison redevienne disponible. Le fait d'augmenter l'utilisation des liaisons accroît la complexité du système de contrôle, qui devient beaucoup plus lourd, même si son débit est meilleur.

La commutation de circuits n'a pas disparu, mais son usage diminue d'environ 10 % chaque année dans le monde. Elle pourrait ne plus exister vers 2015.

Le transfert de messages

Un message est une suite d'informations formant un tout logique pour l'expéditeur et le destinataire, comme un fichier complet, une ligne saisie sur un terminal, un secteur de disque, etc.

Un réseau à transfert de messages se présente sous la forme illustrée à la figure 2.8. C'est un réseau maillé de nœuds. Le message est envoyé de nœud en nœud jusqu'au destinataire. Ce message ne peut toutefois être envoyé au nœud suivant qu'une fois qu'il a été reçu complètement et correctement par le nœud précédent. Le temps de réponse, même dans le cas le plus favorable, est généralement très long puisqu'il correspond à la somme des temps de transmission de chaque nœud, comme l'illustre la figure 2.9.

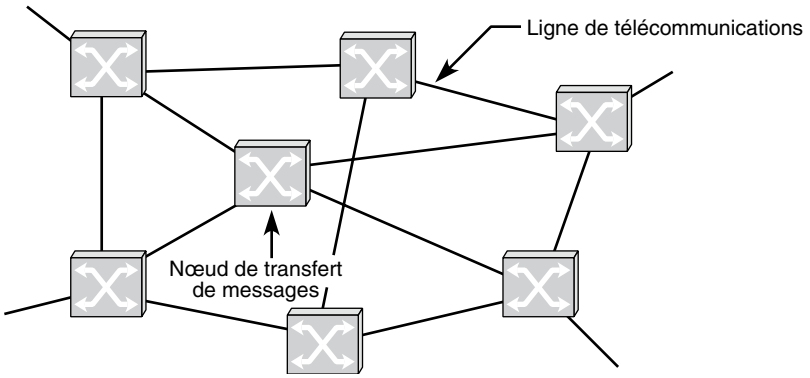


Figure 2.8

Réseau à transfert de messages

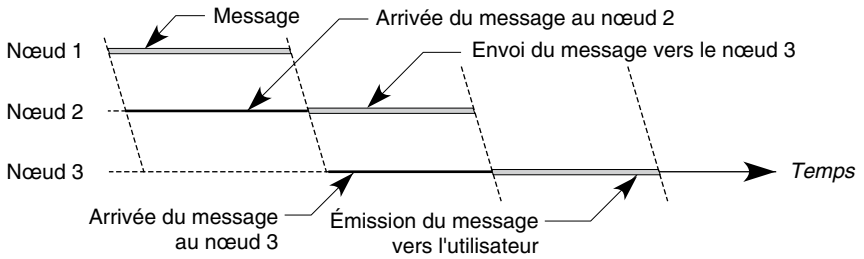


Figure 2.9

Temps de réponse dans le transfert de messages

Pour mémoriser les messages en attendant qu'ils soient correctement stockés dans le nœud suivant, il est nécessaire d'insérer des tampons aux nœuds intermédiaires. Il faut également un système de gestion des transmissions qui accuse réception des messages correctement reçus et demande la retransmission des messages erronés. De plus, comme la capacité des mémoires intermédiaires est limitée, il faut introduire un contrôle sur le flux des messages pour éviter tout débordement. Des politiques de routage des messages peuvent être introduites pour aider à sécuriser les transmissions et faire en sorte que, si une liaison tombe en panne, un autre chemin puisse être trouvé.

Si les messages sont trop longs, ils peuvent être stockés sur disque aux nœuds intermédiaires. Dans ce cas, le temps de réponse de la transmission augmente considérablement. Il est donc très difficile de transmettre correctement de très longs messages. Par exemple, pour un taux d'erreur de 10^{-5} par bit, c'est-à-dire si en moyenne un bit sur 10^5 est erroné, un message de 100 000 octets n'a qu'une probabilité de 0,000 3 d'arriver correctement.

Les deux types de transferts de messages déployés sont la commutation de messages et le routage de messages. Dans le premier cas, les commutateurs de messages utilisent la référence qui se trouve dans l'en-tête du message pour effectuer la commutation. Dans le

second cas, les routeurs de messages utilisent l'adresse complète du destinataire qui se trouve dans l'en-tête du message.

Dans la réalité, ces techniques de transfert de messages ne sont plus utilisées et sont remplacées par des techniques de transfert de paquets.

Le routage de paquets

Nous introduisons ici le routage de paquets plutôt que le transfert de paquets, qui est plus général et contient à la fois le routage et la commutation de paquets. Historiquement, c'est le routage de paquets qui est apparu en premier et qui est devenu le standard d'Internet avec le routage des paquets IP. La commutation de paquets a connu un grand succès entre 1980 et 2000 avec le standard X.25, mais cette solution a aujourd'hui quasiment disparu.

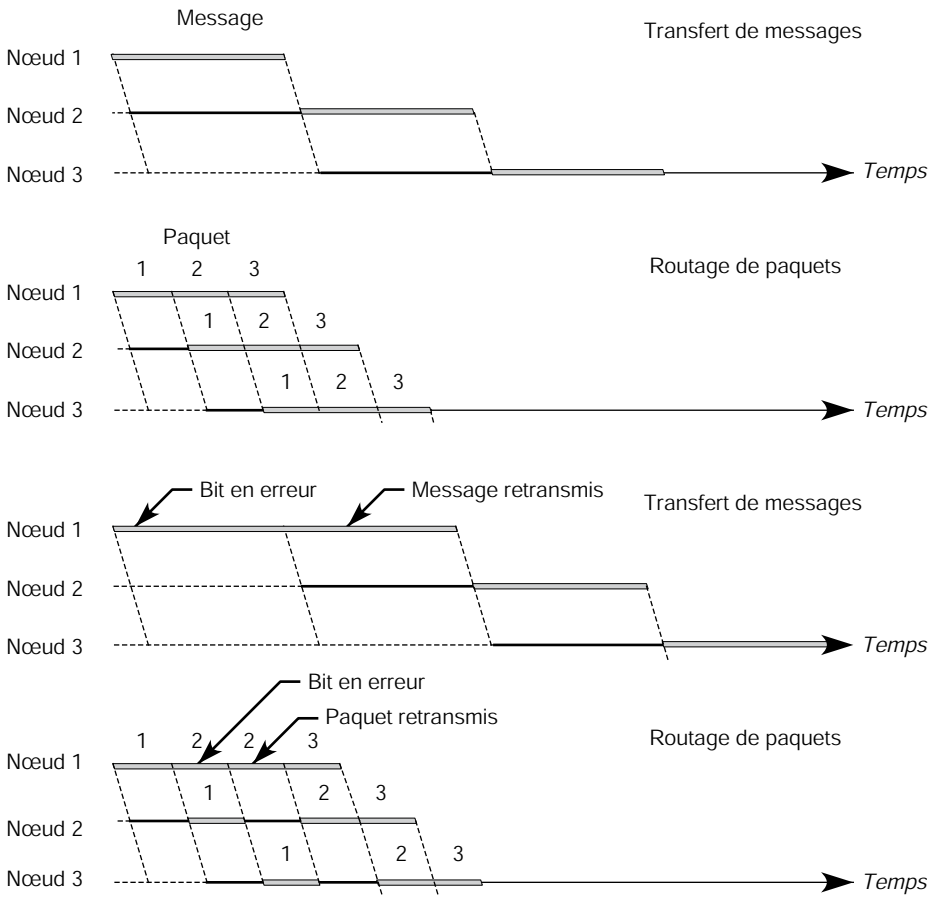


Figure 2.10

Temps de réponse comparés du routage de paquets et du transfert de messages

Pour accélérer la vitesse de transmission et simplifier les reprises sur erreur, on a vu apparaître, au début des années 1970, le concept de réseau à routage de paquets. Le paquet est une suite d'informations binaires dont la taille ne peut dépasser une valeur déterminée à l'avance, de l'ordre de 1 500 octets. Le découpage en paquets des messages des utilisateurs facilite grandement les retransmissions.

La figure 2.10 illustre le comportement dans le temps d'un réseau à transfert de messages comparé à celui d'un réseau à routage de paquets. On constate que le temps de traversée, ou de transit, du réseau à routage de paquets est de loin le plus court. Les paquets étant beaucoup plus petits que les messages, ils peuvent être retransmis vers le nœud suivant plus rapidement.

Dans le routage de paquets, les paquets constituant le message de l'utilisateur sont envoyés indépendamment les uns des autres. Les liaisons entre les nœuds les émettent au fur et à mesure de leur arrivée dans le nœud. Les paquets de plusieurs messages peuvent de la sorte être multiplexés temporellement sur une même liaison, comme illustré à la figure 2.11.

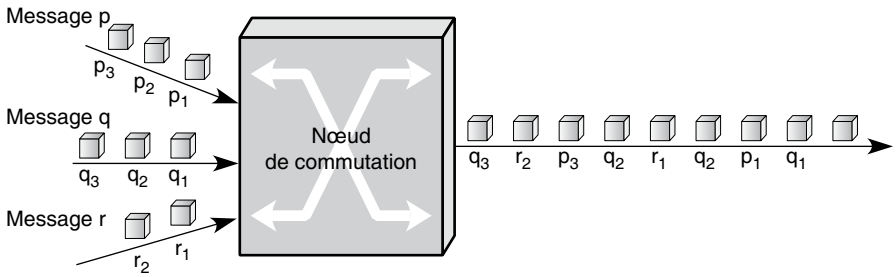


Figure 2.11

Multiplexage temporel des paquets sur une même liaison

Le rôle des nœuds est d'aiguiller les paquets vers la bonne porte de sortie, déterminée par une table de routage. À la figure 2.11, nous supposons que les messages p, q et r sont dirigés vers la même ligne de sortie. Cette représentation serait différente si nous avions une table de routage dynamique, permettant de modifier le routage entre l'émission de deux paquets d'un même message. Dans ce cas, il faudrait représenter au moins deux lignes de sortie. Dans un routage, les liaisons entre nœuds ne sont pas affectées explicitement à une paire source-destination, à la différence de la commutation de circuits.

Le fait que les blocs d'information soient de petite taille permet une gestion plus simple des paquets que dans le transfert de messages, surtout au niveau des reprises sur erreur. En revanche, des problèmes peuvent survenir lors du réassemblage des paquets pour reformer le message original. Si des paquets prennent des routes distinctes et que l'un d'eux se perde, il faut le plus souvent effectuer une reprise de la transmission de l'ensemble du message. Si l'on gagne en temps de réponse et en performance, on complexifie en contrepartie l'architecture en ajoutant au niveau massage une couche de protocoles supplémentaire, le niveau paquet.

La commutation de trames

Comme pour le paquet, deux types de transferts de trames sont théoriquement possibles : la commutation de trames et le routage de trames. Pour avoir un routage de trames, il faudrait cependant une adresse complète du destinataire dans la trame. Cette solution n'existant pas, nous nous focaliserons, après une introduction générale sur le transfert de trames, sur la commutation de trames.

Le transfert de trames est une extension du transfert de paquets. Un paquet ne peut être transmis sur une ligne physique car il ne comporte aucune indication signalant l'arrivée des premiers éléments binaires qu'il contient. La solution pour transporter un paquet d'un nœud vers un autre consiste à placer les éléments binaires dans une trame, dont le début est reconnu grâce à une zone spécifique, appelée drapeau (flag) ou préambule, que nous détaillons au chapitre 4.

Un transfert de trames est donc similaire à un transfert de paquets, à cette différence près que les nœuds de transfert sont plus simples. En effet, dans un transfert de paquets, on encapsule le paquet dans une trame, puis on envoie la trame vers le nœud suivant. À réception de la trame, ce nœud la décapsule pour récupérer le paquet et transfère le paquet à sont tour en l'encapsulant dans une trame, etc. Dans un transfert de trames, il n'y a ni encapsulation ni décapsulation, et il suffit d'envoyer la trame. Lorsque la trame arrive au nœud suivant, la zone portant l'adresse ou la référence est examinée, ce qui permet d'émettre la trame vers le nœud suivant. Comme les transferts de messages ou de paquets, les transferts de trames peuvent être de deux types : commutation ou routage. Dans le premier cas, l'en-tête de la trame contient une référence, et dans le second l'adresse complète du récepteur.

Les transferts de trames sont en réalité uniquement représentés par des commutations, car ils utilisent tous des références. Les deux principales commutations sont l'ATM et la commutation Ethernet. La commutation de trames ATM est si particulière qu'on lui a donné le nom de commutation de cellules. Cette forme de commutation est présentée en détail à la section suivante.

Le relais de trames est la première technique de commutation de trames à avoir été définie. Son objectif était de simplifier au maximum la commutation de paquets du protocole X.25 élaborée à la fin des années 1970 en plaçant la référence directement dans la trame. Pour augmenter les performances de cette commutation, les reprises sur erreur entre nœuds de commutation ont été supprimées, et les procédures de contrôle de flux et de routage simplifiées. Dans les réseaux Ethernet commutés, on commute la trame Ethernet dans des commutateurs. Comme nous le verrons au chapitre 6, dévolu au niveau trame, deux types de références peuvent être utilisés : l'adresse du destinataire, qui est interprétée comme une référence unique pour aller vers ce destinataire, et une référence, dite shim-label, en tout point conforme à la définition du mode commuté.

Les techniques de commutation de trames sont regroupées dans ce qu'on appelle le « label-switching », c'est-à-dire la commutation de références. Ces techniques sont à la base du MPLS.

La commutation de trames ATM

La commutation de trames ATM est une commutation de trames très particulière, dans laquelle toutes les trames ont une longueur fixe de 53 octets. On appelle parfois cette commutation la commutation de cellules. Quelle que soit la taille des données à transporter, la trame occupe toujours 53 octets. Si les données forment un bloc de plus de 53 octets, un découpage est effectué, et la dernière trame n'est pas complètement remplie. La trame ATM en est un exemple. Elle est illustrée à la figure 2.12.

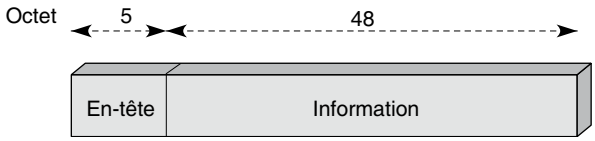


Figure 2.12
La trame ATM

Cette trame est formée de 53 octets, comprenant 5 octets d'en-tête et 48 octets de données.

La commutation de trames ATM a pour objectif de remplacer à la fois la commutation de circuits et la commutation de paquets en respectant les principes de ces deux techniques. Pour y parvenir, il suffit de supposer que les temps de transmission et de commutation sont très brefs en comparaison du temps de propagation. Supposons des lignes de communication qui atteignent 1 Gbit/s. Pour émettre les 53 octets de la trame, il faut un peu moins de 500 ns. Si l'on suppose que la durée de franchissement d'un commutateur est inférieure à 10 µs, on peut considérer que ces valeurs sont négligeables en comparaison du délai de propagation, qui vaut approximativement 1 ms pour 250 km, ou encore 10 ms pour 2 500 km.

En conclusion, la commutation de trames ATM est une technique de transfert qui a pris un essor considérable à la fin des années 1980 grâce à sa simplicité, qui permet de monter facilement en débit. Malheureusement, elle n'a jamais pu s'imposer à l'interface utilisateur, et c'est la commutation Ethernet qui est en train de prendre largement le dessus.

Routeurs et commutateurs

Les commutateurs acheminent les paquets vers le récepteur en utilisant des références, également appelées identificateurs ou étiquettes (en anglais *labels*). Une référence est une suite de chiffres accompagnant un bloc (trame, paquet, etc.) pour lui permettre de choisir une porte de sortie au sein d'une table de commutation. Par exemple, si 147 est une référence, tous les paquets se présentant sur une porte d'entrée déterminée et portant la valeur 147 sont dirigés vers la même ligne de sortie. Les routeurs utilisent une table de routage pour diriger les paquets vers leur destination.

Ces deux possibilités sont assez différentes puisque, dans la commutation, le chemin que suivent les paquets de nœud en nœud est toujours le même, alors que, dans le routage, le paquet est routé à l'entrée de chaque nœud grâce à l'adresse complète du récepteur.

Une fois le chemin ouvert, les mesures montrent que, pour une puissance donnée, un commutateur atteint un débit d'une dizaine de fois supérieur à celui d'un routeur. Cette différence a toutefois tendance à se réduire avec les routeurs gigabit, dits gigarouteurs capable de router plus de 100 000 paquets IP toutes les secondes.

La différence principale entre le routage et la commutation réside dans le type d'information de supervision transportée par le paquet. Dans un routeur, le paquet doit posséder l'adresse complète du destinataire. La décision de router prend donc du temps, puisqu'il faut non seulement trouver la bonne ligne de sortie à l'aide de la table de routage mais encore et surtout gérer cette table de routage. Dans un commutateur, la table de commutation indique la ligne de sortie en fonction de la référence transportée par le paquet. Le paquet ne comporte qu'une seule référence, qui indique une file de sortie du nœud, laquelle est toujours la même, indépendamment de l'état du réseau.

Pour mettre en place le chemin que suivront tous les paquets, une signalisation est nécessaire. Cette signalisation s'effectue grâce à un paquet spécifique, parfois appelé paquet d'appel. Dans un commutateur, c'est la table de routage qui dirige le paquet d'appel nécessaire à l'établissement du chemin. Le commutateur possède donc à la fois une table de routage et une table de commutation.

En cas de cassure de ligne ou de panne d'un nœud, un nouveau chemin doit être déterminé par le système de signalisation, ce qui prend beaucoup de temps (plusieurs centaines de millisecondes). Le réacheminement est donc totalement à éviter mais indispensable sur des pannes. Pour éviter ce cas, il est possible d'ouvrir deux chemins menant de l'émetteur au récepteur dont un seul est utilisé et l'autre mis en secours. Dans ce cas, il faut plus de ressources dans le réseau, et le coût augmente en conséquence.

Pour obtenir de bonnes performances, il faut essayer de limiter le nombre d'entrées dans les tables de routage et de commutation. Une valeur inférieure à 10 000 entrées garantit une bonne vitesse. Lorsque la commutation ne s'effectue que sur une partie de la référence, le commutateur s'appelle un brasseur. Dans le monde de la commutation, le temps de traversée d'un nœud doit rester négligeable par rapport au temps de transit du réseau, pour que celui-ci soit à peu près égal au temps de propagation.

La commutation permet donc d'acheminer des informations au travers d'un réseau en les transportant de nœud en nœud suivant un chemin (path) prédéfini, longtemps appelé circuit virtuel. Ce chemin est défini par une succession de références que tous les paquets d'un même flot doivent suivre, comme s'ils étaient sur un circuit. Le circuit est dit virtuel parce qu'il n'appartient pas de façon exclusive au couple émetteur-récepteur, à la différence d'un circuit véritable.

Fonctionnalités des routeurs et des commutateurs

Les nœuds de transfert doivent être capables de supporter aussi bien les trafics homogènes que les trafics sporadiques. Le fait d'intégrer des services dont les objectifs et les critères de performance peuvent être très différents nécessite l'utilisation de priorités. C'est la raison pour laquelle les paquets sont dotés d'informations de priorité, qui sont traitées dans la file d'attente d'entrée des routeurs et commutateurs.

Les fonctions principales d'un nœud de transfert sont les suivantes :

- analyse et traduction de l'en-tête du paquet ;
- commutation ou routage ;
- multiplexage des paquets sur la sortie déterminée.

L'information utilisateur transportée dans les paquets est transférée de manière asynchrone, c'est-à-dire selon un mode de transmission des données dans lequel l'instant d'émission de chaque caractère ou bloc de caractères est arbitraire. Puisque les communications sont asynchrones et qu'un grand nombre de chemins peuvent partager une même liaison, le nœud de transfert doit être capable de gérer au mieux ses ressources. Ces dernières sont constituées par les mémoires tampons, les files de sortie et la file d'entrée du nœud.

La figure 2.13 illustre la façon de traiter les paquets dans la file d'entrée d'un nœud de transfert, qui peut être un routeur ou un commutateur. Les paquets proviennent de trois nœuds amont, A, B, C. Les paquets sont ensuite dirigés vers une première file d'attente, qui a pour fonction de décider du choix de la ligne de sortie. Une fois la décision prise, le paquet est dirigé vers une des trois files de sortie correspondant aux trois nœuds A, B, C. Normalement, un paquet entrant par l'une des entrées, A par exemple, ne ressort pas vers le même nœud A, car cela générerait une boucle dans le routage.

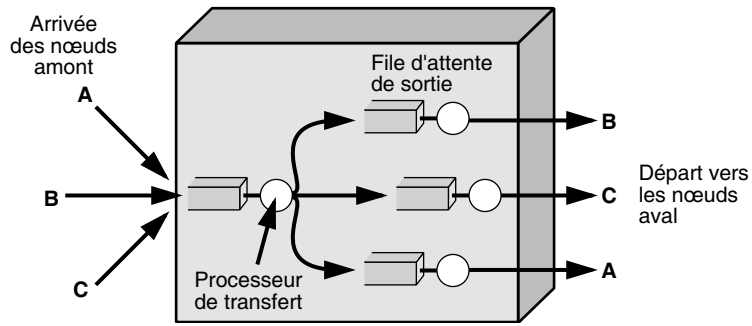


Figure 2.13

Fonctionnement d'un nœud de transfert

Le nœud de transfert examine l'en-tête de chaque paquet pour identifier le port de sortie indiqué. Grâce à sa table de commutation ou de routage, il effectue ensuite le transfert du paquet vers la bonne file de sortie. Le choix de la liaison de sortie est défini à partir soit d'une table de commutation, comme dans le cas de l'Ethernet commuté ou de l'ATM, soit d'une table de routage, qui peut être statique ou dynamique, comme dans le cas du protocole IP. Des paquets de contrôle, de supervision et de gestion sont également pris en charge par l'unité centrale du nœud de transfert.

Dans un commutateur, la ligne de sortie est déterminée par la référence contenue dans l'en-tête du paquet. Des mécanismes de contrôle de collision permettent aux paquets provenant de différentes entrées d'accéder en parallèle à la première file d'attente du nœud, parfois appelée file de commutation. Le mot commutation a longtemps désigné le

transfert d'un paquet d'une ligne d'entrée vers une ligne de sortie. Aujourd'hui, comme cette fonction de transfert recouvre deux modes, le routage et la commutation, il est préférable d'appeler cette fonction un transfert, de sorte à ne pas utiliser le mot commutation lorsqu'on a affaire à un routage.

Il existe une diversité de solutions pour réaliser un nœud de transfert. Dans tous les cas, une fonction de stockage doit se trouver à l'entrée ou à la sortie, ou encore le long de la chaîne de transfert. À l'intérieur du nœud, diverses techniques de routage peuvent être mises en œuvre, telles que circuit virtuel, autoroutage ou datagramme. L'efficacité de ces solutions est assez comparable en matière de contrôle d'accès, de capacité de diffusion, de perte de cellules et de complexité technique.

Diverses méthodes permettent d'aiguiller les paquets et de gérer les mémoires tampons. Des fonctions additionnelles, telles que la correction d'erreur ou le contrôle de flux, sont souvent implémentées dans les nœuds de transfert.

Les commutateurs

En anglais, les commutateurs sont appelés « *label switch* » ou, plus fréquemment, *switch*, pour bien insister sur le fait que les commutateurs utilisent des références (*label*).

L'un des atouts majeurs des systèmes de commutation réside dans l'architecture des commutateurs. Plusieurs types d'architectures ont été proposés, dont les trois principaux sont dits à mémoire partagée (*shared-memory*), à support partagé (*shared-medium*) et à division spatiale (*space-division*). Étant donné les vitesses des lignes de transmission, les commutateurs doivent pouvoir commuter les paquets à des débits extrêmement élevés tout en étant capables de traiter plusieurs milliers de chemins et donc de gérer des tables de commutation à plusieurs milliers d'entrées. De tels commutateurs sont réalisés de façon matérielle plutôt que logicielle.

Les différents commutateurs se distinguent les uns des autres en fonction de critères de fonctionnement internes, tels que l'architecture, le type de liaison, la technique de commutation, le contrôle et la gestion des blocages par les mémoires tampons :

- Les architectures internes se différencient par le nombre d'étapes à traverser. Une étape peut être considérée comme un bloc monolithique, traversé en une seule tranche de temps de base. Plus le nombre d'étapes est faible, plus le temps de réponse est court.
- La liaison à l'intérieur du commutateur de paquets peut être soit dédiée, soit statistique. Sur une liaison dédiée, les paquets vont d'une porte d'entrée à une porte de sortie, en transitant toujours par le même chemin. Dans le cas d'une liaison statistique, tout paquet est apte à emprunter une liaison quelconque à l'intérieur du commutateur. Le routage est alors déterminé par un algorithme de contrôle.
- Les techniques de commutation interne peuvent être classées en deux grandes catégories : la répartition dans l'espace et la répartition dans le temps. Dans une répartition dans l'espace, plusieurs liaisons parallèles peuvent être mises en place pour véhiculer les paquets. Dans une répartition dans le temps, les paquets se partagent les ressources dans le temps. Il peut aussi y avoir superposition des deux techniques de commutation, plusieurs liaisons mettant chacune en œuvre un multiplexage temporel.

- Le contrôle du commutateur s'effectue à l'aide d'algorithmes de gestion des ressources. Ces algorithmes concernent, entre autres, le routage des paquets et les contrôles de flux et de congestion.
- À l'intérieur du commutateur, il peut être nécessaire de mémoriser des paquets en cas de blocage. Un blocage apparaît lorsque deux paquets entrent en compétition pour obtenir une même ressource. Dans ce cas, il faut mettre un paquet en attente. Les mémoires peuvent se situer à l'entrée, à la sortie ou en différents points à l'intérieur du commutateur. Il existe des commutateurs avec blocage et d'autres sans.

Les routeurs

Pendant de longues années, les routeurs ont été considérés comme des machines lentes et complexes à gérer. La fonction de routage exige en effet la connaissance de l'emplacement de tous les destinataires pouvant passer par le même nœud de façon à pouvoir leur router les paquets, cet emplacement étant déterminé par l'adresse complète du destinataire transportée dans le paquet. De plus, la table de routage étant une ressource partagée, elle doit pouvoir répondre à toutes les demandes émises par les paquets en mémoire.

Une première solution aux problèmes de vitesse et d'accès à la table de routage a consisté à réduire sa taille à moins de 10 000 entrées, c'est-à-dire 10 000 destinataires. Chaque ligne indique, en fonction d'une adresse de destination, la ligne de sortie sur laquelle il faut émettre le paquet. Pour restreindre le nombre de destinations, on agrège souvent les adresses, comme nous le verrons au chapitre 17.

Pour accroître encore les performances des routeurs, on a implémenté dans les composants électroniques installés dans le cœur des routeurs des techniques développées pour les commutateurs et aujourd'hui totalement maîtrisées. Cette solution a été rendue possible par la chute des prix des composants des commutateurs, conséquence de leur miniaturisation.

La figure 2.14 illustre le transfert d'un paquet arrivant sur une ligne d'entrée i et acheminé vers une ligne de sortie j.

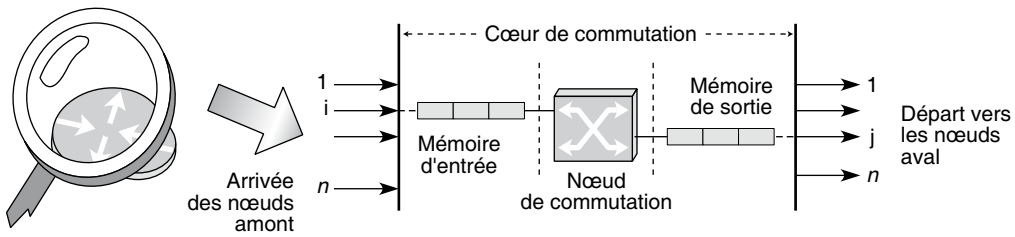


Figure 2.14

Transfert de paquets dans un routeur

La figure ne décrit qu'un seul nœud de commutation, possédant *n* lignes d'entrée et donc également *n* lignes de sortie. Une fois la ligne de sortie j choisie grâce à la table de

routage située dans le routeur, le paquet est transporté *via* le cœur de commutation vers la mémoire de sortie j, dans laquelle sont enregistrés les paquets en attente d'être émis sur la ligne physique. Ces paquets forment une file d'attente pour être émis dans un ordre déterminé par leur priorité, si des priorités existent, sinon suivant la règle « premier arrivé premier sorti ».

La table de routage est gérée par un processeur se trouvant dans le routeur. Les accès à la table de routage sont distribués entre toutes les files d'entrée. Cette architecture est toutefois celle d'un routeur relativement puissant.

Les commutateurs-routeurs ou LSR (Label Switch Router)

Certaines applications sont mieux prises en compte par un routage et d'autres par une commutation. Par exemple, la navigation dans une base de données Web distribuée au niveau mondial est préférable dans un environnement routé. À l'inverse, la commutation est mieux adaptée au transfert de gros fichiers. Ces constatations ont incité beaucoup d'industriels à essayer d'optimiser l'acheminement des paquets en proposant des solutions mixtes, appelées commutateur-routeurs, superposant dans une même boîte un commutateur et un routeur.

Grâce à leur architecture double, les commutateurs-routeurs peuvent répondre aux demandes de commutation ou de routage des clients du réseau. Dans le premier cas, un paquet de signalisation met en place un circuit virtuel, que tous les paquets du flot doivent suivre. Dans le second, chaque paquet est livré à lui-même et, grâce au routage, arrive au destinataire.

Le choix de l'utilisateur n'est pas toujours simple, puisqu'il ne connaît pas forcément la longueur de son flot. Même s'il le sait, il lui faut pouvoir l'indiquer au réseau de façon que celui-ci prenne la bonne décision, entre routage et commutation. En règle générale, le choix se fait à partir du type de l'application transportée. Par exemple, la consultation de pages Web donne automatiquement naissance à un flot routé, tandis que les paquets d'un transfert de fichiers sont automatiquement commutés.

Malgré l'intérêt de ces commutateurs-routeurs, comme il n'a jamais été possible de déterminer facilement la méthode la plus intéressante en fonction de l'application, les évolutions ont poussé à l'adoption de ces commutateurs-routeurs dans un cas simple : on route la signalisation et on commute les données de l'utilisateur.

La commutation a toujours demandé un routage de la signalisation, mais comme le système de signalisation était spécifique dans les anciennes techniques comme X.25 et ATM, on n'utilisait pas le mot routage. Aujourd'hui, dans la technique de base des opérateurs, appelée MPLS, le réseau de signalisation est un réseau IP et on utilise le mot routage pour indiquer l'ouverture du chemin. Une fois le chemin ouvert, on commute tous les paquets de données, encapsulés dans des trames, sur le chemin. Les Anglo-Saxons utilisent le terme « Label Switch Router » (LSR) pour indiquer qu'il y a un commutateur (*label switch*) et un routeur dans chaque nœud du réseau.

Conclusion

Les réseaux de transfert de données offrent deux grandes classes de solutions : les transferts de type routage et les transferts de type commutation. On peut trouver des arguments en faveur d'une solution ou de l'autre, la meilleure dépendant essentiellement de l'objectif recherché.

Si le but visé est d'obtenir une qualité de service et un certain nombre de propriétés de contrôle de l'environnement, la commutation est plus séduisante. En revanche, si l'on recherche un moyen économique, le routage est moins complexe, et donc beaucoup moins cher.

Les solutions hybrides, comme MPLS, semblent former un compromis prometteur, malgré leur prix de revient assez élevé puisque deux technologies se superposent.

3

Le médium de transport

Le médium de transport correspond aux éléments matériels et immatériels capables de transporter des éléments binaires, comme les câbles et les ondes radio. Dans le premier cas, ce sont des fils métalliques ou des fibres optiques qui transportent l'information ; dans le second, ce sont les ondes hertziennes.

Les deux types de support sont plus complémentaires que concurrents. Le hertzien permet la mobilité, mais au prix de débits plus faibles. De son côté, le câble propose des débits de plus en plus importants. Même si les débits des équipements mobiles augmentent, l'écart reste stable avec ceux des câbles. On arrive aujourd'hui à des dizaines de gigabits par seconde sur la fibre optique contre des centaines de mégabits par seconde pour le hertzien.

Ce chapitre examine les caractéristiques de ces différents médias de transport afin de mieux faire comprendre les architectures que l'on peut bâtir au-dessus.

Le médium physique

Par médium physique, il faut entendre tous les composants physiques permettant de transmettre les éléments binaires, suites de 0 et de 1, représentant les données à transmettre.

La nature des applications véhiculées par le réseau peut influer sur le choix du support, certaines applications nécessitant, par exemple, une bande passante importante et, par là même, l'adoption de la fibre optique. Le câble coaxial permet lui aussi de transférer des débits binaires importants, même si ces derniers restent inférieurs à ceux offerts par la fibre optique.

Aujourd'hui, les progrès technologiques rendent l'utilisation de la paire de fils torsadée bien adaptée à des débits de 10 à 100 Mbit/s, voire 1 Gbit/s sur des distances plus courtes. Sa facilité d'installation par rapport au câble coaxial et son prix très inférieur la rendent à la fois plus attractive et plus compétitive.

La fibre optique est présente dans tous les systèmes de câblage proposés par les constructeurs, en particulier sur les liaisons entre locaux techniques. Elle présente l'avantage d'un faible encombrement, l'espace très important requis par les autres supports physiques pouvant devenir contraignant. Un autre avantage de la fibre optique est son immunité au bruit et aux interférences électromagnétiques. Dans certains environnements perturbés les erreurs de transmission peuvent en effet devenir inacceptables. De même, sa protection naturelle contre l'écoute la rend attrayante dans les secteurs où la confidentialité est importante, comme l'armée ou la banque.

On observe une utilisation de plus en plus fréquente de la paire torsadée. Les progrès technologiques lui ont permis de repousser ses limites théoriques par l'ajout de circuits électroniques et d'atteindre des débits importants à des prix nettement inférieurs à ceux du câble coaxial. La paire torsadée est de surcroît plus simple à installer que le câble coaxial, d'autant qu'elle peut utiliser l'infrastructure mise en place depuis longtemps pour le câblage téléphonique. La paire torsadée permet enfin de reconfigurer, de maintenir ou de faire évoluer le réseau de façon simple.

La paire de fils torsadée

La paire de fils torsadée est le support de transmission le plus simple. Comme l'illustre la figure 3.1, elle est constituée d'une ou de plusieurs paires de fils électriques agencés en spirale. Ce type de support convient à la transmission aussi bien analogique que numérique.

Les paires torsadées peuvent être blindées, une gaine métallique enveloppant complètement les paires métalliques, ou non blindées. Elles peuvent être également « écrantées ». Dans ce cas, un ruban métallique entoure les fils.

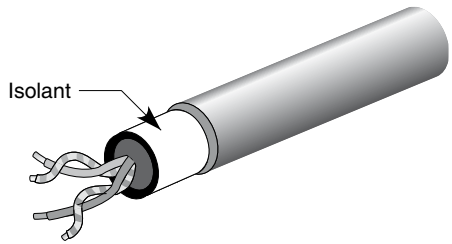


Figure 3.1
Paires de fils torsadées

De très nombreux débats ont lieu sur les avantages et inconvénients du blindage de ces câbles. On peut dire, en simplifiant, qu'un câble blindé devrait être capable de mieux immuniser les signaux transportés. L'inconvénient du blindage est toutefois qu'il exige la mise à la terre de l'ensemble de l'équipement, depuis le support physique jusqu'au terminal. Il faut donc que toute la chaîne de connexion des terres soit correctement effectuée et maintenue. En d'autres termes, un réseau blindé doit être de très bonne qualité, faute de quoi il risque de se comporter moins bien qu'un réseau sans blindage, beaucoup moins onéreux.

Les fils métalliques sont particulièrement adaptés à la transmission d'informations sur de courtes distances. Si la longueur du fil est peu importante, de quelques centaines de mètres à quelques kilomètres, des débits de plusieurs mégabits par seconde peuvent être atteints sans taux d'erreur inacceptable. Sur des distances plus courtes, on peut obtenir sans difficulté des débits de plusieurs dizaines de mégabits par seconde. Sur des distances encore plus courtes, on atteint facilement quelques centaines de mégabits par seconde. Une distance de l'ordre de 100 m permet de faire passer le débit à plusieurs gigabits par seconde.

La normalisation dans le domaine des câbles est effectuée par le groupe ISO/IEC JTC1/SC25/WG3 au niveau international et par des organismes nationaux comme l'EIA/TIA (Electronic Industries Association/Telecommunications Industries Association), aux États-Unis.

Les principales catégories de câbles définies sont les suivantes :

- Catégorie 3 (10BaseT) ;
- Catégorie 4 (10BaseT et Token-Ring 16 Mbit/s) ;
- Catégorie 5 (10BaseT, Token-Ring 16 Mbit/s et 100 Mbit/s TPDDI) ;
- Catégorie 5e (Type R évolué, pour une largeur de bande de 100 MHz) ;
- Catégorie 6 (pour une largeur de bande de 200 MHz) ;
- Catégorie 7 (pour une largeur de bande de 600 MHz).

Il est possible de comparer les paires torsadées en fonction de leur paradiaphonie, c'est-à-dire de la perte d'une partie de l'énergie du signal due à la proximité d'un autre circuit et de son affaiblissement. La figure 3.2 illustre ces comparaisons. Les câbles de types 6 et 7 ne figurent pas dans ce schéma par manque de mesures disponibles. Dans cette même figure, nous avons ajouté un câble spécifique à la France, le câble 120 Ω,, qui est une proposition de France Télécom pour trouver un compromis entre les 100 et 150 Ω et éviter ainsi dans la mesure du possible les adaptateurs d'impédance.

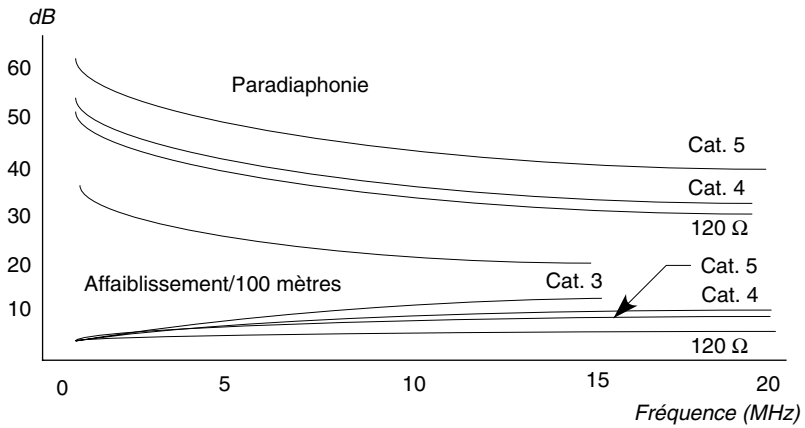


Figure 3.2

Comparaison de la paradiaphonie et de l'affaiblissement du signal sur 100 m de divers types de câbles

Le câble coaxial

Un câble coaxial est constitué de deux conducteurs cylindriques de même axe, l'âme et la tresse, séparés par un isolant (*voir figure 3.3*). Ce dernier permet de limiter les perturbations dues au bruit externe. Si le bruit est important, un blindage peut être ajouté. Quoique ce support perde du terrain, notamment par rapport à la fibre optique, il reste encore très utilisé.

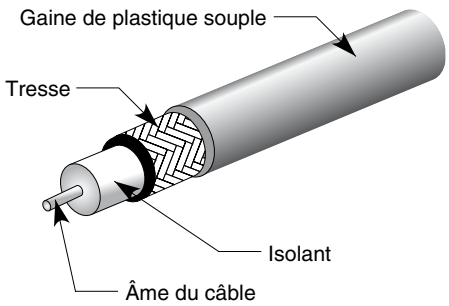


Figure 3.3

Coupe d'un câble coaxial

Les électroniciens ont démontré que le rapport des diamètres des deux conducteurs devait être de 3,6 mm. Les différents câbles utilisés sont désignés par le rapport en millimètre des diamètres de l'âme et de la tresse du câble, les deux plus courants étant les 2,6/9,5 et 1,2/4,4.

Comme pour les fils métalliques, le débit binaire obtenu sur un câble coaxial est inversement proportionnel à la distance à parcourir. Sur un câble coaxial de bonne qualité d'une longueur de 1 km, des débits supérieurs à 100 Mbit/s peuvent être atteints.

Les principales catégories de câbles coaxiaux disponibles sur le marché sont les suivantes :

- câble 50 Ω, de type Ethernet ;
- câble 75 Ω, de type CATV (câble de télévision).

La fibre optique

La fibre optique est utilisée dans les environnements où un très fort débit est demandé, mais également dans les environnements de mauvaise qualité. Elle comporte des composants extrémité qui émettent et reçoivent les signaux lumineux.

Les principaux composants émetteurs sont les suivants :

- Diode électroluminescente (DEL) dépourvue de cavité laser, qui émet des radiations lumineuses lorsqu'elle est parcourue par un courant électrique.
- Diode laser (DL), qui émet un faisceau de rayonnement cohérent dans l'espace et dans le temps.

- Laser modulé.

L'utilisation d'un émetteur laser diminue le phénomène de dispersion, c'est-à-dire la déformation du signal provenant d'une vitesse de propagation légèrement différente suivant les fréquences. Cela donne une puissance optique supérieure aux DEL. La contrepartie de ces avantages est un coût plus important et une durée de vie du laser inférieure à celle d'une diode électroluminescente.

La figure 3.4 illustre une liaison par fibre optique. Cette figure comporte des codeurs et des décodeurs qui transforment les signaux électriques en signaux qui peuvent être émis sous forme de lumière dans la fibre optique et *vice versa*. L'émetteur est un des trois composants extrémité que nous venons de voir et le récepteur un photodétecteur capable de récupérer les signaux lumineux.

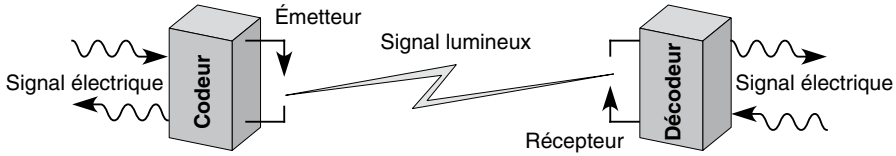


Figure 3.4

Liaison par fibre optique

Le faisceau lumineux est véhiculé à l'intérieur de la fibre optique, qui est un guide cylindrique d'un diamètre allant de quelques microns à quelques centaines de microns, recouvert d'isolant. La vitesse de propagation de la lumière dans la fibre optique est de l'ordre de 100 000 km/s en multimode et de 250 000 km/s en monomode.

Il existe plusieurs types de fibres, notamment les suivantes :

- Les fibres multimodes à saut d'indice, dont la bande passante peut atteindre 50 MHz sur 1 km.
- Les fibres multimodes à gradient d'indice, dont la bande passante peut atteindre 500 MHz sur 1 km.
- Les fibres monomodes, de très petit diamètre, qui offrent la plus grande capacité d'information potentielle, de l'ordre de 100 GHz/km, et les meilleurs débits. Ce sont aussi les plus complexes à réaliser.

On utilise généralement des câbles optiques contenant plusieurs fibres. L'isolant entourant les fibres évite les problèmes de diaphonie, c'est-à-dire de perturbation d'un signal par un signal voisin, entre les différentes fibres.

La capacité de transport de la fibre optique continue d'augmenter régulièrement grâce au multiplexage en longueur d'onde. Dans le même temps, le débit de chaque longueur d'onde ne cesse de progresser. On estime qu'il a été multiplié par deux tous les ans de 2000 à 2010, date à laquelle on a atteint près de 1 000 longueurs d'onde. Comme, sur une même longueur d'onde, la capacité est passée pour la même période de 2,5 à 40 Gbit/s et bientôt 160 Gbit/s, des capacités de plusieurs dizaines de térabits par seconde (Tbit/s, ou 10^{12} bit/s) sont aujourd'hui atteintes sur la fibre optique.

Le multiplexage en longueur d'onde, ou WDM (Wavelength Division Multiplexing), consiste à émettre simultanément plusieurs longueurs d'onde, c'est-à-dire plusieurs lumières, sur un même cœur de verre. Cette technique est fortement utilisée dans les cœurs de réseau. On l'appelle DWDM (Dense WDM) lorsque le nombre de longueur d'onde devient très grand.

Les principaux avantages de la fibre optique sont les suivants :

- très large bande passante, de l'ordre de 1 GHz pour 1 km ;
- faible encombrement ;
- grande légèreté ;
- très faible atténuation ;
- très bonne qualité de transmission ;
- bonne résistance à la chaleur et au froid ;
- matière première bon marché (silice) ;
- absence de rayonnement.

Les médias hertziens

La réussite du GSM et l'arrivée des terminaux mobiles pouvant se connecter à des réseaux locaux sans fil ont rendu très populaires les supports hertziens. Ce succès est encore amplifié par l'interconnexion des équipements personnels (terminal téléphonique, PC portable, agenda électronique, etc.).

L'ensemble des équipements terminaux mobiles qui utilisent la voie hertzienne pour communiquer constitue ce que l'on appelle les réseaux cellulaires, une cellule étant une zone géographique dont tous les points peuvent être atteints à partir d'une même antenne. Parmi les réseaux cellulaires, on distingue les réseaux de mobiles, les réseaux satellite et les réseaux sans fil. Les réseaux de mobiles permettent aux terminaux de se déplacer d'une cellule à une autre sans coupure de la communication, ce qui n'est pas le cas des réseaux sans fil. Les réseaux satellite sont d'un autre genre car ils demandent des délais de propagation bien plus longs que les réseaux terrestres.

Dans un réseau de mobiles, lorsqu'un utilisateur se déplace d'une cellule à une autre, le cheminement de l'information doit être modifié pour tenir compte de ce déplacement. Cette modification s'appelle un changement intercellulaire, ou handover, ou encore hand-off. La gestion de ces handovers est souvent délicate puisqu'il faut trouver une nouvelle route à la communication, sans toutefois l'interrompre.

Chaque cellule dispose d'une station de base, ou BTS (Base Transceiver Station) dans le cas de la 2G (GSM) ou Node-B dans le cas de la 3G (UMTS) ou E-Node-B dans le cas de la 4G (LTE Advanced) ou encore point d'accès (Access Point) dans le cas du Wi-Fi, c'est-à-dire d'une antenne assurant la couverture radio de la cellule.

Nous allons décrire le cas le plus classique de la 2G (GSM), mais on trouve des situations similaires dans les autres réseaux hertziens ; seuls les noms sont en partie modifiés. Tout cela sera détaillé dans des chapitres dédiés (10, 18 et 19).

Une station de base dispose de plusieurs fréquences pour desservir à la fois les canaux de trafic des utilisateurs, un canal de diffusion, un canal de contrôle commun et des canaux de signalisation. Chaque station de base est reliée par un support physique de type câble métallique à un contrôleur de station de base, ou BSC (Base Station Controller). Le contrôleur BSC et l'ensemble des antennes BTS qui lui sont raccordées constituent un sous-système radio, ou BSS (Base Station Subsystem). Les BSC sont tous raccordés à des commutateurs du service mobile, ou MSC (Mobile service Switching Center).

L'architecture d'un réseau de mobiles 2G est illustrée à la figure 3.5.

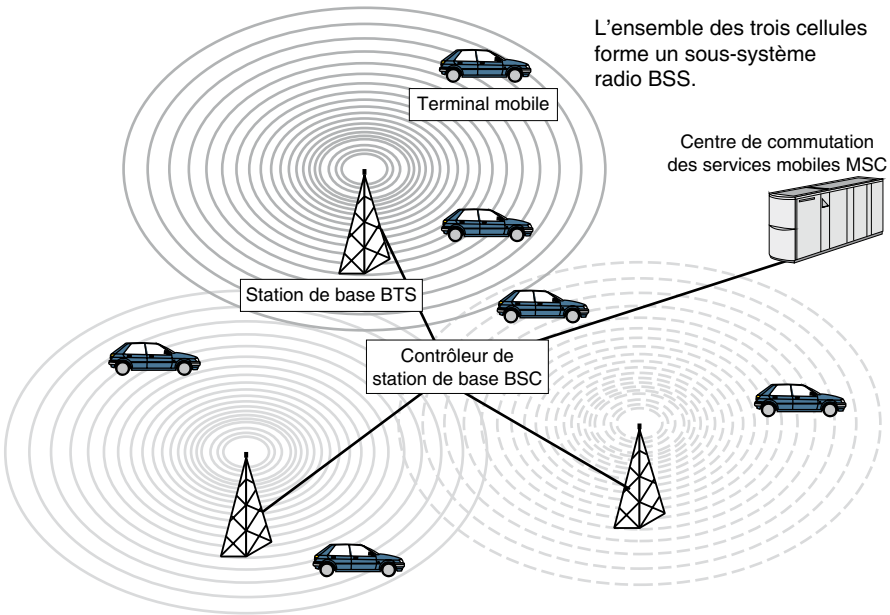


Figure 3.5

Architecture d'un réseau de mobiles

Le câblage

Le câblage des bureaux et des entreprises nécessite des sommes souvent importantes. Lors de l'évaluation de ce coût, il faut prendre en compte non seulement le support mais aussi les équipements situés aux deux extrémités du câble. Il faut en outre évaluer les besoins afin de sélectionner et d'installer le bon câble une fois pour toutes.

Divers paramètres interviennent quant au choix des composants d'un système de câblage, tels le coût, l'environnement, les contraintes particulières des utilisateurs, la fiabilité, l'évolutivité, etc. Il est impératif de caractériser dès le départ l'environnement dans lequel est déployé le réseau. Certains environnements industriels sont critiques et nécessitent des supports spécifiques. Un environnement bruyant, par exemple, peut requérir l'emploi de

la fibre optique. Le réseau peut aussi être exposé à des perturbations électromagnétiques ou climatiques. La sécurité des informations est un autre élément à prendre en compte.

La population d'utilisateurs escomptée détermine le nombre de prises nécessaires pour dimensionner le système. Il faut en outre envisager les types de trafics destinés à être supportés et en évaluer le volume — il peut être important dans le cas de transport d'images numérisées, par exemple — afin d'avoir une idée précise du niveau de fiabilité des transmissions requis, le transfert de données étant très sensible aux erreurs de transmission, contrairement au transfert de voix numérisées.

La topologie du bâtiment est une autre contrainte à prendre en compte. Certains supports sont beaucoup plus maniables que d'autres — le rayon de courbure d'une fibre optique est inférieur à celui d'un câble coaxial, par exemple —, et l'utilisation d'une fibre optique ou d'une paire métallique souple peut être nécessaire dans des bâtiments où le chemin de câblage est quelque peu tortueux.

Les infrastructures de câblage se répartissent entre réseau courant faible pour le transport de l'information (téléphonie, informatique, multimédia) et réseau courant fort pour l'alimentation électrique. Le transport de l'information requiert une puissance très inférieure, de l'ordre du milliwatt, à celle nécessaire au fonctionnement des appareils électriques, qui est de l'ordre de dizaines ou de centaines de watts.

Pour l'implantation d'un réseau de distribution courant faible, il faut décider du chemin des câbles et de la technologie à utiliser de la façon la plus générique possible, indépendamment des types d'information, de matériel et d'utilisateur auxquels le réseau est destiné.

Les répartiteurs

Les répartiteurs sont classés en différentes catégories suivant le type d'installation concerné :

- répartiteur : terme générique ;
- sous-répartiteur d'étage ou de zone ;
- répartiteur général (RG) : soit informatique, soit téléphonique ;
- tableau de communication, ou BRU (boîtier de raccordement usager) : pour le résidentiel.

Les fonctions communes aux répartiteurs sont les suivantes :

- Regrouper les terminaisons des liaisons câblées sur des connecteurs RJ-45 ou optiques.
- Repérer les câblages et les équipements actifs : par exemple, la prise 15 dans le bâtiment B au premier étage sera immédiatement identifiée par son numéro :15B1.
- Gérer les ressources (hub, switch, informatique centrale, autocommutateur) par brassage en fonction des topologies et les connecter aux prises RJ-45 des utilisateurs réparties dans le bâtiment.
- Intégrer les équipements actifs de réseau, soit sous forme de rack 19 pouces (armoire électronique standard), soit sous forme de mini-boîtier.
- Assurer la protection de la connectique et des équipements électroniques (malveillance, poussière, etc.).
- Permettre le test de toutes les parties constituantes d'un réseau ainsi que leur maintenance.

Le plan de câblage d'une entreprise est capital pour la bonne marche des réseaux que l'on souhaite y implanter. Les sections suivantes présentent les différents plans de câblage disponibles.

Le câblage départemental

Les réseaux départementaux, que l'on appelle aussi réseaux SOHO (Small Office/Home Office), ont une taille maximale de l'ordre de la centaine de mètres.

Le rôle du câblage départemental, ou capillaire, est de distribuer les informations vers l'ensemble des bureaux dans un environnement limité. Ces réseaux capillaires sont formés par le câblage sortant du répartiteur d'étage.

La normalisation du câblage départemental a choisi comme support physique quatre paires de fils torsadées distribuées en étoile depuis un local technique central. Cette topologie est illustrée à la figure 3.6.

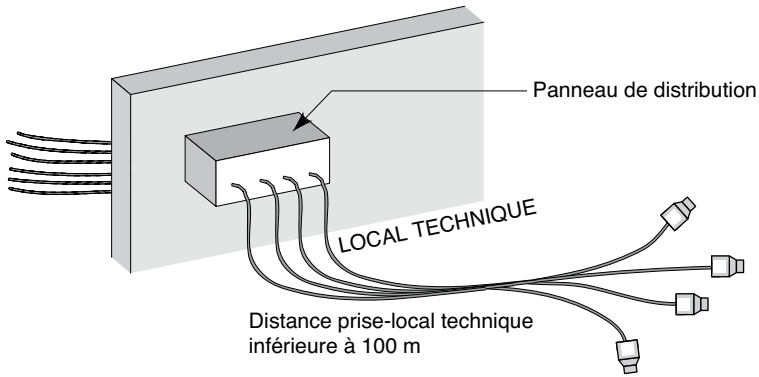


Figure 3.6

Topologie du câblage départemental

La structure en étoile permet de desservir très facilement l'ensemble des pièces du département. On compte généralement une prise pour 6 m^2. Lors du précâblage d'un immeuble neuf, il faut câbler l'ensemble de la surface avec un nombre de prises suffisant pour ne pas à avoir à tirer de nouveaux fils ultérieurement. En effet, lorsqu'on câble un immeuble, le coût à la prise est très bas, comparé au même câblage dans un immeuble ancien, où des travaux d'infrastructure sont nécessaires. Si le coût de la prise d'un précâblage dans un bâtiment neuf est de 75 à 150 euros en moyenne, il faut multiplier ces chiffres par dix pour un immeuble ancien sans infrastructure de câblage.

De plus en plus, les nouveaux bâtiments sont précâblés selon une structure identique à celle des câblages du réseau téléphonique à partir du répartiteur d'étage. Quelques différences doivent toutefois être signalées :

- Le câblage peut être banalisé : on utilise dans ce cas le câble pour y raccorder indifféremment un téléphone ou un équipement informatique.

- Le câblage peut être non banalisé : on raccorde les terminaux téléphoniques sur un câble de faible diamètre et les équipements informatiques sur un câble de meilleure qualité.
- Les câbles peuvent permettre de réaliser divers types de réseaux locaux capillaires. La qualité du câble est importante en cas de contrainte de distance. Pour les réseaux à 100 Mbit/s, voire à 1 Gbit/s, le câble doit être d'excellente qualité pour atteindre la centaine de mètres. Le mieux est de limiter la distance entre le local technique et la périphérie à 50 m et d'utiliser un câble métallique de bonne qualité.

Dans le câblage banalisé, aussi appelé structuré ou universel, la banalisation doit être totale, et la prise du terminal unique. Le choix penche généralement en faveur de la prise normalisée ISO 8877, qui peut se décliner de différentes façons dans chaque pays. La norme de câblage française avec une prise RJ-45 universelle est NF C 15-100 (guide UTE C 90-483). Elle est également applicable au câblage résidentiel.

Tous les câbles arrivent sur un même répartiteur, et ce sont des cordons de connexion, ou jarretières, qui sont utilisés pour connecter, dans le local technique, l'arrivée du câble banalisé aux prises donnant accès au réseau téléphonique ou informatique. Les câbles utilisés sont identiques. En règle générale, on utilise quatre paires de fils torsadées pour être compatible avec la prise RJ-45, qui possède 8 broches, 4 pour les données et 4 pour la téléalimentation.

La non-banalisation permet de poser des câbles de qualités différentes entre l'informatique et la téléphonie. Par exemple, on peut utiliser deux paires de fils torsadées blindées de très bonne qualité pour la partie informatique et quatre paires de fils torsadées non blindées pour la partie téléphonique. Du fait de cette différence entre les deux câblages, les arrivées au répartiteur d'étage sont différentes : la partie informatique arrive sur un tableau de distribution informatique et la partie téléphonique sur un tableau de distribution téléphonique.

Rien n'empêche un utilisateur de demander la pose d'un câble spécifique de meilleure qualité que celui proposé par le constructeur, de façon à éviter tout problème d'adaptation à l'environnement. Une autre solution pour prendre en compte les caractéristiques de tous les types de réseaux locaux consiste à réduire la distance maximale entre le terminal et le tableau de distribution. Cette distance doit être suffisamment courte pour supporter les débits les plus importants des produits disponibles sur le marché.

Nous venons de voir que la topologie normalisée était de type étoile. Cependant, cette topologie en étoile n'est pas toujours adaptée à l'entreprise. D'autres topologies sont possibles, comme le bus ou la boucle.

La topologie en étoile

La topologie en étoile est évidemment parfaitement adaptée à la distribution des réseaux en étoile. Les câblages des autocommutateurs privés, ou PABX, sont conformes à cette topologie. Une difficulté peut toutefois surgir de l'inadéquation des câbles aux débits proposés par les autocommutateurs. Le système de câblage peut dater de nombreuses années et n'avoir été conçu que pour faire transiter un signal analogique à 3 200 Hz de bande passante, par exemple. L'inconvénient de cette topologie en étoile est la centralisation : si le centre est défaillant, tout le système risque de s'arrêter.

La topologie en bus

Largement répandue dans les réseaux locaux Ethernet, la topologie en bus présente de nombreux avantages, en particulier celui de pouvoir être passive, c'est-à-dire sans alimentation électrique. Les câbles associés peuvent être de différents types : paires de fils métalliques ou câble coaxial 50 ou 75 Ω. La fibre optique est mal adaptée à cette structure.

À une vitesse de 10 Mbit/s, le signal peut être propagé plus ou moins loin suivant la qualité du câble. Si l'on reprend les normes en vigueur pour Ethernet, Les distances suivantes sont permises :

- 500 m pour un câble coaxial blindé Ethernet jaune ;
- 180 m pour un câble coaxial fin RG-58 utilisé pour les réseaux Cheapernet ;
- 3 600 m pour un câble CATV 75 Ω.

Les tronçons de câble, ou brins, peuvent être raccordés entre eux par des répéteurs. Un répéteur est un organe non intelligent, qui répète automatiquement vers un deuxième câble tous les signaux passant sur un brin, comme illustré à la figure 3.7.

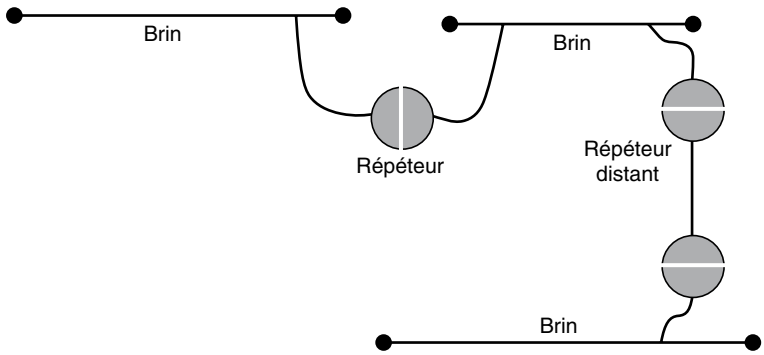


Figure 3.7

Raccordement de brins par des répéteurs

Des répéteurs distants peuvent être reliés entre eux par un autre support de communication, comme la fibre optique.

La topologie en anneau

Sur une topologie en anneau, les coupleurs qui gèrent l'accès au support physique arrêtent l'information, c'est-à-dire mémorisent pendant un certain temps les informations passant sur la boucle. Plusieurs décisions doivent être prises, telles que déterminer si la trame doit être recopiée vers la prochaine station ou détruite dans le registre, si la valeur du jeton doit être modifiée ou non, si la trame doit être recopiée vers le coupleur, etc. Il faut donc couper le support physique et ajouter un registre à décalage, comme illustré à la figure 3.8. Le registre à décalage mémorise les éléments binaires au fur et à mesure de

leur arrivée. À la fin du décalage, ils sont émis sur la boucle en direction de la prochaine station. Le temps de réflexion pour prendre les décisions utiles est égal au temps des décalages et dépend donc du nombre de registres.

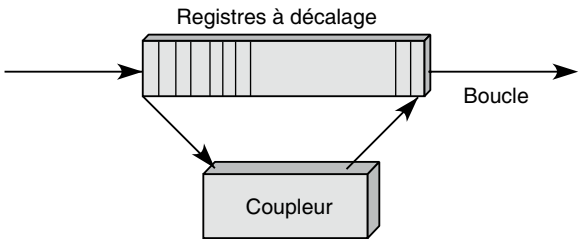


Figure 3.8

Registre à décalage du jeton sur boucle

Le coupleur prend une copie de la trame dans le premier registre. Le nombre de décalages correspond au temps de réflexion du coupleur pour modifier une information ou en introduire une nouvelle. L'incorporation de nouveaux bits ou l'effacement de certains s'effectue sur le dernier bit du registre à décalage.

Le registre à décalage est une structure active, qui doit être alimentée électriquement. Les supports physiques en boucle doivent donc nécessairement être secourus en cas de panne ou de défaut d'alimentation. Les deux grandes techniques utilisées en cas de défaillance sont le by-pass, ou dérivation, illustré à la figure 3.9, et la structuration en étoile, détaillée plus loin.

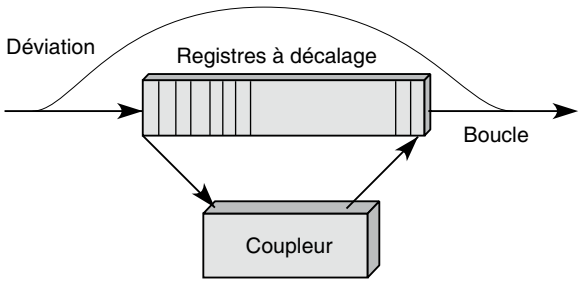


Figure 3.9

Dérivation d'un coupleur

Le passage par un registre à décalage oblige à régénérer le signal à la sortie. C'est un avantage pour la portée totale du réseau mais un défaut du point de vue de la fiabilité. En particulier, l'utilisation d'un by-pass ne permet pas la régénération du signal, ce qui oblige à faire très attention à la portée maximale entre deux coupleurs. Si la portée maximale est de 200 m et que les coupleurs soient disposés tous les 100 m, il n'y a aucun problème lorsqu'un coupleur tombe en panne. En revanche, si deux coupleurs de suite sont en panne, le signal doit parcourir 300 m sans régénération. La distance est trop grande et provoque des dégradations importantes de la qualité de l'information transmise.

Pour éviter ces problèmes, il est possible de proposer une architecture en étoile pour une topologie en boucle. Si un coupleur tombe en panne, la boucle est refermée par l'intermédiaire d'un interrupteur sur le panneau de distribution. Cette solution n'est toutefois guère satisfaisante, puisqu'elle nécessite une intervention manuelle. Dans la réalité, derrière le panneau, on utilise un concentrateur, qui est relié par des jarretières aux prises terminales du câblage. En cas de panne d'un coupleur, le concentrateur est capable de reformer la boucle d'une façon totalement passive.

Pour connecter un utilisateur supplémentaire, on étend la boucle par une nouvelle connexion. L'intérêt de cette technique est qu'elle permet la mise hors circuit, d'une façon simple, de tout élément défaillant. De plus, aucun problème ne se pose au niveau de la répétition du signal, puisqu'on passe directement d'un coupleur au coupleur actif suivant. On peut donc déconnecter les machines et les coupleurs sur l'anneau sans aucun risque pour la qualité du signal.

La distribution en étoile autour du local technique est parfaitement adaptée à cette structure.

L'arbre actif

L'arbre est une configuration qui comporte des nœuds, ou hubs, et des branches. La figure 3.10 illustre cette topologie, avec, au sommet, le nœud racine.

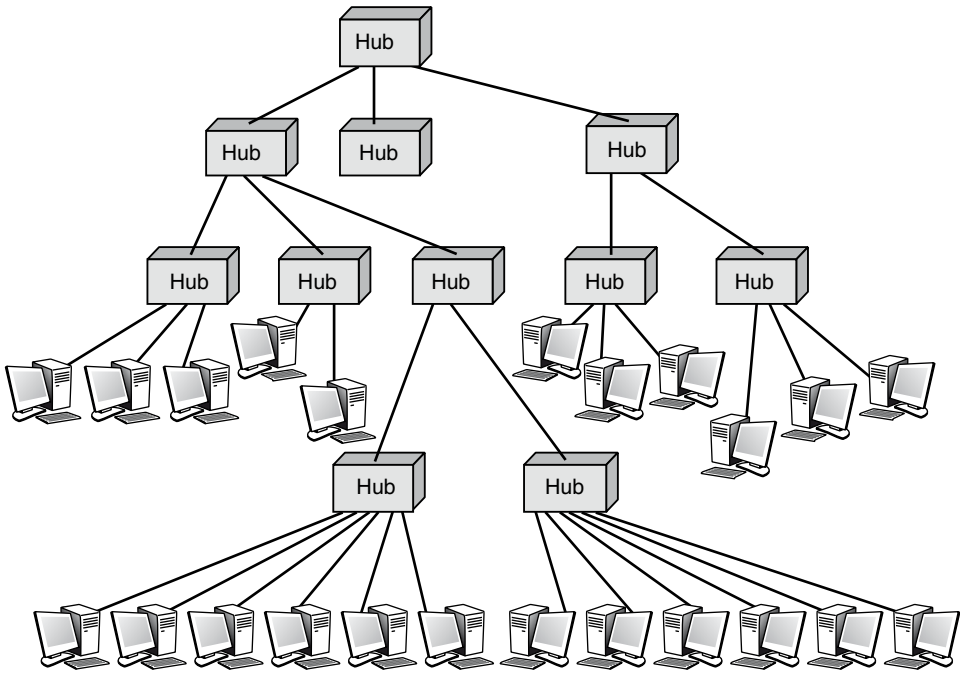


Figure 3.10
Arbre actif

L'arbre actif est caractérisé par une structure arborescente. À chaque intersection correspond un hub alimenté électriquement, dont le rôle est de répéter, dans toutes les directions possibles, une copie du message qui arrive. Cette caractéristique permet, à partir de n'importe quelle station, d'atteindre toutes les autres. Elle se retrouve sur les structures en bus, dans lesquelles, lorsqu'un émetteur envoie de l'information, toutes les stations en prennent une copie au passage et la conservent si l'adresse du destinataire correspond à leur propre adresse. Dans la structure de l'arbre actif, on a exactement les mêmes propriétés : chacun reçoit une copie, et personne n'a à se soucier de savoir qui enlève le signal du câble comme sur une boucle, les signaux disparaissant automatiquement.

Les techniques d'accès correspondant à ce type de réseau en arbre sont identiques à celles des structures en bus, à savoir les techniques Ethernet. Les réseaux en arbre actif avec la technique d'accès Ethernet s'appellent des réseaux Starlan.

La structure en arbre actif est bien adaptée à la distribution en étoile, puisqu'il suffit de placer un hub dans le local technique et de relier, sur le tableau de distribution, les fils correspondant aux machines à raccorder. Plusieurs hubs peuvent être placés dans le même local technique si le nombre de sorties n'est pas suffisant sur un seul hub.

D'autres types de connexions sont possibles à partir d'une structure en arbre, en particulier le raccordement de stations terminales à un contrôleur de communication.

Dans cet exemple, il faut pouvoir connecter le câble de sortie du terminal, correspondant aux caractéristiques du terminal sur le câblage départemental, qui n'a pas forcément la même impédance. Il faut alors ajouter un élément intermédiaire, qui effectue l'adaptation entre les deux types de câbles. Cet élément s'appelle un balun (BALanced-UNbalanced). Ce balun peut être intégré au terminal lui-même.

Le câblage d'établissement

Le câblage d'établissement a pour fonction de raccorder entre eux les différents tableaux de distribution du niveau départemental. On peut envisager pour cela trois possibilités : les rocades, les réseaux locaux et les étoiles.

Les rocades

Les rocades relient les locaux techniques par des faisceaux de câbles. Ces câbles sont utilisés indépendamment les uns des autres, à la demande, pour former des liaisons entre les panneaux de distribution. En règle générale, les rocades sont formées d'un grand nombre de paires de fils : 25, 50, 100 paires ou beaucoup plus. La réalisation d'un réseau Starlan sur trois répartiteurs d'étage est illustrée à la figure 3.11.

Les câbles de rocade peuvent être des fibres optiques, comme on en rencontre dans de nombreux systèmes de câblage.

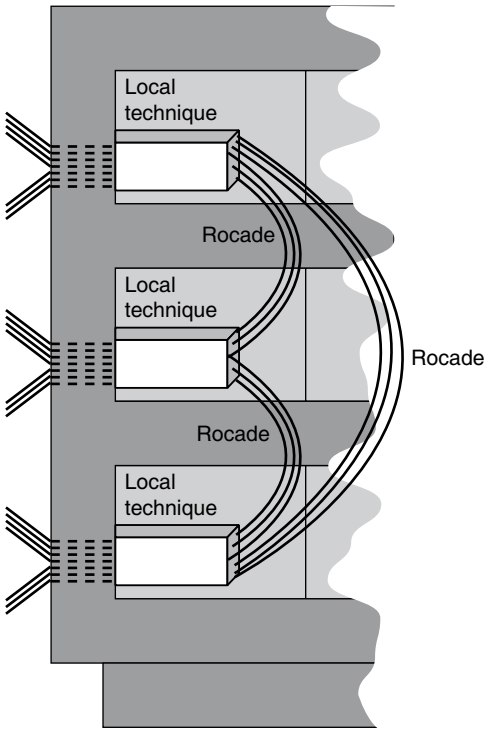


Figure 3.11
Réseau Starlan sur trois répartiteurs d'étages

Les réseaux locaux

Les réseaux locaux représentent la meilleure manière de relier les panneaux de distribution, puisqu'ils ne nécessitent pas le déplacement des jarretières et garantissent une excellente productivité. Parmi les solutions possibles, les sections suivantes présentent brièvement le bus, la boucle et l'étoile.

Les réseaux locaux en bus

Si cette architecture n'est guère adaptée au cadre départemental, elle l'est à celui de l'établissement, où la connexion des différents locaux techniques peut être effectuée en série sur un bus. Les réseaux Ethernet peuvent ainsi utiliser des vitesses de 1 à 10 Gbit/s pour relier des locaux techniques à très haut débit en bus.

Les réseaux locaux en boucle

Les réseaux locaux en boucle ont connu leur heure de gloire avec le Token-Ring d'IBM, à 16 puis 100 Mbit/s, et FDDI (Fiber Distributed Data Interface). Même s'il existe encore de telles structures dans les entreprises, elles sont en voie de disparition au profit des réseaux en bus et en étoile. Nous avons représenté un réseau local en boucle à la figure 3.12.

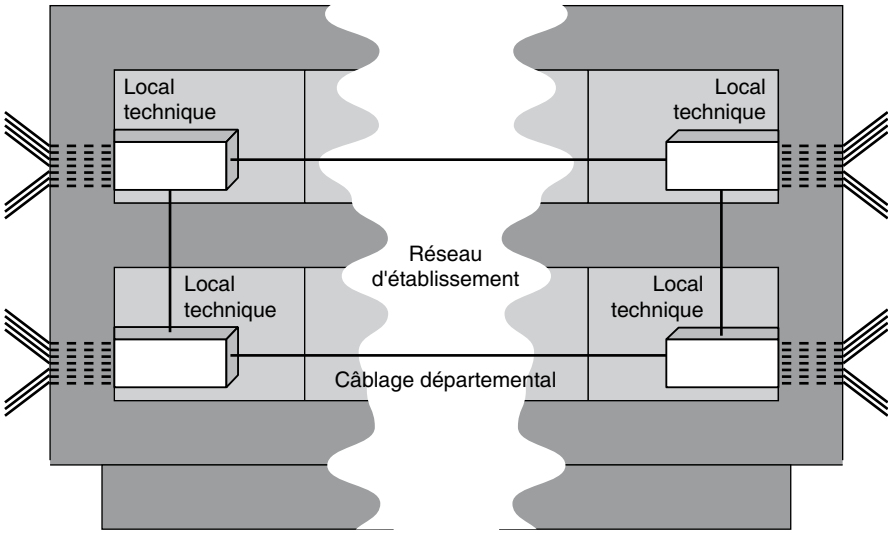


Figure 3.12

Réseau d'établissement en boucle

Les réseaux d'établissement en boucle présentent une difficulté. La régénération des signaux ne s'effectue que dans les cartes coupleurs ajoutées aux machines à connecter. Or les seules machines à connecter dans un réseau d'établissement sont les ponts de connexion des réseaux départementaux. Les régénérations sont effectuées lorsque le signal passe par ces ponts. Si un pont tombe en panne, ou s'il est déconnecté, il faut aller jusqu'au local technique suivant pour que le signal soit régénéré. C'est la raison pour laquelle il est conseillé de doubler les équipements au niveau de l'établissement ou de limiter la distance entre deux répartiteurs d'étage. Cette dernière solution permet au signal de revenir au premier pont ou d'aller au pont suivant.

Les réseaux locaux en étoile

La connexion entre les répartiteurs d'étage ou les tableaux de distribution peut s'effectuer grâce à des étoiles optiques partant d'un point central de l'entreprise. L'étoile peut être passive et répéter dans toutes les directions les informations qui lui proviennent sur une entrée. Pour éviter de diffuser sur tous les câblages raccordés une information destinée à un seul utilisateur, il faut ajouter des ponts dans les locaux techniques.

Dans la plupart des cas, l'étoile optique est un composant passif, générant une perte en ligne importante. Pour cette raison, il ne doit pas y avoir plus de 2 ou 3 étoiles optiques passives en série entre deux points de raccordement. La figure 3.13 illustre une configuration utilisant une étoile optique.

Une deuxième possibilité, beaucoup plus classique, consiste à raccorder les répartiteurs par des faisceaux de câbles qui se dirigent vers un point central. C'est la technique utilisée pour le raccordement des panneaux de distribution téléphonique à un autocommutateur privé (PABX) ou des panneaux de distribution banalisés à un PABX multiservice. Cette structure de raccordement est illustrée à la figure 3.14.

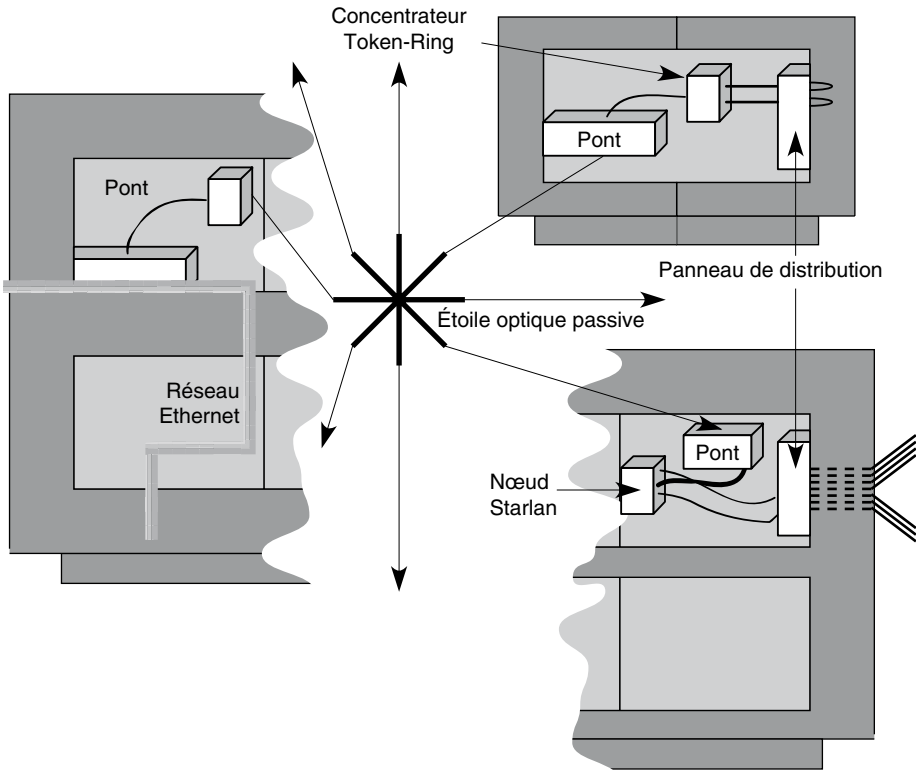


Figure 3.13

Raccordement par étoile optique

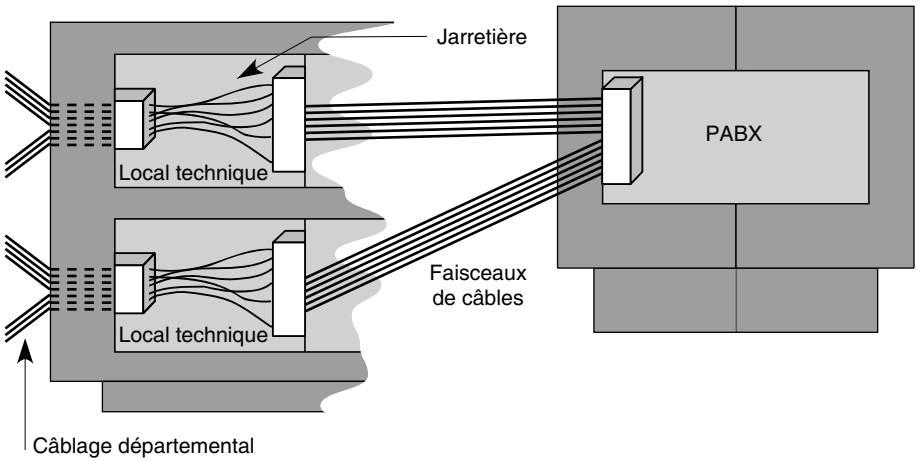


Figure 3.14

Raccordement par faisceaux de câbles

Les raccordements

Le câble à paires torsadées 100 Ω et le connecteur RJ-45 (*voir figure 3.15*) qui lui est associé sont désormais des standards, qui couvrent l'essentiel des besoins de l'entreprise comme de l'habitat.

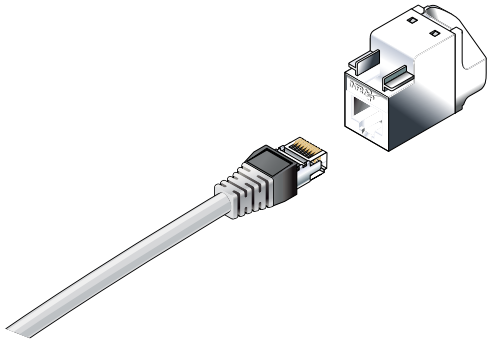


Figure 3.15
Connecteur RJ-45

Pour des besoins particuliers, on peut leur associer d'autres médias, notamment les suivants :

- Fibre optique monomode ou multimode 62,5/125 ou 50/125 pour les environnements électromagnétiques très perturbés, l'interconnexion de bâtiments à des potentiels différents, la transmission sur de longues distances à haut débit ou la distribution des rocades informatiques supportant des réseaux fédérateurs à très haut débit.
- Transmission hertzienne, telle que Wi-Fi ou Bluetooth (*voir les chapitres 21 et 22*), permettant de répondre aux besoins de mobilité (connexions temporaires d'utilisateurs nomades, terminaux mobiles).
- Liaisons par courant porteur en ligne, ou CPL, sur le réseau 230 V (*voir le chapitre 11*).
- Faisceaux laser permettant de relier deux bâtiments peu distants, lorsqu'il est, par exemple, difficile de traverser un domaine public.
- Câble coaxial 75 Ω CATV pour la distribution des rocades TV.

Compte tenu de la généralisation du câblage en paires torsadées, c'est principalement ce médium qui est détaillé ci-après. La figure 3.16 illustre un exemple de câble en paires torsadées.

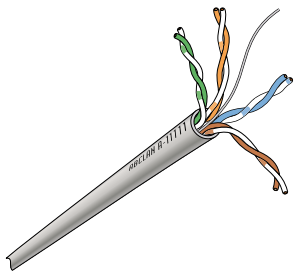


Figure 3.16
Câble en paires torsadées

Ce câblage présente les avantages suivants :

- Pérennité. Un câble en paires torsadées peut conserver ses performances pendant plus de cinquante ans.
- Moindre coût. Les quatre paires d'un câble peuvent véhiculer simultanément plusieurs réseau — il suffit de mettre un duplicateur à chaque extrémité — pour un coût global de l'ordre d'une centaine d'euros.
- Universalité. Ce câblage est passif. Un signal électrique introduit à une extrémité d'une paire en cuivre se retrouve quasiment identique à l'autre extrémité, sans qu'il soit besoin d'ajouter des protocoles intermédiaires nécessitant des interfaces coûteuses comme pour les liaisons hertziennes, CPL ou sur fibre optique. De plus, les paires torsadées permettent de télé-alimenter les équipements qui leur sont raccordés (terminaux Ethernet, téléphones IP, point d'accès Wi-Fi).

Les équipements

Les équipements sont évidemment des éléments indispensables pour gérer la transmission des signaux d'un émetteur vers un récepteur. Ces équipements sont les suivants :

- Les supports physiques d'interconnexion, qui permettent l'acheminement des signaux transportant l'information.
- Les prises (en anglais tap), qui assurent la connexion sur le support.
- Les adaptateurs (en anglais transceiver), qui se chargent notamment du traitement des signaux à transmettre (codage, sérialisation, etc.).
- Les coupleurs, aussi appelés communicateurs ou cartes de transmission, qui prennent en charge les fonctions de communication.

Les interfaces utilisateur assurent la liaison entre l'équipement à connecter et le coupleur. Les données que l'utilisateur souhaite émettre transitent par cette interface à une vitesse qui dépend de la norme choisie. En règle générale, l'interface suit les spécifications du bus de la machine à connecter sur le réseau.

Le connecteur

Le connecteur réalise la connexion mécanique. Il permet le branchement sur le support. Le type de connecteur utilisé dépend évidemment du support physique.

La fibre optique pose des problèmes de raccordement. Le cœur de la fibre étant très fin, de l'ordre de quelques microns, une intervention délicate est nécessaire pour y fixer une prise. La difficulté du branchement sur fibre optique constitue cependant un atout pour la sécurité, dans la mesure où cela en fait un support difficile à espionner, à la différence du câble coaxial.

L'avantage du fil métallique est qu'il permet d'utiliser une prise téléphonique classique, ce qui offre une grande facilité de branchement du coupleur sur le support physique. La prise RJ-45 à 8 contacts en est un exemple. C'est la prise que l'on rencontre désormais dans toutes les entreprises pour réaliser les réseaux de communication courant faible.

L'adaptateur

L'adaptateur (*transceiver*, ou transmetteur) est responsable de la connexion électrique. C'est un composant qui se trouve sur la carte qui gère l'interface entre l'équipement et le support physique. Il est chargé de la mise en série des octets, c'est-à-dire de la transmission des bits les uns après les autres, contrairement à ce qui se passe à l'interface entre la carte de communication et la machine terminale, où l'on a un parallélisme sur 8, 16 ou 32 bits. L'adaptateur effectue la sérialisation et la désérialisation des paquets, ainsi que la transformation des signaux logiques en signaux transmissibles sur le support puis leur émission et leur réception.

Selon la méthode d'accès utilisée, des fonctions supplémentaires peuvent être dévolues à l'adaptateur. Il peut, par exemple, être chargé de la détection d'occupation du câble ou de la détection des collisions de signaux. Il peut aussi jouer un rôle de sécurité en veillant à la limitation d'occupation du support par un émetteur. L'adaptateur est désormais de plus en plus intégré au coupleur.

Le coupleur

L'organe appelé coupleur, ou carte réseau ou encore carte d'accès (une carte Ethernet, par exemple), se charge de contrôler les transmissions sur le câble (*voir figure 3.17*). Le coupleur assure le formatage et le déformatage des blocs de données à transmettre ainsi que la détection d'erreur, mais très rarement les reprises sur erreur lorsqu'une erreur est découverte. Il est aussi chargé de gérer les ressources telles que les zones mémoire ainsi que l'interface avec l'extérieur.

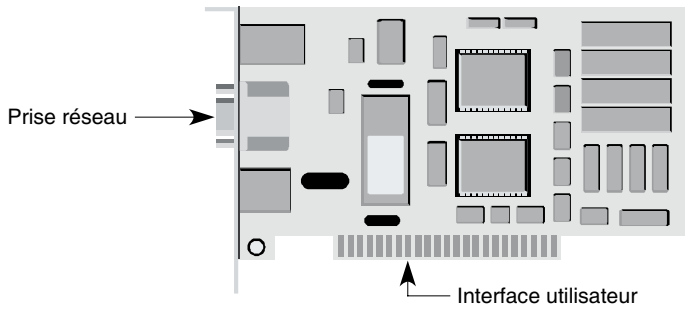


Figure 3.17
Carte coupleur

Le débit d'un coupleur doit s'ajuster au débit permis par le câble. Par exemple, sur un réseau Ethernet possédant un support physique dont la capacité est de 100 Mbit/s, le coupleur doit émettre à cette même vitesse de 100 Mbit/s.

L'interface d'accès au réseau

L'interface d'accès au réseau permettant la connexion d'une machine terminale vers une prise s'est considérablement simplifiée en ce début des années 2000. Il ne reste

pratiquement plus que les interfaces du type RJ-45 pour raccorder les modems ou les postes téléphoniques vers la prise et les coupleurs, qui sont presque exclusivement Ethernet, pour aller vers un réseau local.

Les adaptateurs sont intégrés dans la carte coupleur et ne sont plus visibles des utilisateurs. De nouvelles interfaces informatiques, comme USB (Universal Serial Bus), FireWire ou eLink, permettent d'augmenter sensiblement les débits d'accès. La vraie révolution provient des interfaces sans fil, infrarouge et Bluetooth d'abord puis WUSB (Wireless USB) à 480 Mbit/s. Nous examinons ces interfaces hertziennes au chapitre 22 dans le cadre des réseaux personnels.

Les équipements réseau

Les équipements réseau proviennent de divers horizons, aussi bien informatiques que télécoms. Nous en donnons une description dans un premier temps grossière, mais qui s'affinera au cours de l'ouvrage.

Le nœud de transfert

Comme son nom l'indique, un nœud de transfert sert à transférer des blocs d'informations, ou trames, d'une entrée dans le nœud vers une sortie desservant un nœud suivant.

Le nœud de transfert illustré à la figure 3.18 comporte des files d'entrée et de sortie. Dans une première file du nœud entrent les blocs de données provenant des nœuds qui sont en lien direct avec lui. Cette file possède un processeur de traitement, qui détermine la bonne file de sortie du nœud. Les entrées s'appellent encore des ports d'entrée, et les sorties des ports de sortie.

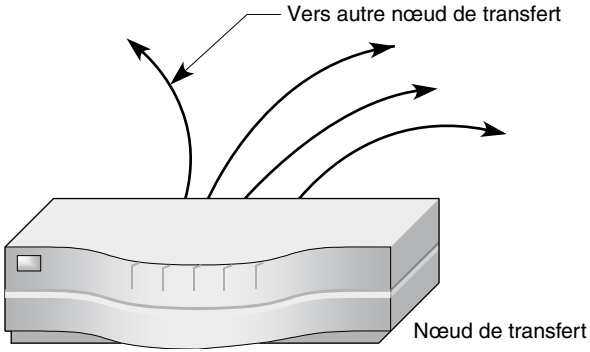


Figure 3.18
Nœud de transfert

Le répéteur et le pont

Parmi les nombreux composants réseau qui font partie du niveau physique, le plus simple est le répéteur (*voir figure 3.19*). Comme expliqué précédemment, il s'agit d'un organe non intelligent, qui répète automatiquement les signaux qui lui arrivent et transitent d'un

support vers un autre support. Dans le même temps, le répéteur régénère les signaux, ce qui permet de prolonger le support physique vers un nouveau support physique. Le répéteur doit avoir des propriétés en accord avec le réseau.

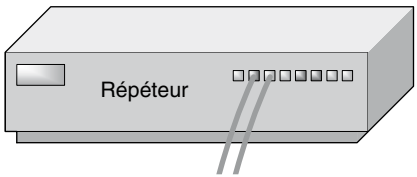


Figure 3.19
Répéteur

Au contraire d'un répéteur, un pont est un organe intelligent, capable de reconnaître les adresses des blocs d'information qui transitent sur le support physique. Un pont filtre les trames et laisse passer les blocs destinés au réseau raccordé. En d'autres termes, un pont ne retransmet que les trames dont l'adresse correspond à une machine située sur le réseau raccordé.

En règle générale, un pont permet de passer d'un réseau vers un autre réseau de même type, mais il est possible d'avoir des ponts qui transforment la trame pour s'adapter au réseau raccordé. Par exemple, un réseau Ethernet peut être connecté à un réseau Token-Ring par un tel pont. Un pont est illustré à la figure 3.20.

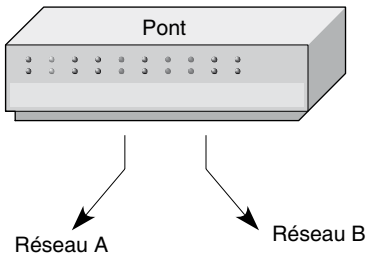


Figure 3.20
Pont

Le concentrateur

Un concentrateur permet, comme son nom l'indique, de concentrer le trafic provenant de différents équipements terminaux. Cela peut se réaliser par une concentration du câblage en un point donné ou par une concentration des données qui arrivent simultanément par plusieurs lignes de communication.

Dans le cadre des réseaux locaux, le terme concentrateur peut prendre l'une ou l'autre signification. Dans le cas de la concentration du câblage, les prises sur lesquelles sont

connectés les terminaux sont reliées au concentrateur par l'intermédiaire du câblage. Ce type de concentrateur est illustré à la figure 3.21.

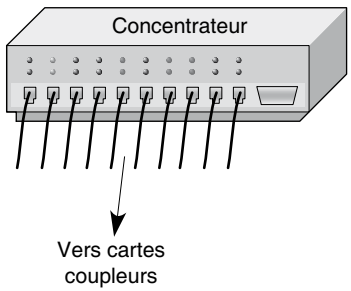


Figure 3.21
Concentrateur de câblage

Les différents concentrateurs d'un réseau peuvent posséder des caractéristiques complémentaires, comme celle de détenir des coupleurs d'accès vers d'autres réseaux de communication ou des couches de protocoles supplémentaires leur permettant de s'interconnecter avec diverses architectures. Ce rôle est souvent dévolu à un organe appelé hub, abordé à la section suivante.

Les concentrateurs peuvent être passifs ou actifs. Dans le premier cas, le signal n'est pas réamplifié, alors qu'il est régénéré dans le second cas.

Le hub

Dans un réseau Ethernet ayant une topologie en arbre, un hub est un concentrateur capable de récupérer le signal arrivant par une entrée et de le dupliquer vers l'ensemble des ports de sortie. Le signal est généralement réamplifié car les données sont enregistrées dans des mémoires de type registre à décalage. Dans ce cas, les hubs sont dits actifs, c'est-à-dire qu'ils possèdent des éléments qui doivent être alimentés électriquement.

La signification du mot hub a évolué ces dernières années pour définir un nœud central. Dans ce sens, les hubs permettent des interconnexions avec des réseaux externes. De même qu'en aéronautique, où les hubs sont les plaques tournantes par lesquelles transitent de nombreux avions, les hubs des réseaux sont des points de transit des paquets en route vers diverses destinations.

Un hub peut interconnecter des réseaux locaux Ethernet, Token-Ring, AppleTalk, etc., ainsi que des réseaux longue distance aux protocoles aussi divers que TCP/IP, ATM, etc.

Conclusion

Ce chapitre a introduit les médias physiques qui permettent de transporter les informations qui transitent sous forme numérique d'une machine terminale à une autre. Les équipements réseaux de base ont également été présentés.

Les progrès technologiques accomplis depuis les années 2000 ont été tels que le goulet d'étranglement n'est plus situé sur l'interface d'accès au médium de transport mais sur le réseau d'accès permettant de raccorder l'équipement terminal à la machine de connexion de l'opérateur. Les interfaces et les supports physiques ou hertziens utilisés sont devenus suffisamment équilibrés pour permettre à chaque client du réseau d'entrer dans l'ère du multimédia.

4

Les équipements réseau

Nous avons introduit aux chapitres précédents les architectures et les protocoles de réseaux. Cependant, nous n'avons pas encore décrit explicitement les équipements impliqués dans ces réseaux. Les termes « routeur », « commutateur » et « passerelle » ont souvent été cités, mais les matériels correspondants ont été décrits par leurs fonctionnalités, non par leur architecture interne.

Dans ce chapitre, nous entrons dans l'architecture interne des routeurs et des commutateurs et détaillons les caractéristiques de ces routeurs particuliers que sont les « gigarouteurs », ainsi que des diverses catégories de passerelles que sont les répéteurs, ponts, b-routeurs, contrôleurs, etc.

Les technologies de transfert doivent permettre de transférer une trame arrivant dans un nœud vers une ligne de sortie. Les techniques qui permettent ce transfert sont de deux types, le routage et la commutation.

La différence entre un routeur et un commutateur tient à ce qui est transporté dans le champ d'adressage : une adresse complète dans le premier cas ; une référence dans le second. La gestion des tables de routage est plus complexe que celle des tables de commutation.

Vocabulaire

Dans ce chapitre, nous utilisons le mot « trame » pour désigner l'entité qui doit être routée ou commutée d'une porte d'entrée vers une porte de sortie. Ce mot « trame » est en effet suffisamment large pour s'appliquer à l'ensemble des routeurs et des commutateurs. Il s'agit d'un équipement de niveau 3, dans lequel la trame est décapsulée. C'est le paquet — et non la trame — qui est ausculté pour déterminer la porte de sortie.

L'architecture interne des deux équipements est assez similaire. La différence essentielle entre eux tient à la façon de déterminer le nœud suivant à atteindre, c'est-à-dire la bonne porte de sortie du nœud.

Architecture des routeurs

Les routeurs sont des équipements réseau capables de router les blocs d'information qui leur arrivent. Ces blocs d'information peuvent être des paquets (pour ce qui concerne le niveau 3) ou des trames (pour le niveau 2). En réalité, il n'existe pas vraiment de routeurs de niveau 2. La seule technologie dans laquelle nous pourrions parler de routeur de niveau 2 est Ethernet. Si nous considérons l'adresse MAC Ethernet comme étant une adresse complète de niveau 2, un commutateur Ethernet devrait s'appeler un routeur Ethernet. En réalité, l'adresse MAC Ethernet est assimilée à une référence. Tous les nœuds d'un réseau Ethernet commuté doivent commuter sur cette référence, qui est égale à l'adresse MAC du destinataire.

Les routeurs les plus connus sont les routeurs IP, puisqu'un paquet IP possède l'adresse complète du destinataire du paquet. On a tendance à faire l'amalgame entre routeur et routeur IP. Cela n'est toutefois pas tout à fait exact, car dans la logique des réseaux un routeur pourrait très bien ne pas être un routeur IP. Par exemple, les routeurs IPX ont été très populaires avant l'arrivée massive d'IP.

L'architecture protocolaire d'un routeur est illustrée à la figure 4.1.

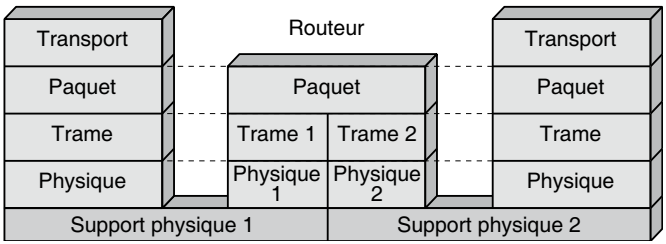


Figure 4.1

Architecture protocolaire d'un routeur

Les routeurs IP se différencient des commutateurs par le traitement de l'adresse du destinataire. Dans un routeur, le traitement s'exerce sur l'adresse complète et la consultation de la table de routage. Dans un commutateur, le traitement s'effectue sur la référence et utilise la table de commutation.

Dans les premiers routeurs, la recherche du port de sortie s'effectuait de façon logicielle, ce qui ralentissait énormément les transferts. La vitesse globale du routeur était en effet limitée par la puissance de traitement du protocole et des adresses. Pour un routeur logiciel, des ports atteignant un débit de 10 Mbit/s sont envisageables, mais il est très rare de disposer de ports à 100 Mbit/s, ou alors en très petit nombre. Les routeurs

matériels utilisent des ASIC (Application Specific Integrated Circuit), microprocesseurs à mémoires rapides, qui leur offrent un niveau de performance sans commune mesure avec celui des routeurs logiciels.

Un routeur est composé d'interfaces d'accès et de sortie, d'un ou plusieurs processeurs, de modules de mémoire et d'une unité d'interconnexion. Cette dernière fait souvent appel à une technologie de commutation que nous détaillons dans la suite du chapitre. Le paquet est d'abord traité par l'interface d'entrée, puis le processeur de traitement de la table de routage choisit l'interface de sortie, le paquet étant mémorisé dans un module mémoire. Le paquet est ensuite transféré vers l'interface de sortie par l'unité d'interconnexion. La figure 4.2 illustre l'architecture interne d'un routeur.

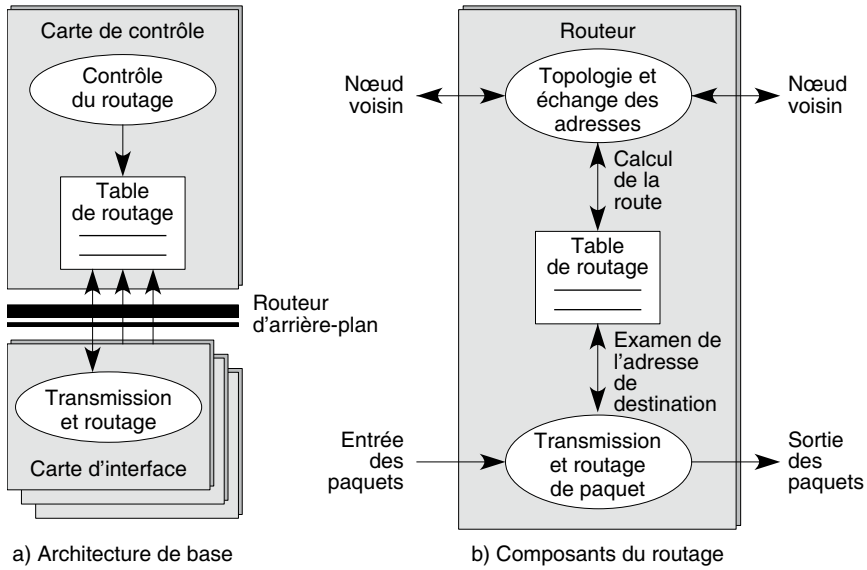


Figure 4.2

Architecture interne d'un routeur

La détermination du port de sortie incombe au processeur gérant la table, qui doit trouver la meilleure route pour aller vers l'adresse de destination du paquet. Dans un environnement IP, on utilise pour cela des protocoles de routage de type RIP (Routing Information Protocol) ou OSPF (Open Shortest Path First) (*voir le chapitre 16*). Cela suppose une connaissance de la topologie du réseau et éventuellement des défaillances des liaisons et des fortes congestions.

Pour router un paquet IP, il faut, dans l'ordre, valider le paquet et ses différents champs puis rechercher le port de sortie, qui peut être local, distant ou multicast. Dans ce dernier cas, il faut éventuellement, après traitement, dupliquer le paquet sur plusieurs ports de sortie. Il convient ensuite de contrôler le temps de vie du paquet (valeur du champ TTL, ou Time To Live). Il faut en outre, que ce soit ans IPv4 ou IPv6, recalculer la zone de

détection d'erreur. Éventuellement, il faut fragmenter ou réassembler les paquets pour les rendre compatibles avec les paquets ou les trames de la ligne de sortie.

Pour accélérer la vitesse de traitement, il est possible d'utiliser un cache de routage, comme illustré à la figure 4.3.

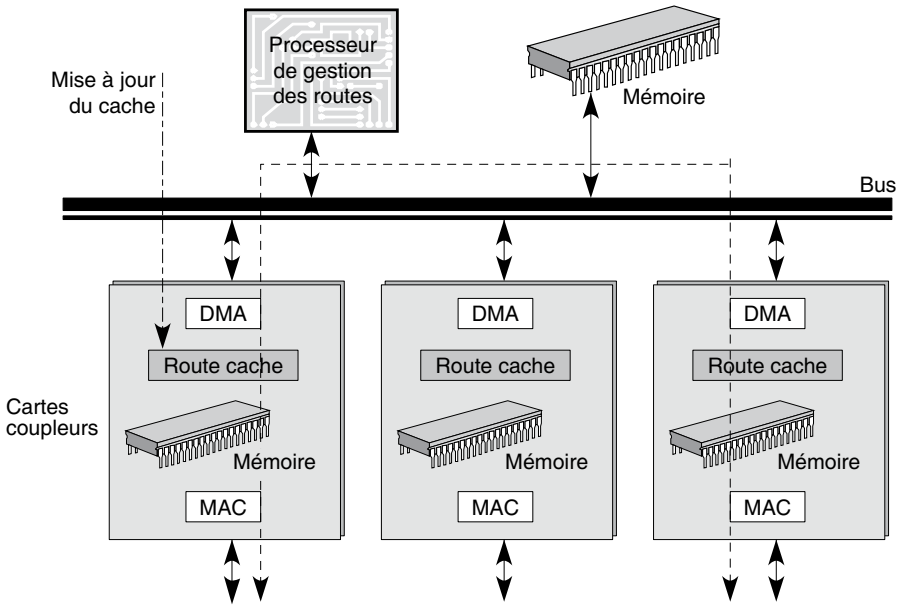


Figure 4.3

Routeurs avec cache mémoire de traitement de l'adresse

Architecture des commutateurs

Les architectures des commutateurs sont assez semblables dans la plupart des technologies de commutation telles que ATM ou Ethernet commuté ainsi que dans le cœur de commutation des routeurs, c'est-à-dire dans l'élément central du routeur permettant le transfert d'un paquet d'une interface d'entrée vers une interface de sortie une fois le nœud suivant choisi. Comme la plupart des commutateurs sont de niveau 2, on parler de commutateur de trames, même s'il s'agit de façon sous-jacente de commutateur de paquets.

De nombreuses catégories d'architectures de commutateurs ont été proposées, et des types très variés de circuits VLSI (Very Large Scale Integration), les fameuses puces de silicium, ont été développés dans les laboratoires de recherche et chez les industriels. Les diverses publications issues de ces travaux distinguent trois types principaux d'architecture, comme nous l'avons vu au chapitre 2 : à mémoire partagée (*shared-memory*), à support partagé (*shared-medium*) et à division spatiale (*space-division*).

Étant donné les vitesses élevées des lignes de transmission modernes, les commutateurs doivent pouvoir transférer les trames à des débits extrêmement rapides, de l'ordre de cent mille à un million de trames par seconde et par ligne d'entrée. La réalisation de tels commutateurs demande des composants à haute performance.

Les commutateurs doivent être capables de supporter des trafics tant homogènes que sporadiques. Par ailleurs, la qualité de service fournie par le réseau étant affectée par le délai de transfert de bout en bout et la probabilité de perte de trames, une différenciation des services est nécessaire. Les objectifs et critères de performance de cette différenciation peuvent toutefois être opposés, tels que la perte d'aucune trame, mais avec un temps de latence important, ou au contraire la perte de trame, mais avec un temps de traversée réduit. Un service de commutation avec priorité est donc essentiel pour que les différentes classes de services puissent coexister à l'intérieur d'un même commutateur.

Rôle et fonctionnalités des commutateurs

Un commutateur est un composant avec *n* entrées et *n* sorties qui achemine les paquets arrivant sur les entrées vers leur destination de sortie.

Le rôle d'un commutateur consiste à assurer les trois fonctions essentielles suivantes :

- analyse de l'en-tête de la trame et sa traduction ;
- commutation spatiale, ou routage ;
- multiplexage des trames sur la sortie requise.

Les données des utilisateurs sont transportées dans le champ de données des trames et transférées de manière asynchrone. Du fait de son comportement statistique et parce qu'un nombre important de flots peuvent partager la même liaison, le commutateur doit se synchroniser sur les instants d'entrée des trames dans le nœud. Le commutateur examine l'en-tête de chaque trame pour identifier la porte de sortie de la trame. Cette identification s'effectue soit par l'intermédiaire de la référence qui détermine le chemin, soit par l'adresse complète du destinataire dans le cas d'un routage. Il convertit la zone de supervision en un nouvel en-tête pour le nœud de commutation suivant, gère le routage et envoie des informations de contrôle et de gestion dans les réseaux associés.

Dans un commutateur ATM, la commutation s'effectue à partir du VCI (Virtual Channel Identifier) ou du VPI (Virtual Path Identifier) contenus dans l'en-tête de la cellule. Des mécanismes de contrôle de collision permettent aux trames provenant de différentes entrées d'accéder à la file d'attente d'un même multiplex, qui n'est autre qu'une voie de communication prenant en charge plusieurs flux simultanément. Les trames sont commutées individuellement, l'horloge interne du commutateur travaillant à un rythme correspondant au temps de transmission d'une trame ATM. Par exemple, si la ligne de communication la plus rapide a un débit de 10 Gbit/s, la durée de la transmission d'une trame ATM est de 42,4 ns. Dans ce cas, le commutateur est rythmé à la cadence d'une décision toutes les 42,4 ns.

Les commutateurs Ethernet ont a prendre en charge des trames un peu plus longues, de 64 octets à 1 500 octets. Le temps de traitement étant identique que la trame soit courte

ou longue, on comptabilise la performance d'un commutateur par le nombre de trames émises par seconde. Bien sûr, il faut tenir compte de la longueur moyenne des trames pour déterminer la vitesse des lignes de sortie.

La réalisation d'un commutateur peut s'effectuer de diverses façons. Dans tous les cas, il faut créer une fonction de stockage, qui peut se trouver à l'entrée, à la sortie ou le long de la chaîne de commutation. À l'intérieur du commutateur, diverses techniques de routage peuvent être mises en œuvre : circuit virtuel, autoroutage ou datagramme. Deux des principales fonctions assurées par le commutateur correspondent au routage et à la mémorisation des trames. Des fonctions optionnelles, telles que le recouvrement d'erreur ou le contrôle de flux, peuvent être éventuellement implémentées dans les commutateurs.

Un commutateur doit satisfaire à de nombreuses contraintes, notamment les suivantes :

- très haut débit ;
- faible délai de commutation ;
- très faible taux de perte de trames ;
- gestion des applications multicast (communication multipoint) ;
- modularité et extensibilité ;
- faible coût d'implémentation.

De plus, un commutateur moderne doit être pourvu de fonctions de distribution et de gestion des priorités.

Les catégories de commutateurs

De nombreux auteurs ont tenté de mettre un peu d'ordre dans la prolifération des propositions de structure des commutateurs. Nous adoptons dans ce livre une classification qui recouvre les architectures de la quasi-totalité des commutateurs et repose sur cinq critères d'architecture :

- architecture interne en fonction du nombre d'étapes élémentaires ;
- type de liaison à l'intérieur du commutateur ;
- technique de commutation interne ;
- contrôle interne du commutateur ;
- position des mémoires et blocages internes.

Les architectures internes se différencient par le nombre d'étapes à traverser. Une étape peut être considérée comme un bloc monolithique traversé en une seule tranche de temps. Plus le nombre d'étapes est faible, plus le temps de réponse est court.

La liaison à l'intérieur du commutateur peut être dédiée ou statistique. Pour les liaisons dédiées, les trames vont d'une porte d'entrée vers une porte de sortie en transitant toujours par le même chemin. Dans le cas statistique, toute trame est apte à emprunter une liaison quelconque à l'intérieur du commutateur. Le routage est déterminé par un algorithme de contrôle.

Le tableau 4.1 récapitule ces cinq catégories de commutateurs et leurs propriétés.

Architecture interne	Liaison interne	Commutation interne	Contrôle du commutateur	Mémoire et blocage
Nombre d'étapes à parcourir	Liaison dédiée Liaison statistique	Répartition dans l'espace Répartition dans le temps	Algorithme de gestion des ressources ; routage, contrôle de flux	Position des mémoires dans le commutateur Possibilité de blocage interne

TABLEAU 4.1 • Critères de classification des commutateurs

Les techniques de commutation interne peuvent se classer en deux grandes catégories : par répartition dans l'espace et par répartition dans le temps. Dans le premier cas, plusieurs chemins parallèles peuvent être mis en place pour véhiculer les trames, tandis que, dans le second, les trames se partagent les ressources dans le temps. Pour simplifier la présentation, nous supposerons qu'avec la répartition dans le temps, toutes les trames transitent par une même liaison interne, liaison nécessairement statistique. Dans la réalité, il peut y avoir superposition des deux techniques de commutation : plusieurs liaisons sont possibles, et, sur ces liaisons, il peut y avoir un multiplexage temporel.

Les algorithmes de gestion des ressources permettent le contrôle du commutateur. Ces algorithmes concernent, entre autres, le routage des trames et les contrôles de flux et de congestion.

Blocage et mémorisation

À l'intérieur du commutateur, il peut être nécessaire de mémoriser des trames lorsqu'un phénomène de blocage se produit, c'est-à-dire quand deux trames entrent en compétition pour obtenir une même ressource. Il faut alors mettre une trame en attente. Les mémoires peuvent se situer à l'entrée, à la sortie ou en différents points à l'intérieur du commutateur.

Les différents types de blocages

Comme nous venons de le voir, il existe des commutateurs avec blocage et d'autres sans blocage. On distingue trois types de blocages, le blocage interne, le blocage en sortie et le blocage en tête de file :

- Blocage interne. Ce blocage survient lorsque plusieurs trames veulent accéder à la même liaison interne. Des conditions de non-blocage ont été spécifiées pour un réseau Banyan (*voir plus loin dans ce chapitre*). Un réseau Banyan est non bloquant si les entrées actives x1, x2,... xk et leurs sorties respectives y1, y2,... yk satisfont les relations suivantes :
  - Les sorties sont monotones, c'est-à-dire que $y_1 < y_2 < ... < y_k$ ou $y_1 > y_2 > ... > y_k$.
  - Les entrées sont concentrées, c'est-à-dire que toute entrée comprise entre deux entrées actives est active.
- Blocage en sortie. Comme il n'y a pas de coordination entre les trames qui arrivent en fonction de leur destination, les trames qui parviennent dans la même tranche de temps peuvent être destinées à une même sortie et donc aboutir à un conflit en sortie.

- Blocage en tête de file, ou HOL (Head Of Line). Ce blocage intervient dans les files d'entrée du commutateur. Considérons deux files d'entrée avec des trames en tête de file entrant en conflit pour une même sortie. Une de ces trames est acceptée pour le routage interne vers la sortie, tandis que les autres sont bloquées. Cette technique impose la contrainte suivante : les trames situées dans la file d'attente derrière les trames bloquées ne peuvent être transmises vers leur sortie, même si elles sont destinées à des sorties non conflictuelles.

Placement des mémoires

Le placement des mémoires tampons, ou buffers, pour stocker les trames et les moyens permettant de résoudre les contentions en sortie affecte à la fois les performances et la complexité des commutateurs.

La figure 4.4 illustre les différents placements de mémoires envisageables.

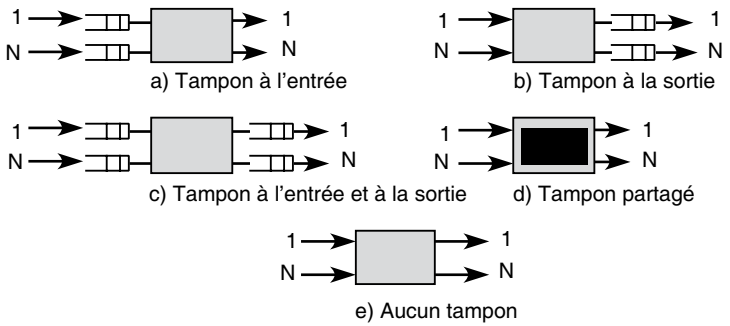


Figure 4.4

Placement des mémoires tampons dans les commutateurs

Les architectures avec mémoire tampon à l'entrée permettent à toute nouvelle arrivée d'être placée dans ces mémoires, résolvant de ce fait les problèmes de contention. Les trames en tête de chaque file essaient d'accéder aux liaisons de sortie. Les trames sélectionnées sont délivrées aux ports de sortie, tandis que les autres restent en tête de file pour un nouveau tour d'arbitrage. Le problème majeur de cette architecture est le blocage en position de tête, qui limite le débit.

Les architectures utilisant une file partagée ne rencontrent pas ce type de blocage. Les trames qui se présentent en entrée sont directement transmises au commutateur, et la résolution de contention pour le port de sortie a lieu avant le transport de la trame. Les trames bloquées restent dans le commutateur et sont recyclées vers leur port, où elles sont resynchronées avec l'ensemble des nouvelles arrivées.

Concernant le taux de perte de trames, les commutateurs à mémoire partagée présentent les meilleures performances. En effet, chaque adresse de la mémoire partagée peut être allouée temporairement à n'importe quel port de sortie, et non à un port de sortie particulier. De la sorte, la limite maximale de longueur de chaque file, et notamment des files de sortie, peut être étendue jusqu'au débordement de la mémoire partagée, réduisant de ce fait le taux de perte des trames.

Les architectures avec mémoires tampons en sortie utilisent des chemins parallèles pour accéder aux ports de sortie. Cela autorise la délivrance de multiples trames simultanément pour chaque destination. Les mémoires tampons situées à chaque port de sortie stockent les trames en attendant l'accès aux liaisons de transmission.

Exemples de commutateurs

Les sections qui suivent présentent les commutateurs les plus connus en fonction des critères que nous avons introduits à la section précédente.

Le commutateur Crossbar

L'un des commutateurs les plus simples se construit en reprenant les concepts des premiers autocommutateurs Crossbar téléphoniques, qui remontent à plusieurs dizaines d'années. Les commutateurs Crossbar électroniques, et non plus mécaniques, font toujours partie, au début des années 2010, des petits commutateurs les plus vendus.

La figure 4.5 illustre le fonctionnement de trois types de commutateurs Crossbar.

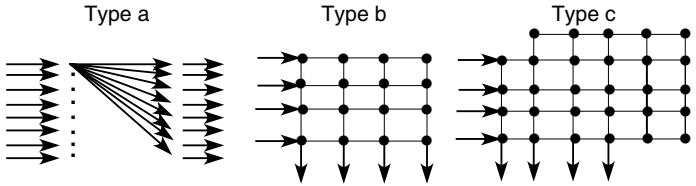


Figure 4.5

Commutateurs Crossbar

Sur la figure, les flots qui entrent dans les commutateurs Crossbar sont représentés par les flèches de gauche et ceux qui sortent par les flèches de droite pour le type a et par les flèches du bas pour les types b et c. Le rôle de ces commutateurs est d'acheminer des flots de trames arrivant sur l'une des entrées vers une des sorties. Dans les types b et c, les points noirs représentent des commutateurs élémentaires permettant à une trame de se diriger vers trois sorties au choix, une sortie vers le haut, une sortie droit devant et une sortie vers le bas. Arrivé aux bords du commutateur, il ne peut y avoir que deux sorties au choix, voire une seule.

Le commutateur Crossbar illustré à la partie gauche de la figure (type a) permet, à partir de toute entrée, d'aller directement à toute sortie. De mécaniques au début du siècle, les relais sont devenus électroniques à partir des années 1980. Le commutateur Crossbar de base de type a ne comporte qu'une étape : une trame entrant dans le Crossbar va directement à la ligne de sortie. Entre la porte d'entrée et la porte de sortie, la liaison est dédiée ; la commutation est répartie dans l'espace, et le routage est fixe. Si deux trames se dirigent en parallèle vers une même porte de sortie, des mémoires sont nécessaires soit à la porte d'entrée, soit à la porte de sortie. De ce fait, il n'y a pas de blocage interne au commutateur.

Il existe des commutateurs Crossbar beaucoup plus complexes, dont l'architecture est profondément modifiée. Par exemple, la partie centrale de la figure 4.5 (type b) décrit un commutateur qui permet de mettre en place une ou plusieurs voies entre l'entrée et la sortie. Dans ce cas, il faut n^2 points de connexion pour n entrées et n sorties du commutateur. Un seul chemin peut être envisagé entre une entrée et une sortie. Plusieurs chemins distincts sont disponibles grâce aux commutateurs élémentaires. Ces commutateurs n'empêchent pas les collisions potentielles entre les trames sur les chemins internes. Il faut donc stocker les trames dans des mémoires en entrée et mettre en place un mécanisme écoulant un maximum de trames en parallèle. Une autre possibilité consiste à placer des mémoires à chaque point de jonction, ce qui augmente d'autant le nombre d'étapes à franchir en interne.

En se servant des cinq critères que nous avons introduits précédemment dans ce chapitre, un commutateur Crossbar avec mémoires se définit par un nombre d'étapes dépendant de la route et des ports d'entrée et de sortie, des liaisons statistiques, une commutation dans l'espace, un routage dynamique et des mémoires intermédiaires nécessaires pour éviter les blocages internes.

On peut modifier le commutateur en agrandissant le nombre de commutateurs élémentaires afin de permettre un plus grand nombre de parcours et d'éviter les collisions. À chaque collision potentielle, la trame est détournée de son chemin direct et doit, soit tourner à gauche, soit aller tout droit. En faisant tourner la trame trois fois à gauche, on finit par retrouver le chemin de départ. On peut se représenter le commutateur comme modélisant les rues de Manhattan, à New York, et la trame comme étant une voiture. Dans Manhattan, pour simplifier la circulation, il est interdit de tourner sur sa gauche, de façon à ne pas couper les flux de circulation. Pour prendre une direction à gauche dans un carrefour, il faut aller tout droit et tourner trois fois à droite. Les commutateurs que nous examinons s'appellent des commutateurs Manhattan pour rappeler cette analogie et la possibilité pour une trame de prendre des chemins détournés pour arriver à la sortie choisie. Un commutateur Manhattan est illustré à la partie droite de la figure 4.5 (type c).

Les caractéristiques comparées des trois architectures Crossbar sont indiquées au tableau 4.2.

	Architecture interne	Liaison interne	Commutation interne	Contrôle du commutateur	Mémoire et blocage
Crossbar (fig 26.5.a)	1 étape	Liaison dédiée	Répartition dans l'espace	Routage fixe	Pas de blocage interne
Crossbar (fig 26.5.b)	*n* étapes	Liaisons statistiques	Répartition dans l'espace	Routage dynamique	Blocage interne résolu par des mémoires
Crossbar (fig 26.5.c)	*n* étapes	Liaisons statistiques	Répartition dans l'espace	Routage spécifique	Blocage interne résolu par le routage

TABLEAU 4.2 • Caractéristiques des commutateurs Crossbar

Le commutateur Banyan et ses extensions

Le commutateur de base qui semble rassembler le plus de suffrages est le commutateur Banyan, illustré à la figure 4.6. Ce commutateur 8x8 possède huit files d'entrée et huit files de sortie. Sur la figure, les trames à commuter se présentent sur la gauche et doivent ressortir sur l'une des huit files de sortie indiquées sur la droite de la figure.

Ce commutateur est construit avec douze commutateurs élémentaires, un commutateur élémentaire étant ici un commutateur possédant deux entrées et deux sorties, ce que l'on appelle encore un commutateur 2x2. Ce commutateur comporte trois étages, un étage étant représenté par la traversée d'un commutateur élémentaire 2x2. En d'autres termes, la trame qui se présente sur l'une des huit entrées doit traverser trois commutateurs élémentaires pour atteindre une sortie.

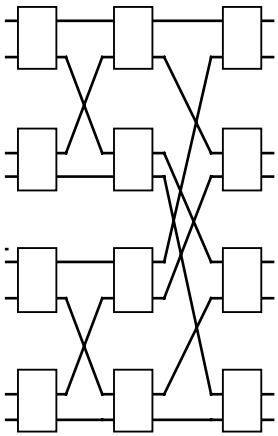


Figure 4.6

Commutateur Banyan

La figure 4.7 illustre la construction d'un commutateur Banyan. À partir des deux premières entrées, celles du haut à gauche, on accède aux huit sorties en utilisant des commutateurs élémentaires à deux entrées et deux sorties. On obtient à l'étape a de la figure 4.7 un commutateur 2x8, qui possède deux entrées et huit sorties. À l'étape b, on ajoute deux nouvelles entrées et un commutateur élémentaire, qui prend en charge ces deux nouvelles entrées. On relie ce commutateur élémentaire aux entrées libres des commutateurs élémentaires du deuxième étage de l'étape a, ce qui permet de construire un commutateur 4x8. L'étape c permet de passer à un commutateur 6x8 et l'étape d à un commutateur Banyan 8x8 complet.

Avec un étage de commutateurs élémentaires, on accède à 2 sorties depuis 2 entrées. Avec deux étages, on accède à 4 sorties depuis 4 entrées, et, plus généralement, avec n étages, on accède à 2^n sorties depuis 2^n entrées, ce qui constitue un avantage par rapport au Crossbar, le nombre de commutateurs élémentaires utilisés pour réaliser le commutateur global étant beaucoup plus petit.

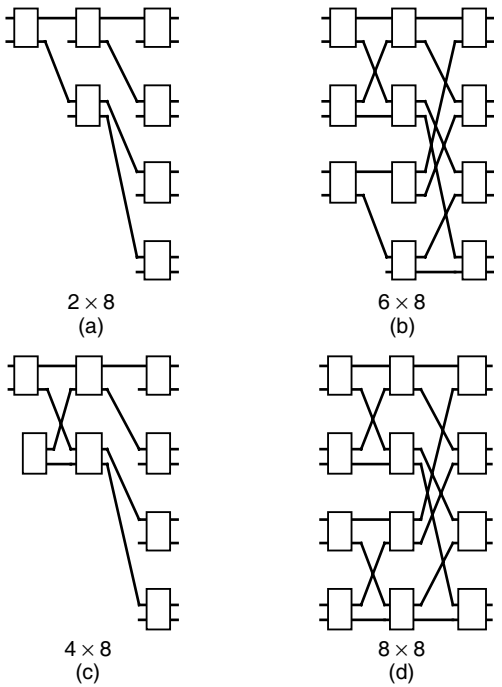


Figure 4.7
Étapes de construction d'un commutateur Banyan

Deux types de collisions entre trames peuvent se produire :

- Deux trames qui convergent vers la même sortie.
- Deux trames qui empruntent la même voie à l'intérieur d'un commutateur élémentaire.

Comme à chaque couple entrée-sortie ne correspond qu'un seul chemin, il n'est pas possible d'éviter la collision en changeant de chemin. De nouveau, pour éviter ces deux types de collisions, on peut ajouter des mémoires à l'entrée, à la sortie ou dans tous les commutateurs élémentaires intermédiaires.

Les passerelles

On ne peut plus concevoir un réseau sans un passage vers l'extérieur. Il faut interconnecter les réseaux pour qu'ils puissent s'échanger des informations. Le nœud qui joue le rôle d'intermédiaire s'appelle une passerelle, ou *gateway* (terme générique). Ce nœud intermédiaire peut être plus ou moins complexe, suivant la ressemblance ou la dissemblance des deux réseaux à interconnecter. Si les deux réseaux sont identiques, la passerelle est extrêmement simple. À l'inverse, si les deux architectures à interconnecter sont dissemblables, les moyens à mettre en œuvre deviennent vite lourds et complexes.

Pour contrecarrer le développement un peu anarchique et la prolifération des solutions réseau côté constructeur, le modèle de référence a eu pour objectif la standardisation des architectures réseau. L'objectif visé était d'éviter de passer d'une architecture à une autre par le biais de passerelles, toujours coûteuses et complexes à mettre en œuvre.

Les interfaces IP ont résolu en grande partie le problème de l'hétérogénéité des infrastructures réseau. Cependant, les solutions pour transporter un paquet IP restent très diverses, que ce soit à l'intérieur d'une entreprise ou dans un réseau d'opérateur. De plus, l'interconnexion doit également se faire dans les niveaux hauts de l'architecture.

Cela explique pourquoi l'interconnexion de technologies différentes rend nécessaire le recours à des passerelles permettant de relier différentes catégories de réseaux. Avec la multiplication des réseaux, Internet, mobiles, sans fil, etc., à laquelle on assiste depuis quelques années, ces passerelles sont devenues indispensables, tant pour les constructeurs que pour les utilisateurs.

De plus, les équipements intermédiaires que l'on rencontre le long d'un chemin pour résoudre des problèmes spécifiques sont également en plein développement, comme les pare-feu et les appliances en tout genre permettant d'assurer le contrôle du trafic ou la répartition de charge.

La convergence fixe/mobile est une autre raison importante de la multiplication des passerelles, même si les systèmes que l'on met en place depuis plusieurs années permettent souvent d'exécuter les mêmes applications sur un terminal mobile et sur un terminal fixe. C'est en particulier l'objectif de l'IMS (IP Multimedia Subsystem). Les nouveaux réseaux sans fil demandent de surcroît des machines intermédiaires pour gérer les cellules, à l'image des contrôleurs, que nous détaillons plus loin dans ce chapitre.

Si l'on s'en tient strictement à la définition d'une passerelle, on peut réaliser une interconnexion de réseaux à n'importe quel niveau de l'architecture du modèle de référence. Cependant, la règle générale est la suivante : l'utilisation d'une passerelle de niveau N est nécessaire lorsque les couches inférieures à N sont différentes mais que toutes les couches, à partir de la couche $N + 1$, sont identiques.

Les trois catégories de passerelles les plus répandues sont les ponts, les routeurs et les relais. On distingue également les ponts-routeurs (*bridge-routers*), qui, bien que non normalisés, sont largement utilisés.

Une hiérarchie de noms a été définie pour prendre en compte le niveau de l'interconnexion en se référant au modèle de référence. Ces différents niveaux sont illustrés à la figure 4.8.

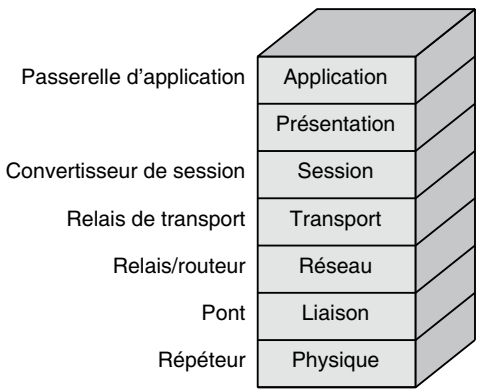


Figure 4.8
Hiérarchie des passerelles

Un répéteur est une passerelle de niveau 1, ou physique ; un pont est une passerelle de niveau 2, ou trame ; un relais est une passerelle de niveau 3, ou paquet ; un relais de transport est une passerelle de niveau 4, ou message, etc.

Les termes « commutateur » et « routeur » ne sont pas liés à un niveau. Un commutateur est un organe de type pont lorsque la commutation est effectuée au niveau 2 et de type relais lorsqu'elle est effectuée au niveau 3. Par exemple, un commutateur Ethernet est de type pont tandis qu'un commutateur X.25 est de type relais. De même, un routeur est de type pont lorsque le routage est effectué au niveau 2 et de type relais lorsque le routage est effectué au niveau 3. Le terme « routeur » a été tellement associé au routage IP de niveau 3 qu'il semble naturel de l'utiliser pour indiquer un relais de niveau paquet. Ce n'est toutefois exact que pour le monde IP, qui représente tout de même quasiment 99 % des relais de niveau 3.

Les répéteurs

Un répéteur est une passerelle de niveau physique entre deux réseaux comportant un niveau trame commun. Par exemple, un répéteur Ethernet est un équipement qui répète automatiquement les trames d'un brin Ethernet vers un autre brin Ethernet.

Le rôle du répéteur est d'envoyer une trame plus loin que ne le permet un simple câble, dont la longueur est limitée par l'atténuation du signal. Dans le cas de l'Ethernet à 10 Mbit/s, un câble coaxial blindé ne peut dépasser une longueur de 500 m sous peine de voir le taux d'erreur devenir inacceptable.

Regardons plus précisément le cas du réseau Ethernet. Nous savons que la couverture maximale d'un réseau Ethernet à 10 Mbit/s est limitée à 2,5 km, puisque le temps de propagation d'une extrémité à l'autre du support physique ne peut dépasser 51,2 µs. La question est de savoir comment atteindre ces 2,5 km si la longueur maximale d'un brin ne peut excéder 500 m. La réponse est simple : il suffit de connecter des brins les uns aux autres en utilisant des répéteurs.

Les répéteurs n'empêchent pas les collisions, mais rendent difficile leur répétition sur le brin suivant. En effet, un répéteur n'est pas autre chose qu'un registre à décalage, c'est-à-dire un ensemble de registres dans lesquels les informations sous forme de 0 et de 1 viennent se mémoriser et se décalent pour laisser entrer un nouvel élément binaire. Le registre d'entrée s'attend à recevoir un 0 ou un 1 et non un signal provenant d'une superposition. Il est donc très difficile de répéter des signaux qui ne sont ni des 0 ni des 1. C'est la raison pour laquelle les répéteurs remplacent les éléments en collision par une série de bits spécifiques permettant aux autres stations de détecter la collision.

Les répéteurs peuvent éventuellement changer de support physique tout en respectant la structure de la trame en cours d'acheminement. Par exemple, on peut passer d'un support métallique à une fibre optique ou à un support hertzien d'un réseau sans fil. C'est la raison pour laquelle il est possible de réaliser des réseaux Ethernet ayant des parties métalliques, optiques et hertziennes.

En résumé, un répéteur est un organe inintelligent qui permet d'allonger la longueur du support physique, au contraire d'un pont, qui filtre les messages sur leur adresse de destination.

Les ponts

Le pont, ou *bridge*, est une passerelle de niveau 2. Cet équipement de réseau assez simple à mettre en œuvre a beaucoup évolué depuis l'apparition des premiers réseaux Ethernet.

Un pont unit des réseaux proches ou distants en remontant jusqu'au niveau trame. Il reçoit une trame et calcule la ligne de sortie grâce à un algorithme de routage ou à la table de commutation. Il filtre les trames reçues en examinant l'adresse de niveau 2 et en ne laissant passer que les trames destinées à l'extérieur.

L'architecture d'un pont est illustrée à la figure 4.9. Le pont crée un réseau virtuel à partir d'un ensemble de sous-réseaux, en ignorant les protocoles des couches supérieures. La couche 2 est en fait divisée en deux sous-couches : la couche MAC (Medium Access Control) et la couche LLC (Logical Link Control). Le pont peut accepter des contrôles d'accès différents, mais doit avoir le même protocole de liaison.

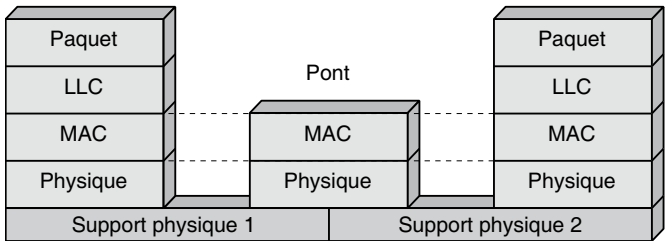


Figure 4.9

Architecture d'un pont

Le pont enregistre dans des tables internes les adresses de toutes les stations connectées au réseau. Si une station est ajoutée ou enlevée, le système doit être reconfiguré. C'est la raison pour laquelle les ponts ne peuvent *a priori* être utilisés que dans des environnements bien localisés. Dès que le nombre de stations est important, la gestion des adresses devient très complexe.

L'interconnexion de sous-réseaux par des ponts autorise des débits élevés, puisque le nombre de niveaux à traverser est petit et qu'on ne remonte que d'un niveau pour arriver au niveau trame. Les passerelles de niveau paquet, ou relais, sont moins puissantes puisque, à chaque passage d'un relais, il faut traverser les niveaux 1 puis 2 pour arriver au niveau 3.

Deux grands protocoles de routage de niveau pont, le Spanning-Tree et le Source-Routing, ont été développés respectivement pour les réseaux Ethernet et Token-Ring. Comme la solution Token-Ring a quasiment disparu, il ne reste dans les faits pratiquement plus que le Spanning-Tree. Cependant, le Source-Routing étant utilisé dans d'autres circonstances, nous allons également le décrire brièvement dans la suite.

Le protocole Spanning-Tree

Normalisé en 1990 par le comité IEEE 802.1, dans le groupe de travail IEEE 802.1D, le protocole STP (Spanning-Tree Protocol) est prévu pour l'interconnexion de tout type de réseau. Il consiste en la constitution, à partir de n'importe quelle topologie, d'un arbre qui recouvre parfaitement le réseau et dans lequel, à partir de n'importe quelle feuille de l'arbre, tout point du réseau est accessible.

Pour le bon fonctionnement du protocole, le réseau doit satisfaire aux conditions suivantes :

- Une identification unique (ID) doit être associée à chaque pont du réseau.
- Le pont ayant le plus petit ID doit être choisi comme racine de l'arbre.

Les ponts échangent des messages appelés « Hello », dans lesquels ils indiquent leur ID ainsi que l'ID du pont qu'ils considèrent comme la racine de l'arbre par lequel doivent transiter leurs trames. Lorsqu'ils reçoivent une ID inférieure à celle désignée comme leur pont racine, ils rectifient l'ID du pont qui leur sert de racine pour prendre la nouvelle valeur. En d'autres termes, ils déterminent un nouveau pont racine. Avec le temps, chaque pont finit par déterminer la racine de l'arbre, c'est-à-dire le pont racine. Ensuite, chaque pont calcule la distance qui le sépare de la racine. Cette distance est calculée de proche en proche : à chaque pont traversé les distances sont incrémentées de 1.

Sur chaque réseau physique, un pont est choisi comme étant le plus proche de la racine. Si deux ponts d'un même réseau sont à la même distance de la racine, la plus petite ID est choisie. Tout le trafic issu de ce réseau et à destination d'un autre réseau physique passe par ce pont, appelé pont élu. Grâce à ce protocole, tout réseau physique est assimilable à un arbre virtuel, et il n'existe pas de boucle dans le réseau.

On peut reprocher à ce protocole des performances éventuellement dépendantes de la topologie du réseau. De plus, si les ID des ponts ne sont pas définies par le gestionnaire du réseau mais par le constructeur, le pont élu comme racine est indépendant de la volonté du gestionnaire et peut constituer un goulet d'étranglement.

L'algorithme du Spanning-Tree possède des variantes dont la plus intéressante est le RSTP (Rapid Spanning-Tree Protocol), normalisé en 1998 par le groupe IEEE 802.1w. Cet algorithme permet de ramener la convergence du protocole de 30 secondes en moyenne à 6 secondes en moyenne.

Le protocole Source-Routing

Normalisé par le comité IEEE 802.5, le protocole Source-Routing a été utilisé au départ pour l'interconnexion de réseaux Token-Ring. Ce protocole est toujours fortement utilisé dans d'autres contextes, aussi bien issus des réseaux IP que des réseaux locaux. Un exemple important que nous verrons au chapitre 23 provient de protocoles normalisés pour les réseaux ad-hoc.

Lorsqu'une station X veut envoyer des informations à une station Y, elle envoie en diffusion une trame de découverte du chemin. Un pont qui voit arriver une trame de ce type

y ajoute sa propre adresse et retransmet cette trame vers tous les réseaux, à l'exception de celui par lequel la trame est arrivée. La station destination Y voit donc arriver une ou plusieurs trames et retourne à X toutes les trames reçues en utilisant les informations d'acheminement trouvées dans chacune. Ensuite, X peut utiliser les routes que le protocole lui a permis de découvrir. Son choix est guidé par divers paramètres, tels que délais d'acheminement, nombre de ponts traversés, longueur de trame permise, etc.

Les trames constituées par chaque station présentent la structure suivante : elles commencent par l'adresse de destination, suivie de l'adresse source, des informations de routage, de l'adresse DSAP (Destination Service Access Point), de l'adresse SSAP (Source Service Access Point), des données de contrôle et enfin des données à transporter, pour se terminer par une zone FCS (Frame Check Sequence). Cette suite s'exprime par la séquence :

@Dest.~@Source~Info-routage~DSAP~SSAP~Contrôle~Données~FCS.

La longueur des adresses destination et source est de 2 ou 6 octets, et celle de chaque élément de l'information de routage de 2 octets.

Les relais-routeurs

Comme nous l'avons vu au début de ce chapitre, « relais » est le terme normalisé pour indiquer une passerelle de niveau 3, ou paquet. Comme le monde IP a maintenant quasiment l'exclusivité du niveau 3, la tendance est d'utiliser le terme « routeur » pour exprimer un relais de niveau paquet IP. Malheureusement, ce terme peut prêter à confusion lorsqu'on parle d'un routeur de niveau trame. Le concept de routeur n'est pas lié à un niveau mais à une technologie. Parler de routeur, c'est donc le plus souvent parler de routeur IP, et c'est ce que nous allons faire dans ce chapitre. Cependant, il faut se rappeler qu'un routeur de niveau 2 est imaginable, même si ce n'est pas un cas classique, si les trames contiennent l'adresse complète du destinataire.

Les routeurs multiprotocoles

Les routeurs multiprotocoles se distinguent par l'éventail de protocoles réseau gérés ainsi que par le nombre et le type des interfaces réseau supportées. Ces produits sont relativement complexes, ce qui explique qu'un faible nombre de sociétés se soit spécialisé dans ces routeurs.

Un routeur multiprotocole possède plusieurs interfaces de niveau trame et plusieurs protocoles de niveau paquet. Lorsque la trame se présente dans le routeur, elle est décapsulée de façon que le paquet soit récupéré. Après examen de la zone d'adresse du paquet, celui-ci peut être transcodé dans le format paquet d'un autre protocole avant d'être encapsulé dans une nouvelle structure de trame.

Les routeurs multiprotocoles peuvent supporter un pont-routeur, ou *bridge-router* (*voir plus loin*). Le nœud peut dans ce cas reconnaître la référence ou l'adresse de niveau trame et router ou commuter la trame sans remonter au niveau paquet. Si la référence ou l'adresse de niveau trame n'est pas reconnue, on passe au niveau paquet pour router le paquet sur l'adresse de niveau 3.

À la différence d'un pont, un routeur peut isoler certains segments du réseau et créer des domaines. Il permet d'offrir une bonne isolation entre chaque réseau connecté, évitant ainsi la propagation des signaux émis en broadcast. Actuellement, les vitesses atteintes par les routeurs d'entreprise sont de 10 000 à 15 000 paquets/s et avoisinent souvent les 100 000 paquets/s. Du fait de l'augmentation constante des débits des applications, il a fallu, à la fin des années 1990, se pencher sur la conception de routeurs beaucoup plus puissants, en particulier pour les opérateurs, capables de router d'un à mille millions de paquets par seconde. Nous les détaillons à la section suivante.

Les gigarouteurs

La génération de routeurs haut débit, appelés gigarouteurs ou térarouteurs, repose sur une distribution de la table de routage et du traitement du paquet dans l'interface d'accès puis sur l'utilisation d'un commutateur pour transporter le paquet d'un port d'entrée vers un port de sortie.

La figure 4.10 donne une idée de l'architecture d'un gigarouteur. Les gigarouteurs permettent aux ports d'accès d'atteindre des vitesses de 10 et de 100 Gbit/s. La transmission de paquets IP à ces vitesses est exploitée aujourd'hui par les techniques IP sur SONET (Synchronous Optical Network) et MPLS.

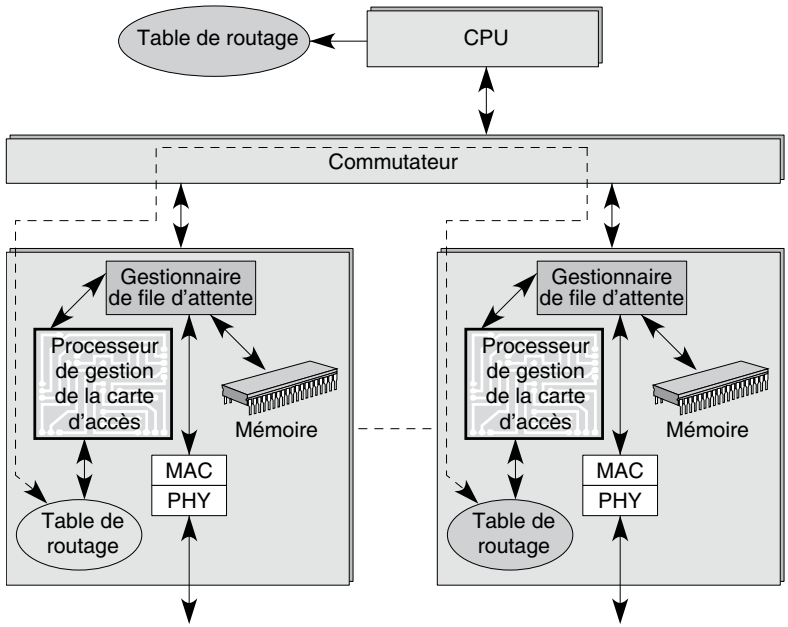


Figure 4.10

Architecture d'un gigarouteur

Les commutateurs forment le cœur des routeurs très haut débit pour permettre de réaliser des accès à plusieurs centaines de mégabits voire de gigabits par seconde.

Les bridge-routers

Les *bridge-routers*, aussi appelés b-routeurs ou ponts-routeurs, ont pour rôle d'allier le meilleur des deux technologies. Ils intègrent, selon les produits, les trois couches basses, physique, liaison et paquet, et essaient d'agir sur le niveau liaison lorsqu'ils en ont la possibilité, faute de quoi ils remontent au paquet pour traiter l'adresse de niveau paquet. En d'autres termes, les *bridge-routers* reçoivent une trame qui est traitée comme si l'organe était un pont. Si le pont de niveau trame ne permet pas de déterminer la direction dans laquelle il faut envoyer la trame, celle-ci est décapsulée pour récupérer le paquet qu'elle transporte dans sa zone de données. La passerelle a maintenant un paquet à examiner, et elle joue le rôle de passerelle de niveau 3 qui est généralement un routeur IP.

Le *bridge-router* est un organe assez complexe puisqu'il demande une gestion des tables de niveau trame et de niveau paquet. En revanche, c'est un équipement très performant du point de vue des possibilités de traitement des références et des adresses.

Les relais de transport

Les relais de transport se situent au niveau 4 de l'architecture du modèle de référence. Leur utilisation est recommandée lorsqu'on veut interconnecter des réseaux de niveau message différents. Par exemple, si l'on veut interconnecter une communication sous TCP et une autre sous UDP, il faut passer par des relais de transport. Ces relais peuvent être aussi appelés des routeurs de niveau message, ou routeurs de niveau 4. Il faut en effet remonter jusqu'au niveau transport pour reconstituer le message et examiner l'adresse du niveau correspondant, c'est-à-dire l'adresse qui se trouve dans le message. En pratique, la gamme de leur utilisation est moins variée, et il existe peu de produits de ce type sur le marché.

L'architecture d'un relais est illustrée à la figure 4.11.

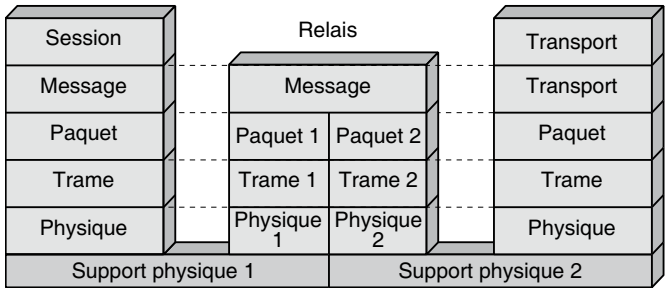


Figure 4.11

Architecture d'un relais

Les techniques de tunneling

Les techniques d'interconnexion que nous avons rencontrées jusqu'à présent ne concernent que la translation de l'information d'une trame vers une autre trame ou d'un paquet vers un autre paquet. Une autre méthode, totalement différente, appelée encapsulation, consiste à placer une trame à l'intérieur d'une autre trame ou un paquet à l'intérieur d'un autre paquet.

Par exemple, l'interconnexion d'un réseau IPv6 avec un réseau IPv4 peut se faire de la façon suivante. Supposons qu'un client IPv6 souhaite transmettre un paquet IPv6 à un client qui travaille sur une machine terminale IPv6. Supposons également que le seul réseau qui interconnecte ces deux machines soit l'Internet de type IPv4. Une première solution serait de faire une translation, c'est-à-dire de transférer l'intérieur du paquet IPv6 dans le paquet IPv4 et, à l'arrivée, de transférer à nouveau le contenu du paquet IPv4 dans un paquet IPv6. Cette solution est possible mais complexe, car il faut redéfinir complètement les zones de supervision des paquets transférés. C'est la raison pour laquelle on préfère utiliser une autre méthode : dans la machine terminale de l'émetteur, on encapsule le paquet IPv6 à l'intérieur d'un paquet IPv4. Le paquet IPv4 est transporté sur Internet, et, à l'arrivée, on décapsule le paquet IPv4 pour retrouver le paquet IPv6. On a en fait utilisé le réseau IPv4 comme un tunnel.

Pour interconnecter deux réseaux sans recourir à une passerelle, l'utilisation d'un tunnel est classique. C'est ce qu'on appelle faire du tunneling.

Translation et encapsulation

Les deux principaux niveaux d'interconnexion sont, comme nous l'avons vu :

- le niveau trame, avec des ponts ;
- le niveau paquet, avec des routeurs.

Si l'on reste au niveau pont, deux solutions sont envisageables : la translation et l'encapsulation.

Dans la translation, les adresses source et destination des stations terminales sont véhiculées dans les en-têtes. Dans l'encapsulation, une trame complète venant du réseau local est incluse dans la trame du réseau qui va servir de tunnel. Cette méthode ne demande pas de traitement de la trame, mais, comme elle n'est pas normalisée, elle présente l'inconvénient de se restreindre à un monde homogène, c'est-à-dire d'aller d'une station terminale avec un protocole X à une station terminale utilisant le même protocole X.

La figure 4.12 illustre l'architecture d'une technique d'encapsulation de niveau paquet. On suppose qu'une machine terminale d'une entreprise utilise le protocole IPv6 et qu'elle veuille se connecter à réseau local IPv6. Le client est représenté par la pile de gauche et l'entreprise par la pile de droite. Le protocole indiqué avec la valeur 3' est donc IPv6.

Pour interconnecter cette station et le réseau local, seul le réseau Internet IPv4 est disponible. IPv4 est représenté par le protocole indiqué par la valeur 3. La station terminale encapsule son paquet IPv6 (protocole 3') dans un paquet IPv4 (protocole 3). Ce paquet

IPv4 est transporté sur Internet jusqu'au routeur d'accès de l'entreprise, qui est symbolisé par la pile de protocoles du milieu. Dans ce routeur, le paquet IPv4 (protocole 3) est décapsulé pour retrouver le paquet IPv6 (protocole 3'). Ce paquet IPv6 est ensuite transporté en IPv6 dans le réseau local, représenté par la partie droite du schéma.

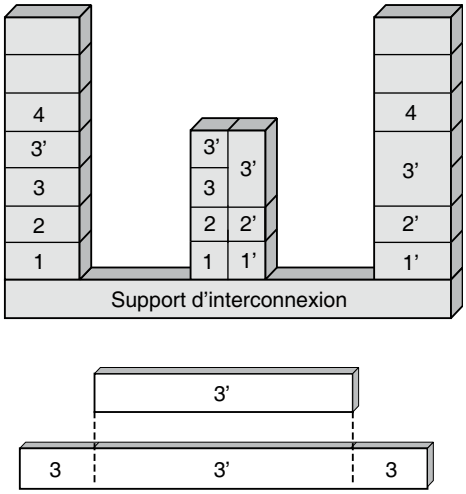


Figure 4.12

Encapsulation de niveau paquet

La même solution s'offre au concepteur de réseau pour interconnecter des machines IPv4 par l'intermédiaire d'un réseau IPv6. Il suffit d'encapsuler le paquet IPv4 dans le paquet IPv6 puis, à l'arrivée, de décapsuler le paquet IPv6 pour retrouver le paquet IPv4.

Les deux solutions d'encapsulation sont comparables. Celle qui sera la plus pratiquée dépendra de la façon de passer d'IPv4 à IPv6. Une première solution consiste à supposer qu'un opérateur se décide à proposer un réseau IPv6 pour effectuer le transfert des paquets pour la simple raison qu'avec IPv6 il pourra offrir plus de services à ces clients qu'avec IPv4. Les clients resteront sûrement encore quelque temps en IPv4 avant de passer en IPv6. Il suffira alors d'encapsuler les paquets IPv4 dans les paquets IPv6 de l'opérateur. Maintenant, si ce sont les clients qui décident de passer en IPv6 — parce qu'ils peuvent indiquer plus d'informations dans leurs zones de supervision — mais que les opérateurs restent en IPv4, on aura des encapsulations de paquets IPv6 dans des paquets IPv4.

Les pare-feu

Les fonctionnalités des pare-feu sont analysées en détail au chapitre 29. Nous introduisons dans ce chapitre ces équipements réseau, car ils deviennent de plus en plus nécessaires dans les réseaux d'aujourd'hui, même pour un particulier dès lors qu'il se rattache à Internet.

Un pare-feu, ou coupe-feu ou encore *firewall*, est, comme son nom l'indique, un équipement dont l'objectif est de séparer le monde extérieur du monde intérieur à protéger. Son rôle est de ne laisser entrer que les paquets dont l'entreprise est sûre qu'ils ne posent pas de problème.

Les pare-feu offrent de nombreuses fonctions, dont la principale est de trier ce qui entre et ce qui sort et de décider d'une action lorsque la reconnaissance a été effectuée. Les actions peuvent aller du rejet du paquet à sa compression-décompression, en passant par son examen par un antivirus, son ralentissement, son accélération, etc.

Divers moyens sont mis en œuvre pour reconnaître un paquet et plus généralement le flot, comme la reconnaissance de l'application qui transite par le pare-feu, l'adresse de destination ou l'adresse source, la machine et l'application sur laquelle le distant veut se connecter, etc.

Les pare-feu se distinguent par le niveau auquel ils travaillent. En règle générale, ils sont de niveau 4, ou message : on essaie de trouver dans le message de niveau TCP un moyen de reconnaître l'application. Les utilisateurs se différencient par leurs adresses source et destination mais surtout, dans la première génération, par le numéro de port, qui indique l'application en cours. Par exemple, le port 80 indique une application HTTP. Cependant, les numéros de port sont de moins en moins fiables, car les attaquants se servent des ports ouverts et souvent du port 80 en utilisant le protocole HTTP comme d'une capsule dans laquelle ils intègrent leur message.

L'utilisation de numéro de port est assez restrictive, dans la mesure où de plus en plus d'applications possèdent des ports dynamiques, comme FTP, la plupart des applications P2P (Peer-to-Peer) ou les signalisations téléphoniques. De plus, deux clients peuvent déterminer entre eux un numéro de port sur lequel ils souhaitent communiquer.

L'évolution des pare-feu a consisté à monter dans les couches de protocoles de façon à atteindre la couche application afin de pouvoir déterminer l'application en cours. On appelle pare-feu applicatif, ou pare-feu de niveau 7, les pare-feu qui sont capables de distinguer clairement les applications.

Si le reproche longtemps adressé aux pare-feu était de prendre beaucoup de temps et de ne pas être capables de déterminer les applications au fil de l'eau, cela n'est plus vrai aujourd'hui. Les produits de pare-feu applicatifs introduits sur le marché depuis quelque temps ne prennent pas plus de temps que la plupart des équipements réseau rencontrés dans le monde IP. Nous pouvons citer le cas du boîtier QoSMOS, qui est capable de filtrer et de déterminer les applications dans un laps de temps très court, de telle sorte que la sortie des paquets n'est retardée que d'un temps maximal égal au temps de traversée d'un routeur courant.

Le pare-feu s'installe souvent dans un boîtier dédié pour simplifier sa mise en œuvre, mais il peut également se trouver en différents points du réseau, allant du routeur au commutateur, en passant par un serveur spécialisé ou le poste client.

Les proxy

Les proxy permettent de rompre avec le modèle classique client-serveur d'une communication en interdisant une connexion directe du client au serveur. Il existe deux types principaux de proxy, les proxy de type applicatif et les proxy de type circuit.

Les proxy applicatifs interviennent au niveau 7, ou application, avec pour objectif de casser le modèle client-serveur pour passer au modèle client-client. Les seconds ne permettent pas une connexion TCP de bout en bout et sont plutôt destinés à du trafic sortant d'utilisateurs authentifiés.

Les proxy applicatifs

Comme expliqué précédemment, les proxy applicatifs interviennent au niveau application du modèle de référence. Leur objectif est de rompre avec le modèle client-serveur classique en le remplaçant par un double modèle client-serveur, comme illustré à la figure 4.13. La relation directe est coupée pour être remplacée par deux relations avec le proxy faisant la transition entre les deux relations c'est-à-dire entre le proxy jouant le rôle de serveur et le proxy jouant le rôle de client. En d'autres termes, une connexion TCP de bout en bout est remplacée par deux connexions mises bout à bout grâce au proxy.

Cette solution apporte une bonne sécurité puisqu'il faut exécuter l'application dans le proxy, ce qui permet de vérifier que le flot de paquets ne forme pas une attaque. On peut réaliser des pare-feu de type proxy qui sont équivalents à des pare-feu de niveau 7. L'inconvénient majeur de cette solution est la lourdeur et la difficulté d'obtenir de bonnes performances.

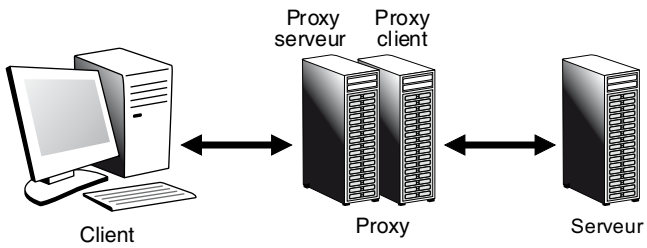


Figure 4.13
Proxy applicatif

Les proxy circuit

Les proxy de type circuit ont pour objectif de vérifier que la suite de paquets sur un chemin, ou circuit virtuel, est conforme aux RFC correspondantes. En effet, beaucoup d'attaques s'effectuent en insérant dans le flux normal de paquets des paquets d'attaque. Avec un proxy circuit, les différents champs des paquets sont vérifiés afin de garantir qu'aucun paquet ne porte une attaque.

Cette solution offre également une bonne sécurité en demandant une authentification de l'utilisateur qui va utiliser le chemin, au début de sa connexion.

Les appliances

Les appliances sont des boîtiers qui possèdent une ou plusieurs fonctions bien déterminées et qui s'insèrent facilement dans le réseau. L'avantage de ces boîtiers est généralement de pouvoir démarrer une nouvelle fonctionnalité sans avoir à programmer ni à adapter les

logiciels existants. Les appliances peuvent servir à la sécurité, et donc intégrer un pare-feu, mais aussi, par le biais de fonctionnalités spécifiques, à la gestion de la qualité de service.

Cette section est essentiellement consacrée aux appliances permettant d'effectuer de la surveillance de la qualité de service et de l'accélération de flux IP.

Les appliances sur la surveillance des flux permettent de déterminer les différents flux qui transitent sur Internet et, après reconnaissance, de les traiter. Les traitements peuvent être extrêmement divers suivant les boîtiers (perte, compression, mise en attente, accélération, etc.).

Pour la reconnaissance de flux, de nombreuses possibilités sont aujourd'hui disponibles, la plus classique consistant à utiliser les numéros de port. Cependant, comme les applications les plus modernes utilisent des ports dynamiques, cette solution s'avère parfois désastreuse du point de vue de la reconnaissance des flots et donc de la sécurité ou de la gestion des flots de paquets IP. Une solution consiste à reconnaître les flots par leur grammaire, c'est-à-dire l'ensemble des règles à suivre pour réaliser l'écriture des messages applicatifs. Comme la grammaire est unique pour chaque application, il est possible de reconnaître un flot, même s'il est encapsulé dans d'autres flots, comme dans des tunnels L2TP. Une fois le flot reconnu, le boîtier peut effectuer une fonction décidée par le gestionnaire du réseau et programmée à l'avance.

On peut classer parmi les appliances les commutateurs ou les routeurs de niveau 4 ou 7, c'est-à-dire capables de commuter ou de router en fonction d'informations recueillies au niveau message ou applicatif. Par exemple, en fonction d'un numéro de port ou d'une reconnaissance de l'application, la décision de routage ou de contrôle peut différer.

Nous pouvons également ranger dans les appliances les accélérateurs de flots IP. Ces accélérateurs intègrent un moyen permettant de faire parvenir à l'émetteur une réponse plus rapidement ou d'effectuer un transfert de données, d'un point vers un autre, en moins de temps que sans accélérateur.

Les accélérations peuvent s'effectuer aux différents niveaux de l'architecture. En règle générale, plus le niveau est bas, plus l'accélération globale est importante. À l'inverse, plus le niveau est haut, plus l'accélération est lente et destinée à des applications particulières. Par exemple, il est possible de compresser le flux de niveau 1, et de réduire ainsi le nombre de paquets à transmettre, ou de diminuer leur taille, ce qui entraîne une charge moindre à l'intérieur du réseau et donc un meilleur temps de transit. Au niveau 2, on peut concevoir des accélérateurs pour la correction d'erreur lorsque le taux d'erreur est important. Au niveau 3, on peut jouer sur les adresses IP et sur le contenu des en-têtes des paquets IP. Enfin, aux niveaux supérieurs, on peut travailler sur des applications particulières plutôt que sur toutes les applications simultanément, comme aux niveaux 1, 2 et 3.

Les appliances concernent également l'accélération par la mémorisation d'informations dans des caches intermédiaires, c'est-à-dire dans des mémoires tampons qui se situent relativement près des entrées du réseau des opérateurs. On met dans le cache soit des pages entières d'information, si celles-ci sont fortement demandées, de telle sorte qu'il ne soit pas nécessaire d'aller rechercher la page sur le serveur d'origine, qui peut se situer à

l'autre bout de la terre. On peut également mémoriser une partie de la page et ne chercher que des informations complémentaires. Par exemple, pour une page Web qui possède un fond assez gourmand en octets, seul le fond est gardé en un cache à proximité du client, et seules sont demandées au serveur les informations de type texte à mettre à jour. Les débits mesurés dans cette solution ne représentent que 5 à 20 % du débit total nécessaire au transport de la page complète.

Les contrôleurs

Les contrôleurs forment une nouvelle génération de boîtiers dont l'objectif est de contrôler un certain nombre d'autres machines. Ils sont notamment utilisés pour la gestion des points d'accès dans les réseaux Wi-Fi.

Un contrôleur a pour rôle de rassembler des fonctionnalités auparavant réparties dans les différents points d'accès. Au lieu d'augmenter la complexité de ces derniers, on a préféré regrouper certaines de leurs fonctions dans le contrôleur. On y trouve notamment des éléments de gestion de la puissance d'émission des points d'accès, ainsi que de la fréquence à utiliser. Les fonctions de sécurité, telles qu'un serveur d'authentification, sont également gérées par le contrôleur. Les clients s'authentifient sur le contrôleur, lequel peut jouer le rôle de proxy pour un serveur d'authentification plus global de l'entreprise. Des fonctions de découverte de points d'accès pirates sont également souvent introduites dans les contrôleurs.

Le contrôleur possède bien entendu des fonctions de contrôle proprement dites, comme le contrôle des handovers, lorsque des clients passent d'une cellule à une autre cellule. Le handover peut être intra-contrôleur, les deux cellules étant gérées par le même contrôleur, ou inter-contrôleur, lorsque les deux cellules n'appartiennent pas au même contrôleur.

Le contrôleur peut posséder de nombreuses fonctions de gestion du nomadisme. Par exemple, le contrôleur Ucopia illustré à la figure 4.14 implémente de nombreuses fonctionnalités, notamment les suivantes :

- gestion de la sécurité par une authentification par portail captif, certificat, carte CPS ;
- identification de l'utilisateur, du poste et des conditions de connexion et contrôle d'accès par profil métier ;
- traçabilité en suivant les lois 2001-1062, 2003-237, LCT du 23 mars 2006 ;
- accès nomade zéro configuration ;
- gestion des personnels permanents ou de passage et des visiteurs ;
- intégration des annuaires, VLAN, VPN, PKI, carte CPS, etc.
- supervision et l'administration centralisée multisite et redondance pour des raisons de disponibilité ;
- indépendance et évolutivité des équipements réseau ;
- gestion simultanée des connexions filaires et sans fil ;
- gestion des points d'accès hétérogènes Wi-Fi a/b/g/n et WiMAX ;
- provisionnement du service (forfait jour, crédit temps).

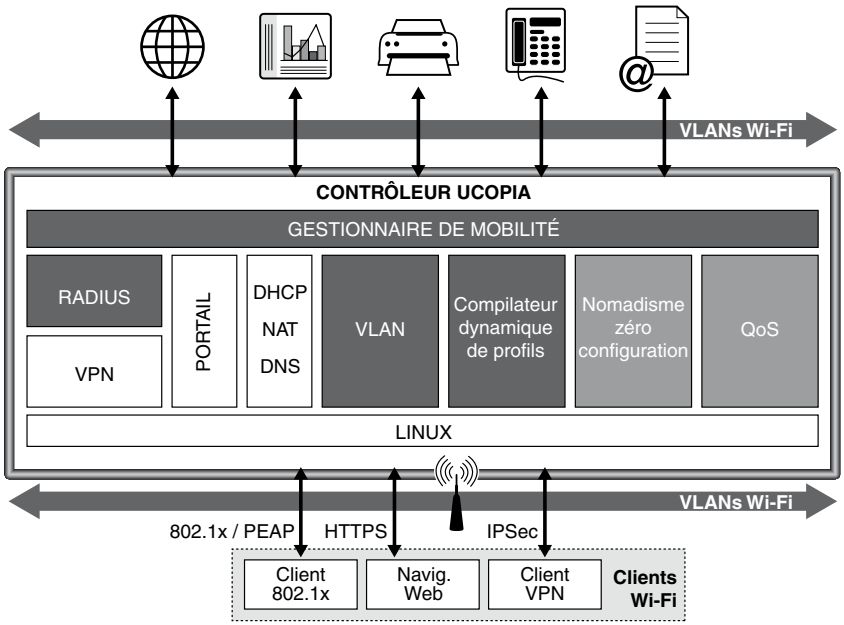


Figure 4.14

Fonctions d'un contrôleur Ucopia

Les contrôleurs de communication sont amenés à se développer de plus en plus pour prendre en charge des fonctions communes à l'intérieur d'un réseau et décharger les autres équipements de ces fonctions.

Conclusion

La convergence au niveau paquet vers la technologie IP n'empêche pas une persistance des techniques d'interconnexion de réseaux. En effet, au niveau trame, une forte diversité existe encore entre les trames ATM et les différentes trames Ethernet. De même, au niveau paquet, la percée d'IPv6 va demander des interconnexions IPv4-IPv6 pendant un certain temps encore.

La tendance des grands opérateurs est de faire converger tous leurs réseaux cœur (réseau téléphonique, réseaux de données, réseaux cœur des réseaux de mobiles, etc.) vers un réseau unique de transport de paquets IP. Pour acheminer ces données, les paquets IP sont soit routés dans des routeurs, soit encapsulés dans des trames, pour être le plus souvent commutés. Pour permettre une sécurité du transport de ces paquets, de nombreuses solutions sont commercialisées avec plus ou moins de puissance et de succès.

Nous avons vu que les appliances offraient diverses fonctions tout en restant généralement simples à mettre en œuvre. Leur rôle principal est d'améliorer les performances du réseau par des moyens extrêmement divers.

Partie II

Les protocoles des niveaux 1 à 4

Cette partie examine en détail les quatre premiers niveaux de l'architecture des réseaux. La couche 1, ou couche physique (niveau élément binaire), permet la transmission d'un élément binaire d'une machine à une autre. En fonction du débit désiré, de l'éloignement et de nombreuses autres caractéristiques physiques, le choix du support doit être pesé avec soin.

La couche 2, ou couche liaison (niveau trame), permet de transporter l'élément binaire en le plaçant dans une trame. Les trames que nous examinerons proviennent des mondes Internet, Ethernet et ATM.

La couche 3, ou couche réseau (niveau paquet), concerne le transport des paquets d'une extrémité à l'autre du réseau. Le protocole IP (Internet Protocol) s'est imposé dans cette fonction, et il a supplanté tous les autres. Nous le décrivons en détail au chapitre 7.

La couche 4, ou couche transport (niveau message), s'occupe du transport des messages de bout en bout. À nouveau, l'environnement protocolaire provenant du monde IP est désormais seul à accomplir cette tâche (*pour une description du niveau message de l'ATM et du modèle de référence, voir l'annexe G*).

5

Le niveau physique

La couche détermine comment les éléments binaires sont transportés sur un support physique. Dans un premier temps, les informations à transmettre sont codées en une suite de 0 et de 1. Pour la transmission vers le récepteur, ces bits 0 et 1 sont ensuite introduits sur le support sous une forme spécifique, reconnaissable du récepteur.

Plusieurs composants de la couche physique sont définis dans ce niveau, comme les modems, multiplexeurs, concentrateurs, etc. Ce chapitre détaille ces éléments de base et introduit les architectures de niveau physique qui seront examinées ultérieurement dans l'ouvrage.

Le codage et la transmission

Les réseaux de données se fondent sur la numérisation des informations, c'est-à-dire la représentation des données par des suites de 0 et de 1. Pour transformer les informations en suites binaires, on utilise des codes, qui font correspondre à chaque caractère une suite précise d'éléments binaires. Le nombre de bits utilisés pour représenter un caractère correspond au nombre de moments d'un code. Un code à n moments permet de représenter 2^n caractères distincts.

Plusieurs codes ont été normalisés pour faciliter les échanges entre équipements informatiques. Le nombre de moments utilisés augmente avec la dimension de l'alphabet, qui n'est autre que la liste des caractères qui doivent être codés. L'alphabet peut n'être constitué que de chiffres. On peut y ajouter les lettres minuscules et majuscules, les signes de ponctuation, les opérateurs arithmétiques, mais aussi des commandes particulières.

Les principaux codes utilisés sont les suivants :

- Code télégraphique, à 5 moments. L'alphabet peut comporter 32 caractères, dont seulement 31 sont utilisés.
- Code ASCII, à 7 moments, soit 128 caractères disponibles.

- Code EBCDIC à 8 moments, qui autorise jusqu'à 256 caractères.
- Unicode, à 16 moments, qui reprend de façon légèrement simplifiée les spécifications du code ISO 10646 UCS (Universal Character Set), à 32 moments. Ce code unique permet de prendre en compte toutes les langues du monde.

Après l'étape du codage intervient celle de la transmission proprement dite, c'est-à-dire l'envoi des suites binaires de caractères vers l'utilisateur final. Ce transport peut s'effectuer en parallèle ou en série.

Dans la transmission en parallèle, les bits d'un même caractère sont envoyés sur des fils métalliques distincts pour arriver ensemble à destination. Il peut y avoir 8, 16, 32 ou 64 fils parallèles, voire davantage dans des cas spécifiques. Cette méthode pose toutefois des problèmes de synchronisation, qui conduisent à ne l'utiliser que sur de très courtes distances, le bus d'un ordinateur, par exemple.

Dans la transmission en série, les bits sont envoyés les uns derrière les autres. La succession de caractères peut être asynchrone ou synchrone. Le mode asynchrone indique qu'il n'y a pas de relation préétablie entre l'émetteur et le récepteur. Les bits d'un même caractère sont encadrés de deux signaux, l'un indiquant le début du caractère, l'autre la fin. Ce sont les bits Start et Stop. Le début d'une transmission peut se placer à un instant quelconque dans le temps, comme illustré à la figure 5.1.

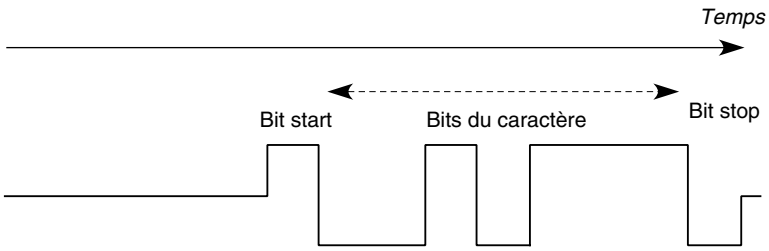


Figure 5.1

Un caractère dans le mode asynchrone

Dans le mode synchrone, l'émetteur et le récepteur se mettent d'accord sur un intervalle constant, qui se répète sans arrêt dans le temps. Les bits d'un caractère sont envoyés les uns derrière les autres et sont synchronisés avec le début des intervalles de temps. Dans ce type de transmission, les caractères sont émis en séquence, sans aucune séparation. Ce mode est utilisé pour les très forts débits.

Dans tous les cas, le signal émis est synchronisé sur une horloge lors de la transmission d'un élément binaire. La vitesse de l'horloge donne le débit de la ligne exprimée en baud, c'est-à-dire le nombre de top d'horloge par seconde. Par exemple, une ligne de communication qui fonctionne à 50 bauds indique qu'il y a 50 intervalles de temps élémentaires dans une seconde. Sur un intervalle élémentaire, on émet généralement un bit, c'est-à-dire un signal à 1 ou à 0. Rien n'empêche de transmettre quatre types de signaux distincts, qui auraient comme signification 0, 1, 2 et 3. On dit, dans ce dernier cas, que le signal a une valence de 2. Un signal a une valence de *n* si le nombre de niveaux transportés dans un

intervalle de temps élémentaire est égal à 2^n. La capacité de transmission de la ligne en nombre de bit transporté par seconde vaut *n* multiplié par la vitesse exprimée en baud. On exprime cette capacité en bit par seconde. Par exemple, une ligne d'une vitesse de 50 bauds qui a une valence de 2 a une capacité de 100 bits par seconde (100 bit/s).

Lors de la transmission d'un signal, des perturbations de la ligne physique par ce qu'on appelle le bruit extérieur peuvent se produire. Si l'on connaît le niveau de ce bruit, on peut calculer la capacité maximale de la ligne. En termes plus précis, le bruit peut avoir pour origine la mauvaise qualité de la ligne elle-même, qui modifie les signaux qui s'y propagent, ainsi que d'éléments intermédiaires, comme les modems et les multiplexeurs, qui n'envoient pas toujours exactement les signaux demandés, ou d'événements extérieurs, telles les ondes électromagnétiques.

Le bruit est considéré comme un processus aléatoire décrit par une fonction *b(t)*. Si *s(t)* est le signal transmis, le signal parvenant au récepteur s'écrit *s(t)* + *b(t)*. Le rapport signal sur bruit est une caractéristique d'un canal : c'est le rapport de l'énergie du signal sur l'énergie du bruit. Ce rapport varie dans le temps, puisque le bruit n'est pas uniforme. Toutefois, on l'estime par une valeur moyenne sur un intervalle de temps. Il s'exprime en décibel (dB). Nous écrirons ce rapport S/B.

Le théorème de Shannon donne la capacité maximale d'un canal soumis à un bruit :

$$C = W\log_2(1 + \mathrm{S/B})$$

où *C* est la capacité maximale en bit par seconde et *W* la bande passante en hertz.

Sur une ligne téléphonique dont la bande passante est de 3 200 Hz, pour un rapport signal sur bruit de 10 dB, on peut théoriquement atteindre une capacité de 10 Kbit/s.

Pour en terminer avec ce bref aperçu des techniques de transmission, voyons les différentes possibilités de transmission entre deux points. Les liaisons unidirectionnelles, ou simplex, ont toujours lieu dans le même sens, de l'émetteur vers le récepteur. Les liaisons bidirectionnelles, à l'alternat ou semi-duplex, ou encore half-duplex, permettent de transformer l'émetteur en récepteur et *vice versa*, la communication changeant de sens à tour de rôle. Les liaisons bidirectionnelles simultanées, ou duplex, ou encore full-duplex, permettent une transmission simultanée dans les deux sens. Nous avons représenté ces divers cas à la figure 5.2.

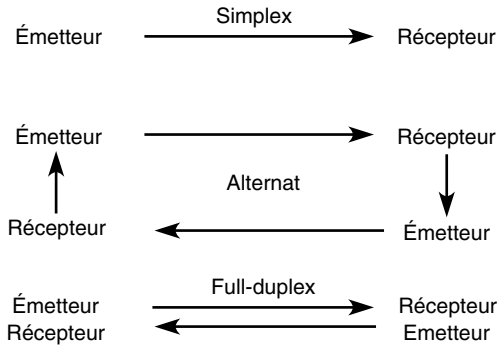


Figure 5.2
Sens de transmission

La transmission en bande de base

Examinons maintenant les techniques de transmission utilisées, c'est-à-dire comment un émetteur peut envoyer un signal que le récepteur reconnaîtra comme étant un 1 ou un 0.

La méthode la plus simple consiste à émettre sur la ligne des courants différents, un courant nul indiquant un 0 et un courant positif un 1. On obtient de la sorte une représentation des bits du caractère à transmettre sous forme de créneaux, comme illustré à la figure 5.3.

Cette méthode est appelée transmission en bande de base. La réalisation exacte de ces créneaux est fort complexe, du fait qu'il est souvent difficile de faire passer du courant continu entre deux stations. La même difficulté se retrouve dans le codage NRZ (Non Return to Zero), également illustré à la figure 5.3. Le codage bipolaire est un codage tout-ou-rien, dans lequel le bit 1 est indiqué par un courant positif ou négatif à tour de rôle, de façon à éviter les courants continus. Ce code laisse le bit 0 défini par un courant nul.

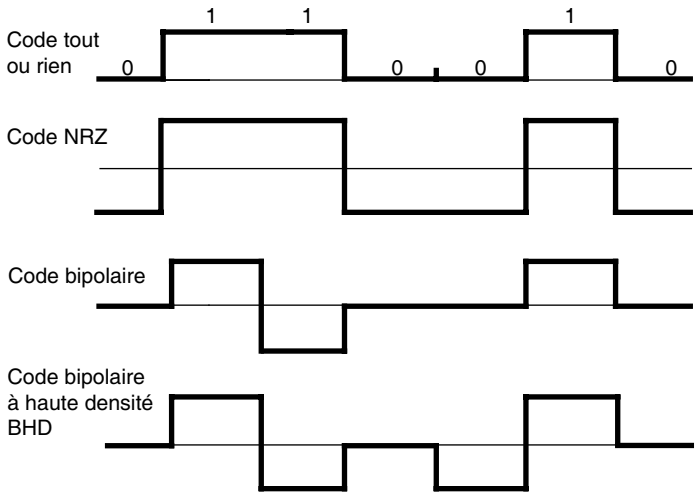


Figure 5.3

Les codages en bande de base

Le codage bipolaire à haute densité permet de ne pas laisser le courant nul pendant les suites de 0. Des suites spéciales de remplissage (courant négatif, nul ou positif) sont alors insérées à la place de ces zéros. Un nouveau 1 est indiqué par un courant positif ou négatif, en violation avec la suite de remplissage.

De nombreux autres codages en bande de base ont été développés au gré de la demande pour améliorer telle ou telle caractéristique du signal. La figure 5.4 illustre les codages RZ (Return to Zero), de Miller, Manchester et biphase-M et S.

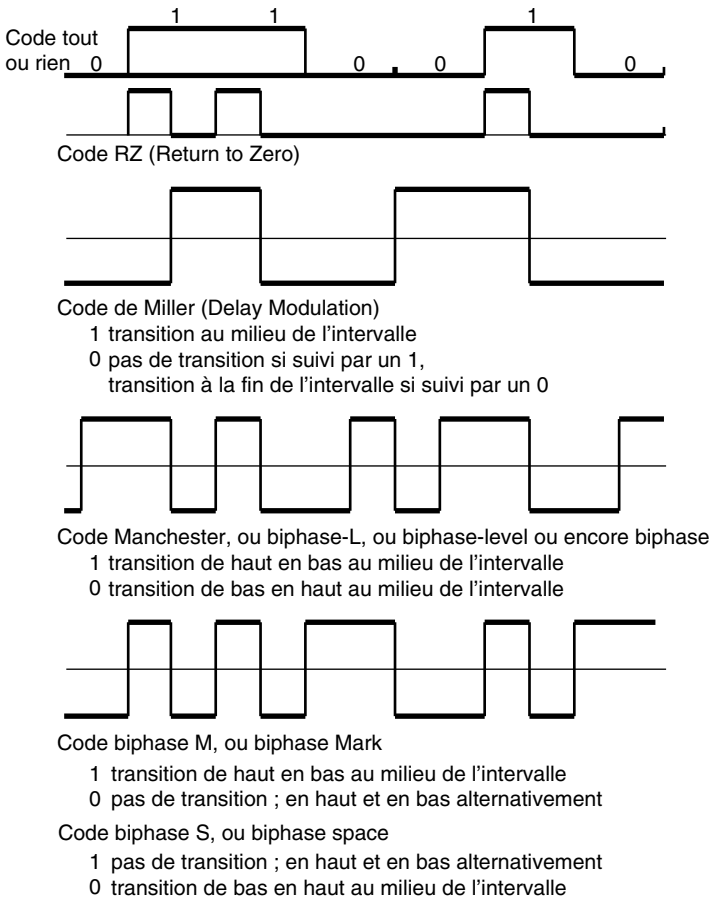


Figure 5.4

Quelques codages en bande de base

La dégradation rapide des signaux au fur et à mesure de la distance parcourue constitue le principal problème de la transmission en bande de base. Si le signal n'est pas régénéré très souvent, il prend une forme quelconque, que le récepteur est incapable de comprendre. Cette méthode de transmission ne peut donc être utilisée que sur de courtes distances, de moins de 5 km. Sur des distances plus longues, on utilise un signal de forme sinusoïdale. Ce type de signal, même affaibli, peut très bien être décodé par le récepteur.

La modulation

Comme expliqué précédemment, pour transmettre un élément binaire, il faut émettre un signal très particulier pour reconnaître si sa valeur est égale à 0 ou à 1. Les techniques en bande de base sous forme de créneau ne sont pas fiables dès que la distance dépasse

quelques centaines de mètres. Pour avoir un signal que l'on puisse récupérer correctement, il faut lui donner une forme spéciale en le modulant.

On distingue les trois grandes catégories de modulation suivantes :

- modulation d'amplitude, ou ASK (Amplitude-Shift Keying) ;
- modulation de phase, ou PSK (Phase-Shift Keying) ;
- modulation de fréquence, ou FSK (Frequency Shift Keying).

Un matériel intermédiaire, le modem (modulateur-démodulateur), est nécessaire pour moduler le signal sous une forme sinusoïdale. Le modem reçoit un signal en bande de base et le module, c'est-à-dire lui attribue une forme analogique sinusoïdale. Le fait de n'avoir plus de fronts montants ni descendants protège beaucoup mieux le signal des dégradations occasionnées par la distance parcourue par le signal dans le câble puisque le signal est continu et non plus discret.

Dès qu'un terminal situé à une distance un peu importante doit être atteint, un modem est nécessaire pour que le taux d'erreur soit acceptable. La distance dépend très fortement du câble utilisé et de la vitesse de transmission. Classiquement, à partir de quelques centaines de mètres pour les très hauts débits et quelques kilomètres pour les débits inférieurs, il faut faire appel à un modem.

La modulation d'amplitude

Dans la modulation d'amplitude, la distinction entre le 0 et le 1 est obtenue par une différence d'amplitude du signal, comme illustré à la figure 5.5.

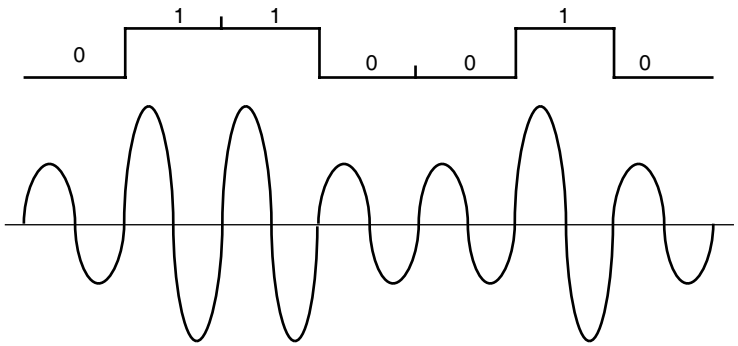


Figure 5.5
Modulation d'amplitude

La modulation de phase

Pour la modulation de phase, la distinction entre 0 et 1 est effectuée par un signal qui commence à des emplacements différents de la sinusoïde, appelés phases. À la figure 5.6, les valeurs 0 et 1 sont représentées par des phases respectives de 0° et de 180°.

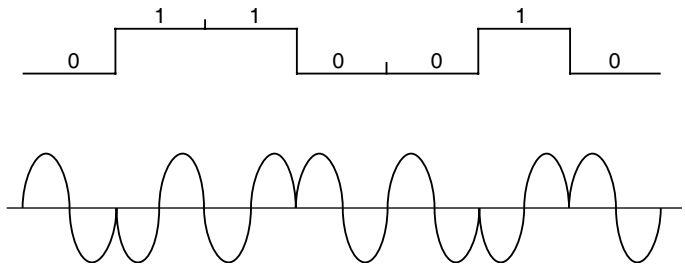


Figure 5.6

Modulation de phase

La modulation de fréquence

En modulation de fréquence, l'émetteur a la possibilité de modifier la fréquence d'envoi des signaux suivant que l'élément binaire à émettre est 0 ou 1, comme l'illustre la figure 5.7.

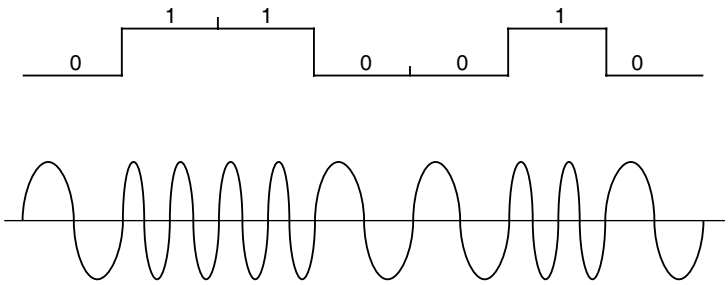


Figure 5.7

Modulation de fréquence

Dans les présentations précédentes des techniques de modulation, la grandeur physique utilisée pour l'amplitude, la phase ou la fréquence ne représente que deux états possibles. Si l'on arrive à émettre et à détecter à l'arrivée plus de deux états d'une même grandeur, on peut donner à chaque état une signification permettant de coder 2 ou plusieurs bits. Par exemple, en utilisant 4 fréquences, 4 phases ou 4 amplitudes, on peut coder 2 bits à chaque état. La figure 5.8 illustre une possibilité de coder 2 bits en modulation de phase.

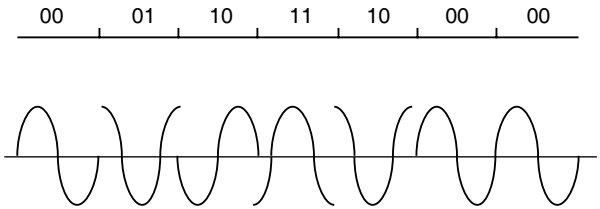


Figure 5.8

Modulation de phase à quatre moments

Les modems

Les modems permettent de transformer les signaux binaires en bande de base en signaux analogiques spécifiques indiquant une valeur numérique. Le signal se présente sous une forme sinusoïdale.

Les modems s'adaptent aux différents types de support, qui peuvent être :

- 2 fils de qualité normale ;
- 4 fils de qualité normale ;
- 4 fils de qualité supérieure conforme à l'avis M.1020 de l'UIT-T ;
- 2 fils en bande de base ;
- 4 fils en bande de base ;
- les groupes primaires, les groupes secondaires, etc.

Le tableau 5.1 répertorie les avis de l'UIT-T concernant les modems classiques. Les modems ADSL sont présentés en détail au chapitre 9. Ils nécessitent des fonctions de multiplexage, que nous introduisons ultérieurement.

Avis CCITT	Débit en bit/s	Type de modulation	Vitesse de modulation	Exploitation
V.21	300	Fréquence	300	Full-duplex (FD)
V.22	600/1 200	Phase	600	FD
V.22bis	1 200/2 400	Phase	600	FD
V.23	600/1 200	Fréquence	600/1 200	Half-duplex (HD)
V.23	1 200/75	Fréquence	1 200/75	FD
V.26	2 400	Phase	1 200	FD
V.26bis	1 200/2 400	Phase	1 200	HD
V.26ter	1 200/2 400	Phase	1 200	FD
V.27	4 800	Phase	1 600	FD ou HD
V.27bis	2 400/4 800	Phase	1 200/1 600	FD ou HD
V.27ter	4 800	Phase	1 200/1 600	HD
V.29	4 800/9 600	Phase + amplitude	4 800/9 600	FD
V.32	4 800/9 600	Phase + amplitude	2 400	FD
V.32bis	Jusqu'à 14 400	Phase + amplitude	3 200	FD
V.34	Jusqu'à 28 800	Phase + amplitude	3 200	FD
V.34+	Jusqu'à 33 600	Phase + amplitude	3 200	FD
V.90	Jusqu'à 56 000/33 600	Phase + amplitude	3 200	FD
V.92	Jusqu'à 56 000/48 000	Phase + amplitude	3 200	FD

TABLEAU 5.1 • Modems normalisés

Il arrive que des fonctionnalités additionnelles soient implémentées dans les modems. Une fonctionnalité importante concerne la compression : plutôt que d'augmenter la vitesse, on compresse les données. Le protocole MNP (Microcom Networking Protocol) est un bon exemple de proposition de compression et de correction d'erreur. Ce protocole, mis au point par le constructeur américain Microcom, est normalisé par l'avis V.42bis de l'UIT-T. Les possibilités offertes par MNP sont plus larges que celles de l'avis V.42bis, qui ne concerne que MNP2, MNP3 et MNP4.

Les principales caractéristiques de ces normes sont les suivantes :

- MNP1 : protocole de correction d'erreur au niveau de l'octet ;
- MNP2 : protocole de correction d'erreur au niveau de l'octet en full-duplex à 2 400 bit/s ;
- MNP3 : protocole de correction d'erreur au niveau bit ;
- MNP4 : protocole de correction d'erreur au niveau paquet ;
- MNP5 : protocole de correction d'erreur et de compression de données de moyenne 2 ;
- MNP6 : protocole de correction d'erreur et de compression de données en half-duplex ;
- MNP7 : protocole de correction d'erreur et de compression de données de moyenne 3 ;
- MNP8 : abandonné ;
- MNP9 : protocole de correction d'erreur et de compression de données pour modem jusqu'à 38,4 Kbit/s ;
- MNP10 : protocole de correction d'erreur au niveau paquet, comme MNP4, mais avec des paquets de taille variable.

Nœuds et terminaux

Les terminaux sont raccordés aux nœuds du réseau par des liaisons plus ou moins longues. Il faut utiliser un modem, par exemple un modem ADSL, qui est caractérisé par plusieurs paramètres, dont les principaux sont les suivants :

- le codage utilisé : bande de base ou modulation ;
- la rapidité de modulation en baud ;
- le débit en bit par seconde ;
- le mode et le sens de transmission ;
- l'interface avec le terminal ETTD.

Lorsque la bande de base est utilisée, un convertisseur est nécessaire pour émettre les signaux. Pour envoyer un signal modulé, il faut utiliser un modem.

Les équipements terminaux rattachés au support de communication se composent des postes de travail utilisateur, ou postes client, et de serveurs. Lorsque les communications se font entre un client et un serveur, on parle d'application client-serveur. Lorsque les communications vont directement d'un utilisateur à un autre, on parle d'application peer-to-peer.

Les multiplexeurs

Sur une ligne de communication formant une liaison entre deux points distants, il peut être intéressant de faire transiter en même temps les données de plusieurs clients. Plutôt que chaque client dispose de sa propre infrastructure, il est plus économique de n'avoir qu'une liaison partagée par plusieurs utilisateurs. Un multiplexeur a pour fonction de recevoir des données de plusieurs terminaux par le biais de liaisons spécifiques, appelées voies basse vitesse, et de les transmettre toutes ensemble sur une liaison unique, la voie haute vitesse.

À l'autre extrémité de la liaison, il faut effectuer la démarche inverse, c'est-à-dire récupérer, à partir des informations arrivant sur la voie haute vitesse, les données des différents utilisateurs et les envoyer sur les bonnes voies de sortie. Cette tâche incombe au démultiplexeur. La machine qui effectue le multiplexage et le démultiplexage s'appelle un mux.

Il existe un grand nombre de possibilités de multiplexage. Les sections qui suivent présentent les principales.

Multiplexages fréquentiel et temporel

Dans le multiplexage en fréquence, chaque voie basse vitesse possède sa propre bande passante sur la voie haute vitesse. Dans ce cas, la voie haute vitesse doit avoir la capacité nécessaire pour absorber toutes les trames qui proviennent des équipements terminaux raccordés.

Le multiplexage temporel suit le même mécanisme, mais au lieu que la voie haute vitesse soit découpée en fréquences distinctes, elle est découpée en tranches de temps, lesquelles sont affectées régulièrement à chaque voie basse vitesse. On comprend que le multiplexage temporel soit plus efficace que le précédent puisqu'il fait une meilleure utilisation de la bande passante. Un problème se pose cependant : lorsqu'une trame se présente à l'entrée du multiplexeur et que la tranche de temps qui est affectée à ce terminal n'est pas exactement à son début, il faut mémoriser l'information jusqu'au moment approprié.

Un multiplexeur temporel doit donc être doté de mémoires tampons pour stocker les éléments binaires qui se présentent entre les deux tranches de temps. Il est très simple de calculer la taille de cette mémoire, puisqu'elle correspond au nombre maximal de bit se présentant entre les deux tranches de temps affectées au terminal. Cette attente n'est pas toujours négligeable par rapport au temps de propagation du signal sur une ligne de communication.

Le multiplexage statistique

Dans les deux types de multiplexage précédents, fréquentiel et temporel, il ne peut y avoir de problème de débit, la voie haute vitesse ayant une capacité égale à la somme des capacités des voies basse vitesse raccordées. En règle générale, cela conduit à un gaspillage de bande passante, puisque les voies basse vitesse ne transmettent pas en continu. Pour optimiser la capacité de la voie haute vitesse, il est possible de jouer sur la moyenne

des débits des voies basse vitesse. C'est ce qu'on appelle le multiplexage statistique. Dans ce cas, la somme des débits moyens des voies basse vitesse doit être légèrement inférieure au débit de la voie haute vitesse. Si, pendant un laps de temps, il y a plus d'arrivées que ne peut en supporter la liaison, des mémoires additionnelles prennent le relais dans le multiplexeur.

Fonctionnement du multiplexage statistique

Le multiplexage statistique se fonde sur un calcul statistique des arrivées et non sur des débits moyens. Par exemple, si dix voies basse vitesse d'un débit de 64 Kbit/s arrivent sur un multiplexeur statistique, le débit total peut atteindre 640 Kbit/s. Cette valeur correspond à la valeur maximale lorsque les machines débitant sur les voies basse vitesse travaillent sans aucun arrêt.

Dans les faits, il est rare de dépasser 50 % d'utilisation de la ligne, c'est-à-dire dans notre exemple 32 Kbit/s par ligne. En jouant statistiquement, on peut prendre une liaison haute vitesse d'un débit égal à 320 Kbit/s. Cependant, rien n'empêche que toutes les stations soient actives à un moment donné. Dans ce cas, une capacité de 640 Kbit/s se présente au multiplexeur, lequel ne peut débiter que 320 Kbit/s. Une mémoire importante doit donc tamponner les données en attente de transmission sur la ligne haute vitesse. Si le calcul statistique n'est pas effectué correctement, des pertes sont à prévoir.

La figure 5.9 donne une représentation du multiplexage statistique.

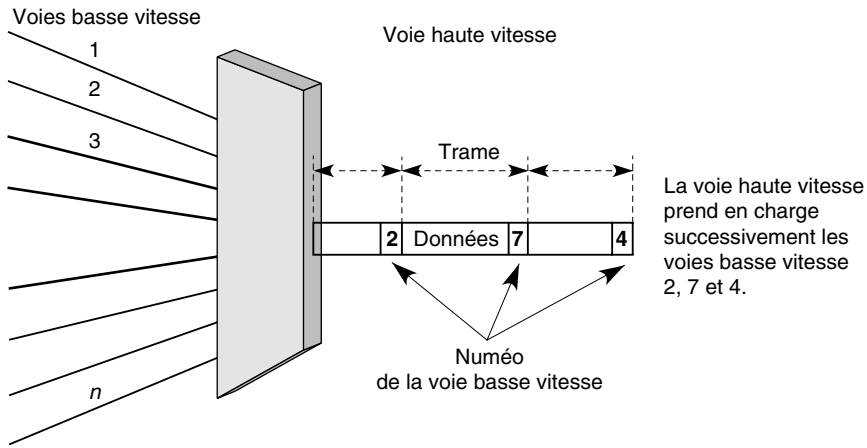


Figure 5.9
Multiplexage statistique

Dans ce schéma, on constate que les informations de la voie basse vitesse sont transportées dans une trame. Cette dernière doit comporter un numéro dans l'en-tête pour que la voie basse vitesse soit reconnue dans le démultiplexeur.

Un concentrateur est un multiplexeur statistique qui possède des fonctionnalités supplémentaires, comme des protocoles de niveau supérieur à la couche physique.

La transmission

Avant de transmettre l'information sur un support de transmission, on doit la coder de façon adéquate. Les réseaux doivent autoriser de très hauts débits sur des distances plus ou moins longues. Dans ce contexte, trois approches sont possibles pour le codage des éléments binaires provenant des applications :

- L'information est véhiculée directement en bande de base, ce qui permet d'obtenir des débits se comptant en gigabits par seconde sur quelques dizaines de mètres. Sur quelques centaines de mètres on peut atteindre plusieurs dizaines de mégabits par seconde. Enfin, sur des distances de quelques kilomètres, on atteint sur des paires de fils métalliques de type téléphonique des débits de l'ordre de quelques centaines de kilobits par seconde.
- L'information est modulée suivant les principes indiqués précédemment dans ce chapitre. Les vitesses atteintes sont beaucoup plus petites, mais les distances bien plus grandes. Pour augmenter la vitesse, il faut être capable de transporter un grand nombre d'éléments binaires par intervalle de temps.
- Les signaux numériques sont modulés sur une porteuse, et chaque type d'information se voit allouer une bande passante en fonction de ses besoins. C'est l'approche dite large bande.

La transmission en bande de base

La transmission en bande de base est la plus simple, puisque aucune modulation n'est nécessaire. La suite binaire représentant l'information est directement transmise sur le support par des changements introduits dans les signaux représentant l'information sous forme de transitions de tension, ou d'impulsions lumineuses si l'on utilise la fibre optique.

Les signaux en bande de base sont sujets à une atténuation, dont l'importance dépend du support employé. Ils doivent donc être régénérés périodiquement sur une longue distance. Cette régénération s'effectue à l'aide de répéteurs, qui reçoivent les signaux et les mémorisent une fraction de seconde avant de les retransmettre sur la ligne sortante.

La transmission large bande

Cette méthode utilise le multiplexage en fréquence. Différents canaux sont créés, résultant de la division de la bande passante du support en plusieurs sous-bandes de fréquences. Cette technique a l'avantage d'autoriser des transmissions simultanées indépendantes.

Chaque appareil sur le câble est équipé d'un modem particulier. Cela permet de choisir le mode de transmission, numérique ou analogique, le mieux adapté et le plus efficace pour le type d'information à transmettre. Par exemple, les données informatiques sont émises sur une bande numérique, et la voix et l'image sur une bande analogique. La transmission large bande augmente toutefois le coût de connexion par rapport à un réseau en bande de base, plus simple à installer et généralement moins cher.

La numérisation des signaux

La façon de coder le signal numérique est une fonction importante du coupleur de communication. Cette opération a pour fonction principale d'adapter les signaux au canal de transmission. Dans le cas des réseaux locaux, la vitesse de transmission est de plusieurs dizaines ou centaines de mégabits par seconde. De ce fait, le choix de la représentation physique des données est important. Pour effectuer la synchronisation bit, c'est-à-dire s'assurer que chaque bit est lu au bon moment, il faut qu'un minimum de transitions soient réalisées pour extraire le signal d'horloge.

Le codage utilisé dans la plupart des réseaux locaux, et notamment dans les réseaux Ethernet, est le codage Manchester, ou sa version Manchester différentiel. Le codage Manchester, dit aussi biphase-L (*biphase-level*), est illustré à la figure 5.10. Il y a toujours une transition par élément binaire, de telle sorte que la valeur du signal passe sans arrêt d'une valeur positive à une valeur négative. Cette transition s'effectue au milieu de l'intervalle.

À la figure 5.10, le 0 est indiqué par une transition allant de haut en bas, tandis que le 1 est indiqué par une transition allant de bas en haut. La figure montre la suite 100110 codée en Manchester. Le signal commence par une polarité négative puis passe à une polarité positive au milieu de l'intervalle. Ce passage d'une polarité négative à une polarité positive s'appelle un front montant. Le 1 est représenté par un front montant et le 0 par un front descendant.

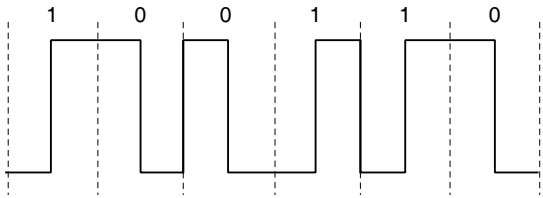


Figure 5.10
Codage Manchester

Le codage Manchester différentiel tient compte du bit précédent, comme l'illustre la figure 5.11. Le bit 0 est représenté par un changement de polarité au début d'un temps bit. Le bit 1 est caractérisé par l'absence de changement de polarité au début d'un temps bit. Ce codage a l'avantage d'être indépendant de la polarité.

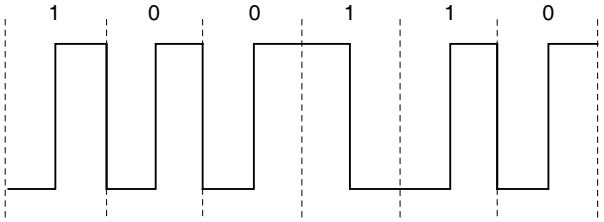


Figure 5.11
Codage Manchester différentiel

Le codage par blocs est une autre méthode très utilisée, en particulier dans les réseaux locaux. Le principe général de ce codage consiste à transformer un mot de *n* bits en un mot de *m* bits, d'où son autre nom de codage *n*B/*m*B. En raison de contraintes technologiques, les valeurs de *n* généralement choisies sont 1, 4 ou 8.

Le principe du codage 1B/2B, ou codage CMI (Codec Mode Indication), est illustré à la figure 5.12. Un signal est émis sur deux temps d'horloge. Le 1 est indiqué par un niveau continu haut puis un niveau continu bas à tour de rôle. La valeur 0 démarre par un niveau continu bas sur le premier signal d'horloge puis se poursuit par un niveau continu haut sur le deuxième signal d'horloge. La suite 1001 représentée sur la figure demande donc huit temps d'horloge pour coder les quatre bits. Les deux premiers temps d'horloge transportent le bit 1, qui correspond à un niveau continu haut. Après les deux bits 00, la valeur 1 est transportée par un niveau continu bas. Le 1 suivant est transporté par un niveau continu haut. Ce codage est facile à implémenter, mais présente l'inconvénient que le signal occupe une double largeur de bande.

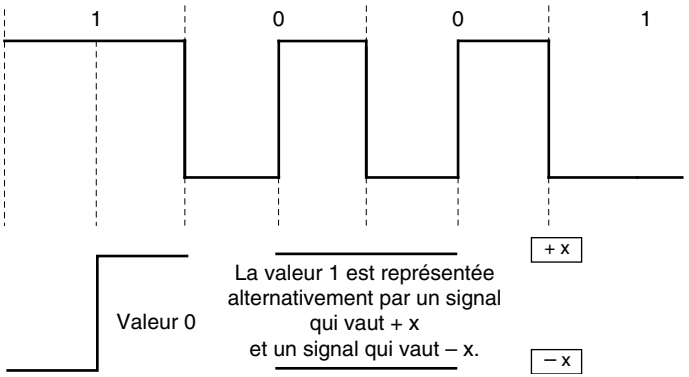


Figure 5.12
Codage CMI

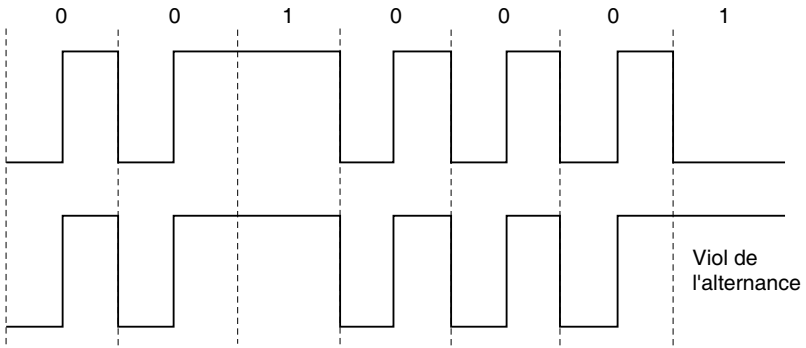


Figure 5.13
Principe du viol de polarité

Les codes *n*B/*m*B ont des propriétés intéressantes. On peut utiliser leurs particularités pour détecter des erreurs de transmission, obtenir des mots interdits ou représenter des séquences particulières, comme des délimiteurs de trames ou des jetons. Par exemple, en mettant deux niveaux haut de suite dans l'exemple précédent on ne représenterait pas la suite 11, mais un mot interdit. Les contrôles d'erreur peuvent s'effectuer en vérifiant que les règles de codage ne sont pas violées. On peut reconnaître une séquence particulière par violation de polarité, c'est-à-dire par le non-respect de l'alternance niveau haut-niveau bas. La figure 5.13 en fournit un exemple.

Numérisation des signaux analogiques

Désormais, la grande majorité des transports d'information s'effectuent en numérique. Les signaux analogiques doivent donc être transformés en une suite d'éléments binaires. La valeur du débit binaire obtenu par la numérisation du signal requiert que la bande passante du support physique soit parfois supérieure à celle nécessaire au transport du signal analogique. Par exemple, la parole téléphonique non compressée, qui demande une bande passante analogique de 3 200 Hz, nécessite un débit numérique de 64 000 bit/s, débit qui ne peut en aucun cas être absorbé par un support physique à 3 200 Hz de bande passante. En effet, le débit maximal acheminé sur une bande de *W* Hz est obtenu par le théorème de Shannon :

$$D = W\log_2(1 + S/B)$$

où S/B est le rapport signal sur bruit exprimé en décibel. Pour un rapport de 10, ce qui est relativement important, on obtient un débit binaire maximal de 10 000 bit/s.

Trois opérations successives doivent être réalisées pour arriver à cette numérisation, l'échantillonnage, la quantification et le codage :

1. **Échantillonnage.** Consiste à prendre des points du signal analogique au fur et à mesure qu'il se déroule. Plus la bande passante est importante, plus il faut prendre d'échantillon par seconde. C'est le théorème d'échantillonnage qui donne la solution : si un signal *f(t)* est échantillonné à intervalle régulier dans le temps et à un taux supérieur au double de la fréquence significative la plus haute, les échantillons contiennent toutes les informations du signal original. En particulier, la fonction *f(t)* peut être reconstituée à partir des échantillons. Cette phase est illustrée à la figure 5.14.

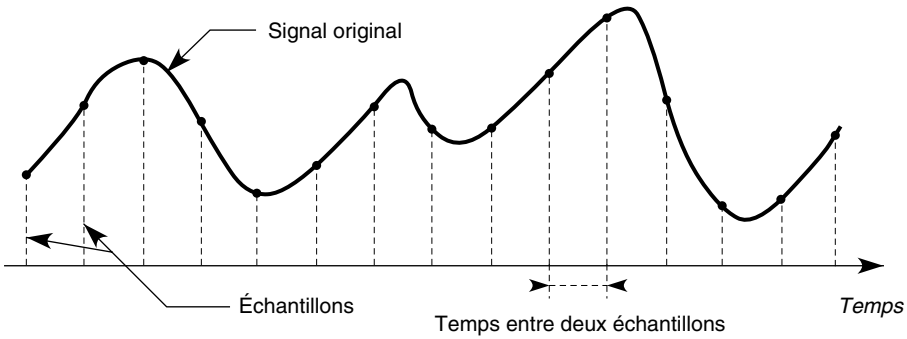


Figure 5.14
Échantillonnage

Si nous prenons un signal dont la largeur de la bande passante est 10 000 Hz, il faut l'échantillonner au moins 20 000 fois par seconde.

2. **Quantification.** Consiste à représenter un échantillon par une valeur numérique au moyen d'une loi de correspondance. Il convient de trouver cette loi de correspondance de telle sorte que la valeur des signaux ait le plus de signification possible. Si tous les échantillons sont à peu près égaux, il faut essayer, dans cette zone délicate, d'avoir plus de possibilités de codage que dans les zones où il y a peu d'échantillons. Pour obtenir une correspondance entre la valeur de l'échantillon et le nombre le représentant, on utilise généralement deux lois, la loi A en Europe et la loi Mu en Amérique du Nord. Ces deux lois sont de type semi-logarithmique, garantissant une précision à peu près constante. Cette phase est illustrée à la figure 5.15.

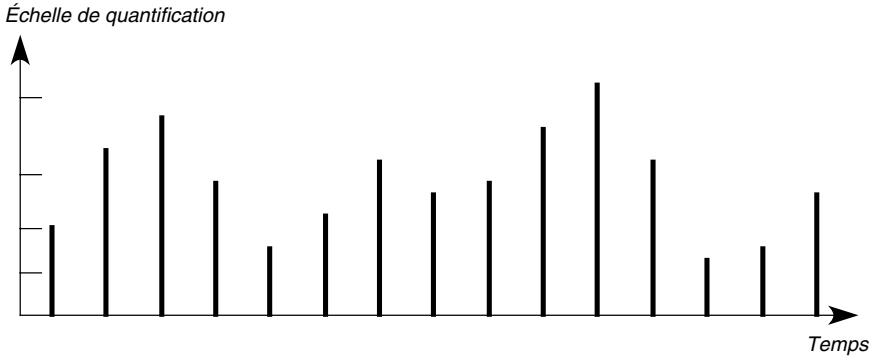


Figure 5.15
Quantification d'un signal échantillonné

3. **Codage.** Consiste à affecter une valeur numérique aux échantillons obtenus lors de la première phase. Ce sont ces valeurs qui sont transportées dans le signal numérique. Cette phase est illustrée à la figure 5.16.

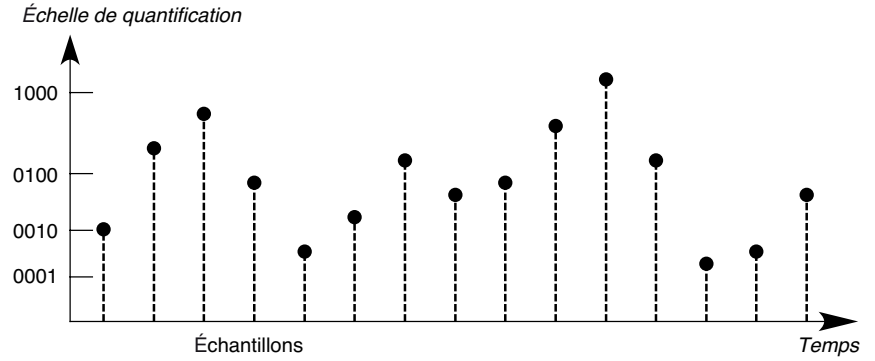


Figure 5.16
Codage

Numérisation de la parole téléphonique

La numérisation de la parole téléphonique s'effectue généralement au moyen des méthodes classiques PCM (Pulse Code Modulation) en Amérique du Nord et MIC (modulation par impulsion et codage) en Europe. Ces méthodes présentent de légères différences, dont la plus visible concerne le débit de sortie, qui est de 56 Kbit/s en Amérique du Nord et de 64 Kbit/s en Europe.

La largeur de bande de la parole téléphonique analogique est de 3 200 Hz. Pour numériser ce signal correctement sans perte de qualité, déjà relativement basse, il faut échantillonner au moins 6 400 fois par seconde. Dans la normalisation, on a adopté la valeur de 8 000 fois par seconde. La quantification s'effectue par des lois semi-logarithmiques. L'amplitude maximale permise se trouve divisée en 128 échelons positifs pour la version PCM, auxquels il faut ajouter 128 échelons négatifs dans la version européenne MIC. Le codage s'effectue soit sur 128 valeurs, soit sur 256 valeurs, ce qui demande, en binaire, 7 ou 8 bits de codage.

La valeur totale du débit de la numérisation de la parole téléphonique est obtenue en multipliant le nombre d'échantillon par le nombre d'échelon. Cela donne :

- 8 000 × 7 bit/s = 56 Kbit/s en Amérique du Nord et au Japon ;
- 8 000 × 8 bit/s = 64 Kbit/s en Europe.

L'échantillonnage a lieu toutes les 125 µs, valeur que nous retrouverons très souvent dans la suite de cet ouvrage.

Tout type de signal analogique peut être numérisé par la méthode générale décrite ci-dessus. On voit que plus la bande passante est importante, plus la quantité d'éléments binaires à transmettre augmente. Pour la parole normale, limitée le plus souvent à 10 000 Hz de bande passante, il faut un flux de 320 Kbit/s si le codage s'effectue sur 16 bits.

D'autres techniques de numérisation de la parole sont également employées. Elles travaillent en temps réel ou en temps différé. Dans le premier cas, l'algorithme qui permet de traduire la loi intermédiaire de quantification est exécuté en temps réel, et les éléments binaires obtenus ne sont pas compressés, ou très peu. Dans le second cas, la parole peut être stockée sur des volumes beaucoup plus faibles, mais le temps nécessaire pour effectuer la décompression est trop long pour régénérer un flot synchrone d'octets et donc le signal analogique de sortie. C'est pourquoi il faut une mémorisation intermédiaire qui enlève l'aspect temps réel de la parole. Pour les messageries numériques, une compression est presque toujours effectuée afin que les capacités de stockage requises ne soient pas trop importantes. Dans ce cas, on descend à des débits inférieurs à 2 Kbit/s.

On peut encore citer dans les techniques temps réel les méthodes Δ (Delta) ou Δ_M (Delta Modulation), qui s'appuient sur le codage d'un échantillon en relation avec le précédent. Par exemple, on peut définir le point d'échantillonnage $k + 1$ par la pente de la droite reliant les échantillons k et $k + 1$, comme illustré à la figure 5.17. On envoie la valeur exacte du premier échantillon, puis on ne transmet que les pentes. Étant donné que la pente de la droite ne donne qu'une approximation du point suivant, il faut régulièrement émettre un nouvel échantillon avec sa valeur exacte.

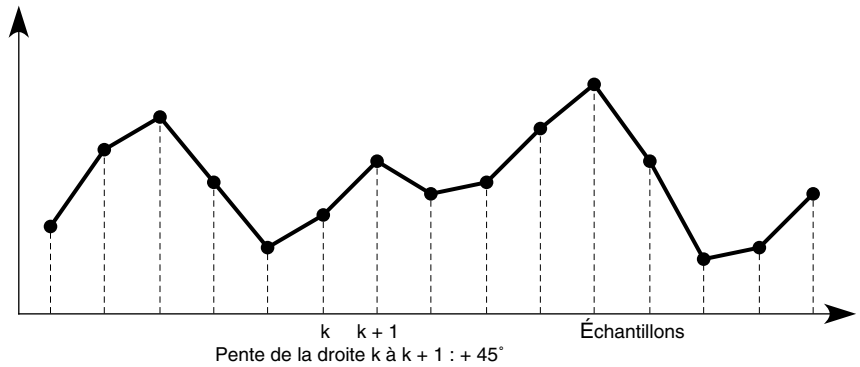


Figure 5.17

Numérisation par une méthode Delta

Grâce à ces méthodes, le débit de la parole numérique peut descendre à 32 ou 16 Kbit/s, voire moins. On peut aller jusqu'à 2 Kbit/s, mais on obtient alors une parole synthétique de qualité médiocre. Nous n'avons parlé dans cette section que de la parole téléphonique. Il va de soi que toutes les informations analogiques peuvent être numérisées de la même façon.

La numérisation de l'image animée suit un processus similaire, l'image étant décomposée en points élémentaires, appelés pixels, et chaque pixel étant codé sur plusieurs bits ou même sur plusieurs octets, si le nombre de couleurs de l'image est élevé. Le tableau 5.2 recense quelques valeurs de débits numériques nécessaires au transport de signaux analogiques numérisés.

Type d'information	Débit du signal numérisé	Débit après compression
Son	64 Kbit/s	1,2 à 9,6 Kbit/s
Images animées noir et blanc/visioconférence	16 Mbit/s	64 Kbit/s à 1 Mbit/s
Images animées couleur/visioconférence	100 Mbit/s	128 Kbit/s à 2 Mbit/s
Images télévision couleur	204 Mbit/s	512 Kbit/s à 4 Mbit/s
Images vidéoconférence	500 Mbit/s	2 Mbit/s à 16 Mbit/s

TABLEAU 5.2 • Débits de quelques signaux numérisés

De très grands progrès ont été réalisés ces dernières années dans le domaine de la compression, qui permettent de réduire considérablement le débit des flots à acheminer. Des expériences de transport d'images animées s'effectuent, par exemple, sur des canaux à 64 Kbit/s. Les équipements terminaux reviennent toutefois encore cher pour les très fortes compressions. Les techniques de codage continuant de progresser très vite, elles représentent une solution pour faire transiter de la vidéo sur des réseaux de mobiles tels que l'UMTS, dans lesquels la bande passante disponible est faible par rapport aux débits envisagés. Les principales d'entre elles sont présentées au chapitre 18.

Les codeurs qui effectuent le passage du signal analogique au signal numérique s'appellent des codecs (codeur-décodeur). Simple à réaliser, le codec MIC est aujourd'hui bon marché. En revanche, les codecs pour signaux analogiques à très large bande passante reviennent encore cher, en raison de la technologie qu'ils emploient.

Détection et correction d'erreur

La détection et la correction des erreurs ont été longtemps automatisées au niveau trame du fait que la qualité des lignes physiques était insuffisante pour obtenir des taux d'erreur acceptables pour les applications s'exécutant sur le réseau. Aujourd'hui, le problème est quelque peu différent, et ce pour deux raisons :

- Le taux d'erreur en ligne est devenu satisfaisant, descendant souvent sous la barre des 10^{-9}, et les quelques erreurs qui subsistent ne modifient pas la qualité de l'application. Cela provient de techniques de codage plus performantes et de l'utilisation de supports physiques tels que la fibre optique.
- Les applications acheminées sont de type multimédia et ne tolèrent pas la perte de temps associée aux reprises sur erreur. La correction des erreurs n'affecte pas la qualité de l'image ou du son. Pour autant que le nombre d'erreurs ne soit pas trop important, l'œil ou l'oreille ne peut détecter des modifications mineures de l'image ou du son. La retransmission est donc une perte de temps inutile. Par exemple, la parole téléphonique, qui demande un temps de transport de 150 ms au maximum, n'autorise pas l'attente de retransmissions. De plus, la correction d'un bit par-ci par-là ne change pratiquement rien à la qualité de la parole.

La détection et la correction des erreurs sont indispensables sur les supports physiques de mauvaise qualité ou pour des applications qui demandent le transport de données précieuses. Dans ce cas, une automatisation au niveau trame ou une reprise particulière au niveau message peuvent être effectuées pour une application particulière. Il est toujours possible d'ajouter au niveau sémantique, la couche 7, ou application, de l'architecture de référence, un processus de correction des erreurs.

Les deux grandes possibilités de reprise sur erreur sont l'envoi de l'information en redondance, qui permet de détecter et de corriger les erreurs dans un même temps, ou l'utilisation seule d'un code détecteur d'erreur, permettant de repérer les trames en erreur et de demander leur retransmission.

Un code à la fois détecteur et correcteur nécessite d'envoyer en moyenne la moitié de l'information transportée en plus. Pour envoyer 1 000 bits en sécurité au récepteur, il faut donc émettre 1 500 bits. Le code détecteur d'erreur demande une zone de 16 bits, parfois de 32 bits. Chaque fois qu'une erreur est détectée, on retransmet l'ensemble de la trame. Pour des trames d'une longueur de 1 000 bits à 10 000 bits, un taux d'erreur bit de l'ordre de 10^{-4} constitue la limite entre les deux méthodes. Un taux inférieur à 10^{-4} rend la technique de détection et de demande de retransmission plus performante que la correction d'erreur seule. Comme la plupart des lignes de communication ont un taux d'erreur bit inférieur à 10^{-4}, c'est pratiquement toujours la méthode de détection et de reprise des trames ou des messages erronés qui est utilisée.

Des cas particuliers, comme la transmission par l'intermédiaire d'un satellite, peuvent être optimisés par une méthode de détection et de correction immédiate. Le temps de l'aller-retour entre l'émetteur et le récepteur étant très long (plus de 0,25 s), les acquittements négatifs réclamant la retransmission prennent 0,5 s après le départ de la trame. Si le débit est de 10 Mbit/s, cela veut dire que 5 Mbit de données ont déjà été transmis, ce qui implique une gestion importante des mémoires tampons de l'émetteur et du récepteur. Même dans le cas d'un satellite, une optimisation est généralement obtenue par des demandes de retransmission.

Avant d'aborder les techniques de détection et de correction proprement dites, penchons-nous sur le fonctionnement d'un protocole de liaison pour montrer les solutions développées pour la reprise sur erreur. L'émetteur formate les trames en ajoutant aux données des champs de supervision, d'adresse, de données et de détection d'erreur, puis il les transmet en en conservant une copie (*voir figure 5.18*) qui se situe dans une mémoire.

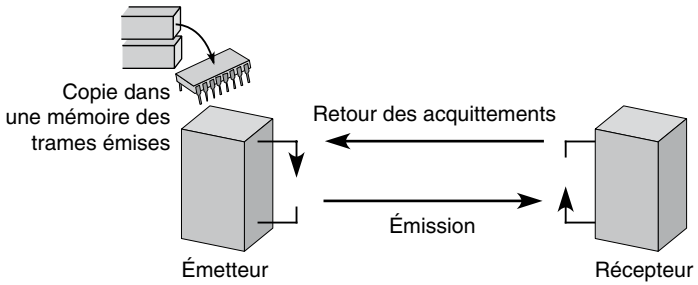


Figure 5.18

Fonctionnement d'un protocole de liaison

Le récepteur émet des acquittements positifs ou négatifs. À chaque acquittement positif, le bloc de données correspondant est détruit. À chaque acquittement négatif, la trame qui n'a pas été correctement reçue est retransmise.

Les politiques d'acquittement et de retransmission les plus utilisées sont les suivantes :

- Les acquittements sont envoyés à chaque trame reçue.
- Les acquittements sont accumulés pour être envoyés tous en même temps.
- Les acquittements sont émis dans les trames transmises dans le sens opposé.
- Seule la trame erronée est retransmise.
- Toutes les trames, à partir de la trame erronée, sont retransmises.

La correction d'erreur

La détection d'erreur suivie d'une retransmission est la solution la plus utilisée en matière de transmission d'information. Une autre solution peut toutefois être mise en œuvre, consistant à détecter et corriger directement les erreurs. Pour corriger, des algorithmes assez complexes sont nécessaires. Surtout, il faut mettre dans le message à transporter

de l'information redondante, qui demande un débit beaucoup plus important. Parmi les techniques de correction, il en existe de simples, qui consistent, par exemple, à envoyer trois fois la même information et à choisir au récepteur l'information la plus probable : à la réception d'un bit qui est deux fois égal à 1 et une fois à 0, on suppose que le bit est égal à 1.

Il existe des techniques plus complexes, telles que FEC (Forward Error Correction), qui consiste à ajouter à chaque bloc de kilobit des bits supplémentaires pour arriver à un total de *n* bits. On appelle un tel code *k*/*n*. Les codes classiquement utilisés correspondent à du 2/3 ou du 1/2, ce qui indique une adjonction respectivement de 50 et 100 % d'informations supplémentaires. Les codages complexes utilisés recourent à de nombreux algorithmes, que nous ne ferons que décrire sommairement. Les algorithmes les plus célèbres sont ceux de Bose-Chaudhuri-Hocquenghem (BCH), Reed-Solomon et les turbocodes.

Supposons que l'information puisse être décomposée en caractères et qu'un caractère comporte 8 bits. On découpe les données 8 bits par 8 bits. Pour pouvoir corriger les erreurs, il faut être capable de distinguer les différents caractères émis, même lorsque ceux-ci ont un bit erroné. Soit un alphabet composé de quatre caractères, 00, 01, 10 et 11.

Si une erreur se produit, un caractère est transformé en un autre caractère, et l'erreur ne peut être détectée. Il faut donc ajouter de l'information pour que les caractères soient différents les uns des autres. Par exemple, on peut remplacer les quatre caractères de base par quatre nouveaux caractères :

- 0000000
- 0101111
- 1010110
- 1111001

De la sorte, si une erreur se produit sur un bit, on peut comparer la donnée transmise avec les quatre caractères ci-dessus et décider que le bon caractère est celui le plus ressemblant. Si le récepteur reçoit la valeur 0010000, on voit tout de suite que le caractère qui aurait dû être reçu est 0000000, puisque l'autre caractère le plus ressemblant que l'on aurait pu recevoir est 0101111, qui présente beaucoup plus de différence avec la valeur reçue.

Si deux erreurs se produisent sur un même caractère, il est impossible dans le contexte décrit de récupérer la valeur exacte. Ce sont là des erreurs dites résiduelles, qui subsistent après la correction.

Formalisons la méthode décrite précédemment. Soit $d(x,y)$ la distance entre les deux caractères x et y définie par :

$$d(x,y) = \sum_{i=1}^{N} (x_i - y_i) \bmod 2$$

où N est le nombre de bits du caractère et x_i, y_i sont les différentes valeurs des N bits ($i = 1... N$).

La distance de Hamming est définie par la formule :

$$d_H = \inf d(x,y)$$

où la borne inférieure s'applique à l'ensemble des caractères de l'alphabet.

Dans le premier exemple, la distance de Hamming est égale à 1. Dans le nouvel alphabet, qui a été déterminé pour corriger les erreurs, $d_H = 3$. Pour pouvoir détecter et corriger une seule erreur, il faut que les différents caractères du même alphabet satisfassent à $d_H = 3$ de sorte que, en cas d'erreur, la distance entre le caractère erroné et le caractère exact soit de 1. On déduit le caractère supposé exact en recherchant le caractère dont la distance est de 1 par rapport au caractère erroné. On comprend que si la distance de Hamming est de 2 pour un alphabet, on ne peut décider du caractère le plus proche.

Si l'on veut corriger deux erreurs simultanément, il est nécessaire d'avoir une distance de Hamming égale à 5. En reprenant l'exemple précédent, on peut remplacer les quatre caractères par :

- 0000000000
- 0101111011
- 1010110101
- 1111001110

Avec ce nouvel alphabet, la distance de Hamming est de 5. Si le caractère 10001010 est reçu, on en déduit que le caractère émis est 11001110 puisque que $d(10001010,11221112) = 2$ et que $d(10001010,x) > 2$ si $x \neq 11001110$.

Ces exemples donnent l'impression que l'on ajoute beaucoup d'information pour chaque caractère. C'est vrai lorsque l'alphabet est composé de peu de caractères et qu'ils sont courts. S'il y a beaucoup de caractères, le nombre d'information à ajouter est proportionnellement bien inférieur.

La détection d'erreur

Il existe de nombreuses techniques de détection d'erreur. Le bit de parité, par exemple, est un bit supplémentaire ajouté au caractère positionné de telle façon que la somme des éléments binaires modulo 2 soit égale à 0 ou à 1. Ce bit de parité est déterminé à partir d'un caractère — on prend souvent un octet — composé soit de bits successifs, soit de bits que l'on détermine de façon spécifique. Cette protection est assez peu performante, puisqu'il faut ajouter 1 bit tous les 8 bits, si le caractère choisi est un octet, et que deux erreurs sur un même octet ne sont pas détectées.

Les méthodes les plus utilisées s'effectuent à partir d'une division de polynômes. Supposons que les deux extrémités de la liaison possèdent en commun un polynôme de degré 16, par exemple $x^{16} + x^8 + x^7 + 1$. À partir des éléments binaires de la trame notés a_i, $i = 0..., M - 1$, où M est le nombre de bit formant la trame, on constitue le polynôme de degré $M - 1$ suivant :

$$M - 1 : P(x) = a_0 + a_1 x + ... + a_{M-1} x^{M-1}$$

Ce polynôme est divisé dans l'émetteur par le polynôme générateur de degré 16. Le reste de cette division est d'un degré maximal de 15, qui s'écrit sous la forme suivante :

$$R(x) = r_0 + r_1\, x + ... + r_{15}x^{15}$$

Les valeurs binaires r_0, r_1... r_{15} sont placées dans la trame, dans la zone de détection d'erreur. À l'arrivée, le récepteur effectue le même algorithme que l'émetteur en définissant un polynôme formé par les éléments binaires reçus et de degré $M - 1$. Il effectue la division par le polynôme générateur et trouve un reste de degré 15, qui est comparé à celui qui figure dans la zone de contrôle d'erreur. Si les deux restes sont identiques, le récepteur en déduit que la transmission s'est bien passée. En revanche, si les deux restes sont différents, le récepteur en déduit une erreur dans la transmission et demande la retransmission de la trame erronée.

Cette méthode permet de trouver pratiquement toutes les erreurs qui se produisent sur le support physique. Cependant, si une erreur se glisse dans la zone de détection d'erreur, on conclut à une erreur, même si la zone de données a été correctement transportée, puisque le reste calculé par le récepteur est différent de celui transporté dans la trame. Si la trame fait 16 000 bits, c'est-à-dire si elle est mille fois plus longue que la zone de détection d'erreur, on ajoute une fois sur 1 000 une erreur due à la technique de détection elle-même.

L'efficacité de la méthode décrite dépend de nombreux critères, tels que la longueur de la zone de données à protéger ou de la zone de contrôle d'erreur, le polynôme générateur, etc. On estime qu'au moins 999 erreurs sur 1 000 sont ainsi corrigées. Si le taux d'erreur sur le médium est de 10^{-6}, il devient 10^{-9} après le passage par l'algorithme de correction, ce qui peut être considéré comme un taux d'erreur résiduelle négligeable.

La zone de détection d'erreur est parfois appelée CRC (Cyclic Redundancy Check), nom générique de la méthode décrite ci-dessus, et parfois FCS (Frame Check Sequence), ou séquence d'éléments binaires engendrée par le contenu de la trame.

Les turbocodes forment une classe de solutions permettant de détecter et de corriger des erreurs en ligne en utilisant simultanément deux codes qui, individuellement, ne donneraient pas de résultat extraordinaire. Les turbocodes apportent ainsi une nouvelle méthode de codage à deux dimensions extrêmement efficace pour la correction d'erreur.

Les architectures de la niveau physique

Nous avons décrit jusqu'à présent les propriétés du niveau physique, dont le rôle est de faire transiter des bits sur le médium de transport. Les architectures de la couche physique sont déterminées par les solutions mises en place pour transporter les messages d'une machine terminale à une autre en n'utilisant que la couche physique. Par exemple, la téléphonie classique utilise une architecture de ce niveau dans laquelle le flot des signaux est émis directement sur un circuit et transite de bout en bout.

Plusieurs architectures de niveau physique peuvent être conçues. Dans les architectures de transport relativement lentes, il n'est pas nécessaire de synchroniser sans arrêt les horloges extrémité, comme la communication entre deux machines utilisant un modem.

En revanche, dans les architectures de transport à très haute vitesse, il faut mettre en place un mécanisme permettant de resynchroniser les horloges sans arrêt. Si la vitesse de transport est de 10 Gbit/s, par exemple, il faut émettre un bit toutes les 100 picosecondes. Il faut donc que le récepteur enregistre la valeur du signal toutes les 100 picosecondes. Si les horloges émetteur et récepteur ne sont pas parfaitement synchronisées, le récepteur risque de lire deux fois le même signal ou de sauter un signal au bout de quelque temps.

Comme expliqué en début de chapitre, la vitesse de synchronisation normalisée est de 125 µs. Cette valeur historique correspond à la vitesse de numérisation de la parole téléphonique. Cela revient à dire qu'il faut synchroniser le récepteur sur l'émetteur pour la réception d'un octet de téléphonie toutes les 125 µs, et plus précisément d'un bit toutes les 15,625 µs. Lorsque le flot a un débit de 64 Kbit/s, la synchronisation doit s'effectuer tous les 8 bits. Lorsque la vitesse est de 10 Gbit/s, la synchronisation s'effectue tous les 1 250 000 bits.

Pour réaliser ces synchronisations, le temps est découpé en tranches de 125 µs. Dans ce laps de temps, l'ensemble des bits transmis représente une trame. Le mot trame a ici le même sens que pour l'entité de la couche 2 qui permet de déterminer le début et la fin d'une émission d'un bloc de données. En un certain sens, il est normal d'utiliser ce même mot puisque la trame de la couche physique permet également de déterminer un début et une fin correspondant à la période de 125 µs et donc de synchroniser les horloges. La trame de la couche physique, que l'on retrouve dans la plupart des réseaux de mobiles et sans fil, est généralement nécessaire dès que la vitesse augmente ou que le support n'est pas de très bonne qualité pour bien ajuster les temps d'écoute des signaux.

Les architectures de la couche physique peuvent offrir d'autres fonctionnalités, comme la fiabilisation des communications, qui permet de reconfigurer le réseau dans des laps de temps très courts de façon que les machines terminales ne s'aperçoivent pas qu'il y a eu coupure de la communication. Pour cela, il doit y avoir redondance dans le support physique, à la manière des systèmes en boucle, pour permettre au signal de passer dans l'autre sens de la boucle en cas de défaillance du premier chemin. La technique de resynchronisation fait partie des fonctionnalités incluses dans l'architecture de la couche physique.

Nous retrouverons ces architectures de la couche physique à la partie IV de l'ouvrage quand nous aborderons les réseaux optiques, qui se développent très vite et formeront bientôt l'ossature des cœurs de réseau, et les interfaces avec la couche physique, qui utilisent la structure en trame et sont véhiculées sur le médium pour communiquer avec l'autre extrémité de la liaison.

Conclusion

La couche physique est indispensable à un réseau. Comme nous l'avons vu, elle concerne tous les équipements qui permettent de transporter des trames d'un point à un autre. Les caractéristiques d'un réseau dépendent fortement de son ossature physique. La couche physique doit gérer tous les éléments nécessaires pour que les signaux

partant de l'utilisateur arrivent au récepteur, comme le codage, les modulations et démodulations ou la transformation des signaux analogiques en signaux numériques.

Cette couche évolue lentement, car les équipements de ce niveau déjà en place ne peuvent être facilement remplacés. Cependant, l'augmentation des débits sur les lignes physiques montre bien la dynamique de ce niveau.

Ce niveau prend également en charge les architectures dans lesquelles l'information est transportée de bout en bout sous la forme d'éléments binaires. Les plus connues d'entre elles viennent du monde SONET/SDH (*voir le chapitre 13*), mais l'arrivée massive des composants Ethernet à ce niveau permet de penser que le très proche avenir verra naître de nouvelles solutions.

6

Le niveau trame

Comme expliqué au chapitre 2, le niveau trame est le niveau où circule l'entité appelée trame. Une trame est une suite d'éléments binaires qui ont été rassemblés pour former un bloc. Ce bloc doit être transmis vers le nœud suivant de telle sorte que le récepteur soit capable de reconnaître son début et sa fin. En résumé, le rôle du niveau trame consiste à transporter de l'information sur un support physique entre un émetteur et un récepteur. Sa fonction principale est de détecter les débuts et les fins des trames.

Le niveau trame est fondamentalement différent suivant que l'on a affaire à un réseau de niveau trame, c'est-à-dire un réseau qui ne remonte dans les nœuds intermédiaires qu'à la couche 2, ou couche liaison, pour router ou commuter, ou de niveau paquet, c'est-à-dire un réseau qui doit remonter jusqu'à la couche 3, ou couche réseau, pour effectuer le transfert. Dans une architecture de niveau trame, l'en-tête contient les zones qui permettent d'acheminer la trame vers le destinataire du message. Dans une architecture de niveau paquet, la zone de données de la trame contient un paquet. Les informations nécessaires à l'acheminement du message se trouvent dans les zones de supervision de ce paquet.

Ce chapitre présente les principales trames qui permettent de transporter des paquets dans une architecture de niveau trame, PPP, Ethernet et ATM. Le protocole HDLC, qui a été très populaire pendant la période de domination de X.25 et qui a quasiment disparu aujourd'hui, est détaillé à l'annexe F. Ce standard HDLC est cependant important car il reste un modèle pour bien comprendre toutes les fonctionnalités de ce niveau.

La trame la plus importante est la trame Ethernet. C'est elle qui domine le monde des petits réseaux et des réseaux d'entreprise. Elle a également pris une place sans partage dans les liaisons de type ADSL et dans les réseaux sans fil. Elle est en train de devenir également le standard des réseaux d'opérateurs.

Nous nous penchons également dans l'annexe F sur l'ancienne génération de niveau trame, appelée niveau liaison, dont la fonction était à la fois de jouer le rôle du niveau

trame et de corriger les erreurs en ligne afin de rendre le taux d'erreur acceptable pour les couches supérieures. Dans ce dernier cas, une zone de détection d'erreur est ajoutée à la fin de la trame afin de déceler si une erreur s'est produite durant le transfert. Si tel est le cas, deux méthodes peuvent être mises en œuvre pour effectuer les réparations. Dans la première, des bits de contrôle ajoutés par l'émetteur permettent de détecter puis de corriger les erreurs. Dans la seconde, une retransmission est demandée au nœud précédent, qui doit avoir gardé une copie de la trame.

L'architecture de niveau trame

Le niveau trame (couche 2) a pour fonction de rendre un service au niveau juste supérieur, c'est-à-dire à le niveau paquet (couche 3). Ce service concerne le transport des paquets de nœud à nœud. Plus précisément, son rôle est de transporter un paquet de la couche 3 ou un fragment de message de la couche 4 d'un nœud vers un autre nœud. Pour cela, le niveau trame demande à son tour au niveau juste inférieur, le niveau physique, un service, consistant à transporter les bits de la trame d'un nœud à un autre nœud. Cette section présente les fonctions nécessaires à la réalisation de toutes ces actions.

Les fonctionnalités du niveau trame

La spécificité du niveau trame est de transmettre les informations le plus rapidement possible entre deux nœuds. La partie importante des protocoles de niveau trame réside dans la structure de la trame et dans la façon de la reconnaître et de la traiter dans le temps le plus court possible.

La première fonctionnalité à implémenter concerne la reconnaissance du début et de la fin de la trame lorsque le flot d'informations binaires arrive au récepteur. Comment reconnaître le dernier bit d'une trame et le premier bit de la trame suivante ? Plusieurs générations de protocoles se sont succédé pour tenter d'apporter la meilleure réponse à ce problème :

- La première génération de protocoles de niveau trame comportait une reconnaissance par drapeau : le début et la fin de la trame étaient reconnaissables par la présence d'une suite d'éléments binaires, qui devait être unique. à cet effet, des techniques d'insertion étaient utilisées pour casser les suites qui ressembleraient à un champ de début ou de fin, appelé drapeau, ou fanion (flag). L'insertion de bits supplémentaires présente toutefois un inconvénient, puisque la longueur totale n'est plus connue à l'avance et que des mécanismes spécifiques sont requis pour ajouter ces bits à l'émetteur puis les retrancher au récepteur.
- La deuxième génération a essayé de trouver d'autres modes de reconnaissance, principalement des violations de codes ou des systèmes utilisant des clés pour repérer le début et la fin d'une trame. L'avantage de ces techniques est de conférer à la trame une longueur déterminée et de ne perdre aucun temps de latence à son arrivée.
- La tendance de la génération actuelle consiste à revenir à la première solution, mais avec un drapeau suffisamment long pour que la probabilité de retrouver la même suite d'éléments binaires soit quasiment nulle. L'avantage de cette solution est de permettre

une reconnaissance très simple du drapeau sans avoir à ajouter de bits ni à calculer la valeur d'une clé. La trame Ethernet correspond à cette définition grâce à un drapeau, appelé préambule, d'une longueur de 64 bits.

Les fonctionnalités du niveau trame ont été fortement modifiées depuis le début des années 1990. On a fait, par exemple, redescendre dans ce niveau les fonctions de la couche 3 (réseau), ou niveau paquet, en vue de simplifier l'architecture et d'augmenter les performances. Le niveau trame jouait dès lors le rôle de cette couche réseau et non plus celui de la couche 2 (liaison), pour lequel il avait été initialement conçu, acquérant un statut capital dans l'acheminement des données jusqu'au récepteur.

La figure 6.1 illustre les rôles potentiels du niveau trame par rapport au modèle de référence.

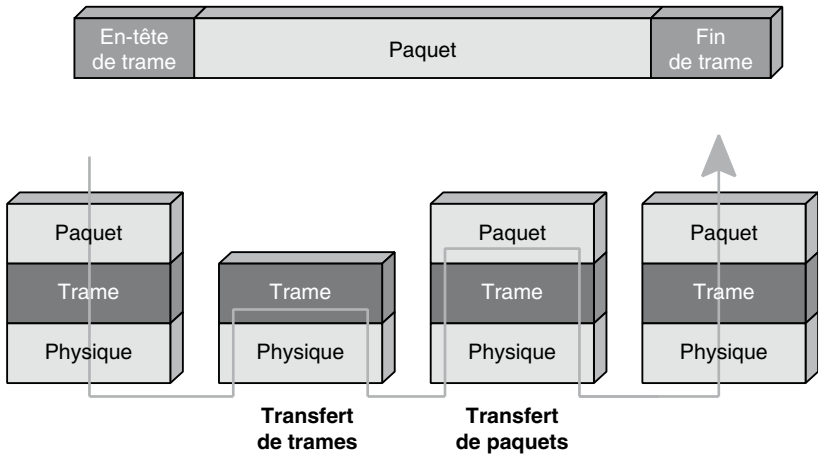


Figure 6.1

Rôles potentiels du niveau trame par rapport au modèle de référence

Les principaux protocoles utilisés par le niveau trame sont les suivants :

- Les protocoles issus de la normalisation internationale dans les années 1980 ou y prenant naissance, tels le protocole de base HDLC, ainsi que ses dérivés LAP-B (Link Access Procedure-Balanced), LAP-D (Link Access Procedure for the D-channel), et LAP-F.
- Le protocole PPP (Point-to-Point Protocol), qui permet de transporter un paquet IP d'une machine vers une autre machine. Ce protocole est fortement utilisé dans le cadre des réseaux personnels pour relier par exemple deux PC entre eux.
- Les protocoles provenant de la commutation de trames Ethernet : plusieurs protocoles sont utilisés dans ce cadre en fonction de ce qui est recherché. Globalement, on trouve le protocole Ethernet partagé et Ethernet commuté.
- La trame ATM est encore utilisée dans les réseaux d'opérateur, mais elle est en forte chute de par l'omniprésence de la trame Ethernet.

Le niveau trame peut avoir pour fonction supplémentaire la gestion de l'accès au support physique, comme dans les réseaux possédant un support de communication partagé. On parle alors de fonction MAC (Medium Access Control).

L'adressage de niveau trame

Comme indiqué précédemment, le niveau trame est issu de la couche 2 (liaison) du modèle de référence. L'adressage n'a donc pas particulièrement été étudié, puisqu'il devait être pris en compte par la couche 3 (réseau). En règle générale, les adresses utilisées sont très simples : une pour l'émetteur et une pour le récepteur. On peut rendre ce modèle plus complexe en introduisant une liaison non plus point-à-point, mais multipoint, dans laquelle plusieurs machines se partagent un même support.

La première adresse pour réseaux multipoint apparue dans le niveau trame provient de l'environnement Ethernet et plus particulièrement des réseaux Ethernet partagés. Comme tous les clients d'un réseau local Ethernet partagé se connectent sur un même câble, lorsqu'une station émet, chaque station peut recevoir une copie. C'est ce qu'on appelle la fonction de diffusion. Les adresses sont apparues dans ce cadre, car il fallait qu'une station puisse distinguer une trame qui lui était destinée d'une trame destinée à un autre utilisateur. L'adressage Ethernet est ainsi né de préoccupations locales. On parle souvent d'adressage physique parce que l'adresse se trouve dans la carte de connexion. Il fallait éviter que deux cartes, même venant de constructeurs différents, aient une même adresse. Comme nous le verrons au chapitre 14, consacré aux réseaux Ethernet, l'adresse a pris une structure plate, ou absolue. Chaque constructeur de carte Ethernet possède un numéro constructeur sur 3 octets. À cette valeur, il suffit d'ajouter un numéro de série, sur 3 octets également, pour obtenir une adresse unique. Puisqu'il y a diffusion sur le réseau local partagé, il est facile de déterminer où se trouve physiquement l'adresse du récepteur.

De nouveaux problèmes ont surgi avec l'arrivée de la nouvelle génération Ethernet remplaçant le mode diffusion par une fonction de transfert de trames, appelée commutation Ethernet. La référence utilisée pour cette commutation est tout simplement l'adresse sur 6 octets de la carte du destinataire. Une zone supplémentaire dans la trame Ethernet a été ajoutée pour disposer d'une vraie référence, indépendante de l'adresse Ethernet. Cette zone portant le *shim label* est notamment utilisée dans les réseaux MPLS.

La cellule ATM se place aussi au niveau trame : on détecte le début de la cellule en comptant le nombre de bits reçus puisque la cellule ATM a une longueur constante. En cas de perte de synchronisation, il est toujours possible de retrouver le premier bit d'une cellule grâce au champ de détection et de correction d'erreur, qui se trouve dans l'en-tête. ATM utilisant un mode commuté, l'en-tête contient une référence.

Les protocoles de niveau trame

Les protocoles définissent les règles à respecter pour que deux entités puissent communiquer de façon coordonnée. Pour cela, il faut que les deux entités communicantes utilisent le même protocole. Pour simplifier les communications de niveau trame, de nombreux protocoles ont été normalisés. Le plus ancien, HDLC, n'est quasiment plus utilisé mais reste un bon exemple de procédure de niveau trame.

Un protocole de niveau trame que l'on utilise souvent sans le savoir est PPP, qui permet de relier deux PC entre eux. Nous allons le décrire succinctement dans la suite. Nous terminerons par le protocole ATM, qui entre dans sa phase de décroissance, mais qui est encore fortement utilisé, et par la trame Ethernet, dont on prédit qu'elle occupera l'ensemble du marché à partir de 2015.

Le protocole PPP (Point-to-Point Protocol)

PPP est utilisé dans les liaisons d'accès au réseau Internet ou sur une liaison entre deux équipements, qu'ils soient des ordinateurs personnels ou des nœuds de réseau. Son rôle est essentiellement d'encapsuler un paquet IP afin de le transporter vers le nœud suivant.

Tout en étant fortement inspiré du protocole HDLC, sa fonction consiste à indiquer le type des informations transportées dans le champ de données de la trame. Le réseau Internet étant multiprotocole, il est important de savoir détecter, par un champ spécifique de niveau trame, l'application qui est transportée de façon à pouvoir l'envoyer vers la bonne porte de sortie.

La trame du protocole PPP ressemble à celle de HDLC. Un champ déterminant le protocole de niveau supérieur vient s'ajouter juste derrière le champ de supervision. La figure 6.2 illustre la trame PPP.

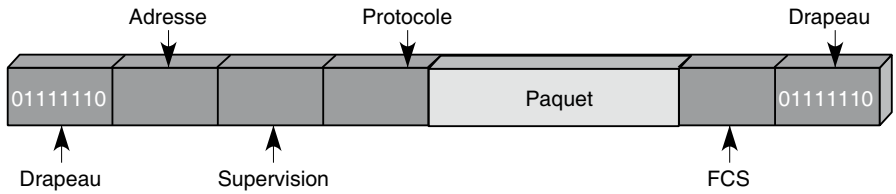


Figure 6.2

Structure de la trame PPP

Les valeurs les plus classiques du champ de protocole sont les suivantes :

- 0x0021 : protocole IPv4 ;
- 0x002B : protocole IPX (Internetwork Packet eXchange) ;
- 0x002D : TCP/IP en-tête compressé ;
- 0x800F : protocole IPv6.

Les fonctionnalités de PPP étant très semblables à celles du protocole HDLC, nous convions les lecteurs à se reporter à l'annexe F.

La trame Ethernet

La trame Ethernet a été conçue pour transporter des paquets dans les réseaux d'entreprise au moyen d'une méthode originale de diffusion sur un réseau local. Cette solution a

donné naissance aux réseaux Ethernet partagés, dans lesquels la trame est émise en diffusion et où seule la station qui se reconnaît a le droit de recopier l'information. À cette solution de diffusion s'est ajoutée la commutation Ethernet.

Avant de se pencher sur les divers types de commutations Ethernet, indiquons qu'Ethernet utilise bien une trame puisque le bloc Ethernet est précédé d'une succession de 8 octets commençant par 10101010101010101, et ainsi de suite jusqu'à la fin du huitième octet, qui se termine par 11. Ce préambule est suffisamment long pour garantir qu'il ne soit pas possible de retrouver la même succession entre deux préambules, la probabilité de retrouver cette succession étant de $1/2^{64}$.

La structure de la trame Ethernet a été normalisée par l'IEEE (Institute of Electrical and Electronics Engineers), après avoir été défini à l'origine par le triumvirat d'industriels Xerox, Digital et Intel. Deux trames Ethernet coexistent donc, la version primitive du triumvirat fondateur et celle de la normalisation par l'IEEE. Le format de ces deux trames est illustré à la figure 6.3.

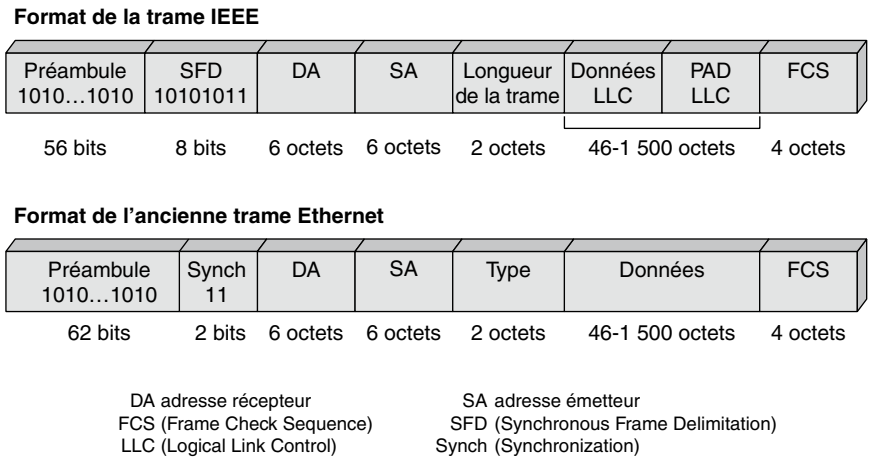


Figure 6.3

Format des deux types de trames Ethernet

Dans le cas de la trame IEEE, le préambule est suivi d'une zone de début de message, appelée SFD (Start Frame Delimiter), dont la valeur est 10101011. Dans l'ancienne trame, il est suivi de 2 bits de synchronisation. Ces deux séquences sont en fait identiques, et seule la présentation diffère d'une trame à l'autre.

La trame contient l'adresse de l'émetteur et du récepteur, chacune sur 6 octets. Ces adresses sont dotées d'une forme spécifique du monde Ethernet, conçue de telle sorte qu'il n'y ait pas deux coupleurs dans le monde qui possèdent la même adresse. Dans cet adressage, dit plat, les trois premiers octets correspondent à un numéro de constructeur, et les trois suivants à un numéro de série. Dans les trois premiers octets, les deux bits initiaux ont une signification particulière. Positionné à 1, le premier bit indique une adresse

de groupe. Si le deuxième bit est également à la valeur 1, cela indique que l'adresse ne suit pas la structure normalisée.

Regardons dans un premier temps la suite de la trame IEEE. La zone Longueur (Length) indique la longueur du champ de données provenant de la couche supérieure. La trame encapsule ensuite le bloc de niveau trame proprement dit, ou trame LLC (Logical Link Control). Cette trame encapsulée contient une zone PAD, qui permet de remplir le champ de données de façon à atteindre la valeur de 46 octets, qui est la longueur minimale que doit atteindre cette zone pour que la trame totale fasse 64 octets en incluant les zones de préambule et de délimitation.

L'ancienne trame Ethernet comporte en outre un type, qui indique comment se présente la zone de données (Data). Par exemple, si la valeur de cette zone est 0800 en hexadécimal, cela signifie que la trame Ethernet transporte un paquet IP.

La détection des erreurs est assurée par le biais d'un polynôme générateur $g(x)$ selon la formule :

$$g(x) = x^{32} + x^{26} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1$$

Ce polynôme donne naissance à une séquence de contrôle (CRC) sur 4 octets.

Pour se connecter au réseau Ethernet, une machine utilise un coupleur, c'est-à-dire une carte que l'on insère dans la machine et qui supporte le logiciel et le matériel réseau nécessaires à la connexion.

Comme nous l'avons vu, la trame Ethernet comporte un préambule. Ce dernier permet au récepteur de synchroniser son horloge et ses divers circuits physiques avec l'émetteur, de façon à réceptionner correctement la trame. Dans le cas d'un réseau Ethernet partagé, tous les coupleurs du réseau enregistrent la trame au fur et à mesure de son passage. Le composant électronique chargé de l'extraction des données incluses dans la trame vérifie la concordance entre l'adresse de la station de destination portée dans la trame et l'adresse du coupleur. S'il y a concordance, le paquet est transféré vers l'utilisateur après vérification de la conformité de la trame par le biais de la séquence de contrôle.

La commutation Ethernet

Plusieurs sortes de commutations Ethernet se sont succédé. La première, qui est très répandue dans les entreprises, consiste à se servir de l'adresse MAC sur 6 octets comme d'une référence unique sur tout le chemin qui mène à la carte coupleur Ethernet. Toutes les trames qui se servent de la même référence vont au même endroit, c'est-à-dire à la carte coupleur qui possède l'adresse MAC indiquée. Cela signifie que tous les commutateurs du réseau doivent posséder une table de commutation, appelé « *lookup table* » , comportant autant de lignes que de cartes Ethernet à atteindre.

Les mises à jour de ces fichiers sont complexes, car il faut ajouter ou retrancher des lignes sur l'ensemble des commutateurs du réseau pour toutes les cartes Ethernet qui s'activent ou se désactivent. La reconnaissance des adresses s'effectue par apprentissage. Lorsqu'une trame entre dans un nœud et que ce nœud ne possède pas l'adresse source de la trame dans sa table de commutation, le nœud ajoute une ligne à sa table, indiquant la nouvelle référence et la direction d'où vient la trame.

Lorsqu'une trame arrivant dans un nœud ne trouve pas dans la table de commutation (*lookup table*) l'adresse du destinataire, la solution est d'émettre la trame en diffusion de telle sorte que le récepteur finisse par la recevoir.

Malgré ces solutions d'apprentissage automatique, la commutation Ethernet n'a pu se développer sur les très grands réseaux. En effet, la gestion des tables de commutation devenait vite trop contraignante. On a là l'exemple d'un réseau commuté sans véritable système de signalisation. Cette solution s'est fortement développée dans les réseaux d'entreprise, en structurant le réseau en plusieurs sous-réseaux de façon à éviter les inondations de trames lorsque la table de commutation est incomplète.

La seconde solution de commutation a été apportée par MPLS. Elle est présentée en détail au chapitre 15. Elle consiste à introduire dans la trame Ethernet une référence spécifique, le *shim label*, ou *shim* MPLS, dans une nouvelle zone ajoutée à la trame Ethernet derrière l'adresse MAC.

La trame Ethernet est commutée de façon classique en utilisant la ligne d'entrée et la référence. Pour cela, il faut mettre en place les références tout le long du chemin. Les trames se succèdent en restant dans l'ordre d'émission. C'est pourquoi une signalisation explicite est indispensable dans ce type de réseau. MPLS a adopté le réseau IP comme système de signalisation. Cette solution a été étendue dans la technique dite *label-switching*, que nous présentons ci-dessous.

Le label-switching

Les technologies commutées demandent une référence (*label*) pour permettre aux blocs de données, que ce soit des trames, des paquets ou d'autres entités, d'avancer dans le réseau. L'ensemble de ces techniques est appelé aujourd'hui label-switching, ou commutation de références. En font partie les trames ATM et Ethernet, qui utilisent une commutation sur une référence, ainsi que toutes les techniques qui peuvent gérer une référence ou auxquelles on peut ajouter une référence.

L'introduction de références dans le label-switching est illustrée à la figure 6.4.

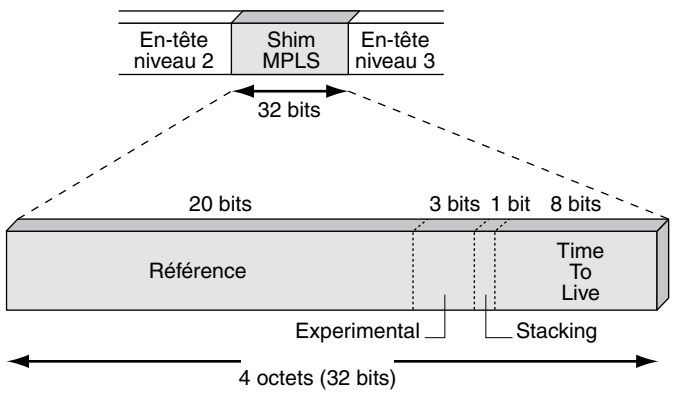


Figure 6.4

Introduction de références dans le label-switching

La référence se trouve dans un champ appelé Shim MPLS, ou dérivation MPLS, que nous détaillons au chapitre 15. Ce champ contient la référence elle-même ainsi qu'un champ de 3 bits appelé Experimental et destiné aux équipementiers, un bit appelé Stacking, qui permet d'empiler les références, c'est-à-dire de mettre plusieurs Shim MPLS de suite entre l'en-tête de niveau trame (couche 2) et celui du niveau paquet (couche 3), et un dernier champ, dit TTL (Time To Live), sur 8 bits, qui définit le temps au bout duquel le paquet sera détruit.

D'autres types de références peuvent être introduits, comme le numéro de la longueur d'onde d'une fibre optique dans un système à multiplexage en longueur d'onde ou le numéro d'une fibre optique ou d'un câble métallique dans un faisceau de plusieurs dizaines ou centaines de câbles. Ces dernières solutions sont explicitées à la section du chapitre 15 consacré à GMPLS.

Le protocole ATM

L'idée de réaliser un réseau extrêmement puissant avec une architecture de niveau trame (couche 2), susceptible de prendre en charge les applications multimédias, a vu le jour vers le milieu des années 1980. De là est né le protocole ATM et sa trame, d'une longueur constante de 53 octets, comme illustré à la figure 6.5.

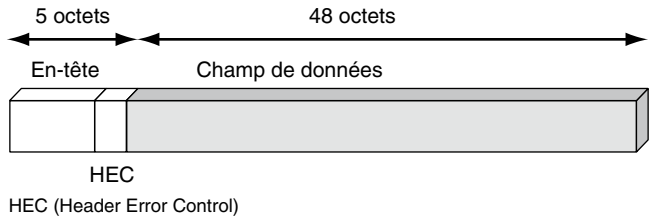


Figure 6.5

Structure de la trame ATM

Cette longueur constante de 424 bits permet de découvrir les débuts et les fins de trame en se contentant de comptabiliser le nombre de bit reçus. En cas de perte de la synchronisation trame, il est possible de découvrir le début d'une trame ATM en utilisant la zone HEC (Header Error Control), le cinquième octet de la zone d'en-tête, lequel permet en outre de corriger une erreur dans l'en-tête.

La zone HEC porte une clé sur 8 bits, qui est assez complexe à manipuler. La perte de synchronisation entraîne un important travail. À l'arrivée de chaque élément binaire, il faut en effet effectuer une division polynomiale pour regarder si le reste correspond à la valeur indiquée dans la zone HEC. En dépit de l'augmentation actuelle des débits, il devient pour cette raison difficile de dépasser 1 Gbit/s sur une liaison ATM.

L'en-tête de la trame ATM comporte une référence, qui permet de commuter les trames de nœud en nœud. Aux extrémités du réseau, il faut encapsuler les données utilisateur, qui proviennent d'applications diverses, allant de la parole téléphonique au transfert de

données, dans le champ de données de 48 octets. Cette décomposition du message en fragments de 48 octets s'effectue dans la couche AAL (ATM Adaptation Layer), de telle sorte que le message, une fois découpé, soit rapidement commuté sur le circuit virtuel jusqu'à l'équipement distant.

Le système de signalisation constitue le dernier élément de l'environnement commuté. Il permet d'ouvrir et de fermer le circuit virtuel. Issu d'extensions du système de signalisation du monde téléphonique, le circuit virtuel de la technique de transfert ATM est propre à cette technologie. Nous ne l'explicitons pas ici mais en donnons quelques éléments à l'annexe K.

L'en-tête de la trame ATM

Les 5 octets de supervision de la trame ATM formant l'en-tête (Header) sont illustrés à la figure 6.6. Nous en détaillons les fonctionnalités ultérieurement dans ce chapitre.

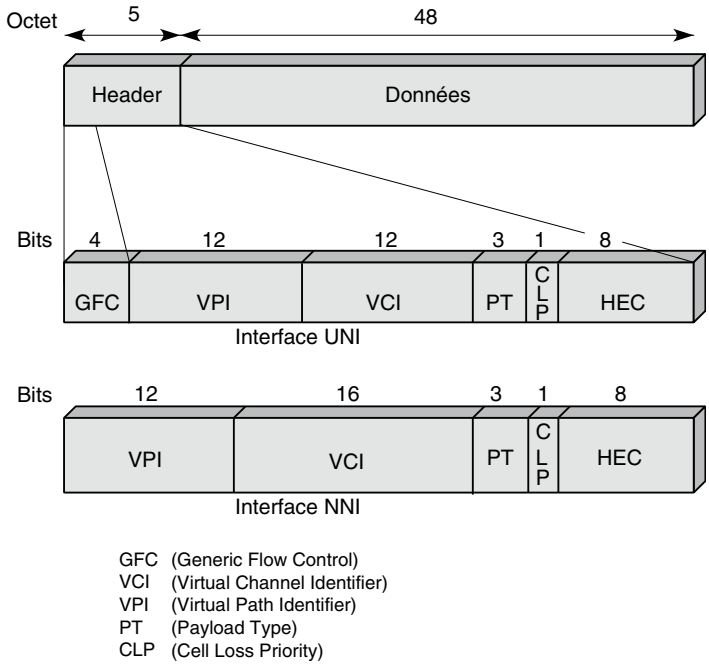


Figure 6.6

Format de l'en-tête de la cellule ATM

Les bits GFC (Generic Flow Control) servent au contrôle d'accès et au contrôle de flux sur la partie terminale, entre l'utilisateur et le réseau. Lorsque plusieurs utilisateurs veulent entrer dans le réseau ATM par un même point d'entrée, il faut ordonner leurs demandes. Ce contrôle est simultanément une technique d'accès, comme dans les réseaux locaux,

et un contrôle de flux sur ce qui entre dans le réseau. Malheureusement pour le monde ATM, cette zone n'a jamais été normalisée, ce qui constitue un fort handicap pour les interfaces utilisateur. En l'absence de norme sur les interfaces terminales, il n'a pas été possible à l'ATM de rivaliser avec l'interface IP, qui a fini par s'imposer partout.

Dans le champ de contrôle, 3 bits PT (Payload Type) définissent le type d'information transporté dans la cellule, notamment pour la gestion et le contrôle du réseau. Les huit possibilités pour ce champ sont les suivantes :

- 000 : cellule de données utilisateur, pas de congestion ; indication d'un niveau utilisateur du réseau ATM vers un autre utilisateur du réseau ATM = 0 ;
- 001 : cellule de données utilisateur, pas de congestion ; indication d'un niveau utilisateur du réseau ATM vers un autre utilisateur du réseau ATM = 1 ;
- 010 : cellule de données utilisateur, congestion ; indication d'un niveau utilisateur du réseau ATM vers un autre utilisateur du réseau ATM = 0 ;
- 011 : cellule de données utilisateur, congestion ; indication d'un niveau utilisateur du réseau ATM vers un autre utilisateur du réseau ATM = 1 ;
- 100 : cellule de gestion pour le flux OAM F5 de segment ;
- 101 : cellule de gestion pour le flux OAM F5 de bout en bout ;
- 110 : cellule pour la gestion des ressources ;
- 111 : réservé à des fonctions futures.

Vient ensuite le bit CLP (Cell Loss Priority), qui indique si la cellule peut être perdue (CLP = 1) ou, au contraire, si elle est importante (CLP = 0). Ce bit a pour fonction d'aider au contrôle de flux. Avant d'émettre une cellule dans le réseau, il convient de respecter un taux d'entrée, négocié au moment de l'ouverture du circuit virtuel. Il est toujours possible de faire entrer des cellules en surnombre, mais il faut les munir d'un indicateur permettant de les repérer par rapport aux données de base. L'opérateur du réseau ATM peut perdre ces données en surnombre pour permettre aux informations entrées dans le cadre du contrôle de flux de transiter sans problème.

La dernière partie de la zone de contrôle, le HEC (Header Error Control), est réservée à la protection de l'en-tête. Ce champ permet de détecter et de corriger une erreur en mode standard. Lorsqu'un en-tête en erreur est détecté et qu'une correction n'est pas possible, la cellule est détruite. Nous revenons sur ce point un peu plus loin pour décrire la procédure utilisée et montrer l'utilisation de ce champ pour récupérer la synchronisation lorsque celle-ci est perdue.

Comme expliqué en début de chapitre, deux interfaces ont été définies dans l'ATM : l'interface UNI d'entrée et de sortie du réseau et l'interface NNI entre deux nœuds à l'intérieur du réseau. La structure de la cellule ATM n'est pas exactement la même sur les deux interfaces. La structure de la cellule ATM sur l'interface UNI est illustrée à la figure 6.7 et celle sur l'interface NNI à la figure 6.8.

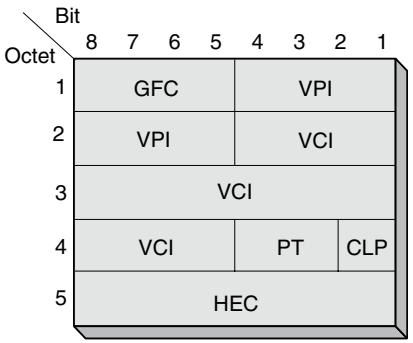


Figure 6.7

Structure de la cellule ATM sur l'interface UNI

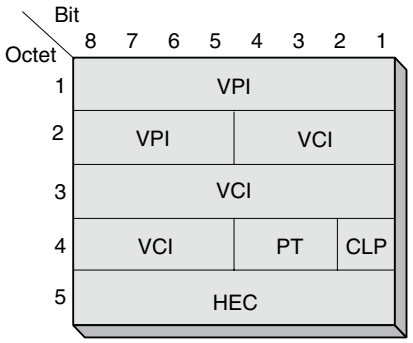


Figure 6.8

Structure de la cellule ATM sur l'interface NNI

Le champ GFC permet de contrôler les flux de cellules entrant dans le réseau, de les multiplexer et de diminuer les périodes de congestion du réseau de l'utilisateur final, appelé CPN (Customer Premise Network). Le GFC garantit les performances requises par l'utilisateur, comme la bande passante allouée ou le taux de trafic négocié. L'UIT-T a défini dans la recommandation I.361 deux séries de procédures pour le GFC, les procédures de transmission contrôlées et celles non contrôlées. Pour les procédures de transmission non contrôlées, le code 0000 est placé dans le champ GFC. Dans ce cas, le GFC ne joue aucun rôle.

En résumé, les deux fonctions principales réalisées par le GFC sont :

- le contrôle de flux à court terme ;
- le contrôle de la qualité de service dans le réseau de l'utilisateur final.

Le champ GFC n'existe que sur l'interface UNI. Les quatre bits de ce champ GFC sont remplacés à l'intérieur du réseau sur les interfaces NNI par quatre autres bits, qui viennent allonger la référence. Lorsqu'un utilisateur positionne les quatre bits GFC sur son

interface, ces quatre bits sont effacés dans le réseau pour être remplacés par un complément du numéro de référence et n'arrivent donc jamais au destinataire. En d'autres termes, ces quatre bits ne peuvent servir à une transmission d'information de bout en bout mais uniquement en local sur l'interface d'entrée dans le réseau.

Conclusion

Comme le niveau physique, le niveau trame est indispensable au transport de l'information dans un réseau de transfert. Il y a quinze ans, ce niveau trame n'était qu'un intermédiaire vers le niveau paquet et s'occupait essentiellement de détecter des erreurs et de demander une retransmission en cas d'erreur. Tout le travail de routage et de commutation s'effectuait au niveau supérieur, le niveau paquet.

Aujourd'hui, le niveau trame des architectures réseau ne s'occupe plus de détection d'erreur, puisqu'il n'y en a plus qu'un nombre négligeable et que les applications multimédias s'en suffisent largement. En revanche, les fonctionnalités traitées autrefois dans la couche 3 ont été descendues dans la couche 2. Les architectures de niveau trame sont devenues le standard dans les réseaux d'opérateurs.

7

Le niveau paquet

Le rôle du niveau paquet est de transporter d'une extrémité à l'autre du réseau des blocs de données provenant d'une fragmentation des messages du niveau supérieur, le niveau transport.

Le paquet est l'entité de la couche 3 qui possède l'adresse du destinataire ou la référence nécessaire à son acheminement dans le réseau. Le niveau paquet est en outre responsable du contrôle de flux, qui, s'il est bien conçu, évite les congestions dans les nœuds du réseau. Comme nous l'avons vu, les fonctionnalités du niveau paquet peuvent se trouver au niveau trame. Un paquet ne peut être transmis directement sur un support physique, car le récepteur serait incapable de reconnaître les débuts et fins de paquet.

L'ensemble des paquets allant d'un même émetteur vers un même destinataire s'appelle un flot. Celui-ci peut être long ou court, suivant la nature du service qui l'a créé. Si un gros fichier donne naissance à un flot important, une transaction ne produit qu'un flot très court, d'un à quelques paquets. Le niveau paquet peut faire appel ou non à une connexion (*voir le chapitre 2*) pour négocier une qualité de service avec le destinataire du flot.

Avant d'aborder en détail les fonctionnalités du niveau paquet, nous commencerons par rappeler les caractéristiques de ce niveau, définies dans le cadre du modèle de référence. Le rôle de la couche 3 (réseau) est de transporter les paquets d'une extrémité à l'autre du réseau.

Caractéristiques du niveau paquet

Le niveau paquet, ou couche réseau, est situé au troisième niveau de la hiérarchie de l'architecture du modèle de référence, comme illustré à la figure 7.1.

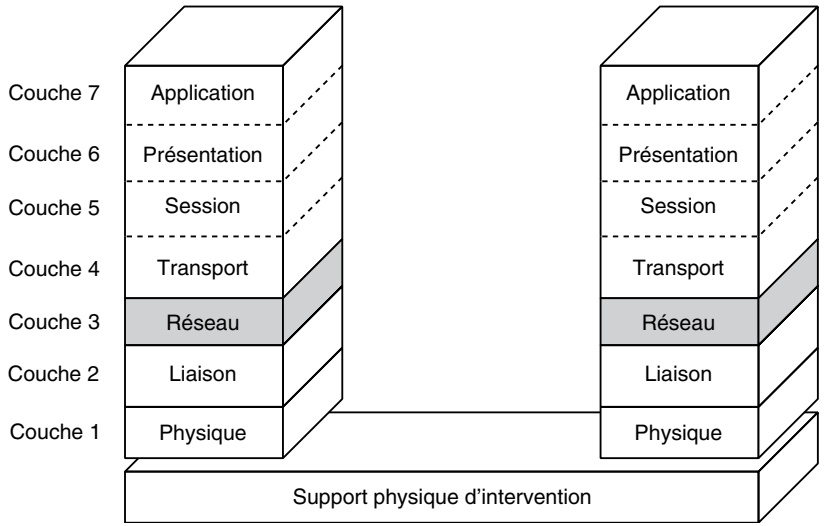


Figure 7.1

Le niveau paquet, ou couche réseau

Cette couche existe quand le réseau utilise un niveau paquet. Les fonctions définies par la normalisation internationale dans le cadre du modèle de référence sont les suivantes :

- Mise en place des connexions réseau pour acheminer les paquets. Cette fonction n'est toutefois pas une obligation dans le niveau paquet, et le protocole IP travaille en mode sans connexion. En revanche, la technique X.25 qui a presque disparu utilisait une mode avec connexion (*voir l'annexe F*).
- Prise en charge de l'acheminement des paquets et des problèmes de passerelles pour atteindre un autre réseau.
- Multiplexage des connexions réseau.
- Prise en charge de la segmentation et du groupage.
- Détection de perte de paquets et reprise des paquets perdus. Cette fonction n'est pas obligatoire au niveau paquet. IP, par exemple, protocole de niveau paquet, n'a aucun moyen de récupérer les paquets perdus.
- Maintien en séquence des données remises à la couche supérieure, sans que cela soit une obligation.
- Contrôle de flux, de façon qu'il n'y ait pas de débordement des mémoires en charge de la transmission des paquets.
- Transfert de données expresses (non obligatoire).
- Réinitialisation de la connexion réseau (non obligatoire).
- Qualité de service (non obligatoire).
- Gestion de la couche réseau.

Les modes avec et sans connexion

Dans le mode avec connexion, il faut établir une connexion entre les deux extrémités avant d'émettre les paquets de l'utilisateur, de façon que les deux entités communicantes s'échangent des informations de contrôle. Dans le mode sans connexion, au contraire, les paquets peuvent être envoyés par l'émetteur sans concertation avec le récepteur. On ne s'occupe pas de savoir si l'entité destinataire est prête à recevoir les paquets, et l'on suppose que le fait d'avoir une connexion au niveau de la session et, le cas échéant, de la couche transport est suffisant pour assurer un transfert simple de l'information à la couche 3. Il est vrai que les protocoles en mode sans connexion sont beaucoup plus simples que les protocoles en mode avec connexion.

En mode avec connexion, le réseau emploie généralement une technique de commutation. Quitte à envoyer un paquet de supervision pour demander l'ouverture de la connexion, autant se servir de la traversée du réseau par ce paquet de supervision, que l'on appelle aussi paquet d'appel, pour mettre en place des références, lesquelles permettront d'émettre à très haut débit sur le chemin ainsi mis en œuvre. En mode sans connexion, les gestionnaires réseau préfèrent le routage puisqu'il n'y a pas de signalisation. Il faut néanmoins noter qu'un réseau avec connexion peut se satisfaire d'une technique de routage et qu'un réseau sans connexion peut utiliser une commutation.

En mode sans connexion, une entité de réseau émet un paquet sans avoir à se soucier de l'état ni des désirs du récepteur. Comme pour l'ensemble des modes sans connexion, l'autre extrémité doit être présente, ou du moins représentée. Cette connexion implicite a été mise en place à un niveau supérieur, généralement le niveau session. Le mode sans connexion est beaucoup plus souple, puisqu'il ne tient pas compte de ce qui se passe au niveau du récepteur.

Les deux modes présentent des avantages et des inconvénients.

Les principaux avantages du mode avec connexion sont les suivants :

- sécurité de la transmission ;
- séquencement des paquets sur la connexion ;
- réglage facile des paramètres du protocole réseau.

Ses principaux désavantages sont les suivants :

- lourdeur du protocole mis en œuvre, en particulier pour les paquets de petite taille ;
- difficultés à atteindre les stations en multipoint ou en diffusion, du fait de la nécessité d'ouvrir autant de connexions qu'il y a de points à atteindre ;
- débit relativement faible acheminé sur la connexion.

Les avantages du mode sans connexion sont les suivants :

- diffusion et émission en multipoint grandement facilitées ;
- simplicité du protocole, permettant des performances assez élevées.

Ses désavantages sont les suivants :

- faible garantie de la sécurité du transport des paquets ;
- réglage plus complexe des paramètres en vue d'atteindre les performances désirées.

Les principaux protocoles de niveau paquet

Le protocole de niveau paquet quasiment exclusif est IP. Il est également un des plus anciens puisque les premières études provenant du ministère de la Défense aux États-Unis et du projet Cyclades en France ont démarré à la fin des années 1960. Le protocole IP est devenu stable au tout début des années 1980.

IP est une norme de fait de l'IETF (Internet Engineering Task Force). Cet organisme, qui n'a aucun pouvoir de droit propose des protocoles, dont certains finissent par s'imposer de par le nombre d'industriels qui les choisissent.

Un deuxième protocole du niveau paquet a connu son heure de gloire entre les années 1980 et 2000. Il a été normalisé par l'ISO (International Organization for Standardization) et l'UIT-T, les deux organismes de normalisation de droit puisque dépendant des États et représentant les utilisateurs et les industriels des télécommunications. Ce protocole est connu par son numéro de recommandation, X.25.3, ou X.25 PLP (Packet Level Protocol), et par son numéro de norme, ISO 8208.

Les grandes fonctionnalités du niveau paquet

Comme expliqué précédemment, le rôle du niveau paquet consiste à prendre en charge les paquets et à les transporter d'une extrémité à l'autre du réseau vers le bon point de destination et dans les meilleures conditions possibles. Il existe pour cela deux façons de procéder : mettre en place un chemin, ou circuit virtuel, entre l'émetteur et le récepteur ou bien utiliser le mode sans connexion. Le mot chemin supplante l'expression circuit virtuel, le monde IP n'appréciant guère cette dernière expression, qui rappelle les technologies anciennes de téléphonie commutée. L'expression anglaise *path* est de plus en plus utilisée. Lorsque le chemin utilise une technique de commutation, l'expression consacrée est *label-switched path*, ou chemin commuté.

Dans le mode chemin, les paquets circulent de façon ordonnée pour arriver dans l'ordre où ils ont été émis. Pour ouvrir le chemin, il est nécessaire de se servir d'une signalisation. Celle-ci doit déposer au fur et à mesure de sa progression dans les nœuds du réseau les références qui seront utilisées par les paquets de données, comme illustré à la figure 7.2.

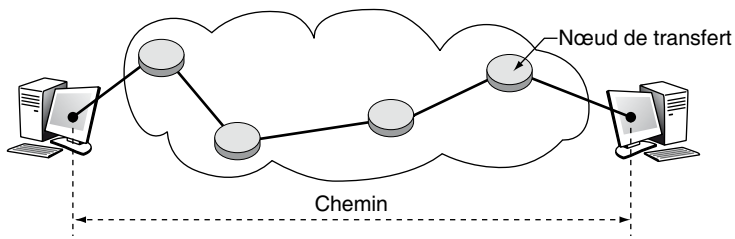


Figure 7.2

Pose des références dans les nœuds du réseau

Dans le mode sans connexion, dit aussi mode datagramme, chaque paquet est considéré comme indépendant des autres, même si tous les paquets appartiennent au même flot. Les paquets peuvent prendre des chemins différents et arriver dans n'importe quel ordre au récepteur, contrairement à ce qui se produit dans le mode chemin, où les paquets arrivent toujours dans l'ordre d'émission. Le contrôle des différents paquets isolés demande des algorithmes spécifiques, qui sont présentés plus loin dans les sections consacrées aux contrôles de flux et de congestion.

Rien n'empêche de réaliser un réseau avec connexion en utilisant en interne un mode datagramme pour le transport des paquets, comme illustré à la figure 7.3. Un paquet de supervision est acheminé vers le récepteur pour établir la connexion. L'ouverture de la connexion peut avoir lieu sans l'existence d'un chemin.

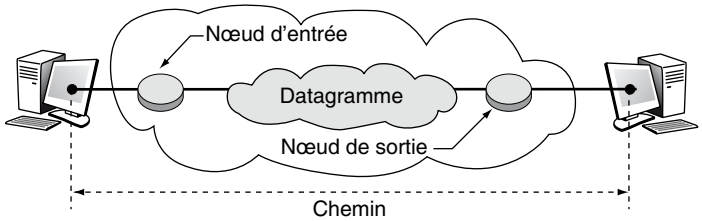


Figure 7.3

Un chemin au-dessus d'un datagramme

À l'inverse, rien ne s'oppose à bâtir un réseau sans connexion utilisant des chemins, mais cela n'apporte strictement rien. Il suffit d'envoyer un paquet de contrôle, qui dépose les références sans demander de connexion à l'hôte de destination.

Les trois fonctionnalités principales prises en charge par un protocole de niveau paquet sont le contrôle de flux, c'est-à-dire les moyens d'éviter que les flux ne grossissent trop par rapport aux ressources du réseau, la gestion des adresses ou des références et les algorithmes liés au routage.

Le contrôle de flux

Le contrôle de flux est la première fonctionnalité demandée au niveau paquet. Il s'agit de gérer les paquets pour qu'ils arrivent au récepteur dans le laps de temps le plus court et, surtout, d'éviter des pertes par écrasement dans les mémoires tampons des nœuds intermédiaires en cas de surcharge. Les réseaux à transfert de paquets sont comme des autoroutes : s'il y a trop de paquets, personne ne peut avancer. La régulation du flux est toutefois un problème complexe.

De très nombreuses méthodes ont été testées dans des contextes spécifiques. Dans tous les cas, le contrôle s'effectue par une contrainte sur le nombre de paquets circulant dans le réseau. Cette limitation s'exerce soit sur le nombre de paquets en transit entre une entrée et une sortie ou sur l'ensemble du réseau, soit sur le nombre de paquets qu'on

laisse entrer à l'intérieur du réseau par unité de temps. À ces contrôles peuvent s'ajouter des techniques d'allocation des ressources pour éviter toute congestion. Nous détaillons ci-après quelques-uns de ces contrôles de flux.

Le contrôle par crédit

Dans le contrôle par crédit, il existe un nombre *N* de crédits qui circulent dans le réseau. Pour qu'un paquet entre, il doit acquérir un crédit, qui est libéré une fois la destination atteinte. Le nombre total de paquets circulant dans le réseau est évidemment limité à *N*. Les crédits peuvent être banalisés ou dédiés. La méthode isarythmique gère des crédits totalement banalisés. La difficulté consiste à distribuer les crédits aux bonnes portes d'entrée de façon à offrir un débit maximal. Cette technique est très difficile à maîtriser, et ses performances n'ont pas été prouvées comme optimales.

Une première amélioration apportée au contrôle par crédit a consisté à définir des crédits dédiés à un nœud d'entrée dans le réseau. Une file d'attente de crédits, associée au nœud d'entrée, permet aux paquets d'entrer dans le réseau. Une fois le paquet arrivé au nœud destinataire, le crédit utilisé est libéré et réacheminé, avec l'acquittement par exemple, vers l'émetteur. De nouveau, le contrôle est assez délicat puisqu'il ne se fait que localement et non à l'intérieur du réseau.

On utilise le plus souvent des crédits dédiés à un utilisateur ou, du moins, à un chemin. Cette méthode est connue sous le nom de fenêtre de contrôle de flux. La figure 7.4 en donne une illustration.

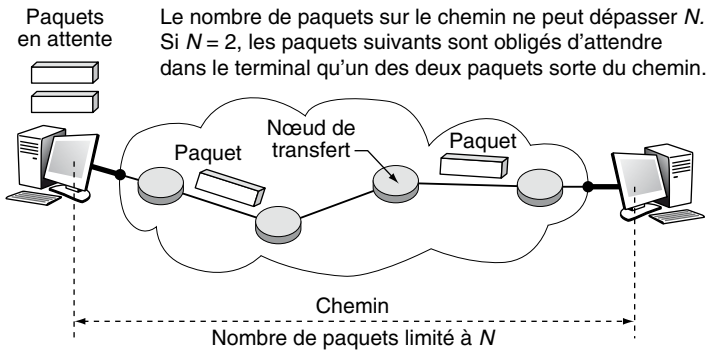


Figure 7.4

Fenêtre de contrôle de flux

Le monde IP utilise une fenêtre de ce type. Chaque connexion est contrôlée par une fenêtre de taille variable, qui s'ajuste à tout moment pour éviter que le réseau ne soit trop surchargé. Cette solution est astucieuse pour un réseau comme Internet, où le contrôle est effectué par les centaines de millions de machines terminales. La fenêtre part d'une valeur 1 et augmente exponentiellement : 2, 4, 8, 16, 32, etc. Dès que le temps de retour des acquittements augmente, le PC considère que le flux engendré est trop important, et il

redémarre avec une fenêtre de 1. Ce contrôle de flux est détaillé au chapitre 17, consacré aux réseaux IP.

Le contrôle de seuil

Une autre grande politique de contrôle de flux consiste à utiliser des seuils d'entrée dans le réseau. Un interrupteur situé à l'entrée du réseau s'ouvre plus ou moins pour laisser passer plus ou moins de paquets, suivant des indications qui lui sont fournies par le gestionnaire du réseau.

Plusieurs mises en œuvre du contrôle de seuil peuvent être effectuées, notamment les suivantes :

- Des paquets de gestion apportent aux nœuds d'entrée du réseau les informations nécessaires pour positionner les interrupteurs à la bonne valeur. Cette méthode, qui est l'une de celles qui donnent les meilleurs résultats, présente l'inconvénient que le réseau risque de s'effondrer si le contrôle n'est pas effectué assez vite, à la suite, par exemple, d'une panne d'une liaison ou d'un nœud. En effet, les paquets de contrôle sont expédiés à peu près à la même vitesse que les autres et peuvent demander un temps trop long lors d'une congestion effective d'un point du réseau.
- L'entrée du réseau est contrôlée par une fenêtre. Dans ce cas, les paquets doivent être acquittés localement pour permettre à la fenêtre de s'ouvrir à nouveau. En cas de problème, le gestionnaire réseau peut ne pas envoyer les acquittements, ce qui a pour effet de bloquer les émissions en fermant l'interrupteur (*voir figure 7.5*).

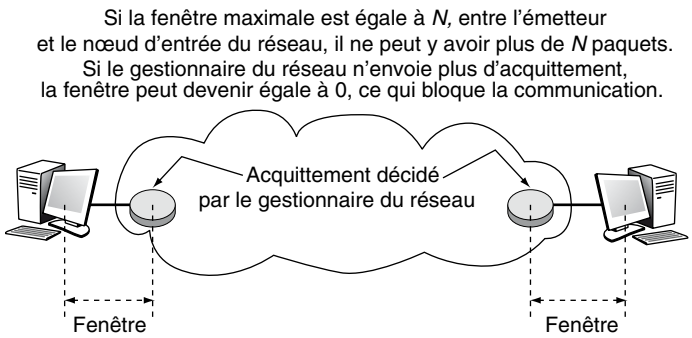


Figure 7.5

Contrôle de flux par fenêtre

L'allocation de ressources

Les politiques d'allocation de ressources ou de préallocation sont une troisième grande catégorie de contrôle de flux. Ces politiques sont essentiellement adaptées au mode commuté avec connexion, dans lequel un paquet d'appel est nécessaire à la mise en place des références et de la connexion. Ce paquet réserve des ressources intermédiaires dans les différents nœuds traversés par le chemin.

L'algorithme d'allocation de ressources prend des allures très différentes suivant le réseau. On peut notamment superposer un contrôle de flux de bout en bout sur un circuit virtuel et une méthode de préallocation. Par exemple, si *N* est le nombre de crédits dédiés à la connexion et que le paquet d'appel réserve exactement la place de *N* paquets dans ses mémoires tampons, le contrôle de flux est parfait, et aucun paquet n'est perdu.

Malheureusement, ce contrôle s'avère extrêmement coûteux à mettre en place, car il faut disposer d'une quantité de ressources bien supérieure à celle qui existe dans les implémentations réalisées. Comme illustré à la figure 7.6, le nombre total de mémoires réservées dans le réseau vaut $N \times M$, M étant le nombre de nœuds traversés. De plus, sur un circuit virtuel, la probabilité qu'il y ait effectivement N paquets en transit est très faible, et ce pour de nombreuses raisons : retour des acquittements, utilisateur inactif ou peu actif, mise en place de la connexion, etc.

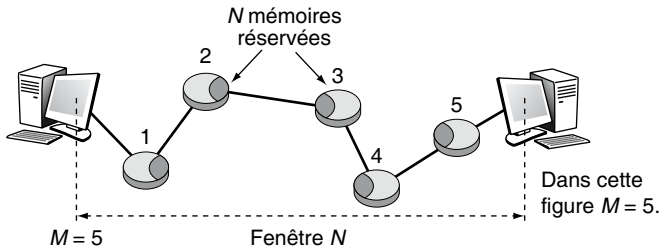


Figure 7.6

Contrôle de flux par allocation totale

Pour minimiser le coût de mise en place d'une telle solution, il est possible d'effectuer une surallocation. La surallocation consiste à ne donner à un paquet d'appel qui entre dans un nœud de commutation qu'une partie de ce qu'il demande. On espère que, statistiquement, s'il y a plus de paquets que prévu sur une connexion, il y en aura moins sur une autre. Soit k, $0 < k \leq 1$, le facteur de surallocation. Si N est toujours la fenêtre de contrôle de bout en bout, le nœud intermédiaire qui possède un facteur de surallocation de k réservera kN mémoires tampons. La valeur de k dépend en grande partie du taux d'occupation des chemins dans le réseau. Les valeurs classiques sont très faibles, le taux d'utilisation d'un circuit virtuel étant souvent inférieur à 10 %, et des facteurs de surallocation de 0,2 sont assez courants.

La surallocation permet, à un coût assez faible, d'augmenter fortement le nombre de chemins pouvant passer par un nœud. Si toutes les mémoires tampons sont allouées, le paquet d'appel est refusé. On augmente alors d'un facteur $1/k$ le nombre de chemins ouverts et, de ce fait, le débit global du réseau. Il est évident qu'il existe un risque de dysfonctionnement si, pour une raison quelconque, le taux d'utilisation des chemins vient à augmenter. Le risque grandit encore si le nombre moyen de paquets dans les chemins dépasse la limite de surallocation.

On peut tracer la courbe classique de surallocation en fonction du taux d'utilisation des chemins pour un nombre M de nœuds à traverser et un nombre K de mémoires

disponibles, de façon que la probabilité de perte de paquets reste à une valeur $\varepsilon = 10^{-7}$ (*voir figure 7.7*).

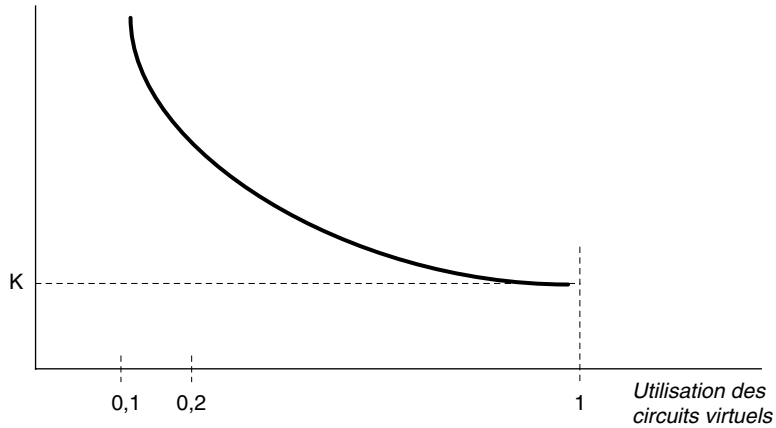


Figure 7.7

Surallocation des mémoires tampons

On voit qu'aux environs d'un taux d'utilisation de 0,1 ou 0,2, la surallocation possible change énormément. Il faut donc contrôler que le taux d'utilisation ne varie pas trop. À cet effet, il est préférable de libérer des chemins plutôt que de perdre des paquets de façon incontrôlée.

Une autre possibilité pour contrôler le flux dans un réseau, toujours pour la méthode par allocation de ressources, consiste à allouer des parties de la bande passante à chaque paquet d'appel. Pour un coefficient *k'* de surallocation, si le débit d'une liaison est D_i, le chemin se réserve un débit de $k'D_i$. Une fois l'ensemble du débit D disponible affecté, le nœud ne peut plus accepter de nouveaux paquets d'appel, et donc de nouvelles ouvertures de chemins.

À quelques exceptions près, ces techniques de contrôle de flux présentent le défaut, au coût très élevé, de ne pas fonctionner correctement dans certains cas de figure, où il se produit une congestion dont il faut sortir. Les méthodes de contrôle de congestion présentées ci-après permettent de faire face aux dysfonctionnements du réseau, même si aucune n'est vraiment efficace.

Le contrôle de congestion

Le contrôle de congestion désigne les moyens mis en œuvre pour sortir d'un état de congestion. Les contrôles de flux sont là pour éviter d'entrer dans des états de congestion, mais il est évident que, malgré les efforts pour contrôler les flux, des états de congestion restent possibles.

Une méthode de contrôle de congestion assez utilisée consiste à garder en réserve dans les nœuds de commutation de la place mémoire non prise en compte dans les allocations.

Lorsque les tampons sont tous remplis, on ouvre la place supplémentaire. Pour peu convaincante qu'elle paraisse, cette méthode présente un intérêt. Lorsque deux paquets, ou deux trames au niveau liaison, doivent être échangés sur une liaison, le fait de garder en mémoire les informations en attendant l'acquittement peut amener à un blocage, ou *deadlock*. En disposant d'une place supplémentaire, on peut résoudre le problème (*voir figure 7.8*).

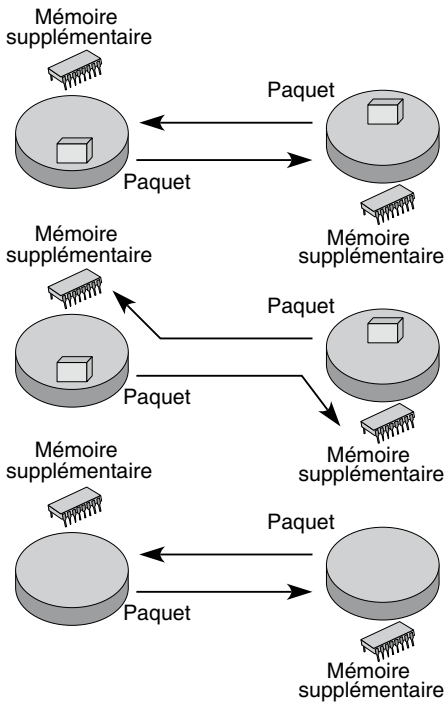


Figure 7.8

Résolution d'un blocage par allocation de mémoire supplémentaire

L'utilisation d'un temps maximal de résidence dans le réseau est une deuxième possibilité de contrôle de congestion. On place dans le paquet entrant la valeur d'une horloge commune à l'ensemble du réseau. Cette méthode, dite de temporisateur, permet de contrôler le temps passé dans le réseau et de détruire les paquets bloqués dans un nœud. Elle aide en outre à supprimer les paquets égarés à la suite d'une fausse adresse ou d'une erreur de routage. Elle est cependant assez difficile à mettre en œuvre, puisqu'elle nécessite une horloge commune et des comparateurs de temps. La plupart des protocoles qui l'implémentent, parmi lesquels IP, simplifient énormément l'algorithme à suivre : dans la zone réservée au temps maximal figure un nombre qui est décrémenté à chaque traversée de nœud.

Le routage

Dans un réseau maillé, le routage des paquets fait partie d'une algorithmique complexe, de par la distribution des décisions à prendre, qui relèvent à la fois de l'espace et du temps. Un nœud devrait connaître l'état de l'ensemble des autres nœuds avant de décider où envoyer un paquet, ce qui est impossible à réaliser.

Dans un premier temps, regardons les composantes nécessaires à la mise en place d'un routage. Il faut tout d'abord une table de routage, qui se présente comme illustré à la figure 7.9.

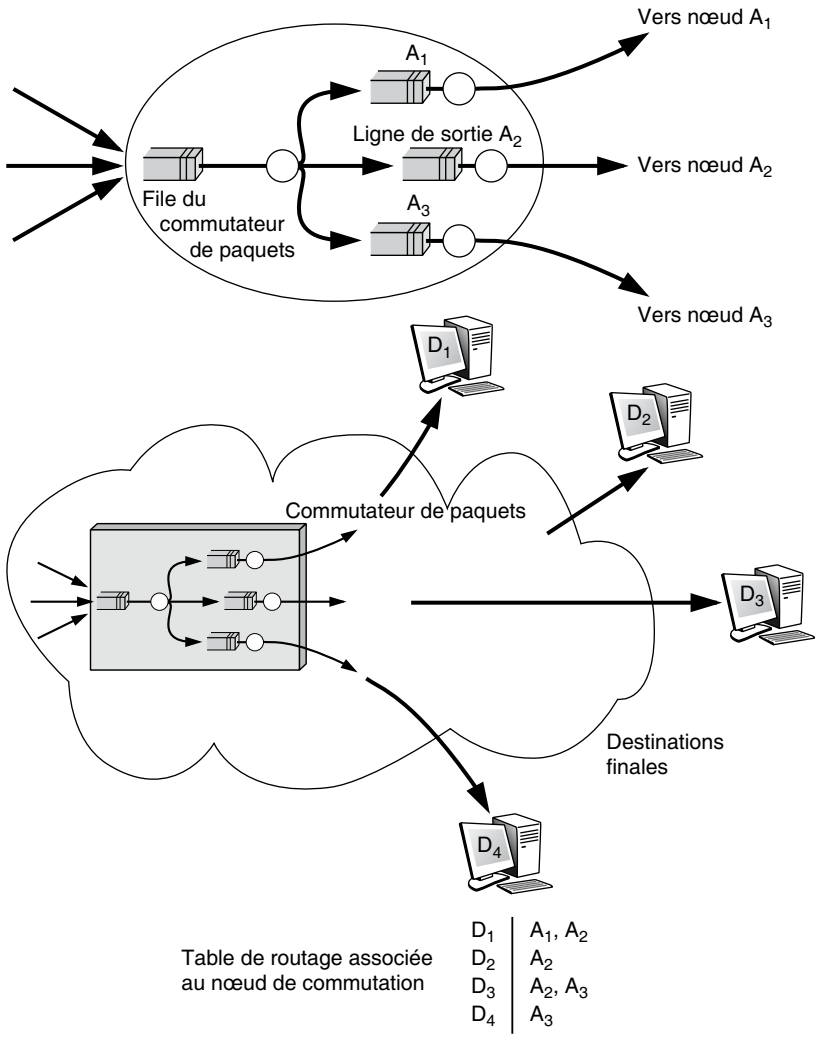


Figure 7.9

Table de routage

On voit qu'un nœud de transfert est formé de lignes de sortie, qui émettent des trames obtenues à partir de paquets. Les paquets sont routés par le nœud vers une ligne de sortie grâce à la table de routage. Si un paquet se présente au nœud avec, pour destination finale, le nœud D_1, le nœud peut envoyer ce paquet vers la ligne de sortie A_1 ou vers la ligne de sortie A_2. La décision s'effectue sur des critères locaux dans le cas considéré. Par exemple, on envoie le paquet sur la file la plus courte. Si la destination finale est D_2, le paquet est placé dans la file A_2.

Le routage centralisé

Le routage centralisé est caractérisé par l'existence d'un centre, qui prend les décisions quant à la définition d'une nouvelle table et de l'envoi de cette table à l'ensemble des nœuds de transfert du réseau. Ce nœud central reçoit les informations de la part de tous les composants du réseau, et il conçoit sa table de routage suivant des algorithmes déterminés à l'avance.

Les principales considérations à prendre en compte pour déterminer les meilleures routes dans un réseau, que ce soit en routage ou pour l'ouverture d'un chemin, sont les suivantes :

- coût des liaisons ;
- coût du passage dans un nœud ;
- débit demandé ;
- délai de transit demandé ;
- nombre de nœuds à traverser ;
- sécurité du transport de certaines classes de paquets ;
- occupation des mémoires des nœuds de commutation ;
- occupation des coupleurs de ligne.

Les algorithmes de routage utilisent la plupart du temps des critères de coût. On trouve, par exemple, l'algorithme du coût le plus bas, qui, comme son nom l'indique, consiste à trouver le chemin qui minimise le plus le prix. Le plus simple des algorithmes, et presque toujours le plus performant, donne un coût de 1 à chaque passage dans un nœud. C'est l'algorithme de la route la plus courte. Contrairement à ce que l'on pourrait penser, c'est souvent une bonne façon de procéder. On peut facilement ajouter des biais pour prendre en compte l'occupation des mémoires intermédiaires, l'utilisation des lignes de sortie, etc.

Le routage fixe est une autre technique particulièrement simple puisque la table ne varie pas dans le temps. Chaque fois qu'un paquet entre dans un nœud, il est envoyé dans la même direction, qui correspond, dans presque tous les cas, à l'algorithme de la route la plus courte. On ne peut toutefois parler d'algorithme de routage dans ce cas, puisque le routage est fixe et ne requiert pas de mise à jour. Le routage fixe va de pair avec un centre de contrôle, qui gère les pannes graves et génère une nouvelle table lorsqu'un nœud tombe en panne ou qu'une ligne de communication est rompue. On appelle ce routage fixe entre les mises à jour.

On peut améliorer le routage fixe en tenant compte d'événements indiqués par le réseau, telles des congestions ou des occupations de lignes ou des mémoires trop importantes. Toutes les dix secondes, tous les nœuds du réseau envoient un paquet de contrôle indiquant leur situation. À partir de ces comptes rendus, le nœud central élabore une nouvelle table de routage, qui est diffusée.

L'envoi des tables de routage d'une façon asynchrone est une technique plus élaborée. Le nœud central diffuse vers l'ensemble des nœuds une nouvelle table de routage dès que cette table a suffisamment changé par rapport à celle en vigueur. En d'autres termes, le centre de contrôle dresse des tables de routage au fur et à mesure de l'arrivée de nouvelles informations puis envoie à tous les nœuds la première table de routage qui lui paraît suffisamment différente de la précédente. L'adaptation est ici asynchrone et non pas synchrone, comme précédemment.

Les performances de ce routage centralisé dépendent de l'architecture et de la topologie du réseau. En effet, le principal problème du routage et de l'adaptation est qu'ils doivent s'effectuer en temps réel. Entre le moment où un nœud envoie un compte rendu impliquant un nouveau routage et celui où la nouvelle table de routage arrive, il ne doit pas y avoir de changement substantiel de l'état du système. Cette condition est très mal réalisée si le réseau est important et les artères surchargées, les paquets de contrôle étant peu prioritaires par rapport aux paquets transportant des informations.

La qualité du routage correspond à première vue à une adaptation de plus en plus sophistiquée. C'est là que se pose le deuxième grand problème concernant les performances, d'ailleurs lié au premier : la sophistication entraîne une surcharge du réseau par des paquets de contrôle, laquelle peut empêcher un fonctionnement en temps réel.

On voit qu'un algorithme de routage donné n'a pas la même efficacité pour un réseau à trois nœuds, par exemple, que pour un réseau à vingt nœuds. La première conclusion que nous pouvons en tirer est qu'il n'existe pas d'algorithme meilleur qu'un autre, même pour un réseau bien déterminé, puisque tout dépend du trafic. Par ailleurs, il semble qu'il existe un optimum dans la complexité de l'algorithme d'adaptation pour ne pas surcharger le réseau inutilement.

Le routage distribué

La plus simple des techniques de routage distribué, l'inondation, n'est pas adaptative. Lorsqu'un paquet est reçu dans un nœud, il est retransmis vers toutes les destinations possibles. Ce routage efficace est toutefois pénalisant en termes de flux et ne peut être adopté que dans des cas spécifiques, comme les réseaux dans lesquels le temps réel est primordial et le trafic faible.

Dans les algorithmes un peu plus complexes, l'adaptabilité commence à apparaître. Elle ne concerne qu'une dimension, le temps. Pour un paquet en transit dans le nœud i et se dirigeant vers le nœud j, plusieurs lignes de sortie peuvent être choisies. Dans la méthode de routage appelée *hot-potatoe*, on essaie de se débarrasser du paquet le plus rapidement possible en le transmettant sur la première ligne de sortie vide. En réalité, on ne se sert jamais d'une méthode hot-potatoe pure. On préfère des techniques plus élaborées, dans

lesquelles des coefficients sont affectés aux différentes lignes de sortie pour une destination donnée (*voir figure 7.10*).

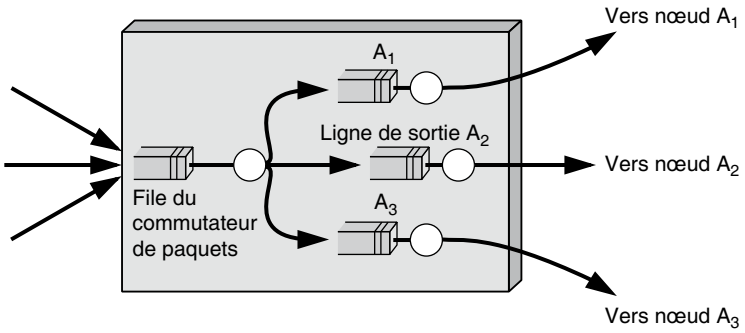


Table de routage associée au nœud de commutation

D_1	A_1 si la file A_2 a plus de deux clients de plus que la file A_1, sinon A_2
D_2	A_2
D_3	A_2 ou A_3 (la file la plus courte)
D_4	A_3

Figure 7.10

Routage hot-potatoe avec biais

Il existe presque toujours une ligne de sortie plus appropriée que les autres. Toutes ces techniques sont locales, puisque les états des autres nœuds ne sont pas pris en compte. Pour adapter l'algorithme dans l'espace, il convient en premier lieu de se faire une idée de ce qui se passe dans les nœuds voisins. Sans utiliser de paquets de contrôle, on obtient un échantillon du trafic des nœuds voisins en comptabilisant les arrivées en provenance de ces nœuds. Ces derniers peuvent également envoyer de façon synchrone ou asynchrone des comptes rendus de leur état. En tenant compte de ces informations implicites ou explicites, il est possible de choisir la file de sortie en connaissance de cause. L'adaptation spatiale est encore limitée, puisqu'une cassure, deux chaînons plus loin, risque de ne pas être prise en compte par les comptes rendus des nœuds voisins. Une technique plus fine est définie à la section suivante, permettant à un nœud de déterminer sa table de routage en fonction de l'ensemble des états du réseau.

L'algorithme de routage distribué, qui doit s'adapter pleinement à la fois dans l'espace et dans le temps, demande une connaissance complète de l'état de tous les nœuds du réseau. Les divers nœuds doivent donc s'échanger des messages. Si chaque nœud transmet un message à tous les autres, le trafic total risque d'augmenter de façon inquiétante. Pour rester dans des limites raisonnables, un nœud ne transmet un compte rendu qu'à ses voisins. Ceux-ci doivent en tenir compte dans leur propre compte rendu. De nouveau, les instants de mise à jour peuvent être synchrones ou asynchrones. Les inconvénients et les avantages de ces deux types de mesure sont les mêmes que dans le cas centralisé.

Exemple de routage distribué

Soit le nœud illustré à la figure 7.11, possédant trois voisins : N_1, N_2, N_3. Le processeur de ce commutateur est capable de connaître le temps de réponse de ses trois files de sortie, que nous notons respectivement W_1, W_2 et W_3. Ce temps de réponse est obtenu en comptabilisant le nombre d'octets en attente dans le coupleur de lignes et en le multipliant par la vitesse d'émission sur le support physique.

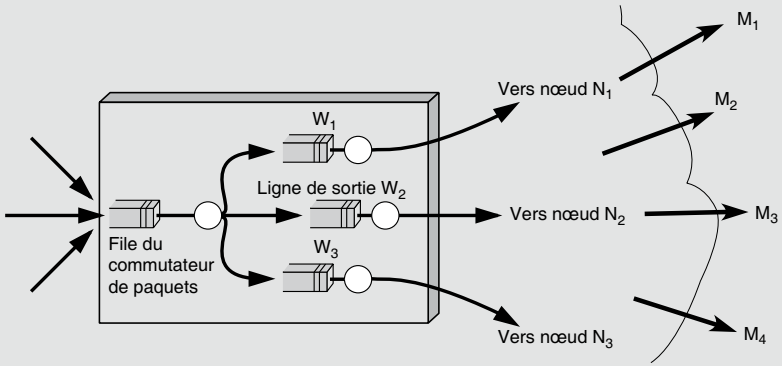


Figure 7.11

Routage distribué dans un nœud de commutation

Intéressons-nous à quatre destinataires possibles : M_1, M_2, M_3 et M_4, et supposons que les nœuds N_1, N_2 et N_3 soient capables de connaître les délais d'acheminement optimaux d'un paquet entrant dans leur commutateur pour atteindre un nœud terminal. Ces délais sont recensés au tableau 7.1.

Exemple de routage distribué

Soit le nœud illustré à la figure 7.11, possédant trois voisins : N_1, N_2, N_3. Le processeur de ce commutateur est capable de connaître le temps de réponse de ses trois files de sortie, que nous notons respectivement W_1, W_2 et W_3. Ce temps de réponse est obtenu en comptabilisant le nombre d'octets en attente dans le coupleur de lignes et en le multipliant par la vitesse d'émission sur le support physique.

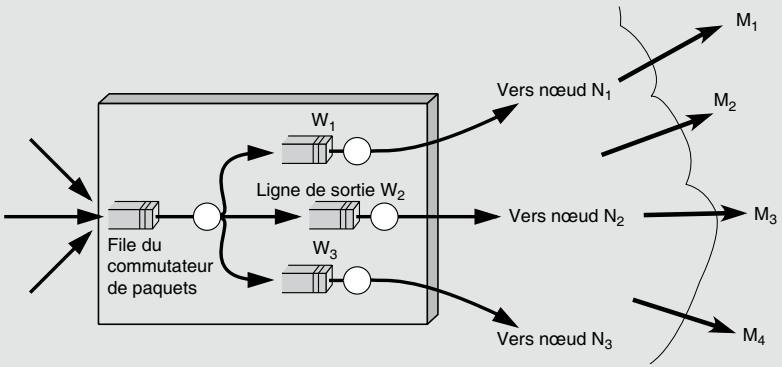


Figure 7.11

Routage distribué dans un nœud de commutation

Intéressons-nous à quatre destinataires possibles : M_1, M_2, M_3 et M_4, et supposons que les nœuds N_1, N_2 et N_3 soient capables de connaître les délais d'acheminement optimaux d'un paquet entrant dans leur commutateur pour atteindre un nœud terminal. Ces délais sont recensés au tableau 7.1.

	M_1	M_2	M_3	M_4
N_1	160	260	180	218
N_2	140	255	175	200
N_3	100	247	140	220

TABLEAU 7.1 • Délai d'acheminement d'un paquet

L'intersection de la colonne M_3 et de la ligne N_2 indique le délai d'acheminement optimal vers la destination M_3 pour un paquet entrant dans le nœud N_2. Prenons les valeurs indiquées au tableau 7.2 comme temps de réponse des files de sortie du nœud étudié.

W_1	W_2	W_3
26	40	64

TABLEAU 7.2 • Temps de réponse des files de sortie

Nous pouvons calculer, pour chaque destination, les délais d'acheminement à partir du nœud étudié en passant par chacun des voisins de ce nœud. Ces délais sont indiqués au tableau 7.3.

	Vers M_1	Vers M_2	Vers M_3	Vers M_4
Par N_1	160 + 26	260 + 26	180 + 26	218 + 26
Par N_2	140 + 40	255 + 40	175 + 40	200 + 40
Par N_3	100 + 64	247 + 64	140 + 64	220 + 64

TABLEAU 7.3 • Délai total d'acheminement d'un paquet

Nous en déduisons la table de routage du nœud étudié (*voir tableau 7.4*).

	M_1	M_2	M_3	M_4
Destination finale	N_3	N_1	N_3	N_2
File de sortie	140	255	175	200
Temps de propagation	100	247	140	220

TABLEAU 7.4 • Table de routage déduite

L'hypothèse d'un nœud capable de connaître les délais d'acheminement vers un destinataire n'a plus lieu d'être puisque nous venons de voir que la connaissance de ces délais pour chaque nœud permettait de les obtenir pas à pas. Pour ce faire, chaque nœud doit envoyer à tous ses voisins sa table de délais. Les temps de propagation pour ces diverses transmissions s'ajoutent. De ce fait, les informations en la possession d'un nœud risquent de ne pas être à jour. Les problèmes de surcharge dus aux paquets de contrôle et à l'exactitude des informations sont les deux générateurs de trouble dans les politiques de routage distribué qui veulent tenir compte de l'ensemble des ressources de transport.

L'un des problèmes cruciaux posés par le routage distribué, qu'il soit adaptatif ou non, est celui du rebouclage, un paquet pouvant repasser plusieurs fois par le même nœud. Un exemple caractéristique est fourni par le réseau ARPAnet, la première version du réseau Internet, qui a expérimenté le dernier algorithme décrit et pour lequel les mesures effectuées ont montré un grand nombre de rebouclages.

Caractéristiques de l'adaptation

À partir des exemples précédents, nous pouvons déduire les caractéristiques suivantes de l'adaptation et de l'algorithme de routage :

- Le réseau doit réagir promptement à la moindre défaillance.
- Un routage centralisé est souvent à exclure du fait de son long temps de réponse.
- L'adaptation doit se faire dans l'espace et dans le temps. Pour cela, chaque nœud doit avoir une connaissance aussi complète que possible de l'état global du réseau. En revanche, il faut limiter au maximum les échanges d'informations.
- Pour éviter les rebouclages, il faut opter pour un algorithme centralisé ou noter les paquets qui reviennent pour les émettre vers une autre destination.

Nous voyons que ces conditions sont quelque peu contradictoires et que les solutions distribuées et centralisées présentent des avantages et des inconvénients. Le choix de l'adaptation synchrone ou asynchrone n'est pas simple non plus. En effet, comme le routage asynchrone augmente le trafic dès que le réseau commence à être chargé, les mises à jour doivent se faire de plus en plus souvent.

L'adressage

Les données situées chez l'utilisateur ou sur des serveurs d'un réseau ne peuvent être atteintes que par l'intermédiaire d'un adressage spécifiant l'interface de sortie ou par une référence permettant d'acheminer le paquet jusqu'à l'interface recherchée. Dans ce dernier cas, il faut se servir de l'adresse du destinataire pour que le paquet de signalisation ouvre un circuit virtuel. Nous ne nous intéressons dans un premier temps qu'à l'adressage et revenons ensuite sur les systèmes utilisant des références.

L'adressage peut être physique ou logique. Une adresse physique correspond à une jonction physique à laquelle est connecté un équipement terminal. Une adresse logique correspond à un utilisateur, un terminal ou un programme utilisateur qui peut se déplacer géographiquement. Le réseau téléphonique offre un premier exemple d'adressage physique : à un numéro correspond un utilisateur, ou plus exactement une jonction. Dans

ce réseau, l'adressage est hiérarchique. Il utilise un code différent pour le pays, la région et l'autocommutateur, les quatre derniers chiffres indiquant l'abonné. Si l'abonné se déplace, il change de numéro. Les autocommutateurs temporels peuvent dérouter l'appel vers un autre numéro à la demande de l'abonné, mais l'adressage n'est pas conservé.

Un second exemple est proposé par le réseau Ethernet et plus globalement par les réseaux locaux. Il s'agit d'un adressage de niveau trame et non de niveau paquet. Nous l'introduisons dans ce chapitre comme exemple car il aurait très bien pu être implémenté dans un paquet.

Par l'intermédiaire de l'IEEE (Institute of Electrical and Electronics Engineers), à chaque coupleur est affecté un numéro unique (*voir figure 7.12*). Il n'y a donc pas deux coupleurs portant la même adresse. Si la partie portant l'adresse ne peut être déplacée, l'adressage est physique. En revanche, si l'utilisateur peut partir avec son terminal et son interface et se reconnecter ailleurs, l'adressage devient logique. Dans ce dernier cas, le routage dans les grands réseaux est particulièrement complexe.

Dans le cas du réseau Ethernet, l'adressage est absolu. Il n'y a donc pas de relation entre des adresses situées sur des sites proches l'un de l'autre. Comme indiqué à la figure 7.12, le premier bit de l'adressage Ethernet précise si l'adresse correspond à un seul coupleur (adresse unique) ou si elle est partagée par d'autres coupleurs pour permettre des communications en multipoint ou en diffusion. Le deuxième bit indique si l'adressage utilisé est celui défini par l'IEEE, c'est-à-dire si les champs d'adresse possèdent bien l'adresse Ethernet du coupleur ou si l'utilisateur a remplacé les deux champs par une adresse spécifique. Il est fortement conseillé de garder l'adresse IEEE d'origine du coupleur pour éviter toute collision avec une autre adresse IEEE.

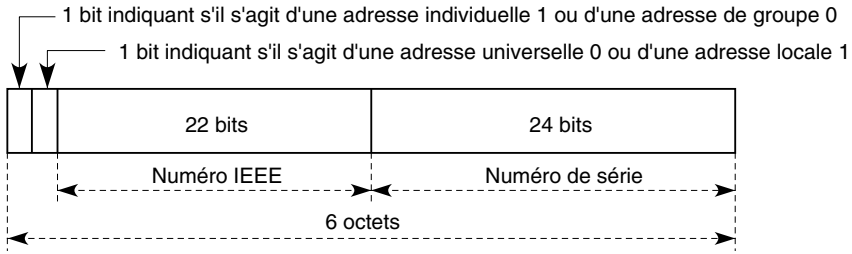


Figure 7.12

Adressage Ethernet

Dans l'adressage Ethernet que nous venons de décrire, la situation géographique de l'abonné est impossible à connaître, et le routage délicat à mettre en œuvre. C'est la raison pour laquelle le routage de niveau trame ne s'est jamais développé. Il aurait fallu pour cela développer un adressage hiérarchique.

Le réseau Internet donne un bon exemple d'adressage hiérarchique logique. L'adresse est décomposée en deux parties donnant deux niveaux de hiérarchie. La première identifie une machine terminale sur un réseau déterminé, et la seconde le numéro de ce réseau. On

voit que l'adresse n'est pas forcément géographique, puisqu'un réseau peut contenir cinq PC, un dans chaque continent. Il faut trouver une route pour aller dans le réseau d'appartenance puis rechercher à l'intérieur du réseau la route allant au destinataire. Les adresses IP sont examinées en détail au chapitre 16.

Les fonctionnalités du niveau paquet

Comme expliqué en début de chapitre, le niveau paquet (couche 3), également appelé couche réseau, offre un service au niveau message, ou couche transport. Ce service doit être fourni par le protocole réseau en tenant compte du service qui est offert par la couche inférieure, comme illustré à la figure 7.13.

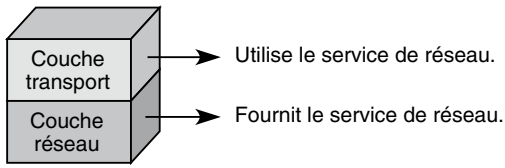


Figure 7.13

Relation entre couche réseau et transport

Les services qui doivent être rendus par le niveau paquet doivent satisfaire les cinq critères suivants :

- Indépendance par rapport aux supports de transmission sous-jacents. Le service réseau libère ses utilisateurs de toutes les préoccupations liées à la façon dont sont utilisés les divers sous-réseaux pour assurer le service réseau. Il masque à l'utilisateur du service réseau la façon dont ses paquets sont transportés. En effet, ce dernier ne souhaite généralement pas connaître les protocoles utilisés pour le transport de ses paquets mais désire seulement être sûr que ses paquets arrivent au destinataire avec une qualité définie.
- Transfert de bout en bout. Le service réseau assure le transfert d'une extrémité à l'autre des données utilisateur. Toutes les fonctions de routage et de relais sont assurées par le fournisseur du service réseau, y compris dans le cas où diverses ressources de transmission, similaires ou différentes, sont utilisées en tandem ou en parallèle.
- Transparence des informations transférées. Le service réseau assure le transfert transparent des informations sous la forme d'une suite d'octets de données utilisateur ou d'informations de contrôle. Il n'impose aucune restriction quant au contenu, au format ou au codage des informations et n'a pas besoin d'interpréter leur structure ou leur signification.
- Choix de la qualité de service. Le service réseau offre aux utilisateurs la possibilité de demander ou d'accepter la qualité de service prévue pour le transfert de données utilisateur. La qualité de service est spécifiée par des paramètres de QoS exprimant des caractéristiques telles que le débit, le temps de transit, l'exactitude et la fiabilité.

- Adressage de l'utilisateur du service réseau. Le service réseau utilise un système d'adressage qui permet à chacun de ses utilisateurs d'identifier de façon non ambiguë d'autres utilisateurs du service réseau.

Pour respecter ces critères, le service réseau dispose d'une panoplie de possibilités. L'une des plus importantes consiste à établir une connexion entre les deux entités communicantes. Comme nous l'avons vu à plusieurs reprises, une connexion est un lien entre l'émetteur et le récepteur, qui doit permettre à la communication de s'effectuer dans les meilleures conditions possibles. Ce lien donne la possibilité à l'émetteur de négocier avec le récepteur les caractéristiques et la qualité de service qu'il souhaite obtenir.

On peut reprocher au mode avec connexion d'être relativement lourd, puisque, avant toute émission de paquets, une discussion avec le récepteur est nécessaire pour que les deux entités distantes se mettent d'accord. Le mode avec connexion est également pénalisant dès que l'on veut mettre en place des communications en diffusion ou en multipoint, puisqu'il faut ouvrir autant de connexions qu'il y a de points à atteindre. En contrepartie, son avantage évident réside dans une plus grande fiabilité de la communication grâce au contrôle effectué sur la connexion.

Le mode sans connexion est plus souple puisque l'émetteur envoie ses paquets sans avoir à se préoccuper du récepteur. Il est bien entendu que l'utilisateur distant est présent ou représenté par une boîte aux lettres et que cette présence peut être garantie par l'ouverture d'une connexion à un niveau supérieur. C'est le plus souvent au niveau session que l'assurance de cette présence est garantie.

La qualité de service

La notion de qualité de service, ou QoS, concerne certaines caractéristiques d'une connexion réseau relevant de la seule responsabilité du fournisseur du service réseau.

Une valeur de QoS s'applique à l'ensemble d'une connexion réseau. Elle doit être identique aux deux extrémités de la connexion, même si cette dernière est prise en charge par plusieurs sous-réseaux interconnectés offrant chacun des services différents.

La QoS est décrite à l'aide de paramètres. La définition d'un paramètre de QoS indique la façon de mesurer ou de déterminer sa valeur, en mentionnant au besoin les événements spécifiés par les primitives du service réseau.

Deux types de paramètres de QoS ont été définis :

- Ceux dont les valeurs sont transmises entre utilisateurs homologues au moyen du service réseau pendant la phase d'établissement de la connexion réseau. Au cours de cette transmission, une négociation tripartite peut avoir lieu entre les utilisateurs et le fournisseur du service réseau afin de définir une valeur pour ces paramètres de QoS.
- Ceux dont les valeurs ne sont ni transmises ni négociées entre les utilisateurs et le fournisseur du service réseau. Pour ces paramètres de QoS, il est toutefois possible d'obtenir, par des moyens locaux, l'information relative aux valeurs utiles au fournisseur et à chacun des utilisateurs du service réseau.

Les principaux paramètres de QoS sont les suivants :

- Délai d'établissement de la connexion réseau. Correspond au temps qui s'écoule entre une demande de connexion réseau et la confirmation de la connexion. Ce paramètre de QoS indique le temps maximal acceptable par l'utilisateur.
- Probabilité d'échec de l'établissement de la connexion réseau. Cette probabilité est établie à partir des demandes qui n'ont pas été satisfaites dans le temps normal imparti pour l'établissement de la connexion.
- Débit du transfert des données. Le débit définit le nombre d'octets transportés sur une connexion réseau dans un temps raisonnablement long (quelques minutes, quelques heures ou quelques jours). La difficulté à déterminer le débit d'une connexion réseau provient de l'asynchronisme du transport des paquets. Pour obtenir une valeur acceptable, il faut observer le réseau sur une suite de plusieurs paquets et considérer le nombre d'octets de données transportés en tenant compte du temps écoulé depuis la demande ou l'indication de transfert des données.
- Temps de transit lors du transfert des données. Le temps de transit correspond au temps écoulé entre une demande de transfert de données et l'indication de transfert des données. Ce temps de transit est difficile à calculer du fait de la distribution géographique des extrémités. La satisfaction d'une qualité de service sur le temps de transit peut de surcroît entrer en contradiction avec un contrôle de flux.
- Taux d'erreur résiduelle. Se calcule à partir du nombre de paquets qui arrivent erronés, perdus ou en double sur le nombre total de paquets émis. C'est donc un taux d'erreur par paquet. Désigne également la probabilité qu'un paquet n'arrive pas correctement au récepteur.
- Probabilité d'incident de transfert. Est obtenue par le rapport du nombre d'incident répertorié sur le nombre total de transfert effectué. Pour avoir une estimation correcte de cette probabilité, il suffit d'examiner le nombre de déconnexion du réseau par rapport au nombre de transfert effectué.
- Probabilité de rupture de la connexion réseau. Se calcule à partir du nombre de libération et de réinitialisation d'une connexion réseau par rapport au nombre de transfert effectué.
- Délai de libération de la connexion réseau. C'est le délai maximal acceptable entre une demande de déconnexion et la libération effective.
- Probabilité d'échec lors de la libération de la connexion réseau. C'est le nombre d'échec de libération demandée par rapport au nombre total de libération demandé.

Les trois paramètres additionnels suivants permettent de caractériser la qualité de service :

- Protection de la connexion réseau. Détermine la probabilité que la connexion réseau soit en état de marche durant toute la période où elle est ouverte par l'utilisateur. Il y a plusieurs moyens de protéger une connexion en la dupliquant ou en ayant une connexion de sauvegarde prête à être ouverte en cas de coupure. La valeur pour un réseau téléphonique est de 99,999 %, que l'on appelle les cinq neuf, ce qui équivaut à quelques minutes d'indisponibilité par an. La protection est beaucoup plus faible pour un réseau IP, avec une valeur de l'ordre de 99,9 %, ou trois neuf. Cette valeur pose

d'ailleurs problème pour la téléphonie sur IP, qui demande une protection plus forte des connexions téléphoniques.

- Priorité de la connexion réseau. Détermine la priorité d'accès à une connexion réseau, la priorité de maintien d'une connexion réseau et la priorité des données sur la connexion.
- Coût maximal acceptable. Détermine si la connexion réseau est tolérable ou non. La définition du coût est assez complexe puisqu'elle dépend de l'utilisation des ressources nécessaires à la mise en place, au maintien et à la libération de la connexion réseau.

IP (Internet Protocol)

Le protocole de base du réseau Internet s'appelle IP, pour Internet Protocol. L'objectif de départ assigné à ce protocole est d'interconnecter des réseaux n'ayant pas les mêmes protocoles de niveau trame ou de niveau paquet. Le sigle Internet vient d'*inter-networking* et correspond à un mode d'interconnexion : chaque réseau indépendant doit transporter dans sa trame ou dans la zone de données de son paquet un paquet IP, comme illustré à la figure 7.14.

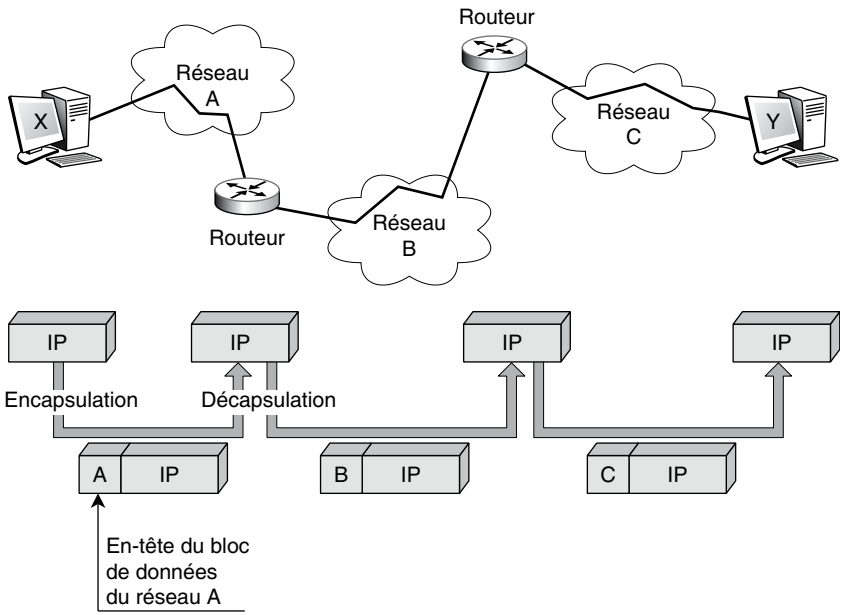


Figure 7.14

Interconnexion réseau

Il existe deux générations de paquets IP, appelées IPv4 (IP version 4) et IPv6 (IP version 6). IPv4 a été prépondérant jusqu'à maintenant. Le passage à IPv6 pourrait s'accélérer du fait de son adoption dans de nombreux pays asiatiques. La transition est cependant difficile et durera de nombreuses années.

Les protocoles IPv4 et IPv6

Première génération du protocole IP, IPv4 est implémenté dans toutes les stations connectées au réseau Internet. La différence fondamentale avec IPv6 réside dans un paquet pourvu de peu de fonctionnalités, puisqu'il n'est vu que comme une syntaxe commune pour échanger de l'information. Avec la deuxième génération IPv6, qui commence à être mise en œuvre, le changement de vision est sans équivoque, puisque le paquet IP devient un véritable paquet, avec toutes les fonctionnalités nécessaires pour être traité et contrôlé dans les nœuds du réseau.

Comme nous l'avons déjà vu à plusieurs reprises, IP propose un service sans connexion. Ce mode sans connexion explique les attentes assez longues lors de l'interrogation de serveurs très fréquentés. Même surchargés, ces derniers ne peuvent refuser l'arrivée de nouveaux paquets puisque l'émetteur ne demande aucune connexion, c'est-à-dire ne se préoccupe pas de savoir si le serveur accepte de les servir.

Les paquets d'un même flot, partant d'une machine et allant vers une autre, peuvent utiliser des routes différentes, Internet se chargeant du routage des paquets IP indépendamment les uns des autres. Le protocole IP définit l'unité de donnée ainsi que le format de toutes les données qui transitent dans le réseau. Il inclut également un ensemble de règles, qui définissent comment traiter les paquets, gérer la fonction de routage et répondre à certains types d'erreurs.

Il existe une analogie entre le réseau physique et le réseau logique dans lequel s'inscrit IP. Dans un réseau physique, l'unité transférée est la trame — en réalité un paquet ou une trame — du sous-réseau traversé. Cette trame comporte un en-tête et des données, ces dernières étant incluses dans le paquet IP. L'en-tête contient les informations de supervision nécessaires pour acheminer la trame.

Dans le réseau IP logique, l'unité de base à transférer est le paquet IP, que l'on appelle datagramme IP, Les datagrammes peuvent être d'une longueur quelconque. Comme ils doivent transiter de routeur en routeur, ils peuvent être fractionnés, de sorte à s'adapter à la structure de la trame sous-jacente. Ce concept est appelé l'encapsulation. Pour un sous-réseau, un datagramme est une donnée comme une autre. Dans le meilleur des cas, le datagramme est contenu dans une seule trame, ce qui rend la transmission plus performante.

Les sections qui suivent examinent la structure des paquets IPv4 et IPv6. Le chapitre 16 est consacré aux réseaux IP en général.

IPv4

Le service rendu par le protocole IPv4 se fonde sur un système de remise de paquets non fiable, que l'on appelle service best-effort, c'est-à-dire « au mieux » et sans connexion. Le service est dit non fiable, car la remise ne présente aucune garantie. Un paquet peut être perdu, dupliqué ou remis hors séquence, sans qu'Internet ne le détecte ni n'en informe l'émetteur ou le récepteur.

La figure 7.15 illustre le format du paquet IPv4. Après la valeur 4, pour le numéro de version, est indiquée la longueur de l'en-tête, qui permet de connaître l'emplacement du

début des données du fragment IP. Le champ suivant, ToS (Type of Service), précise le type de service des informations transportées dans le corps du paquet. Ce champ n'a jamais été réellement utilisé avant l'arrivée des nouveaux protocoles de gestion relatifs à la qualité de service, comme DiffServ (Differentiated Services), qui sont présentés au chapitre 17. Vient ensuite la longueur totale (Length). Le champ suivant (Identification) identifie le message auquel appartient le paquet : le message a été découpé en paquets et il faut être capable au récepteur de savoir à quel message appartient le paquet.

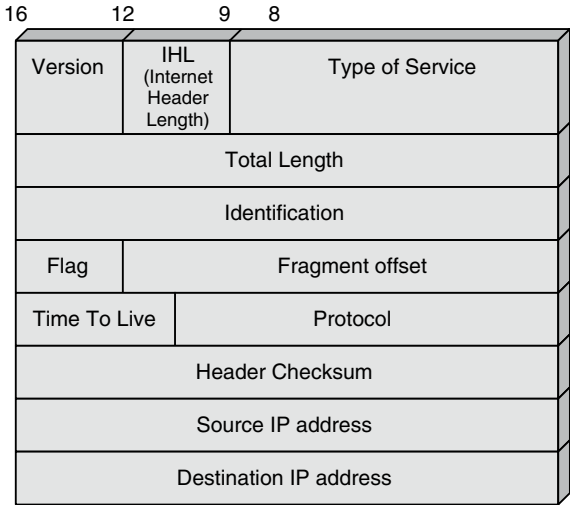


Figure 7.15

Format du paquet IPv4

Le drapeau (Flag) porte plusieurs notifications. Il précise, en particulier, si une segmentation a été effectuée. Si oui, la place du segment, provenant de la segmentation du message de niveau 4, est indiquée dans le champ Offset, ou emplacement du segment. Le champ TTL (Time To Live), ou temps de vie, spécifie le temps après lequel le paquet est détruit. Si le paquet ne trouve plus son chemin ou effectue des allers-retours, il est éliminé au bout d'un certain temps. Dans la réalité, cette zone contient une valeur entière, indiquant le nombre de nœuds qui peuvent être traversés avant destruction du paquet. La valeur 16 est utilisée sur Internet pour indiquer qu'un paquet IP qui traverse plus de 15 routeurs est détruit.

Le numéro de protocole indique le protocole qui a été encapsulé à l'intérieur du paquet. La zone de détection d'erreur permet de déterminer si la transmission du paquet s'est effectuée correctement ou non. Enfin, les adresses de l'émetteur et du récepteur sont précisées dans la dernière partie de l'en-tête. Elles prennent une place de 4 octets chacune.

Comme Internet est un réseau de réseaux, l'adressage est particulièrement important. Les machines reliées à Internet ont une adresse IPv4 représentée sur un entier de 32 bits. L'adresse est constituée de deux parties : un identificateur de réseau et un identificateur

de machine pour ce réseau. Il existe quatre classes d'adresses, chacune permettant de coder un nombre différent de réseaux et de machines :

- classe A, 128 réseaux et 16 777 216 hôtes (7 bits pour les réseaux et 24 pour les hôtes) ;
- classe B, 16 384 réseaux et 65 535 hôtes (14 bits pour les réseaux et 16 pour les hôtes) ;
- classe C, 2 097 152 réseaux et 256 hôtes (21 bits pour les réseaux et 8 pour les hôtes) ;
- classe D, adresses de groupes (28 bits pour les hôtes appartenant à un même groupe).

Ces adresses sont illustrées à la figure 7.16.

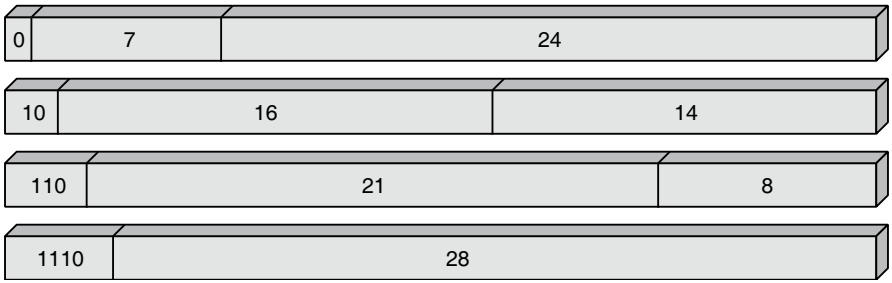


Figure 7.16
Classes d'adresses d'IPv4

Les adresses IP ont été définies pour être traitées rapidement. Les routeurs qui effectuent le routage en se fondant sur le numéro de réseau sont dépendants de cette structure. Un hôte relié à plusieurs réseaux possède plusieurs adresses IP. En fait, une adresse n'identifie pas simplement une machine mais une connexion à un réseau.

IPv6

IPv6, parfois appelé IPng (*next generation*), est un protocole entièrement repensé, qui appartient au niveau paquet. Le format du paquet IPv6 est illustré à la figure 7.17.

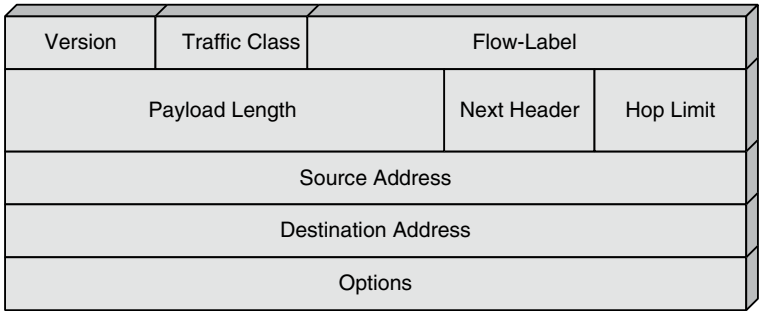


Figure 7.17
Format du paquet IPv6

Pour améliorer les performances, IPv6 interdit la fragmentation et le réassemblage dans les routeurs intermédiaires. Le protocole doit donc choisir la bonne valeur de longueur du datagramme afin qu'il puisse s'encapsuler directement dans les différentes trames ou paquets rencontrés. Si, dans un environnement IPv6, un datagramme se présente à l'entrée d'un sous-réseau avec une taille non acceptable, il est détruit. Comme expliqué précédemment, le niveau paquet représenté par IP est considéré comme un niveau logique d'interconnexion entre sous-réseaux. Ce niveau IP peut devenir un protocole de niveau paquet autosuffisant, utilisable pour transporter les informations sur un réseau. C'est exactement le rôle joué par IPv6.

Le paquet IPv6 comporte les champs suivants :

- Version. Porte le numéro 6.
- Priority (priorité). Indique un niveau de priorité, qui permet de traiter les paquets plus ou moins rapidement dans les nœuds du réseau.
- Flow-Label (référence de flot). Également nouveau, ce champ permet de transporter une référence (label) capable de préciser le flot auquel appartient le paquet et donc d'indiquer la qualité de service exigée par les informations transportées. Cette référence permet aux routeurs de prendre des décisions adaptées. Grâce à ce nouveau champ, le routeur peut traiter de façon personnalisée les paquets IPv6, autorisant ainsi la prise en compte de contraintes diverses.
- Length (longueur). Indique la longueur totale du datagramme en octet, sans tenir compte de l'en-tête. Ce champ étant de 2 octets, la longueur maximale du datagramme est de 64 Ko.
- Next-Header (en-tête suivant). Indique le protocole encapsulé dans la zone de données du paquet. Ce processus est illustré à la figure 7.18. Les options les plus classiques pour la valeur de ce champ sont 0 pour Hop-by-Hop Option Header, 4 pour IP, 6 pour TCP et 17 pour UDP (*voir l'encadré « Valeurs du champ Next-Header »*).

Valeurs du champ Next-Header

- 0 Hop-by-Hop Option Header
- 4 IP
- 6 TCP
- 17 UDP
- 43 Routing Header
- 44 Fragment Header
- 45 IRP (Interdomain Routing Protocol)
- 4 RSVP (ReSource Reservation Protocol)
- 50 ESP (Encapsulating Security Payload)
- 51 Authentication Header
- 58 ICMP
- 59 No Next-Header
- 60 Destination Options Header

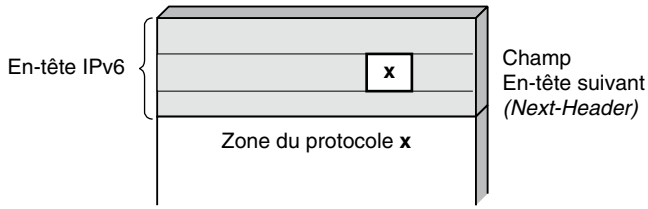


Figure 7.18
Champ en-tête suivant (Next-Header)

- Hop limit (nombre maximal de nœuds traversés). Indique après combien de nœuds le paquet est détruit.
- Address. La zone d'adresse est souvent présentée comme la raison d'être de la nouvelle version d'IP. En fait, c'est seulement une raison parmi d'autres. L'adresse IPv6 tient sur 16 octets. La difficulté réside dans la représentation et l'utilisation rationnelle de ces 128 bits. Le nombre d'adresses potentielles dépasse 1023 pour chaque mètre carré de la surface terrestre. La représentation s'effectue par groupe de 16 bits et se présente sous la forme 123:FCBA:1024:AB23:0:0:24:FEDC. Des séries d'adresses égales à 0 peuvent être abrégées par le signe ::, qui ne peut apparaître qu'une seule fois dans l'adresse, comme dans l'exemple 123:FCBA:1024:AB23::24:FEDC. Ce signe n'indique pas le nombre de 0 successifs. Pour déduire ce nombre, les autres séries ne peuvent être abrégées. S'il existait deux séries abrégées, il serait impossible d'en déduire la longueur respective de chacune. L'adressage IPv6 est hiérarchique. Une allocation des adresses a été proposée, dont le détail est donné au tableau 7.5.

Adresse	Premiers bits de l'adresse	Caractéristiques
0 :: /8	0000 0000	Réservée
100 :: /8	0000 0001	Non assignée
200 :: /7	0000 0001	Adresse ISO
400 :: /7)	0000 010	Adresse Novell (IPX)
600 :: /7	0000 011	Non assignée
800 :: /5	0000 1	Non assignée
1000 :: /4	0001	Non assignée
2000 :: /3	001	Non assignée
4000 :: /3	010	Adresse de fournisseur de services
6000 :: /3	011	Non assignée
8000 :: /3	100	Adresse géographique d'utilisateur
A000 :: /3	101	Non assignée
C000 ::/3	110	Non assignée
E000 :: /4	1110	Non assignée
F000 :: /5	1111 0	Non assignée
F800 :: /6	1111 10	Non assignée
FC00 :: /7	1111 110	Non assignée
FE00 :: /9	1111 1110 0	Non assignée
FE80 :: /10	1111 1110 10	Adresse de liaison locale
FEC0 :: /10	1111 1110 11	Adresse de site local
FF00 :: /8	1111 1111	Adresse de multipoint

TABLEAU 7.5 • Adresses d'IPv6

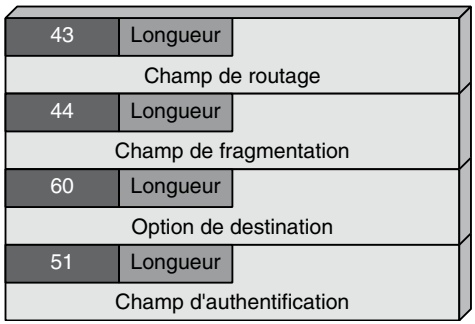


Figure 7.19

Champs d'options du paquet IPv6

- Options. L'en-tête du paquet IPv6 se termine par un champ d'options qui permet l'ajout de nouvelles fonctionnalités, en particulier concernant la sécurité. La figure 7.19 illustre le fonctionnement de ce champ d'options. Chaque zone d'option commence par un champ portant un numéro correspondant au type d'option. Dans ce champ d'options, les différentes zones se suivent dans un ordre prédéterminé, qui est dicté par leur utilisation potentielle dans les nœuds intermédiaires. Si un nœud intermédiaire ne peut prendre en charge une option, plusieurs cas de figure se présentent : destruction du paquet, émission sans traitement, émission d'une signalisation ou attente d'une réponse pour prendre une décision. La figure 7.20 donne une idée de l'ordre de traitement.

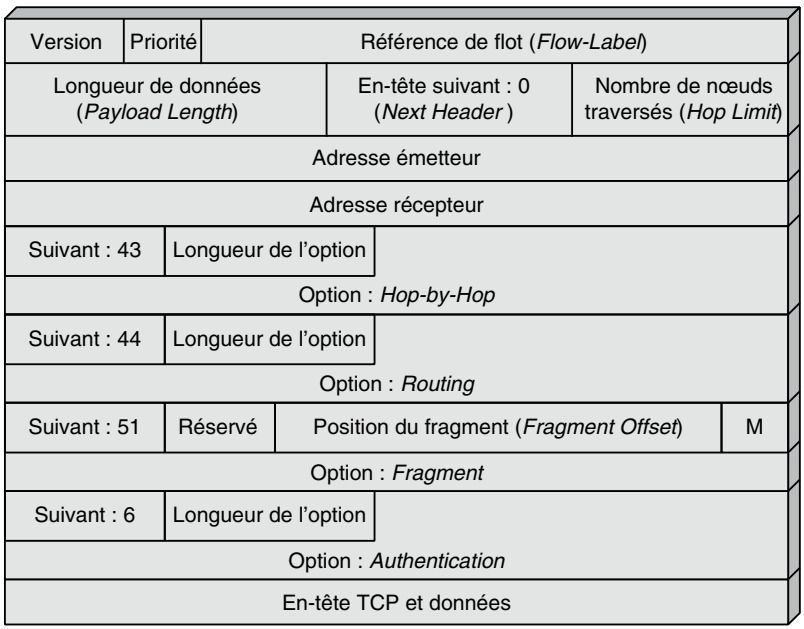


Figure 7.20

Traitement des options d'extension

Conclusion

Le protocole IP a pris le devant de la scène depuis les années 95. C'est une norme de fait, vieille de plus de vingt-cinq ans, bien connue aujourd'hui et qui a le grand mérite d'être conceptuellement simple. En revanche, l'ingénierie des réseaux IP reste un domaine complexe, pas encore totalement maîtrisé. Le rôle de la version IPv6 est de proposer un protocole beaucoup plus maîtrisable, grâce à de nouveaux champs permettant d'introduire une adresse mieux construite, une zone d'identification des flux et de nombreuses options, en particulier dans le domaine de la sécurité. Cependant, toutes les nouveautés introduites dans IPv6 ont été ajoutées à IPv4.

Reste que le coût de passage à IPv6 est loin d'être négligeable. Le monde occidental considère souvent que ce coût est disproportionné en comparaison de l'apport réel d'IPv6 par rapport aux dernières versions d'IPv4.

Quoi qu'il en soit, IPv6 remplace petit à petit IPv4. L'arrivée massive de terminaux mobiles et l'adressage direct de toutes les stations terminales impliquent l'adoption de l'adresse de nouvelle génération. La reconnaissance des flux aidera à l'introduction de nouvelles fonctions de sécurité, de qualité de service et de contrôle de la mobilité.

8

Le niveau message

Le niveau message concerne le transfert de bout en bout des données d'une extrémité à une autre d'un réseau. Les données de l'utilisateur sont regroupées en messages, bien que cette entité ne soit pas parfaitement définie. Ces messages doivent être transportés de l'émetteur vers le récepteur. C'est la raison pour laquelle ce niveau s'appelle également couche transport. C'est d'ailleurs le terme que l'on retrouve dans la nomenclature du modèle de référence.

Le message est une entité logique de l'utilisateur émetteur, sa longueur n'étant pas déterminée à l'avance. Le niveau message s'appuie sur des fonctionnalités capables d'acheminer les informations d'une extrémité à l'autre du réseau. Il correspond à un protocole de bout en bout. Sa définition est précise : garantir l'acheminement du message de l'émetteur au récepteur, éventuellement en traversant plusieurs réseaux. En comparaison, le niveau paquet n'a pour ambition que de faire le nécessaire pour assurer la traversée d'un réseau. Par déduction, aucun niveau message ne doit être traversé avant d'atteindre l'équipement terminal de destination, sinon la transmission ne serait pas de bout en bout.

Après avoir examiné les fonctionnalités que l'on retrouve dans tout niveau message, ce chapitre présente assez succinctement les principaux protocoles provenant des architectures OSI, ATM et Internet.

Les fonctionnalités du niveau message

Le niveau message est directement lié aux fonctionnalités de la couche 4 (transport) du modèle de référence, mais il prend aussi en compte les niveaux équivalents des autres architectures, TCP en particulier. Son rôle peut être décrit assez formellement par les trois propriétés définies pour la couche transport, à savoir le transport de bout en bout, la sélection d'une qualité de service et la transparence.

La couche transport doit permettre la communication entre deux utilisateurs situés dans des systèmes différents, indépendamment des caractéristiques des sous-réseaux sur lesquels s'effectue le transfert des données. Un utilisateur du service de transport n'a pas la possibilité de savoir si un ou plusieurs réseaux sous-jacents sont mis en jeu dans la communication qui l'intéresse.

La figure 8.1 illustre une connexion de transport mettant en jeu plusieurs réseaux mis bout à bout, ou concaténés. Le rôle de la couche transport est de réaliser l'exploitation de la liaison de transport établie entre X et Y. Les problèmes inhérents au routage et à la concaténation des liaisons de réseau sont pris en compte par la couche 3. Dans une connexion de transport, les informations doivent être délivrées dans l'ordre, sans perte ni duplication.

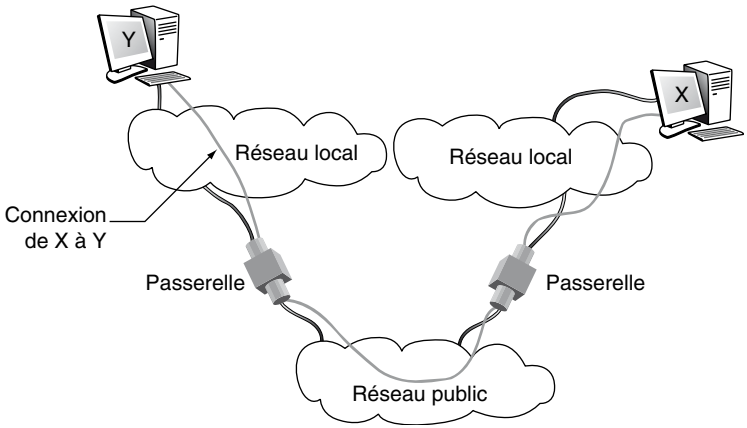


Figure 8.1

Exemple de connexion de bout en bout

Pour atteindre la qualité de service souhaitée par les utilisateurs du service de transport, le protocole de transport doit optimiser les ressources réseau disponibles, et ce au moindre coût. La notion de qualité de service est définie par la valeur de certains paramètres, dont l'ISO a établi une liste exhaustive :

- délai d'établissement d'une connexion de transport ;
- probabilité d'échec de l'établissement d'une connexion ;
- débit des informations sur une connexion de transport ;
- temps de traversée de la connexion : temps écoulé entre l'émission des données et leur réception à l'autre extrémité de la connexion ;
- taux d'erreur résiduelle : taux des erreurs non corrigées rencontrées sur une connexion ;
- probabilité de panne : probabilité d'arrêt d'une connexion de transport non souhaitée par les utilisateurs ;
- délai de déconnexion : temps maximal acceptable pour déterminer proprement une connexion de transport ;

- probabilité d'échec de déconnexion : probabilité d'une déconnexion non coordonnée entre les utilisateurs, aboutissant souvent à des pertes d'information ;
- protection des connexions de transport, au sens de maintien d'une sécurité, pour éviter les manipulations non autorisées de données circulant sur une connexion de transport ;
- priorité des connexions : importance relative d'utiliser différentes connexions en cas de problème majeur au risque de dégrader la qualité de service d'une liaison, voire de la terminer ;
- fragilité d'une connexion : probabilité de coupure accidentelle d'une connexion de transport déjà établie.

Les informations échangées sur une connexion de transport le sont indépendamment de leur format, de leur codage ou de leur signification. C'est ce qu'on appelle un mode transparent. Cette transparence s'obtient essentiellement par des protocoles de plus bas niveau, qui doivent également travailler dans un mode transparent.

La couche transport se fonde sur une méthode d'adressage indépendante des conventions utilisées dans les couches inférieures. Son rôle consiste à réaliser une correspondance entre l'adresse de transport d'un utilisateur donné et une adresse de réseau pour pouvoir initialiser la communication.

Caractéristiques du niveau message

Il est intéressant de remarquer le parallèle qui existe entre les spécifications du niveau message, ou couche 4 (transport) et celles du niveau paquet, ou couche 3 (réseau). En un certain sens, ces deux niveaux doivent réaliser des transports performants au travers de plusieurs nœuds. Les différences fondamentales suivantes entre les deux niveaux sont toutefois à considérer :

- Les problèmes d'adressage sont plus simples au niveau paquet qu'au niveau message.
- La notion d'établissement d'un circuit virtuel au niveau paquet a un sens plus pratique : il faut ouvrir un chemin que les différents paquets vont suivre.
- La connexion établie au niveau message se caractérise par une quantité d'information importante en cours de transmission à l'intérieur du réseau. Cette propriété provient de la traversée potentielle de plusieurs réseaux de couche 3 (*voir figure 8.1*). Au niveau paquet, la mémoire du support de transmission est souvent beaucoup plus faible, à l'exception des réseaux par satellite.

La notion de transparence, énoncée précédemment en tant que propriété de la couche transport, implique la possibilité d'acheminer des informations de taille quelconque. C'est la transparence vis-à-vis du format des données. En pratique, cela signifie que la réalisation d'une entité de transport nécessite une gestion complexe des mémoires de stockage des informations. En pratique, il faut être capable de gérer des tampons à même de stocker des TPDU d'une taille variant entre 128 et 8 192 octets dans le protocole normalisé et jusqu'à 64 Ko dans Internet.

Adresses et chemins de données

La figure 8.2 illustre les connexions entre plusieurs utilisateurs situés sur deux machines distantes. Nous supposons que le réseau de communication utilise des circuits virtuels.

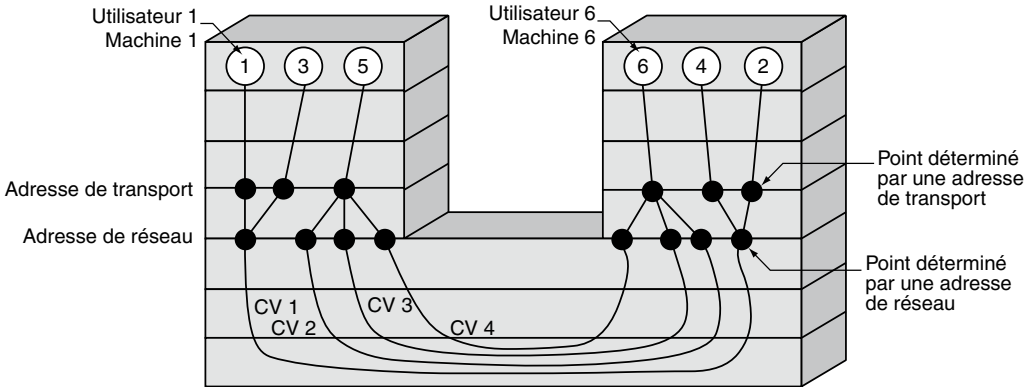


Figure 8.2

Adressage et chemin de données

Les adresses de transport indiquées sont les points d'accès au service de transport visibles par la couche de protocole supérieure, c'est-à-dire la couche session. Cet exemple montre l'optimisation que prend en charge le niveau message grâce au multiplexage et à l'éclatement. Le multiplexage correspond au partage d'une connexion réseau (CV, ou circuit virtuel, 1) par plusieurs connexions de transport (1-2 et 3-4). L'éclatement correspond à l'utilisation de plusieurs connexions réseau (CV 2, CV 3 et CV 4) par une même connexion de transport (5-6). Ces deux mécanismes permettent d'optimiser les coûts et les performances d'une connexion. On a recours au multiplexage lorsque, par exemple, des connexions de transport à faible débit sont nécessaires en grand nombre. On utilise l'éclatement pour maximiser le débit d'une connexion de transport qui doit s'établir sur un réseau à faibles performances.

Localisation des couches de protocoles dans un système informatique

Il est intéressant de situer dès maintenant les différentes couches de protocoles de communication dans un système informatique en contexte réseau. La figure 8.3 montre comment se répartissent le plus souvent les couches de protocoles entre un ordinateur et son frontal chargé des communications. Le partage des fonctions met en évidence la séparation entre les couches hautes (5, 6 et 7) et les couches basses (1, 2 et 3) de l'ISO — les premières sont orientées traitement, et les secondes communication —, ainsi que le rôle charnière joué par le niveau message.

L'informatique personnelle a toutefois modifié cette répartition. L'ordinateur personnel gère en effet les couches hautes, le niveau message et le niveau paquet IP. La carte réseau que l'on ajoute s'occupe pour sa part des couches inférieures (1 et 2). Comme le montre la figure 8.3, les couches 3 et 4 qui se trouvaient chez l'opérateur sur la machine frontale se retrouvent ici du côté de l'ordinateur, devenu un micro-ordinateur. La carte coupleur qui a pris la place du frontal ne prend plus en compte que les deux couches les plus basses.

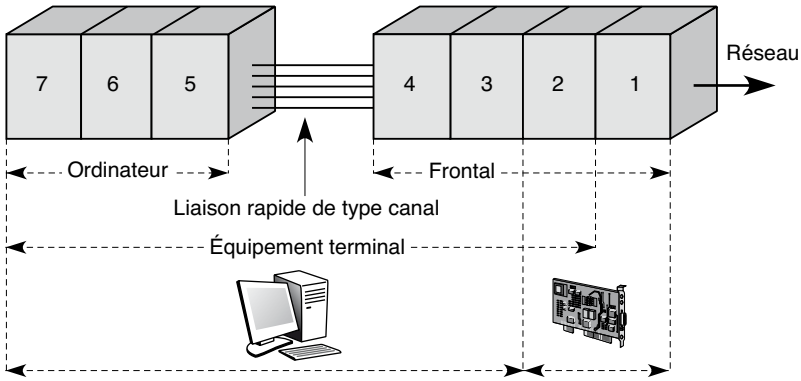


Figure 8.3

Répartition des couches de protocoles dans un équipement terminal

Négociation d'une qualité de service

Nous avons vu précédemment que la sélection d'une qualité de service figurait parmi les possibilités du niveau message. On peut se demander qui sélectionne cette qualité de service. La réponse est relativement simple : l'utilisateur du service de transport exprime son souhait en termes de qualité de service, et le prestataire de service lui indique en réponse s'il peut ou non satisfaire ses exigences. S'il ne le peut pas, il précise la qualité de service qu'il peut offrir par rapport aux demandes initiales. Ce processus s'appelle la négociation. Elle s'applique à chaque paramètre négociable d'une connexion de transport.

La figure 8.4 illustre le déroulement d'une telle négociation pour le choix du débit effectif d'information sur une connexion en cours d'établissement. Dans une situation réelle, tous les paramètres sont négociés de cette façon, soit successivement, soit simultanément. Dans certains cas, des explications peuvent être fournies par le prestataire du service de transport indiquant les raisons du choix final.

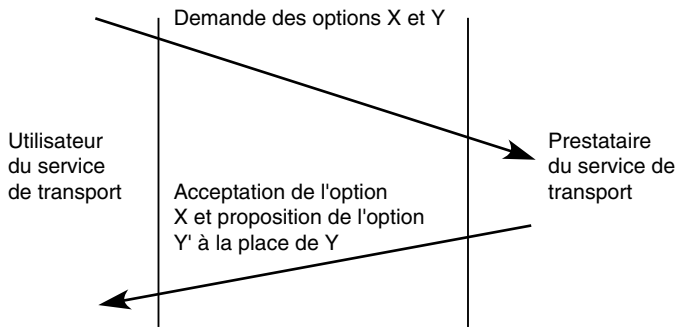


Figure 8.4

Négociation d'un paramètre de connexion

La vie d'une connexion de transport

Comme pour les connexions de niveau inférieur, la vie d'une connexion de transport peut être divisée en trois phases : établissement, transfert de données et libération. La phase d'établissement permet la négociation des différents paramètres de qualité de service puis l'ouverture des connexions réseau nécessaires. La phase de libération garantit une fin de connexion reconnue aux deux extrémités de la liaison. Les deux participants à une connexion doivent savoir s'il y a eu perte de données ou non lors de la déconnexion.

Les protocoles de niveau message

Cette section se penche sur les protocoles de niveau message provenant des architectures Internet, Ethernet et ATM. Nous examinons le cas de l'architecture OSI à l'annexe G.

TCP et UDP, les deux protocoles de niveau message les plus importants, proviennent du monde Internet. Nous allons les étudier en premier. Nous regarderons ensuite plus succinctement les protocoles de niveau message associés aux mondes Ethernet et ATM.

Le protocole TCP

Le réseau Internet utilise le protocole IP au niveau paquet. Le niveau message offre deux autres possibilités : le protocole TCP (Transmission Control Protocol), qui introduit plusieurs fonctionnalités garantissant une certaine qualité du service de transport, et le protocole UDP (User Datagram Protocol), beaucoup plus simple mais ne donnant aucune garantie sur le transport des messages. La simplicité d'UDP offre en contrepartie des débits plus élevés.

TCP offre un service de transport fiable. Les données échangées sont considérées comme un flot de bits divisé en octets, ces derniers devant être reçus dans l'ordre où ils sont envoyés. Le transfert des données ne peut commencer qu'après l'établissement d'une connexion entre deux machines. Cet établissement est illustré à la figure 8.5. Durant le transfert, les deux machines continuent à vérifier que les données transitent correctement.

Les programmes d'application envoient leurs données en les passant régulièrement au système d'exploitation de la machine. Chaque application choisit la taille de données qui lui convient. Le transfert peut être, par exemple, d'un octet à la fois. L'implémentation TCP est libre de découper les données en paquets d'une taille différente de celle des blocs reçus de l'application. Pour rendre le transfert plus performant, l'implémentation TCP attend d'avoir suffisamment de données avant de remplir un datagramme et de l'envoyer sur le sous-réseau.

Ouverte dans les deux sens de transmission à la fois, la connexion garantit un transfert de données bidirectionnel, avec deux flots de données inverses, sans interaction apparente. Il est possible de terminer l'envoi dans un sens sans arrêter celui dans l'autre sens. Cela permet d'envoyer des acquittements dans un sens de transmission en même temps que des données dans l'autre sens.

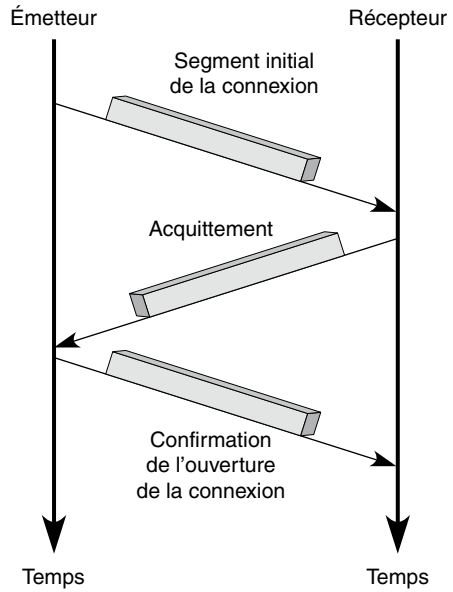


Figure 8.5
Établissement d'une connexion TCP

Le protocole TCP définit la structure des données et des acquittements échangés, ainsi que les mécanismes permettant de rendre le transport fiable. Il spécifie comment distinguer plusieurs connexions sur une même machine et comment détecter des paquets perdus ou dupliqués et remédier à cette situation. Il définit en outre la manière d'établir une connexion et de la terminer. TCP autorise plusieurs programmes à établir une connexion simultanée et à multiplexer les données reçues des différentes applications. Il utilise pour cela la notion abstraite de port, qui identifie une destination particulière dans une machine.

TCP est un protocole en mode avec connexion. Il n'a de sens qu'entre deux points extrémité d'une connexion. Le programme d'une extrémité effectue une ouverture de connexion passive, c'est-à-dire qu'il accepte une connexion entrante en lui affectant un numéro de port. L'autre programme d'application exécute une ouverture de connexion active. Une fois la connexion établie, le transfert de données peut commencer. La notion de port est illustrée à la figure 8.6.

Pour le protocole TCP, un flot de données est une suite d'octets groupés en fragments. Les fragments donnent généralement naissance à un paquet IP. Le protocole TCP utilise un mécanisme de fenêtre pour assurer une transmission performante et un contrôle de flux. Le mécanisme de fenêtre permet l'anticipation, c'est-à-dire l'envoi de plusieurs fragments sans attendre d'acquittement. Le débit s'en trouve amélioré.

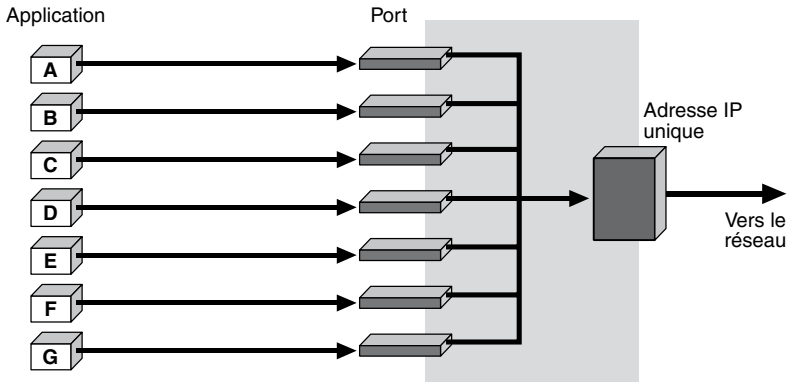


Figure 8.6

Connexion de plusieurs applications sur une même adresse IP

La fenêtre permet également de réaliser un contrôle de flux de bout en bout, en autorisant le récepteur à limiter l'envoi des données tant qu'il n'a pas la place de les recevoir dans ses mémoires. Le mécanisme de fenêtre opère au niveau de l'octet et non du fragment. Les octets à transmettre sont numérotés séquentiellement. L'émetteur gère trois pointeurs pour chaque fenêtre. De la même façon, le récepteur doit tenir à jour une fenêtre en réception, qui indique le numéro du prochain octet attendu, ainsi que la valeur extrême qui peut être reçue. La différence entre ces deux quantités indique la valeur du crédit accepté par le récepteur, valeur qui correspond généralement à la mémoire tampon disponible pour cette connexion. Le contrôle de flux TCP est illustré à la figure 8.7. Nous y revenons un peu plus loin dans ce chapitre.

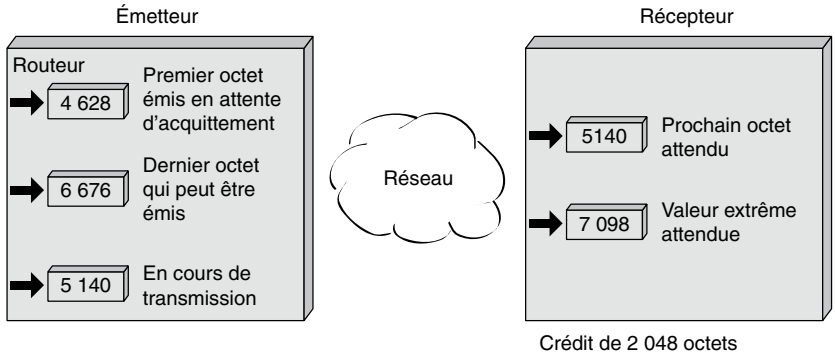


Figure 8.7

Contrôle de flux TCP

Lors d'une connexion, il est possible d'échanger des données dans chaque sens, chaque extrémité de la connexion devant dans ce cas maintenir deux fenêtres, l'une en émission, l'autre en réception.

Le fait que la taille de la fenêtre varie dans le temps constitue une différence importante par rapport à un mécanisme de fenêtre classique. Chaque acquittement, spécifiant combien d'octets ont été reçus, contient une information de taille de fenêtre sur le nombre d'octets supplémentaires que le récepteur est en mesure d'accepter. La taille de la fenêtre peut être considérée comme l'espace disponible dans la mémoire du récepteur. Celui-ci ne peut réduire la fenêtre en deçà d'une certaine valeur, qu'il a acceptée précédemment. Le fait que la taille de la fenêtre puisse varier dans le temps constitue une différence importante par rapport à un mécanisme de fenêtre classique.

L'unité de protocole de TCP étant le fragment, des fragments sont échangés pour établir la connexion, transférer des données, modifier la taille de la fenêtre, fermer une connexion et émettre des acquittements. Chaque fragment est composé de deux parties : l'en-tête et les données. Le format d'un fragment est illustré à la figure 8.8. Les informations de contrôle de flux peuvent être transportées dans le flot de données inverse.

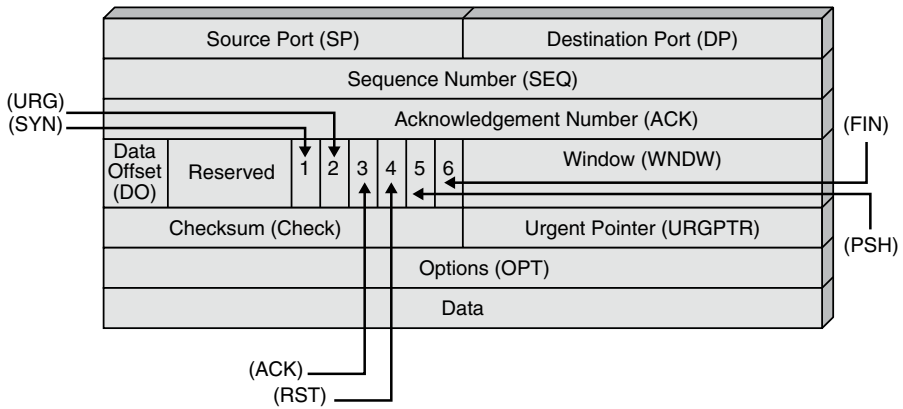


Figure 8.8

Format d'un fragment TCP

Le fragment TCP comporte les zones suivantes :

- SP (Source Port), ou port source. Champ sur 16 bits contenant l'adresse du port d'entrée. Associée à l'adresse IP, cette valeur fournit un identificateur unique, appelé socket, formé à partir de la concaténation de l'adresse IP et du numéro de port. L'identificateur permet de déterminer une application s'exécutant sur une machine terminale.
- DP (Destination Port), ou port de destination. Champ sur 16 bits, dont la fonction est identique au précédent mais pour l'adresse destination.
- SEQ (Sequence Number), ou numéro de séquence. Champ sur 32 bits indiquant le numéro du premier octet porté par le fragment.
- ACK (Acknowledgement Number), ou numéro d'acquittement. Champ sur 32 bits indiquant le numéro SEQ du prochain fragment attendu et correspondant à l'acquittement de tous les octets reçus auparavant. La valeur ACK indique le numéro du premier octet attendu, soit le numéro du dernier octet reçu + 1.

- DO (Data Offset), ou longueur de l'en-tête. Champ sur 4 bits indiquant la longueur de l'en-tête par un multiple de 32 bits. Si la valeur 8 se trouve dans ce champ, la longueur totale de l'en-tête est de 8 × 32 bits. Cette valeur est nécessaire du fait que la zone d'option peut avoir une taille quelconque. On en déduit que la longueur de l'en-tête ne peut dépasser 15 × 32 bits, soit 60 octets.
- La zone suivante est réservée à une utilisation ultérieure. Ce champ doit être rempli de 0.
- URG (Urgent Pointer), ou pointeur d'urgence. Champ sur 1 bit, numéroté 1 à la figure 8.8. Si ce bit a pour valeur 1, le champ Urgent Pointer situé dans la suite de l'en-tête comporte une valeur significative.
- ACK (Acknowledgement), ou acquittement. Champ sur 1 bit, numéroté 3 à la figure 8.8. Si ACK = 1, le champ Acknowledgement Number situé dans l'en-tête comporte une valeur significative, à prendre en compte par le récepteur.
- PSH (Push Function), ou fonction de push. Champ sur 1 bit, numéroté 5 à la figure 8.8. Si PSH = 1, l'émetteur souhaite que les données de ce fragment soient délivrées le plus tôt possible au destinataire.
- RST (Reset), ou redémarrage. Champ sur 1 bit, numéroté 4 à la figure 9.8. Si RST = 1, l'émetteur demande que la connexion TCP redémarre.
- SYN (Synchronization), ou synchronisation. Champ sur 1 bit, numéroté 2 à la figure 8.8. SYN = 1 désigne une demande d'ouverture de connexion. Dans ce cas, le numéro de séquence porte le numéro du premier octet du flot.
- FIN (Terminate), ou fermeture. Champ sur 1 bit, numéroté 6 à la figure 8.8. FIN = 1 signifie que l'émetteur souhaite fermer la connexion.
- WNDW (Window), ou fenêtre. Champ sur 16 bits indiquant le nombre d'octet que le récepteur accepte de recevoir. Plus exactement, la valeur de WNDW contient l'ultime numéro d'octet que l'émetteur du fragment accepte de recevoir. En retranchant le numéro indiqué de la valeur du champ ACK, on obtient le nombre d'octet que le récepteur accepte de recevoir.
- CHECK (Checksum). Champ sur 16 bits permettant de détecter les erreurs dans l'en-tête et le corps du fragment. Les données protégées ne se limitent pas au fragment TCP. Le checksum tient également compte de l'en-tête IP de l'adresse source, appelée pseudo-header, pour protéger ces données sensibles. Un pseudo-header est un en-tête modifié, dont certains champs ont été enlevés et d'autres ajoutés, que la zone de détection d'erreur prend en compte dans son calcul.
- URGPTR (Urgent Pointer), ou pointeur d'urgence. Champ sur 16 bits spécifiant le dernier octet d'un message urgent.
- OPT (Options), ou options. Zone contenant les différentes options du protocole TCP. Si la valeur du champ DO (Data Offset), indiquant la longueur de l'en-tête, est supérieure à 5, c'est qu'il existe un champ d'option. Pour déterminer la longueur du champ d'option, il suffit de soustraire 5 de la valeur de DO. Deux formats travaillent simultanément. Dans un cas, le premier octet indique le type de l'option, lequel définit

implicitement sa longueur, les octets suivants donnant la valeur du paramètre d'option. Dans l'autre cas, le premier octet indique toujours le type de l'option, et le second la valeur de la longueur de l'option. Les principales options concernent la taille du fragment, celle des fenêtres et des temporisateurs, ainsi que des contraintes de routage.

Le fragment se termine par les données transportées.

Les fragments étant de taille variable, les acquittements se rapportent à un numéro d'octet particulier dans le flot de données. Chaque acquittement spécifie le numéro du prochain octet à transmettre et acquitte les précédents.

Les acquittements TCP étant cumulatifs, ils se répètent et se cumulent pour spécifier jusqu'à quel octet le flot a été bien reçu. Par exemple, le récepteur peut recevoir un premier acquittement du flot jusqu'à l'octet 43 568 puis un deuxième jusqu'à l'octet 44 278 et un troisième jusqu'à l'octet 44 988, indiquant trois fois que jusqu'à l'octet 43 568 tout a été bien reçu. Ce principe cumulatif permet de perdre les deux premiers acquittements sans conséquence.

Ce processus présente des avantages mais aussi des inconvénients. Un premier avantage est d'avoir des acquittements simples à générer et non ambigus. Un autre avantage est que la perte d'un acquittement n'impose pas nécessairement de retransmission. En revanche, l'émetteur ne reçoit pas les acquittements de toutes les transmissions réussies mais seulement la position dans le flot des données qui ont été reçues. Ce processus est illustré à la figure 8.9. Pour simplifier la figure, nous avons indiqué des numéros de paquet. En fait ce sont des numéros d'octet qui sont transmis.

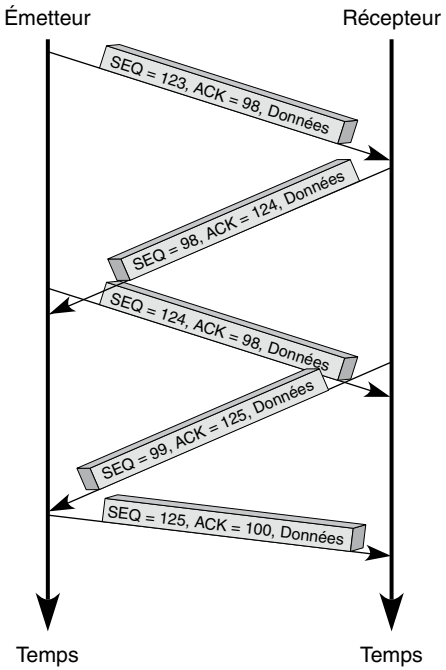


Figure 8.9

Processus des acquittements dans TCP

La façon de gérer les temporisateurs et les acquittements constitue l'une des caractéristiques essentielles du protocole TCP, qui se fonde sur le principe des acquittements positifs. Chaque fois qu'un fragment est émis, un temporisateur est déclenché, en attente de l'acquittement. Si l'acquittement arrive avant que le temporisateur parvienne à échéance, le temporisateur est arrêté.

Si le temporisateur expire avant que les données du fragment aient été acquittées, TCP suppose que le fragment est perdu et le retransmet. Ce processus est illustré à la figure 8.10.

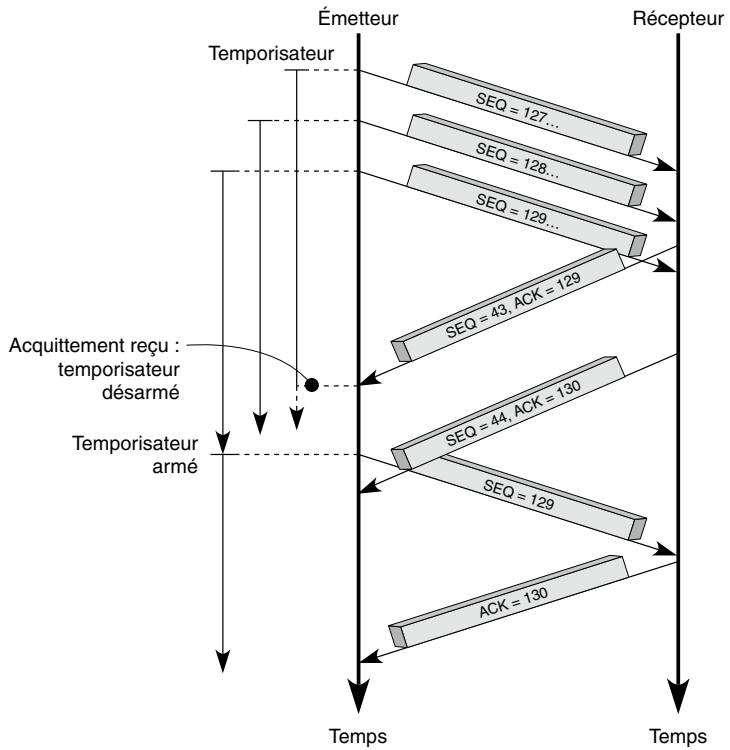


Figure 8.10
Processus de reprise dans TCP

Fonctionnement du temporisateur de reprise

TCP ne faisant aucune hypothèse sur le temps de transit dans les réseaux traversés, il est impossible de connaître *a priori* l'instant d'arrivée d'un acquittement. De plus, le temps de traversée des routeurs et des passerelles dépend de la charge du réseau, laquelle varie elle-même dans le temps. TCP utilise un algorithme adaptatif pour prendre en compte ces variations. Il enregistre pour cela l'heure à laquelle il a envoyé le fragment et l'heure à laquelle il reçoit l'acquittement correspondant. Après plusieurs mesures de ce type, l'émetteur effectue une estimation du temps nécessaire à la réception de l'acquittement. Cette estimation lui permet de déterminer une durée pour le temporisateur de reprise.

Lors d'une congestion, TCP réagit en réduisant le débit de la connexion. Le protocole a la possibilité de mesurer l'importance du problème en observant l'augmentation du temps de réponse. Si le protocole ne réagit pas aux congestions, le nombre de retransmission peut continuer à augmenter et aggraver ainsi la congestion.

C'est la raison pour laquelle un algorithme de contrôle réduit le flux en cas de congestion. Cet algorithme, appelé *slow-start and collision avoidance*, littéralement « départ lent et évitement de collision », doit être entièrement distribué puisqu'il n'existe pas de système central de contrôle dans TCP. Son principe consiste à débuter d'une fenêtre de taille 1 et à doubler la taille de la fenêtre chaque fois que l'ensemble des paquets de la fenêtre a été bien reçu avant la fin des temporisateurs de reprise respectifs. Lorsqu'un fragment arrive en retard, c'est-à-dire après que le temporisateur est arrivé à échéance, il est retransmis en redémarrant à une fenêtre de 1.

Au cours de la deuxième phase de l'algorithme, collision avoidance, lorsqu'un retard est détecté, qui oblige à un redémarrage sur une fenêtre de 1, la taille de la fenêtre *N* qui a provoqué le retard est divisée par 2 (*N*/2). À partir de la valeur de la taille 1 de redémarrage, la taille double jusqu'à ce que la taille de la fenêtre dépasse *N*/2. À ce moment, on revient à la taille précédente, qui était inférieure à *N*/2, et, au lieu de doubler, on ajoute seulement 1 à la taille de la fenêtre. Ce processus d'ajout de 1 se continue jusqu'à ce qu'un retard d'acquittement redémarre le processus à la fenêtre de taille 1. La nouvelle valeur qui déclenche la partie collision avoidance est calculée à partir de la fenêtre atteinte divisée par deux.

Un exemple de comportement de cet algorithme est illustré à la figure 8.11.

On pourrait croire que le système n'est jamais stable, mais il conserve un moyen de se stabiliser. Lorsque les acquittements arrivent avant que la fenêtre soit atteinte, cela indique que le débit maximal de la liaison est atteint et qu'il n'est plus nécessaire d'augmenter la valeur de la fenêtre.

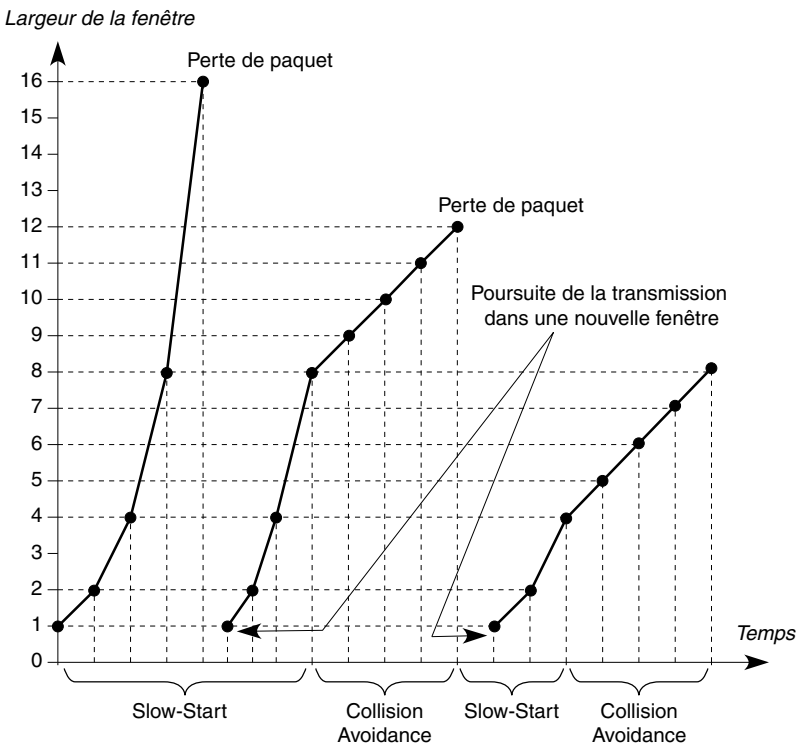


Figure 8.11

Fonctionnement de l'algorithme slow-start and collision avoidance

Le protocole UDP

Le protocole UDP permet aux applications d'échanger des datagrammes. Il utilise pour cela la notion de port, qui permet de distinguer les différentes applications qui s'exécutent sur une machine. Outre le datagramme et ses données, un message UDP contient un numéro de port source et un numéro de port destination.

Le protocole UDP fournit un service en mode sans connexion et sans reprise sur erreur. Il n'utilise aucun acquittement, ne reséquence pas les messages et ne met en place aucun contrôle de flux. Il se peut donc que les messages UDP qui se perdent soient dupliqués, remis hors séquence ou qu'ils arrivent trop tôt pour être traités lors de leur réception. Comme expliqué précédemment, UDP est un protocole particulièrement simple du niveau message de l'architecture du modèle de référence. Il présente l'avantage d'une exécution rapide, tenant compte de contraintes temps réel ou d'une limitation de place sur un processeur. Ces contraintes ou limitations ne permettent pas toujours l'utilisation de protocoles plus lourds, comme TCP.

Les applications qui n'ont pas besoin d'une forte sécurité au niveau transmission, et elles sont nombreuses, ainsi que les logiciels de gestion, qui requièrent des interrogations rapides de ressources, préfèrent utiliser UDP. Les demandes de recherche dans les annuaires transitent par UDP, par exemple.

Pour identifier les différentes applications, UDP impose de placer dans chaque fragment une référence qui joue le rôle de port. La figure 8.12 illustre le fragment UDP. Une référence identifie, un peu comme le champ En-tête suivant dans IPv6, ce qui est transporté dans le corps du fragment. Les applications les plus importantes qui utilisent le protocole UDP correspondent aux numéros de port suivants :

- 7 : service écho ;
- 9 : service de rejet ;
- 53 : serveur de nom de domaine DNS (Dynamic Name Server) ;
- 67 : serveur de configuration DHCP ;
- 68 : client de configuration DHCP.

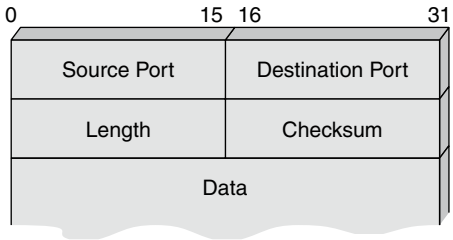


Figure 8.12
Fragment UDP

Les protocoles associés à Ethernet

Ethernet symbolise la couche 2 et non les couches 3 et 4. En fait, Ethernet est très lié au monde IP puisque c'est la trame principale, avec la trame PPP, permettant de transporter des paquets IP et donc des messages TCP et UDP. Comme Ethernet, dans le cadre standard, ne détecte pas les pertes de trames, c'est le protocole TCP qui s'en occupe. Lorsqu'un segment TCP n'est pas reçu, la fenêtre de contrôle de TCP s'en aperçoit. Le protocole interprète cette perte comme une congestion du réseau puisque l'acquittement n'a pas été reçu dans les temps. Le protocole TCP demande dans ce cas la retransmission du segment manquant et régénère le paquet IP et la trame Ethernet associée.

En conclusion, le niveau message associé à Ethernet est le même que celui du monde IP, c'est-à-dire TCP et UDP.

Le protocole AAL

AAL (ATM Adaptation Layer) est un troisième exemple de protocole de niveau message. Il s'agit de la couche d'adaptation à l'ATM, qui se charge de l'interface avec les couches supérieures. Cet étage est lui-même subdivisé en deux niveaux, l'un prenant en compte les problèmes liés directement à l'interfonctionnement avec la couche supérieure et l'autre ceux concernant la fragmentation et le réassemblage des messages en cellules.

Le rôle de cette couche est de transporter de bout en bout des messages dont le format est spécifié, leur taille maximale ne pouvant dépasser 64 Ko, comme dans Internet. Ce bloc doit être découpé en petits fragments de 48 octets pour entrer dans la cellule ATM. Ce découpage peut en fait descendre en dessous de 48 octets, par exemple 47 voire 44 octets, pour récupérer des octets de supervision dans la partie donnée.

Dans la couche AAL, quatre classes de services, 1, 2, 3 et 4, ont été définies, auxquelles correspondent quatre classes de protocoles. Cette subdivision a été modifiée en 1993 par le regroupement des classes 3 et 4 et par l'ajout d'une nouvelle classe de protocoles, la classe 5, qui définit un transport de données simplifié. Enfin, en 2000, la classe 2 a été transformée, ce qui a conduit à la définition de trois classes, 1, 2 et 5 :

- Classe 1. Correspond à une émulation de circuit, c'est-à-dire à la mise en place d'un circuit virtuel susceptible de transporter ce qui proviendrait d'un circuit et de redonner en sortie le même circuit. On se sert de cette classe pour transporter la parole téléphonique non compressée. Les opérateurs télécoms classiques ont des protocoles de ce type pour desservir toutes les demandes de circuit.
- Classe 2. Correspond au transport d'une information qui serait de type circuit au départ mais que l'on aurait compressée de telle sorte que le débit devienne variable. Cette classe transporte des applications comportant des contraintes de synchronisation, comme la classe A, mais avec un débit variable. On y trouve toutes les applications de parole téléphonique et de vidéo compressée. L'UMTS, en particulier, a choisi cette solution pour le transport de ses voies de parole.
- Classe 5. Permet de faire tout transiter sans ajouter de fonction supplémentaire, sauf éventuellement un contrôle d'erreur.

Ces classes ainsi que le protocole AAL sont détaillés à l'annexe K.

Conclusion

Le niveau message se préoccupe essentiellement de découper l'information en segments exploitables par les niveaux inférieurs. Il peut apporter des fonctionnalités supplémentaires, comme une demande de retransmission d'un message si une erreur est détectée ou un contrôle de flux, comme dans TCP.

Il n'existe pratiquement plus que deux protocoles de transport dans les réseaux, TCP et UDP, tous deux provenant du monde IP. Les solutions issues du monde ATM sont en cours de disparition et celles provenant du modèle de référence et de la normalisation de l'ISO ont quasiment toutes disparu.

Partie III

Les réseaux d'accès

Les réseaux d'accès forment la partie qui relie l'équipement terminal de l'utilisateur et le réseau de l'opérateur. Cette partie est parfois désignée par l'expression « derniers kilomètres du réseau ». Lorsqu'un opérateur possède à la fois le réseau cœur et le réseau d'accès, le coût de développement, de mise en place et de maintenance de la partie réseau d'accès est très supérieur à celui du réseau cœur. Les chiffres annoncés sont souvent supérieurs de 80 à 90 % pour le réseau d'accès et de 10 à 20 % pour le réseau cœur de l'opérateur. Ces coûts élevés s'expliquent par le fait qu'il faut atteindre chaque utilisateur dans son habitation et chaque société dans son local.

De multiples moyens permettent de réaliser ce réseau d'accès, même s'ils ont longtemps été l'apanage du câble métallique, avec le réseau téléphonique. Une certaine diversification est apparue ensuite, avec le câble coaxial, la fibre optique et les fils électriques. Les supports hertziens prennent une place qui devient prépondérante et qui ne cesse d'augmenter. L'arrivée de la 4G est même synonyme d'une prise en charge de la boucle locale par le hertzien.

Les trois chapitres qui composent cette partie examinent les grandes solutions disponibles sur le marché puis détaillent les accès haut débit sur les câbles métalliques, avec les techniques ADSL et modem câble, avant de passer en revue les solutions en vogue dans le monde hertzien.

9

Les réseaux d'accès terrestres

La boucle locale, aussi appelée réseau de distribution, ou réseau d'accès, est une des parties les plus importantes du réseau d'un opérateur qui distribue de l'information à des utilisateurs. Elle constitue son capital de base en même temps que son lien direct avec le client

Le coût global de mise en place et de maintenance d'un tel réseau est énorme. Il faut en règle générale compter entre 500 et 3 000 euros par utilisateur pour mettre en place cette interface. Ce coût comprend l'infrastructure, le câble et les éléments extrémité de traitement du signal mais ne tient pas compte du terminal. Pour déterminer l'investissement de base d'un opérateur, il suffit de multiplier ce coût par le nombre d'utilisateurs raccordés.

La boucle locale correspond à la desserte de l'utilisateur. Ce sont les derniers mètres ou kilomètres avant d'atteindre le poste client. Il existe des solutions extrêmement variées pour la réaliser. Pour les opérateurs historiques, installés depuis longtemps, la solution la plus répandue passe par l'utilisation d'un modem *x*DSL, qui permet le passage de plusieurs mégabits par seconde sur les paires métalliques de la boucle locale. La capacité dépend essentiellement de la distance entre l'équipement terminal et le raccordement au réseau de l'opérateur, qui s'effectue au niveau du DSLAM (Data Subscriber Line Access Module).

La valeur cible pour l'accès au multimédia par la boucle locale augmente chaque année avec l'apparition de nouveaux services demandant chaque fois des débits plus importants. Parmi ces services, le P2P, la télévision, la vidéo à la demande, les murs de présence, etc. Le progrès des codages et des techniques de compression est pourtant un facteur de limitation de l'augmentation des débits par une compression plus forte. Une vidéo de qualité télévision devrait pouvoir être acheminée à un débit de l'ordre de 512 Kbit/s dans quelques années. Quant à la parole sous forme numérique, elle ne demande plus que quelques kilobits par seconde.

La fibre optique

Une première solution pour mettre en place une boucle locale puissante consiste à recâbler complètement le réseau de distribution en fibre optique. Cette technique, dite FITL (Fiber In-The-Loop), donne naissance à plusieurs techniques en fonction de l'emplacement de l'extrémité de la fibre optique. La solution la plus attendue est celle qui dessert directement le domicile de l'utilisateur. Jusqu'en 2007, la fibre optique a été réservée à des zones industrielles, mais elle touche aujourd'hui le grand public sous la forme de la solution FTTH (Fiber to the Home), dans laquelle se lancent de nombreux opérateurs pour proposer le très haut débit à leurs clients : de 50 Mbit/s jusqu'à plusieurs centaines de mégabits par seconde.

La boucle locale optique se présente sous plusieurs formes. Elle peut simplement être une étoile optique : à partir d'une tête de réseau ; chaque client reçoit une fibre optique pour lui tout seul. Dans ce cas, il faut des chemins de câbles importants pour poser toutes les fibres simultanément. Cette solution a l'avantage évident l'apporter le plus haut débit possible à l'utilisateur.

Une seconde solution normalisée par l'UIT-T consiste à multiplexer plusieurs utilisateurs sur la même fibre optique. Elle prend la forme illustrée à la figure 9.1. Sa topologie est un arbre optique passif, ou PON (Passive Optical Network). La tête de réseau se trouve derrière l'OLT (Optical Line Termination). L'autre extrémité, l'ONU (Optical Network Unit), dessert directement le domicile de l'utilisateur ou peut être poursuivi par un réseau métallique faisant la jonction entre l'extrémité de la fibre optique et l'utilisateur.

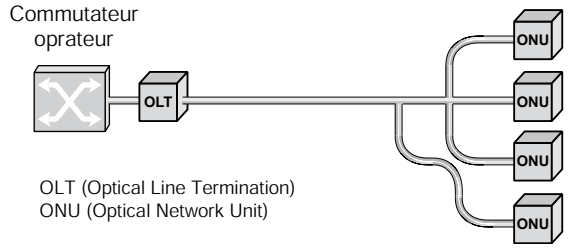


Figure 9.1

Boucle locale optique de type PON

Il est à noter que les étoiles optiques passives diffusent les signaux dans toutes les directions à l'exception du port d'entrée. Cette propriété est particulièrement intéressante puisque, si un utilisateur n'utilise pas son accès ou qu'il l'utilise peu, son débit peut-être attribué aux autres utilisateurs. Si un seul utilisateur est connecté sur l'arrivée de la fibre, il possède donc l'ensemble du débit. Comme ces réseaux PON utilisent des débits de 1, 2,5 et 10 Gbit/s, on mesure aisément l'augmentation potentielle des débits sur la boucle locale.

En règle générale, une terminaison OLT dessert 48 clients, ce qui donne une moyenne approximative de 50 Mbit/s par utilisateur pour un réseau PON à 2,5 Gbit/s, avec des

pointes à la vitesse maximale du support optique. Il convient cependant d'observer que la gestion du multipoint ne permet pas d'atteindre réellement le débit maximal, mais plutôt un débit estimé à la moitié de la valeur maximale.

Ces nouvelles capacités permettent d'exploiter de nouveaux services, comme le P2P (peer-to-peer) avec de nombreuses connexions simultanées, la vidéo de très grande qualité, comme la télévision haute définition, ou les murs de présence utilisant un son et une image animée de très haute qualité.

La mise en place d'un câblage optique est acceptable dans les zones urbaines disposant de conduits mis en place par les précédents câblages. Le coût d'une prise dans les meilleures conditions est de 1 000 euros pour aller à des valeurs de plus de 10 000 euros si du génie civil est nécessaire. Il est possible d'en réduire le coût en ne câblant pas la portion allant jusqu'à la prise terminale de l'utilisateur. Il faut pour cela déterminer le point jusqu'où le câblage doit être posé. Plusieurs solutions s'offrent pour cela à l'opérateur :

- FTTC (Fiber to the Curb). On câble jusqu'à un point assez proche de l'immeuble ou de la maison qui doit être desservi, le reste du câblage étant effectué par l'utilisateur final.
- FTTN (Fiber to the Node). On câble jusqu'à un répartiteur dans l'immeuble lui-même.
- FTTH (Fiber to the Home). On câble jusqu'à la porte de l'utilisateur.
- FTTT (Fiber to the Terminal). On câble jusqu'à la prise de l'utilisateur, à côté de son terminal.

Le prix de revient augmentant fortement avec la proximité de l'utilisateur, la tendance a longtemps été de câbler en fibre optique jusqu'à des points de desserte répartis dans le quartier et à choisir d'autres solutions moins onéreuses pour aller jusqu'à l'utilisateur. Le câblage métallique étant capable de prendre en charge des débits de quelques mégabits par seconde sur les derniers kilomètres avec l'aide de modems *x*DSL, que nous détaillons ultérieurement dans ce chapitre, il est possible de câbler en fibre optique jusqu'à un point situé à 5 km au plus de l'utilisateur. En ville, cette distance est facile à respecter, mais hors des agglomérations, d'autres solutions sont à rechercher.

Les technologies associées aux PON sont de type ATM, Ethernet ou Gigabit (UIT-T), ce qui donne naissance aux APON, EPON et GPON. La première permet de mettre en place des FSAN (Full Service Access Network). Dans la solution Ethernet, chaque trame émise est envoyée en diffusion comme sur un réseau Ethernet partagé. La troisième solution met en œuvre les technologies de transmission définies par l'UIT-T au niveau physique.

APON (ATM Over PON)

Sur le réseau optique passif (PON), il est possible de faire transiter des cellules ATM suivant la technique développée par le groupe de travail FSAN (Full Service Access Network). Cette solution a ensuite été normalisée dans la recommandation G.983 de l'UIT-T. Les deux ex

rémités de l'arbre optique s'appellent OLT (Optical Line Termination) et ONU (Optical Network Unit). Pour des raisons de déperdition d'énergie, il n'est pas possible de dépasser une cinquantaine de branches sur le tronc.

La figure 9.2 illustre l'architecture d'un réseau optique passif.

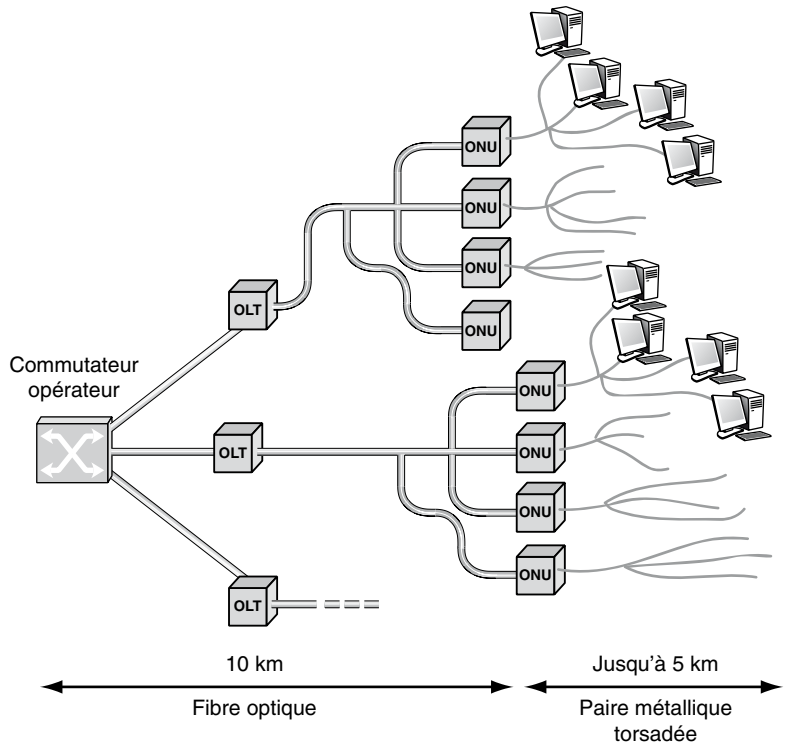


Figure 9.2
Architecture d'un PON

Un « superPON » a également été défini, connectant jusqu'à 2 048 ONU sur un même OLT. Dans ce cas, le débit montant est de 2,5 Gbit/s. Sur les réseaux d'accès en fibre optique mis en place par les opérateurs, c'est le protocole ATM qui a généralement été retenu au début de cette technologie. Le système a pris alors le nom d'APON (ATM Over PON).

Les difficultés engendrées par les boucles passives optiques, comme celle de l'accès CATV, que nous examinons plus loin, viennent du partage de la bande passante montante, c'est-à-dire de l'utilisateur vers le réseau. Si plusieurs centaines de clients se connectent simultanément, voire plusieurs milliers dans les superPON (jusqu'à 20 000), la bande passante peut ne pas être suffisante. Si, sur le canal descendant, les canaux vidéo sont diffusés et ne prennent qu'un canal sur le tronc de l'arbre, les canaux montants des utilisateurs sont tous différents et doivent se partager une certaine bande passante sur le tronc. Il faut donc une technique d'accès MAC (Medium Access Control) pour prendre en charge cette superposition.

Le multiplexage en longueur d'onde offre une solution simple à ce problème, puisque chaque utilisateur possède une longueur d'onde différente de celle des autres utilisateurs. Cela ne peut toutefois convenir que si le nombre de branches est limité. Il faut se résoudre le plus souvent à une technique de partage. De très nombreuses solutions ont été proposées pour permettre à l'ONU de faire une requête vers l'OLT, ce dernier réservant une bande passante aux clients demandeurs.

Dans le sens descendant, les cellules ATM sont émises de façon classique, en « *cell-based* ». Une cellule OAM (Operations And Maintenance) est émise toutes les 26 cellules utilisateur pour gérer le flot. Dans le sens montant, une réservation est nécessaire. Elle s'effectue à l'intérieur des trames FSAN divisées en tranches de 56 octets comportant une cellule et 3 octets de supervision. Au centre de la trame, une tranche particulière de 56 octets est destinée à la réservation d'une tranche de temps.

La figure 9.3 illustre ces zones de données.

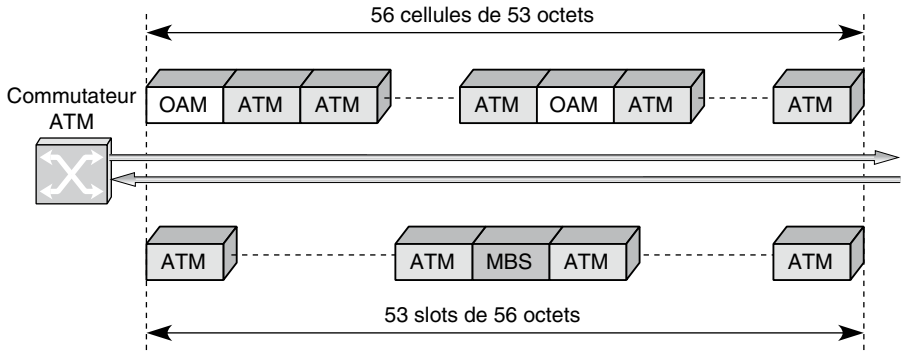


Figure 9.3

Structure de la trame FSAN

EPON (Ethernet Passive Optical Network)

Lorsque les trames qui sont émises sur le PON sont de type Ethernet, on parle d'EPON. Les caractéristiques de ce réseau sont identiques à celles des autres PON : diffusion sur l'ensemble du réseau, où seule la station indiquée dans la trame Ethernet peut récupérer l'information véhiculée. Cette solution a été développée par le groupe de travail EFM (Ethernet in the First Mile) de l'IEEE. L'objectif était de remplacer la technologie ATM, très coûteuse à mettre en œuvre sur une technologie multipoint, par la technologie Ethernet.

Dans la technologie EPON, la trame provenant de l'OLT est diffusée vers l'ensemble des ONU (64 au maximum). L'ONU qui reconnaît son adresse récupère la trame Ethernet, dont la taille peut atteindre une longueur de 1 518 octets. Dans le sens montant, les trames Ethernet sont émises suivant une technologie TDM (Time Division Multiplexing) la solution classique utilisée dans Ethernet, CSMA/CD, étant inadaptée aux vitesses

des EPON. Le multiplexage dans le sens descendant s'exerce sur des slots de longueur constante de telle sorte que les trames Ethernet doivent être divisées en segments de longueur constante, à l'exception de la dernière partie, qui peut être inférieure à la longueur du slot.

Une synchronisation est indispensable pour qu'il n'y ait pas de collision entre les slots. Cette synchronisation s'effectue toutes les 2 ms, correspondant à la longueur de la trame physique qui comporte l'ensemble des slots des ONU.

Le niveau physique utilise deux ou trois longueurs d'onde. Avec deux longueurs d'onde, il est possible d'utiliser les canaux montants et descendants. La longueur du réseau dans ce cas atteint une vingtaine de kilomètres avec 32 étoiles passives. Avec trois longueurs d'onde, il est possible d'ajouter une voie descendante pour diffuser des canaux de télévision.

La qualité de service peut être obtenue en introduisant une priorité en utilisant, comme nous le verrons au chapitre 16, dédié à Ethernet, une zone indiquant la priorité de la trame.

GPON (Giga Passive Optical Network)

Les GPON ont pour objectif d'augmenter encore les débits pour suivre les progrès technologiques et atteindre 10 puis 40 Gbit/s. Ces solutions proviennent d'une normalisation de l'UIT-T et des progrès de la fibre optique, comme nous le verrons aux chapitres 12 et 13.

Les réseaux câblés (CATV)

Une autre solution pour obtenir un réseau de distribution à haut débit consiste à utiliser le câblage des câblo-opérateurs, lorsqu'il existe. Ce câblage a pendant longtemps été constitué de CATV (câble TV), dont la bande passante dépasse facilement les 800 MHz.

Aujourd'hui, cette infrastructure est légèrement modifiée par la mise en place de systèmes HFC (Hybrid Fiber/Coax), qui associent une partie en fibre optique entre la tête de réseau et le début de la desserte par le CATV. Cette topologie est illustrée à la figure 9.4.

La technologie utilisée sur le CATV est de type multiplexage en fréquence. Sur la bande passante globale, une division en sous-canaux indépendants les uns des autres est réalisée, comme illustré à la figure 9.5.

Cette solution présente de nombreux avantages, mais aussi quelques défauts majeurs. Son avantage principal réside dans la possibilité d'optimiser ce qui est transmis dans les différents canaux, puisque chaque canal est indépendant des autres canaux. Le multimédia est facilement supporté en affectant un média par sous-bande, chaque sous-bande ayant la possibilité d'être optimisée. Il suffit pour cela de conserver les informations analogiques ou de les numériser.

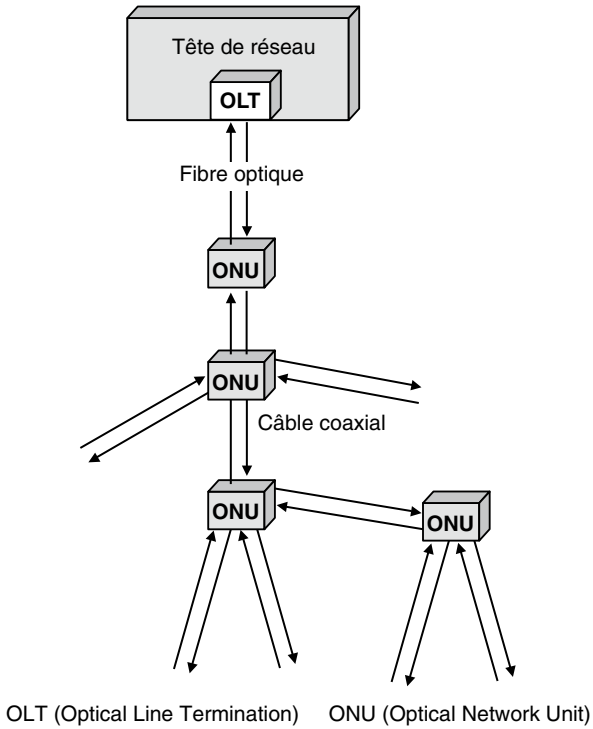


Figure 9.4
Topologie HFC

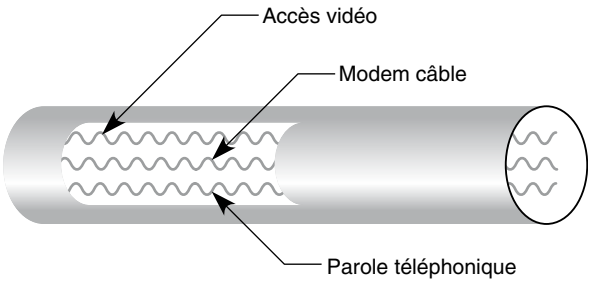


Figure 9.5
Multiplexage en fréquence dans un CATV

Les canaux de télévision transitent dans des sous-bandes distinctes. Une sous-bande spécifique peut être dédiée à une connexion de parole téléphonique et une autre sous-bande à la connexion Internet. Cet accès au réseau Internet demande l'utilisation d'un modem câble, qui permet d'accéder à la sous-bande connectée à Internet. Ce type de modem requiert une fréquence déterminée, correspondant à la sous-bande choisie pour

la connexion Internet. Son débit peut atteindre, grâce à une bande passante importante, plusieurs mégabits par seconde.

La distribution de la bande passante entre les différentes sous-bandes est illustrée à la figure 9.6. La bande des 50-550 MHz est réservée aux canaux de télévision analogique. Chaque canal demandant une bande passante de 6 MHz, il est possible de diffuser ainsi jusqu'à 80 canaux de télévision. La télévision numérique, présentée en détail au chapitre 29, demande une bande passante plus faible, ce qui permet de multiplier par trois ou quatre le nombre des chaînes de télévision acheminées par le câble.

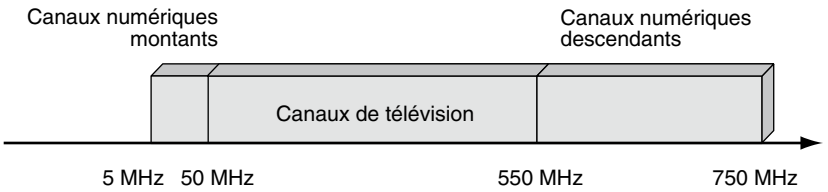


Figure 9.6

Distribution du spectre à l'intérieur d'un CATV

La bande des 5-550 MHz correspond aux canaux allant de l'utilisateur à la tête de réseau. La bande des 550-750 MHz part de la tête de réseau pour desservir le terminal utilisateur. Elle peut être utilisée à la fois pour la parole téléphonique et les connexions Internet.

La faiblesse de cette technique vient de ce que le multiplexage en fréquence n'utilise pas au mieux la bande passante et ne permet pas réellement l'intégration des différents services qui transitent dans le CATV. Un multiplexage temporel apporterait une meilleure utilisation de la bande passante disponible et intégrerait dans un seul composant l'accès à l'ensemble des informations au point d'accès. Un transfert de paquets représenterait également une solution adaptée, à condition de modifier complètement les composants extrémité.

En résumé, on peut réaliser une application multimédia sur le câble coaxial des câblo-opérateurs mais en étant obligé de considérer le transport des médias sur des bandes parallèles et non sur une bande unique.

HFC (Hybrid Fiber/Coax) est une autre solution, qui consiste à utiliser de la fibre optique pour permettre au réseau de transporter jusqu'à une distance peu éloignée de l'utilisateur des communications haut débit, en étant relayé par du câble coaxial jusqu'à la prise utilisateur. Grâce à sa capacité très importante, la fibre optique permet de véhiculer autant de canaux qu'il y a d'utilisateurs à atteindre, ce dont est incapable le CATV dès que le nombre d'utilisateurs devient important. Pour ce dernier, il faut trouver une solution de multiplexage des voies montantes vers le cœur de chaîne pour arriver à faire transiter l'ensemble des demandes des utilisateurs sur le réseau. Ce problème est illustré à la figure 9.7.

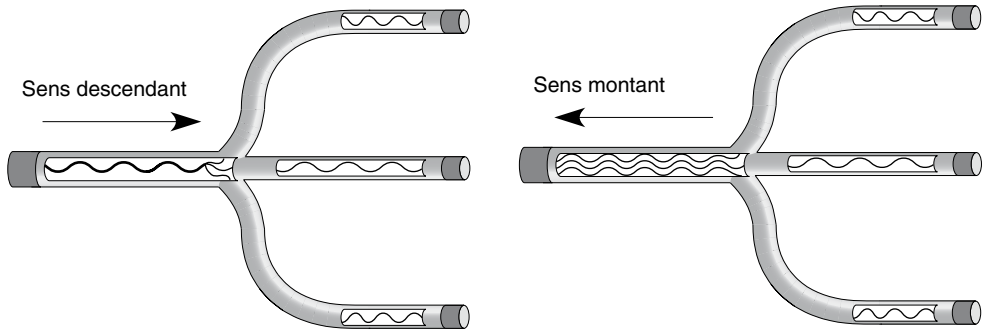


Figure 9.7

Multiplexage des voies montantes dans la boucle locale en CATV

Supposons qu'un canal associé à la connexion Internet ait un débit de 34 Mbit/s, ce qui est aujourd'hui le cas standard. Si, sur un arbre CATV, 10 000 prises sont connectées et actives, le débit total sur la voie descendante et sur la voie montante représente 3,4 Kbit/s par utilisateur. Pour offrir un meilleur débit, il faut réaliser un multiplexage statistique afin de récupérer la bande passante non utilisée par certains utilisateurs. Il est toutefois évident que s'il y a trop d'utilisateurs simultanés, le débit est insuffisant.

Les normes suivantes ont été proposées comme techniques d'accès pour permettre un multiplexage temporel des utilisateurs sur une bande commune :

- MCNS-DOCSIS (Multimedia Cable Network System-Data Over Cable Service Interoperability Specification), qui est devenu le standard de base.
- IEEE 802.14, qui utilise une technologie ATM en cours de disparition au profit de DOCSIS.
- DVB-DAVIC (Digital Video Broadcasting-Digital Audio VIsual Council), qui provient d'un groupement d'industriels de la vidéo.

La norme DOCSIS divise le temps en slots, numérotés entre 1 et 4 096. Les standards disponibles, DOCSIS 1.0, 1.2, 2.0 et 3.0 utilisent des tables d'allocation de slots qui indiquent qui a le droit de transmettre dans un slot. Jusqu'à 14 slots peuvent être utilisés simultanément pour une même communication. Les slots avec accès aléatoire, que l'on appelle slots de contention, permettent aux stations d'effectuer leur réservation. L'accès aléatoire n'est pas vraiment aléatoire, puisqu'il utilise l'algorithme en arbre BEB (Binary Exponential Backoff) pour résoudre les collisions.

La différence entre les standards réside dans la prise en charge de la qualité de service, qui n'est garantie qu'à partir de la version 1.2. Cette qualité de service est totalement compatible avec le modèle DiffServ, qui consiste à marquer le champ de qualité de service de chaque paquet d'une valeur correspondant à son niveau de priorité.

Les paires métalliques

La boucle locale métallique

Les paires métalliques sont très fortement utilisées sur la boucle locale, principalement pour l'accès au réseau téléphonique. Lorsque l'accès se fait en commutation de circuits, ce qui représente aujourd'hui un cas qui diminue de plus en plus, avec une disparition totale vers 2015, on peut utiliser une paire en full-duplex. Il est évidemment possible d'émettre des données binaires en utilisant un modem. La vitesse peut atteindre en ce cas quelques dizaines de kilobits par seconde.

La paire métallique peut devenir une liaison spécialisée lorsque des répéteurs *ad hoc* sont placés à distance régulière. On atteint généralement 2 Mbit/s ou 1,5 Mbit/s (liaison T1). Cette solution a été développée il y a fort longtemps dans le but de faire transiter de la parole téléphonique à 3 200 Hz et non quelques mégabits par seconde.

Comme la bande passante de la téléphonie est faible, on n'a pas besoin d'un médium physique de bonne qualité. C'est la raison pour laquelle la paire métallique utilisée pour la distribution téléphonique, avec son diamètre de 0,4 mm, est plutôt de qualité médiocre. De plus, la distribution de la téléphonie depuis les locaux de l'opérateur s'effectue souvent par le biais de câbles de 50 paires, qui sont assez mal protégés et peuvent être la source de nombreux problèmes de distorsion de phase, de diaphonie, etc. Cela complique le passage d'une bande passante importante permettant d'obtenir les débits proposés par les modems ADSL.

Les accès xDSL

Les modems *x*DSL permettent d'utiliser les paires métalliques du réseau d'accès pour réaliser une boucle locale à haut débit. Le débit dépend fortement de la qualité du câble utilisé et de la distance à parcourir. Plusieurs catégories de modems *x*DSL sont commercialisées, la lettre *x* permettant de les différencier.

Les modems ADSL (Asymmetric Digital Subscriber Line) sont les plus répandus. Leurs vitesses sont dissymétriques, plus lentes entre le terminal et le réseau que dans l'autre sens. En règle générale, le sens montant est au moins quatre fois moins rapide que le sens descendant. Les vitesses sur le sens descendant peuvent atteindre 28 Mbit/s pour une distance courte de l'ordre du kilomètre et de 1Mbit/s pour une distance de 5 km. Le modem ADSL utilise une modulation d'amplitude quadratique, c'est-à-dire que 16 bits sont transportés à chaque signal. Avec une rapidité de modulation de 340 kilobauds et une atténuation de l'ordre d'une trentaine de décibels, on atteint plus de 5 Mbit/s.

Devant le succès rencontré par la technique ADSL, des dérivés en ont été développés, notamment la technique consistant à faire varier le débit sur le câble, qui a donné naissance au RADSL (Rate Adaptive DSL). Pour les hauts débits, les solutions HDSL (High bit rate DSL) et VDSL (Very high bit rate DSL) peuvent être exploitées avec succès si le câblage, souvent en fibre optique, le permet. Les mesures effectuées chez les opérateurs montrent que les débits deviennent de plus en plus symétriques depuis l'apparition des

applications peer-to-peer (P2P), les stations des utilisateurs client devenant des serveurs. Les techniques SDSL (Symmetric DSL) vont donc devenir de plus en plus courantes.

Le modem ADSL

La technologie ADSL a été normalisée par l'UIT-T sous la recommandation G.992.1. Une extension a été apportée dans la recommandation G.992.3 déterminant l'ADSL2. Des extensions permettant l'amélioration de l'ADSL2 sont adoptées pour allonger la distance entre le client et le DSLAM. Ces améliorations ont permis l'adoption de l'ADSL2+ ou LDSL (Long-reach DSL) ou encore READSL (Range Extended ADSL).

Deux techniques sont utilisées pour augmenter le débit sur une communication *x*DSL : le full-duplex, qui est assuré sur une même paire grâce à l'annulation d'écho, et l'utilisation d'un code spécifique, 2B1Q.

Les modems ADSL offrent une bande montante de 4 à 100 kHz, qui est utilisée pour des débits de 0,64 Mbit/s. La bande descendante utilise une bande comprise entre 100 kHz et 1,1 MHz, qui permet d'atteindre le débit de 8,2 Mbit/s. La parole analogique, entre 0 et 4 kHz, passe en parallèle des données utilisant le modem.

Les codes en ligne des modems ADSL reposent soit sur la modulation CAP (Carrierless Amplitude and Phase), soit sur la norme DMT (Discrete MultiTone), de l'ANSI (American National Standards Institute) et de l'ETSI (European Telecommunications Standards Institute). La méthode DMT consiste en l'utilisation de 256 canaux de 4 kHz, chaque canal permettant l'émission de 15 bits par hertz au maximum.

La figure 9.8 illustre la partie du spectre utilisée par les modems ADSL.

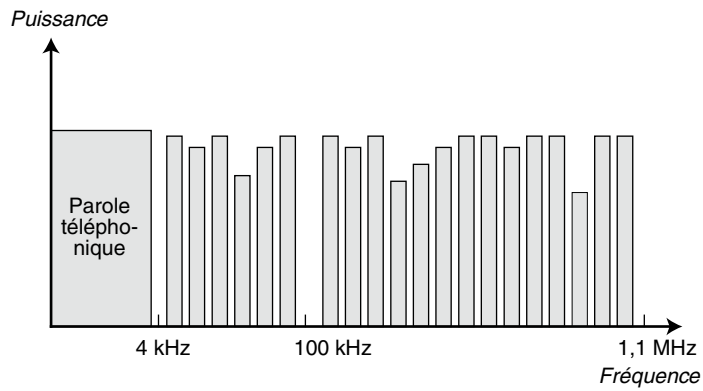


Figure 9.8

Partie du spectre utilisée par l'ADSL

Le spectre est donc découpé en trois parties, une entre 0 et 4 kHz, pour faire passer la parole téléphonique qui continue à être acheminée en parallèle des données, une entre 4 et 100 kHz, pour la voie montante allant du terminal vers le réseau, et une entre 100 kHz et 1,1 MHz pour la voie descendante allant du réseau au terminal.

La partie montante du spectre est divisée en bandes de 4,3 kHz, et plus exactement en 20 sous-bandes de 4,3 kHz. Chaque sous-bande est capable de transporter de 4 à 15 bits en parallèle. En choisissant 8 bits par intervalle d'horloge, avec quatre mille intervalles de temps par seconde, le modem ADSL permet de transporter :

$$4\,000 \times 8 \text{ bits} = 32 \text{ Kbit/s par sous-bande}$$

Comme il y a 20 sous-bandes, on arrive au total de $32 \times 20 = 640$ Kbit/s.

La partie montante de la communication est découpée en 256 tranches de 4,3 kHz. Toujours pour un transport de 8 bits par intervalle de temps, on arrive au débit de :

$$4\,000 \times 8 \text{ bits} \times 256 = 8{,}2 \text{ Mbit/s}$$

Il est possible d'améliorer le débit en augmentant le nombre de bits par intervalle de temps et, surtout, la bande passante. Les modems ADSL2+ permettent ainsi de monter jusqu'à 28 Mbit/s en augmentant fortement la partie du spectre utilisée sur la voie descendante.

Des versions simplifiées de modems ADSL sont parfois mises en œuvre dans certains pays, telles que l'ADSL Lite, ou G-Lite, et l'U-ADSL (Universal ADSL). L'objectif de cette simplification est d'offrir un accès à Internet à très bas prix. Les capacités de transmission sont respectivement de 1,5 Mbit/s et 512 Kbit/s. Des cartes ADSL Lite sont commercialisées pour les PC.

Les modems G-Lite ressemblent aux modems ADSL, mais ils sont capables de s'adapter aux possibilités de la ligne. Le modem G-Lite ne se place pas à côté de la communication téléphonique, comme dans l'ADSL, mais prend toute la capacité de la ligne. Le modem s'interrompt si une communication téléphonique doit passer par la ligne. Les modems G-Lite s'adaptent bien aux accès haut débit, en particulier pour l'ATM. Dans ce cas, le protocole PPP peut être utilisé. Il a été standardisé dans cette configuration par l'ADSL Forum et par l'ANSI. Nous revenons sur les protocoles utilisés par les modems ultérieurement dans ce chapitre.

L'ADSL Forum a défini l'interface à respecter. Cette dernière suit l'architecture ATM, déployée par les opérateurs et les équipementiers du secteur des télécommunications vers le début des années 1990. À cette époque, l'ATM représentait une potentialité forte pour l'unification des réseaux des années 2000.

Les octets provenant des différentes sous-bandes sont encapsulés dans des trames ATM. Les trames ATM sont elles-mêmes encapsulées dans une trame de niveau physique, ou supertrame, qui correspond à la vitesse de l'accès ADSL. Par exemple, pour une connexion d'une capacité utile de 1,5 Mbit/s, les trames ATM sont transmises dans une supertrame de 68 cellules ATM, plus une cellule de synchronisation. Chaque supertrame demande un temps de 17 ms pour être émise, ce qui correspond à un peu moins de 250 µs par trame. La vitesse de transmission utile pour le client atteint dans ce cas 1,5 Mbit/s, une fois enlevées les synchronisations et bits de redondance ou de correction d'erreur.

La trame ATM est aujourd'hui de plus en plus remplacée par la trame Ethernet. Cette solution s'explique aisément pour réaliser une continuité Ethernet entre la connexion de l'utilisateur et l'utilisation de solution Gigabit Ethernet entre le DSLAM et le réseau de l'opérateur. Cette solution est introduite au chapitre 14, dévolu à Ethernet.

Les DSLAM (DSL Access Module)

Les DSLAM forment l'autre extrémité de la liaison, chez l'opérateur. Ce sont des équipements dont le rôle est de récupérer les données émises par l'utilisateur depuis son équipement terminal au travers de son modem ADSL. Ces équipements intègrent des modems situés à la frontière de la boucle locale et du réseau de l'opérateur.

La figure 9.9 illustre le positionnement d'un DSLAM.

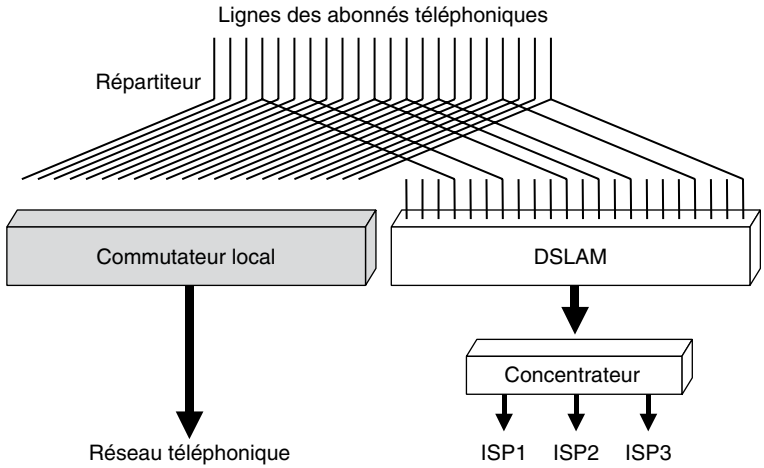


Figure 9.9

Positionnement d'un DSLAM

Les lignes des abonnés à l'opérateur local arrivent sur un répartiteur, qui permet de connecter l'utilisateur au commutateur téléphonique et au DSLAM s'il a un abonnement DSL. Le DSLAM est lui-même connecté à un concentrateur, que nous présentons un peu plus loin du point de vue protocolaire. Ce cas de figure est celui de l'opérateur historique.

Le dégroupage désigne l'arrivée d'opérateurs alternatifs pour offrir des services téléphoniques, de données à haut débit et même de vidéo, comme la télévision.

Parmi les diverses possibilités de réalisation pratique du dégroupage, la pose de câbles a été envisagée pour réaliser une boucle locale différente de celle de l'opérateur historique, lequel en possédait, jusqu'à la fin des années 1990, le contrôle total. En raison du prix très élevé de la pose d'un réseau d'accès et de l'aberration que représenterait l'arrivée de plusieurs boucles locales jusque chez l'utilisateur, une par opérateur, d'autres solutions ont été adoptées. Certains opérateurs ont choisi de se positionner au niveau du répartiteur. À partir de ce répartiteur, ils ont installé leurs propres connexions et leur propre DSLAM.

L'inconvénient de cette solution provient de la situation géographique du DSLAM de l'opérateur alternatif, qui doit se trouver dans une salle connexe de celle de l'opérateur historique. De plus, l'opérateur alternatif doit tirer une liaison vers son propre réseau, sans connaître avec précision le nombre d'utilisateurs qui le choisiront.

Une autre possibilité consiste à se positionner derrière le DSLAM, en ayant son propre concentrateur ou bien, comme sur la figure, en se connectant à la sortie du concentrateur. L'opérateur qui prend en charge la connexion entre le modem de l'utilisateur et la sortie du concentrateur s'appelle le fournisseur d'accès, ou NAP (Network Access Provider).

Une dernière solution consiste à utiliser le réseau de France Télécom pour atteindre un PoP (Point of Presence) de l'opérateur alternatif. Nous examinons cette solution à la section suivante.

Jusqu'en 2004, les utilisateurs étaient obligés d'avoir un abonnement à France Télécom pour transmettre sur la boucle locale entre l'équipement terminal et le DSLAM. Désormais, la dérégulation est totale, et la facture de la communication sur la boucle locale est gérée par l'opérateur alternatif, qui doit cependant louer la ligne de la boucle locale à France Télécom.

Les protocoles de l'ADSL

L'utilisateur générant des paquets IP, il faut pouvoir transporter ces paquets IP vers le modem ADSL. Pour cela, on utilise soit une trame Ethernet, soit une trame PPP, soit une trame USB (Universal Serial Bus), soit une superposition de ces trames, comme une trame PPP encapsulée dans une trame Ethernet ou une trame PPP encapsulée dans une trame USB.

Prenons l'exemple de paquets IP encapsulés dans une trame Ethernet. Cette trame est envoyée soit sur un réseau Ethernet reliant le PC du client au modem, soit dans une trame PPP sur une interface de type USB. Dans le modem ADSL, il faut décapsuler la trame pour récupérer le paquet IP puis l'encapsuler de nouveau, mais cette fois dans une trame ATM. Cette fragmentation en morceaux de 48 octets est réalisée par le biais d'une couche AAL-5 (ATM Adaptation Layer de type 5).

Une fois la trame ATM arrivée dans le DSLAM, plusieurs cas de figure peuvent se présenter suivant l'architecture du réseau du FAI auquel le client est connecté. Une première solution consiste à décapsuler les cellules ATM et à récupérer le paquet IP qui est transmis vers le concentrateur dans une trame Ethernet. Le concentrateur l'envoie vers le FAI également dans une trame Ethernet.

Une deuxième solution consiste à laisser les trames sous forme ATM. C'est le cas lorsque l'opérateur de la boucle locale et le FAI utilisent la même technologie. Dans ce cas, la cellule ATM est directement envoyée vers le concentrateur, qui joue le rôle de commutateur ATM. Celui-ci envoie les trames ATM par des circuits virtuels vers des BAS (Broadband Access Server), qui sont les équipements intermédiaires permettant d'accéder aux réseaux des FAI alternatifs.

Ces topologies sont illustrées à la figure 9.10.

Une autre solution, qui est aussi très utilisée, consiste à placer le paquet IP de départ dans une trame PPP et à garder cette trame tout le long du chemin, quitte à l'encapsuler dans d'autres trames. Cela a donné naissance au protocole PPPoE (PPP over Ethernet) dans le cas où la trame PPP est émise sur Ethernet. La trame PPP peut être encapsulée dans plusieurs trames ATM après avoir été découpée en morceaux de 48 octets.

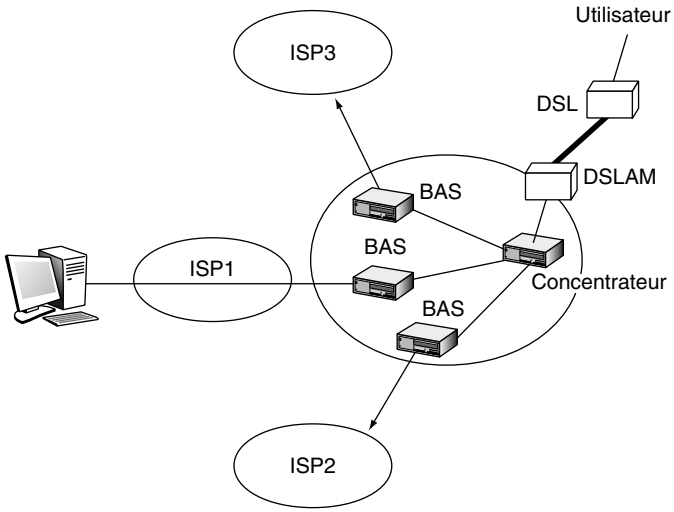


Figure 9.10

Équipements de concentration entre l'utilisateur et le serveur

Les modems VDSL

Les modems VDSL (Very high bit rate DSL) permettent d'atteindre des vitesses beaucoup plus élevées que les modems ADSL, mais sur quelques dizaines de mètres seulement. Leur capacité est de plusieurs dizaines de mégabits par seconde. Les modems VDSL peuvent se mettre à la sortie d'un PON (Passive Optical Network) pour prolonger leur liaison vers l'utilisateur

Les débits peuvent être asymétriques ou symétriques, au choix de l'utilisateur. Selon les propositions de l'ANSI, les débits en asymétrique devraient atteindre 6,4 Mbit/s dans le sens montant et 52 Mbit/s dans le sens descendant sur une distance de 300 m. Pour une distance de 1 000 m, il devrait être possible d'obtenir la moitié des débits précédents. La bande de fréquences située entre 300 et 700 kHz est dévolue à la bande montante. La partie du spectre située entre 700 kHz et 30 MHz sert à la bande descendante. La partie basse du spectre est réservée à la parole téléphonique.

Comme dans le cas de l'ADSL, un filtre permet de séparer la partie téléphonique, qui va vers un répartiteur téléphonique, et la partie données, qui va vers l'équivalent d'un DSLAM, lequel peut utiliser la fibre optique du PON pour atteindre le local technique de l'opérateur.

Le Multi-Play

Les modems ADSL ont été développés au départ pour réaliser un transport de données à haut débit de plusieurs mégabits par seconde. Ils se sont améliorés en introduisant de la téléphonie puis de la télévision.

Le principe de fonctionnement du Triple-Play est illustré à la figure 9.11.

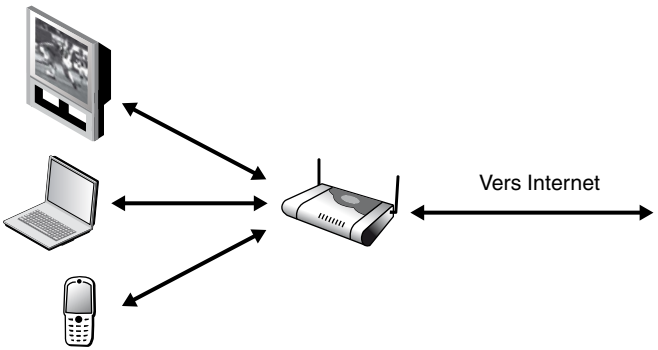


Figure 9.11
Le Triple-Play

Dans cette génération, chaque média passe par une prise différente permettant de récupérer facilement les flots de chacun des médias et de leur affecter des priorités associées : la parole téléphonique a une priorité supérieure à la télévision, qui a une priorité plus grande que les paquets de données.

Les flots peuvent être de nature différente. Par exemple, le téléphone peut encore être analogique ainsi que la télévision. Les codeurs-décodeurs se trouvant dans le modem ADSL, le boîtier de connexion prend le nom de Home Gateway ou encore InternetBox, car il intègre en plus du modem *x*DSL de nombreux codeurs-décodeurs et la paquétisation des flots téléphoniques et de télévision. Cette solution correspond aux Home Gateways développées entre 2004 et 2008 (LiveBox, FreeBox, etc.).

Les Home Gateways commencent à posséder des filtres applicatifs permettant de reconnaître directement le type de flot traversant le boîtier et de lui affecter la priorité correspondante. Cette solution permet de ne plus différencier les flots au niveau du terminal, qui peuvent de ce fait tous devenir IP. Elle est illustrée à la figure 9.12.

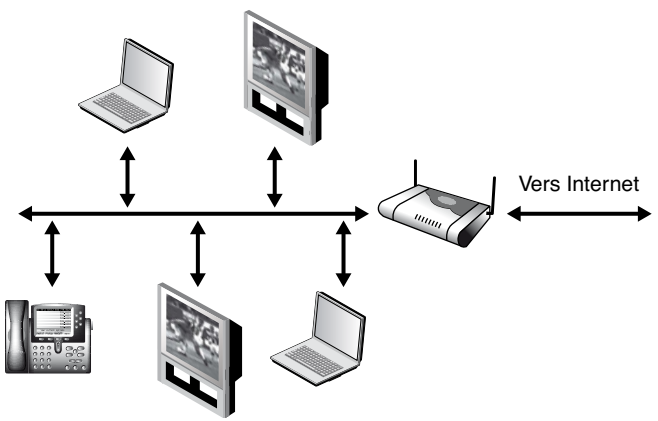


Figure 9.12
Le Triple-Play de seconde génération

Le Quadruple-Play est apparu en 2006 pour ajouter la mobilité aux accès à la Home Gateway. Dans cette solution, le combiné téléphonique se raccorde au réseau sans fil inclus dans le boîtier : Wi-Fi en général mais également Bluetooth. Le téléphone peut-être uniquement Wi-Fi ou Bluetooth mais peut également être bi-mode pour permettre de passer au GSM en cas de coupure de la communication Wi-Fi ou Bluetooth. Cette solution s'apparente à la téléphonie sur IP puisque les octets de téléphonie sont encapsulés dans un paquet IP dans le combiné et que le paquet IP est lui-même encapsulé dans la trame associée à la technologie du réseau sans fil pour traverser l'interface radio.

Une extension particulièrement intéressante concerne la possibilité de se connecter sur une Home Gateway d'un autre utilisateur et de pouvoir téléphoner au coût de l'abonnement du FAI. Cette solution demande à ce que l'opérateur permette l'accès aux multiples Home Gateway à partir de connexions externes. Pour cela, une authentification est nécessaire, qui peut être réalisée par une carte SIM (Subscriber Identity Module). Le Quadruple-Play est illustré à la figure 9.13.

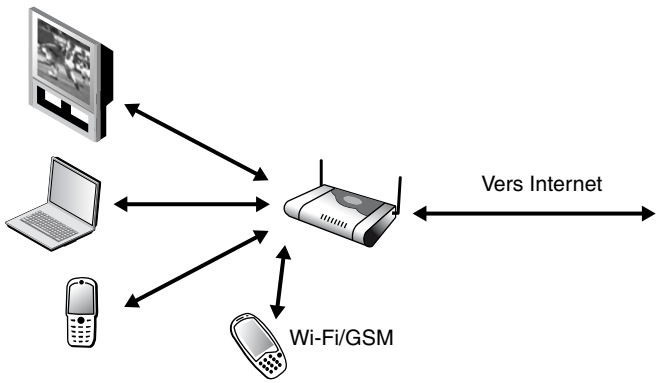


Figure 9.13
Le Quadruple-Play

Cette solution n'est pas forcément simple à gérer. En effet, la vitesse de la connexion dépend en grande partie de l'éloignement de l'utilisateur. Suivant les opérateurs, différentes solutions ont été développées pour contrer ce problème : limiter fortement le nombre de connexions, interdire les connexions quand l'utilisateur se sert de sa Home Gateway, limiter le débit accessible depuis l'extérieur, etc.

Le Penta-Play est une extension de la téléphonie mobile *via* la télévision. Le flot de paquets IP provenant du client transporte les images et le son du canal de télévision. L'inconvénient majeur de cette solution est une capacité plus importante de transmission, qui ajoute une difficulté de gestion de la Home Gateway pour éviter que plusieurs clients externes ne perturbent le boîtier d'un utilisateur.

La boucle locale électrique

Le courant fort représente un remarquable réseau d'accès, aussi étendu et aussi dense que le réseau d'accès des opérateurs télécoms, sinon plus. Sur ces câbles métalliques, il est tentant de vouloir faire passer simultanément du courant électrique et du courant faible. Cependant, la perturbation est très importante, et les débits atteints sur des distances de quelques kilomètres sont faibles.

On peut effectuer un certain nombre de télétraitements à faible débit, comme le relevé de compteur à distance. On imagine très bien la possibilité d'offrir un trafic téléphonique de qualité correcte avec une compression à quelques kilobits par seconde de la parole téléphonique. Le passage d'applications multimédias semble plus problématique de par son coût élevé sur la boucle locale. Cette solution semble toutefois concurrentielle dans les environnements domestiques.

Les techniques de passage de données informatiques sur des courants électriques portent le nom de CPL (courant porteur en ligne), en anglais PLC (Power Line Communication). On utilise l'infrastructure basse tension sur 50 ou 60 Hz depuis le transformateur basse tension ou simplement à l'intérieur de la maison. Comme pour les réseaux des câblo-opérateurs, la communication se fait à partir d'une tête de réseau (le transformateur basse tension) vers les utilisateurs, c'est-à-dire par une communication multipoint allant d'un point vers plusieurs points. Dans le sens descendant, il n'y a pas de problème particulier puisqu'il y a diffusion et que le destinataire se reconnaît. En revanche, de l'utilisateur vers le réseau, une méthode d'accès au support physique est nécessaire.

Les méthodes classiques à base de CDMA (Code Division Multiple Access) peuvent être employées au même titre que d'autres techniques, telles que le passage d'un jeton ou le polling (une machine maître donne aux terminaux le droit de transmettre à tour de rôle).

Le CPL sur la boucle locale

L'objectif du CPL sur la boucle locale est de desservir les utilisateurs avec un équivalent de l'ADSL, c'est-à-dire un débit allant de quelques centaines de kilobits par seconde à plusieurs mégabits par seconde. Il faut pour cela utiliser à la fois les chemins électriques de type primaire utilisant un voltage de quelques kilovolts et la partie terminale de quelques centaines de volts. Il faut donc traverser des transformateurs électriques, ce qui n'est pas possible directement. Le moyen d'y parvenir est de tirer des dérivations autour de ces transformateurs. Cette architecture est illustrée à la figure 9.14.

Les résultats des tests qui ont été effectués dans de nombreux pays sont très divergents, ce qui semble indiquer la sensibilité du système et l'importance de la mise en place des dérivations. Bien évidemment, la longueur du tronçon électrique à emprunter est déterminante. Comme dans les techniques ADSL, il ne faut pas que l'accès à l'équivalent du DSLAM soit éloigné de plus de quelques kilomètres.

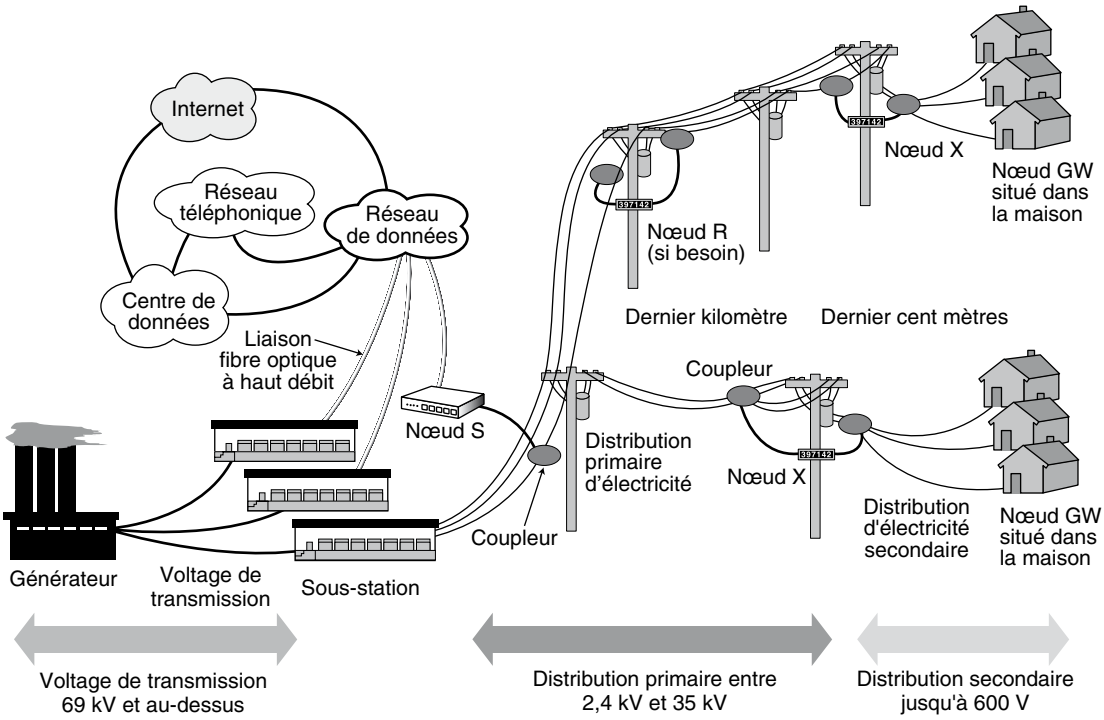


Figure 9.14

Distribution de l'accès haut débit sur courant électrique

Conclusion

Ce chapitre a présenté les différentes technologies d'accès terrestre. Dans les différentes options, le câble téléphonique est le plus utilisé en France. Cela s'explique par le nombre d'utilisateurs qui peuvent être connectés par ce moyen. Cependant, le câble téléphonique est généralement de faible qualité, et la distance y est un critère important de détermination du débit. Une nouvelle boucle locale est en cours de réalisation avec la fibre optique pour passer aux très hauts débits.

La boucle locale hertzienne est beaucoup plus jeune mais déjà très compétitive par rapport à la boucle locale terrestre. Deux grandes solutions se développent en parallèle : les réseaux qui acceptent les mobiles, c'est-à-dire qui sont capables de réaliser des changements intercellulaires, et les réseaux sans fil qui offrent de plus hauts débits, mais sans mobilité. Nous examinons ces solutions au chapitre suivant.

10

Les réseaux d'accès hertziens

Les réseaux hertziens apportent une grande flexibilité de par leur interface, qui permet à un utilisateur de changer de place tout en restant connecté. Les communications entre équipements terminaux peuvent s'effectuer directement ou par le biais de stations de base, appelées encore points d'accès, ou AP (Access Point). Les communications des points d'accès vers le réseau sont généralement effectuées par câble, sauf dans le cas des réseaux mesh et ad-hoc que nous détaillons plus spécifiquement au chapitre 23. Les débits de ces réseaux se comptent en dizaines de mégabits par seconde.

Les réseaux hertziens se décomposent en deux grandes catégories : les réseaux dits sans fil et les réseaux de mobiles. À la différence des réseaux sans fil, les réseaux de mobiles permettent de passer d'une cellule à une autre sans couper la communication.

Ces deux catégories de réseaux sont fondamentalement différentes : les réseaux de mobiles sont complexes et permettent le passage intercellulaire, ou handover ou encore handoff. Les réseaux sans fil sont beaucoup plus simples, mais l'utilisateur doit rester dans sa cellule.

Plusieurs gammes de produits sont actuellement commercialisées dans les deux catégories. Dans le cadre des réseaux sans fil, le groupe de travail qui se charge de cette normalisation provient essentiellement de l'IEEE. Les réseaux de mobiles sont normalisés par le 3GPP (3rd Generation Partnership Project) et le 3GPP2 suivant le type de standard. On y trouve quatre générations : 1G, 2G, 3G et 4G. La 1G a disparu dans la plupart des pays, la 2G correspond au GSM, la 3G à l'UMTS et la 4G au LTE-Advanced ou LTE-A.

Les normes des réseaux sans fil

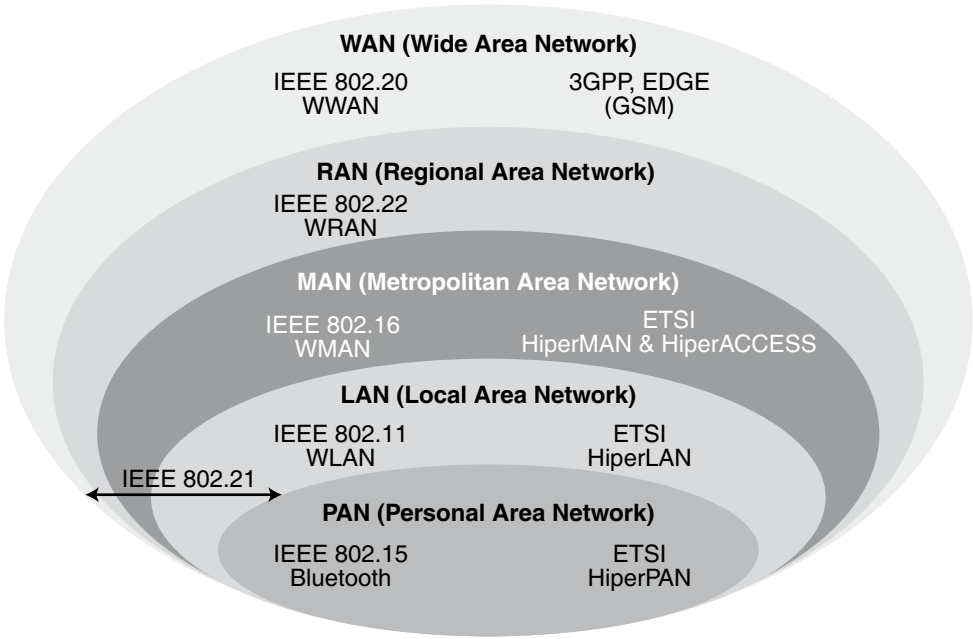


Figure 10.1

Classement des réseaux sans fil suivant leur étendue

Les principales normes de réseaux sans fil illustrées à la figure 10.1 sont les suivantes :

- IEEE 802.15, pour les petits réseaux personnels d'une dizaine de mètres de portée ;
- IEEE 802.11, ou Wi-Fi, pour les réseaux WLAN (Wireless Local Area Network) ;
- IEEE 802.16, pour les réseaux WMAN (Wireless Metropolitan Area Network) atteignant plus de dix kilomètres de portée ;
- IEEE 802.22, pour les WRAN (Wireless Regional Area Network).

L'ensemble des normes de réseaux sans fil sont récapitulées à la figure 10.2.

Dans le groupe IEEE 802.15, trois principaux sous-groupes normalisent des gammes de produits en parallèle :

- IEEE 802.15.1, le plus connu, qui a pris en charge la norme Bluetooth jusqu'en 2005.
- IEEE 802.15.3, qui définit la norme UWB (Ultra-Wide Band).
- IEEE 802.15.4 s'occupe de la norme ZigBee.
- D'autres groupes de travail en cours d'élaboration sont détaillés au chapitre 21.

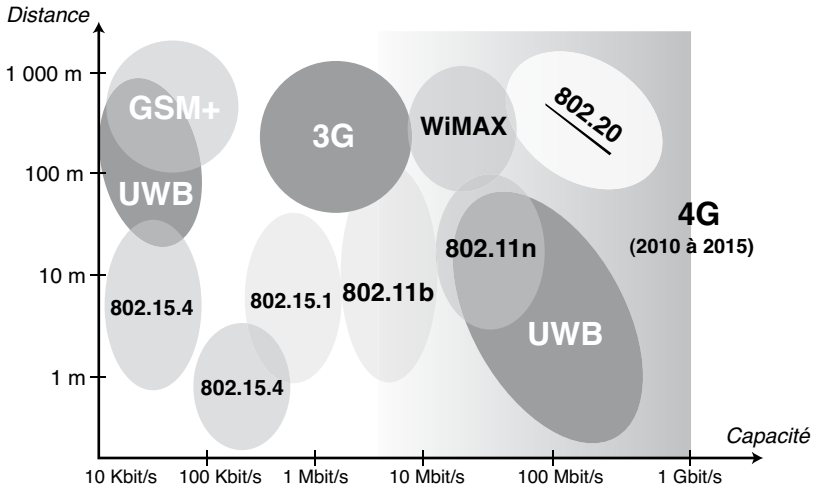


Figure 10.2

Principales normes de réseaux sans fil

Du côté de la norme IEEE 802.11, ou Wi-Fi (Wireless-Fidelity), quatre propositions ont été avalisées, dont les débits vont de 11 Mbit/s (IEEE 802.11b), puis 54 Mbit/s (IEEE 802.11a et g) jusqu'à 600 Mbit/s en pointe (IEEE 802.11n). Deux autres propositions, provenant des travaux du groupe IEEE 802.11ac et IEEE 802.11af, permettent d'augmenter fortement le débit, avec plusieurs gigabits par seconde en débit crête. Les fréquences utilisées se placent dans la bande 2,4-2,483 5 GHz pour les extensions b et g, dans la bande 5,15-5,35 GHz pour 802.11a, dans les deux bandes à la fois dans le 802.11n et ac, et dans les bandes de télévision pour l'IEEE 802.11af.

Les réseaux hertziens IEEE 802.16 visent à remplacer les modems ADSL, que l'on trouve sur les réseaux téléphoniques fixes, pour donner à l'utilisateur final des débits du même ordre de grandeur, c'est-à-dire jusqu'à plusieurs mégabits par seconde. Ces réseaux forment ce que l'on appelle la boucle locale radio.

Plusieurs normes sont proposées suivant la fréquence utilisée. Un consortium s'est mis en place pour développer les applications de cette norme sous le nom de WiMAX Forum. Deux versions sont commercialisées, l'une fixe, dont l'objectif est clairement de remplacer l'ADSL dans les zones rurales, l'autre mobile, permettant d'avoir un modem ADSL dans sa poche et toujours connecté.

Les réseaux régionaux sont étudiés par l'IEEE 802.22. Le rayon de la cellule peut atteindre 50 km pour les gammes de fréquences en dessous de 1 GHz. La distance potentielle du terminal à l'antenne étant importante, le débit montant est assez limité. En revanche, sur la bande descendante, 4 Mbit/s sont disponibles. L'application de base est la télévision interactive ou les jeux vidéo interactifs.

Les WWAN (Wireless Wide Area Network) sont plutôt concernés par les réseaux de mobiles, grâce à leur architecture permettant de changer de cellule sans couper la communication. Nous examinons le cas des réseaux de mobiles plus loin dans ce chapitre..

Typologie des réseaux hertziens

Cette section introduit les solutions issues de l'utilisation de fréquences hertziennes pour la desserte des entreprises et des utilisateurs résidentiels en lieu et place des câbles métalliques ou de la fibre optique enfouis dans le sous-sol. Les débits des réseaux hertziens peuvent se révéler très importants grâce à des techniques de codage de plus en plus sophistiquées, une méthode d'accès adaptée et une bonne réutilisation des ressources spectrales.

Nous commencerons par décrire la boucle locale hertzienne, puis examinerons les méthodes d'accès dans ces réseaux. Nous donnerons ensuite quelques exemples de réseaux d'accès radio. Enfin, nous présenterons les différentes générations de réseaux de mobiles.

La boucle locale satellite est une autre solution pour accéder au réseau terrestre d'un opérateur. Dans ce cas, le signal part de l'entreprise et, grâce à une antenne, accède au satellite, qui renvoie le signal vers le central d'accès d'un opérateur de télécommunications. Nous détaillerons également le fonctionnement de cette boucle locale.

La boucle locale sans fil

La technologie hertzienne est facilement utilisable dans la boucle locale puisque les techniques sans fil permettent, au prix d'infrastructures terrestres minimales, de relier un opérateur à ses clients. La différence avec les réseaux de mobiles provient de l'immobilité du client : il s'agit dans ce cadre de relier un domicile au réseau de l'opérateur. Il n'y a pas besoin de gérer la mobilité de l'utilisateur ce qui évidemment simplifie considérablement le système.

L'abréviation BLR (boucle locale radio) est la terminologie adoptée en France. Elle recouvre un certain nombre de techniques adaptées au cas français. Une autre façon de présenter cette solution est de parler de WDSL (Wireless Data Subscriber Line). Nous essaierons dans la suite de ce chapitre de nous positionner de façon plus générale en incluant les technologies et les fréquences utilisées à l'étranger.

La boucle locale radio est une technologie sans fil bidirectionnelle, dans laquelle l'équipement terminal ne peut être mobile — du moins pour le moment — au sens d'un réseau de mobiles. L'antenne de réception doit être grande et fixe.

Une boucle locale radio est illustrée à la figure 10.3. Elle est formée d'un ensemble de cellules (en grisé sur la figure). Chaque cellule est raccordée à une station de base, qui dessert les utilisateurs abonnés. La station de base est constituée d'une ou plusieurs antennes reliées aux utilisateurs directement par un faisceau hertzien. Les stations de base sont interconnectées par un réseau terrestre. L'accès à ce réseau terrestre s'effectue par le biais d'un commutateur.

L'avantage de cette solution de réseau d'accès réside dans la simplicité de sa mise en place. Il suffit de relier l'antenne de l'utilisateur à l'antenne de la station de base, évitant de la sorte tous les travaux de génie civil que demande la pose de câbles. Cependant, il ne faut pas négliger la mise en place de l'infrastructure à l'intérieur du ou des bâtiments de l'utilisateur pour connecter toutes les machines à l'antenne, laquelle doit être généralement en vue directe de l'antenne de l'opérateur.

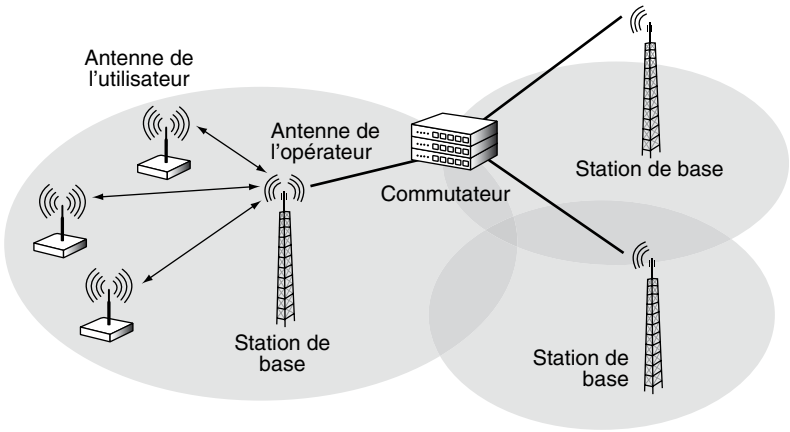


Figure 10.3
Boucle locale radio

Dans la suite, nous appelons WLL (Wireless Local Loop) toutes les boucles locales sans fil, incluant à la fois les technologies adoptées en France sous le nom de BLR et celles utilisées hors de France.

Les systèmes WLL

Les systèmes WLL proviennent de différentes technologies hertziennes qui ont pour but de transférer des données à la plus haute vitesse possible. Ils doivent être compétitifs par rapport à leur homologue fixe et, de ce fait, posséder les propriétés suivantes :

- Modems à faible coût, à peine plus élevé que les modems ADSL ou câble.
- Bande passante importante, pour que, en période de forte occupation, chaque utilisateur puisse continuer à travailler de façon satisfaisante.
- Techniques de transmission des données évoluées, afin d'offrir des débits acceptables pour chaque utilisateur, même en période de pointe.
- Grande flexibilité, permettant de prendre en charge les différents types de trafic, allant de la parole téléphonique aux transports de données à très haute vitesse.
- Architecture modulaire, pour permettre les mises à niveau en cas d'améliorations techniques des interfaces air.

Les systèmes WLL disponibles sur le marché sont de plus en plus nombreux. Nous allons en décrire trois exemples :

- Les technologies IEEE 802.11 directives, dites encore Wi-Fi directif.
- IEEE 802.16, ou WiMAX, une norme stabilisée en décembre 2004 et qui s'est fortement répandue depuis. Une version spécifique, le WiBro a été développée en Corée.
- IEEE 802.22, qui préfigure les connexions sur de plus longues portées afin de diminuer les coûts de déploiement. Cette dernière technologie devrait profiter du dividende

numérique, c'est-à-dire de la récupération de bandes de télévision qui se trouvent libérées lorsqu'un pays passe à la télévision tout numérique. Ce passage intervient depuis 2007 et devrait s'achever en 2015 (en France fin 2011).

L'allocation de ressources

Dans un système de transmission, chaque communication consomme une ressource physique dont le volume dépend de la quantité d'information à envoyer. Sur l'interface radio, la ressource est le canal physique. Le système commence par définir ce canal, puis il planifie la distribution du canal entre les différents utilisateurs à l'aide de mécanismes d'allocations de ressources. L'ensemble des ressources disponibles forme la *bande passante*. Cette bande est divisée en plusieurs ensembles de canaux radio non interférents. Ces canaux peuvent être utilisés simultanément, à condition qu'ils garantissent une qualité acceptable. Le multiplexage de plusieurs communications sur une même bande passante se fait à l'aide des techniques FDMA, TDMA, CDMA ou SDMA, que nous détaillons un peu plus loin. La technique OFDMA, qui est de plus en plus utilisée, est introduite à la section suivante.

La principale caractéristique de l'interface radio est l'affaiblissement de la puissance en fonction de la distance qui sépare l'utilisateur mobile de sa station de base.

L'atténuation ou l'affaiblissement

La puissance reçue (C) est directement liée à la puissance émise (P_e). Elle est calculée par la formule $C = P_e d^{-\alpha}$, α étant le paramètre de l'environnement de propagation, qui peut être urbain ou rural ; le α caractérise cet environnement, lequel peut varier de 2 à 4.

La puissance d'émission de chaque canal doit être optimisée. Cela permet d'assurer une bonne qualité de service de la communication sur le lien radio. L'allocation de ressources, qui consiste en la réutilisation d'un canal, doit respecter un certain rapport signal sur interférence, ou C/I (Carrier to Interference Ratio), qui est un paramètre d'optimisation du réseau. La variable C correspond à la puissance du signal reçu, et la variable I à la somme de tous les signaux des utilisateurs naviguant sur le même canal.

Les schémas d'allocation de ressources

En résumé, l'allocation d'un canal est le produit de l'interaction entre plusieurs paramètres, tels que l'interférence, la distance de réutilisation, etc., que des schémas d'allocation de ressources permettent de contrôler à travers le réseau.

Il existe trois grandes familles de schémas d'allocation de ressources :

- FCA (Fixed Channel Assignment). La plupart des systèmes existants fonctionnent avec une assignation fixe. Ce schéma a l'avantage de la simplicité et de la rapidité. Il s'agit d'une attribution fixe de ressources à toutes les stations. Cette attribution dépend du dimensionnement du réseau et des prévisions de trafic. Ce schéma trouve ses limites

dans le fait qu'il ne permet pas de gérer les variations brutales et instantanées du trafic, telles que les embouteillages et les grandes manifestations, ce qui rend l'utilisation de la bande passante peu efficace. Cette situation peut se traduire par un manque de ressources pour certaines stations et une sous-utilisation pour d'autres.

- DCA (Dynamic Channel Assignment). Dans le DCA, toutes les ressources sont concentrées dans un groupe commun, ou common pool, tandis qu'un système central ou distribué tente d'allouer les canaux à la demande des utilisateurs. Ce procédé, qui respecte le taux d'interférences C/I sur le canal, peut accroître de façon considérable la capacité du système, en particulier dans le cas d'une distribution du trafic non uniforme dans le temps. La mise en place de ce schéma requiert en contrepartie une importante charge de signalisation et une forte puissance de calcul pour trouver rapidement une solution d'allocation optimale.
- HCA (Hybrid Channel Assignment). Dans ce schéma, qui mélange les deux précédents, une partie des ressources est allouée directement aux stations, le reste étant rassemblé dans un groupe commun, auquel toutes les stations peuvent accéder lorsque leur ensemble fixe est complètement alloué.

Les techniques d'accès FCA

Dans les réseaux radio qui partagent le canal radio entre plusieurs utilisateurs, il faut une technique d'accès qui permette à l'utilisateur d'émettre ses paquets. Par exemple, le satellite pouvant être vu comme un miroir qui reflète les signaux reçus, si plusieurs paquets lui arrivent simultanément, leurs signaux se superposent. Pour éviter ces collisions, différentes techniques d'accès ont été proposées, des plus simples aux plus complexes. Comme les stations sont indépendantes les unes des autres et que le temps aller-retour permettant à une station de correspondre avec une autre peut devenir important, il faut pouvoir, dans certains cas, allouer le canal d'une façon anticipée.

Des méthodes de réservation fixe, ou FAMA (Fixed-Assignment Multiple Access), allouent la ressource canal à une station déterminée à un instant donné ou sur un code déterminé à l'avance ou encore sur un espace dédié. Les quatre principales d'entre elles sont les suivantes :

- FDMA (Frequency Division Multiple Access), qui divise la ressource canal en plusieurs bandes de fréquences pouvant être de largeur variable. Les fréquences sont attribuées aux différentes stations selon leur besoin.
- TDMA (Time Division Multiple Access), qui consiste à découper le temps en tranches et à allouer les tranches aux stations. Soit les tranches sont de taille différente, et les stations terrestres se voient affecter une tranche correspondant à leur débit, soit les tranches sont d'une longueur fixe assez petite, correspondant à un débit de base, les stations qui souhaitent un débit plus important possédant plusieurs tranches de temps.
- CDMA (Code Division Multiple Access), qui consiste à allouer aux différentes stations la bande passante globale mais avec un code tel que tous les signaux sont émis en même temps, le récepteur étant capable de déterminer les signaux à capter en fonction du code et de la puissance associée.

- SDMA (Space Division Multiple Access), qui consiste à diviser l'espace en plusieurs secteurs, de sorte qu'une antenne directive n'émette que sur un espace réduit au lieu de diffuser ses signaux dans toutes les directions. Cette solution permet de beaucoup mieux utiliser l'espace hertzien et donne une forte réutilisation des fréquences. De plus, le signal étant directif, la portée peut-être beaucoup plus grande.

FDMA, TDMA, CDMA et SDMA

Utilisé en premier, le FDMA tend à disparaître dans les réseaux d'accès pour renaître sous une autre forme, avec l'OFDM (Orthogonal Frequency Division Multiplexing) que nous détaillons plus loin dans ce chapitre.

Supposons un nombre *n* de stations terrestres. On découpe la bande de fréquences f1 en *n* sous-bandes, comme illustré à la figure 10.4, de façon à permettre à chaque station d'émettre indépendamment des autres liaisons.

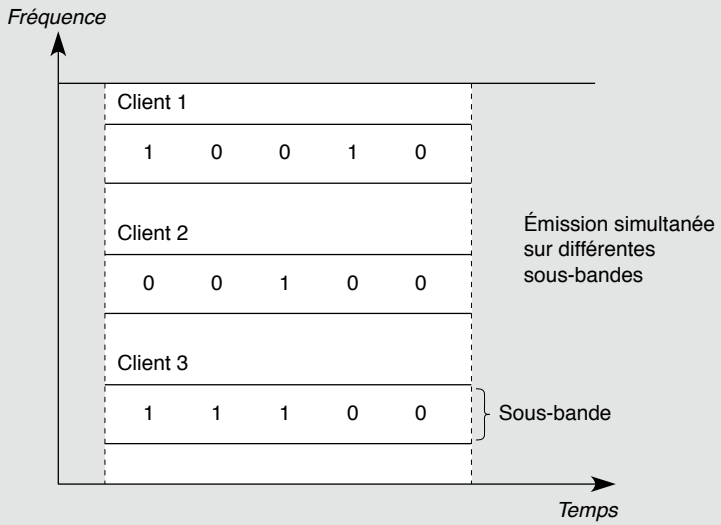


Figure 10.4
Le FDMA

Chaque station comporte de ce fait un modulateur, un émetteur, *n* récepteurs et *n* démodulateurs. Lorsque la solution est utilisée pour une connexion par satellite, le satellite doit amplifier simultanément les *n* porteuses. Il se crée donc nécessairement des brouillages, qui croissent rapidement en fonction de la puissance, avec pour conséquence que plus de la moitié de la capacité de transmission peut être perdue.

Pour éviter les collisions, on répartit le canal équitablement entre les divers utilisateurs. Les limites de cette technique sont évidentes : si une ou plusieurs liaisons sont inutilisées, il y a perte sèche des bandes correspondantes. Si l'on veut rendre cette politique dynamique en répartissant la fréquence f1 entre les utilisateurs actifs ou si l'on veut introduire une nouvelle station dans le réseau, il faut imposer une nouvelle répartition des fréquences, ce qui pose de nombreux problèmes et ne peut se faire que sur des tranches de temps assez longues.

Avec le TDMA, on découpe le temps en tranches, que l'on affecte successivement aux différentes stations d'émission, comme illustré à la figure 10.5.

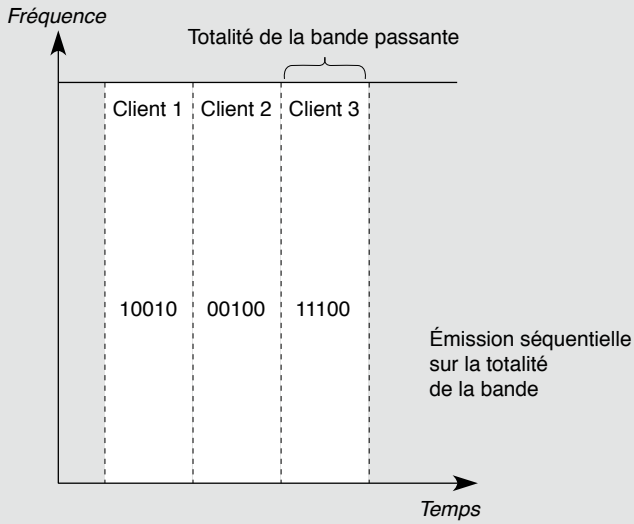


Figure 10.5
Le TDMA

Toutes les stations émettent avec la même fréquence sur l'ensemble de la bande passante, mais successivement. À l'opposé du fonctionnement en FDMA, chaque station possède un seul récepteur démodulateur. Chaque tranche de temps est composée d'un en-tête, ou préambule, qui a plusieurs fonctions : les premiers éléments binaires permettent d'acquérir les circuits de recouvrement de porteuse et de rythme du démodulateur. L'en-tête transmet également les informations nécessaires à l'identification de la station émettrice. Il est nécessaire de synchroniser l'émission en début de tranche de façon qu'il n'y ait pas de chevauchement possible. Il existe entre chaque tranche un intervalle réservé à cet effet.

Globalement, le rendement du TDMA est meilleur que celui du FDMA. De plus, il est facile de découper de nouvelles tranches de temps si des stations supplémentaires se connectent sur le canal. La tranche de temps, ou slot, a une durée variable, qui dépend de l'application sous-jacente. Par exemple, dans le cas du transport de la parole téléphonique numérisée sur un multiplex normalisé de 2 Mbit/s (correspondant à 30 voies téléphoniques), une tranche de temps est composée de 6 blocs de 125 µs. Les signaux transmis pendant cette tranche forment une trame de 750 µs précédée d'un préambule. Il est évident que l'augmentation de la durée des tranches de temps diminue la fraction du temps perdu en en-tête et augmente l'efficacité de la transmission et le taux d'utilisation réel du canal.

Comme nous venons de le voir, toute la difficulté du TDMA est de passer le relais aux émetteurs qui en ont réellement besoin, au bon moment et avec la tranche de temps la plus longue possible. Il convient dans ce cas de recourir à une politique d'allocation dynamique : les stations demandent, au fur et à mesure de leurs besoins, les tranches nécessaires pour écouler leur trafic. Ces demandes d'allocation ont toutefois l'inconvénient d'alourdir la gestion du système et d'augmenter sensiblement le temps de réponse, puisqu'il faut au minimum deux allers-retours pour obtenir de la station maître qui gère le système les tranches de temps correspondant à la demande.

Avec le CDMA, que l'on trouve dans les réseaux de mobiles terrestres de troisième génération, la station terrestre émet sur l'ensemble de la bande passante mais avec un code qui détermine sa puissance en fonction de la fréquence. Cette solution permet au récepteur de décoder les signaux et de les récupérer. La difficulté de cette méthode réside dans une émission avec une puissance déterminée, de façon que la station terrestre de réception puisse démêler tous les signaux reçus simultanément. La figure 10.6 illustre ce processus.

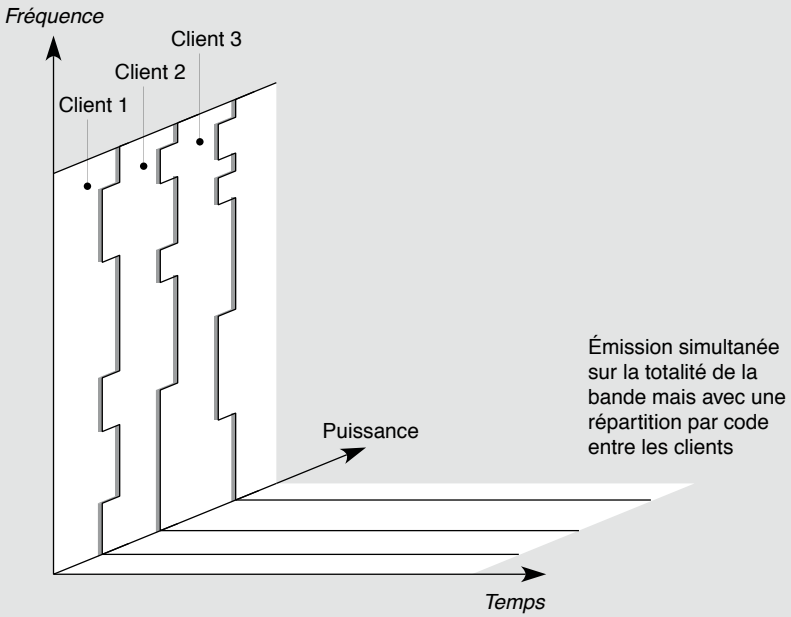


Figure 10.6
Le CDMA

Le SDMA est une technologie encore peu utilisée qui demande une antenne intelligente capable de s'adapter pour émettre sur un secteur précis, avec une puissance déterminée. Si une station est située près de l'antenne de réception, il est en effet inutile d'émettre avec une forte puissance et dans toutes les directions à la fois. La méthode SDMA permet de limiter géographiquement la surface sur laquelle la fréquence est utilisée permettant ainsi une excellente réutilisation.

L'OFDM

L'OFDM est une des techniques les plus utilisées aujourd'hui dans les réseaux modernes. Elle utilise la technique d'allocation FDMA, mais au lieu d'être obligé de séparer les canaux des différentes fréquences, on utilise des fréquences orthogonales : lorsque la puissance est maximale sur une fréquence, elle est nulle sur les fréquences connexes. Cette solution est illustrée à la figure 10.7.

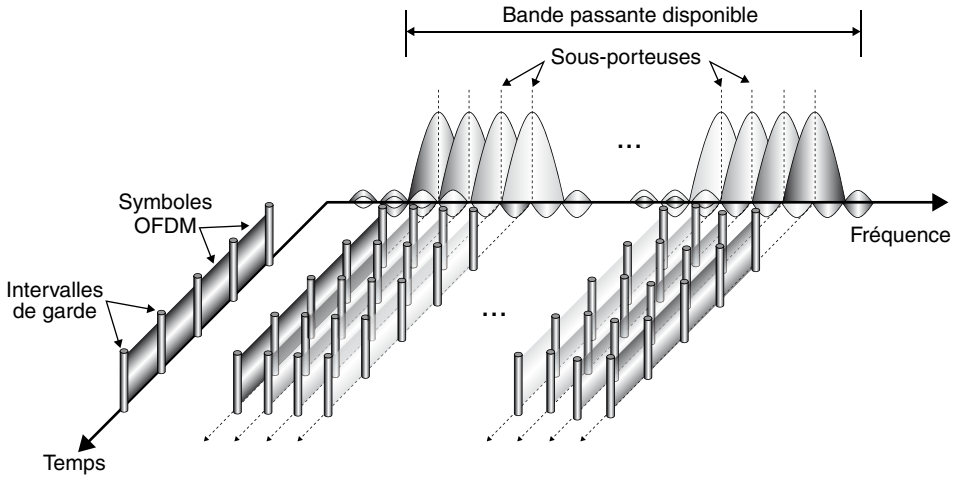


Figure 10.7
Les fréquences de l'OFDM

Cette solution permet de transporter des éléments binaires différents sur chaque sous bande, de telle sorte que plusieurs bits voire octets peuvent être transmis simultanément.

Il est possible d'y associer temporellement un découpage dans le temps, qui permet d'allouer les sous-bandes à des stations différentes. On obtient dans ce cas la technique d'accès OFDMA. Cette technique, utilisée, par exemple, dans le WiMAX, est illustrée à la figure 10.8. On remarque que chaque émission temporelle utilise l'ensemble de toutes les fréquences.

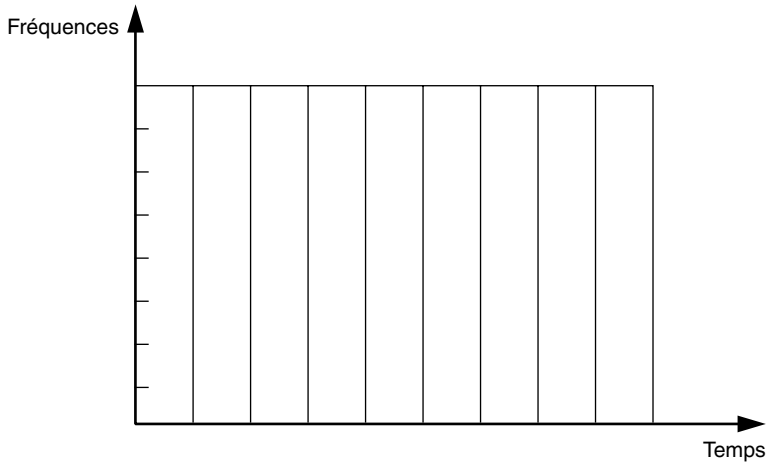


Figure 10.8
La technique d'accès OFDMA

Il est possible d'améliorer encore cette solution, en affectant les sous-bandes à des stations différentes, comme cela se fait dans le WiMAX mobile. On parle alors de SOFDMA (Scalable OFDMA). Comme l'illustre la figure 10.9, il est ainsi possible de partager de façon beaucoup plus fine le canal radio et de donner à chaque station le débit exact dont elle a besoin.

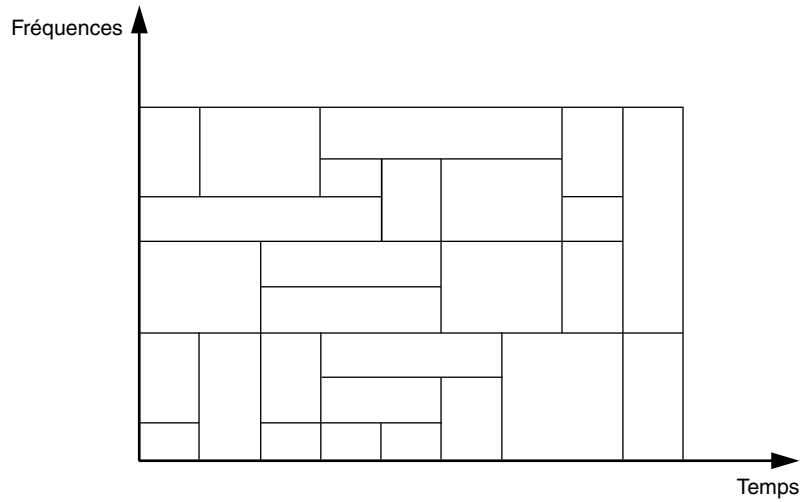


Figure 10.9
La technique SOFDMA

Les méthodes dynamiques DCA

Les méthodes DCA (Dynamic Channel Assignment) ont pour objectif de mieux utiliser le canal, mais avec un effort de calcul beaucoup plus important.

Les politiques d'accès aux canaux doivent favoriser une utilisation maximale du canal, celui-ci étant la ressource fondamentale du système. Dans les réseaux locaux, le délai de propagation très court permet d'arrêter les transmissions après un temps négligeable. Dans le cas de satellites géostationnaires, les stations terrestres ne découvrent qu'il y a eu chevauchement des signaux que 0,27 s après leur émission — elles peuvent s'écouter grâce à la propriété de diffusion —, ce qui représente une perte importante sur un canal d'une capacité de plusieurs mégabits par seconde.

Les trois grandes catégories de techniques DCA sont les suivantes :

- méthodes d'accès aléatoires, ou RA (Random Access) ;
- méthodes de réservation par paquet, ou PR (Packet Reservation) ;
- méthodes de réservation dynamique, ou DAMA (Demand Assignment Multiple Access).

Les techniques d'accès aléatoires donnent aux utilisateurs la possibilité de transmettre leurs données dans un ordre sans corrélation. En revanche, ces techniques ne se prêtent à aucune qualité de service. Leur point fort réside dans une implémentation simple et un coût de mise en œuvre assez bas.

La méthode la plus connue est celle qui est utilisée dans le cadre des réseaux Ethernet terrestres avec le CSMA/CD. Cette solution est étudiée en détail au chapitre 14. Dans les réseaux radio, la solution de base ne peut plus être utilisée, car il est impossible d'émettre et d'écouter en même temps. De ce fait, la solution a été modifiée en utilisant du CSMA/CA, que nous étudions en détail au chapitre 22.

Les méthodes de réservation par paquet évitent les collisions par l'utilisation d'un schéma de réservation de niveau paquet. Comme les utilisateurs sont distribués dans l'espace, il doit exister un sous-canal de signalisation à même de mettre les utilisateurs en communication pour gérer la réservation. Ces solutions sont surtout utilisées dans les réseaux satellite, que nous abordons un peu plus loin dans ce chapitre.

Les méthodes dynamiques de réservation ont pour but d'optimiser l'utilisation du canal. Ces techniques essaient de multiplexer un maximum d'utilisateurs sur le même canal en demandant aux utilisateurs d'effectuer une réservation pour un temps relativement court. Une fois la réservation acceptée, l'utilisateur vide ses mémoires tampons jusqu'à la fin de la réservation puis relâche le canal.

Exemples de réseaux d'accès hertziens

Cette section introduit trois techniques de réseaux radio qui peuvent être utilisées dans la boucle locale.

IEEE 802.11

Le groupe de travail IEEE 802.11 a normalisé un ensemble de standards correspondant aux différents réseaux Wi-Fi que nous détaillons au chapitre 22. Nous nous intéressons ici uniquement à l'utilisation directionnelle d'un environnement Wi-Fi de façon à arroser une zone lointaine ou relier des stations situées à plusieurs kilomètres l'une de l'autre. Beaucoup de municipalités utilisent cette solution très peu onéreuse, dont le seul inconvénient est d'utiliser des fréquences partagées, puisque situées dans les bandes libres des 2,4 ou 5,15 GHz.

La réglementation française autorise une puissance d'émission maximale en intérieur de 100 mW dans la bande des 2,4 GHz et à l'extérieur de 100 mW également dans la bande 2,400-2,454 GHz et 10 mW dans la bande 2,454-2,483 5 GHz. La bande des 5 GHz n'est utilisable qu'en milieu intérieur et est formellement interdite à l'extérieur.

Le choix d'une antenne dépend de ce que l'on veut en faire. Pour le cas illustré à la figure 10.10, la puissance d'émission, ou PIRE (puissance isotropique rayonnée effective), équivaut à la somme des puissances de l'émetteur (P_e), de l'amplificateur (P_{ampli}) et du gain de l'antenne ($G_{antenne}$) moins la perte sur la ligne, exprimée en dBm. Dans le cas où il n'y a pas d'amplificateur, le calcul se résume à la somme de la puissance de l'émetteur et

du gain de l'antenne moins la perte sur la ligne due au câble reliant l'antenne à l'émetteur. Dans le cas général, on obtient :

$$PIRE = P_e + P_{ampli} + G_{antenne} - Perte$$

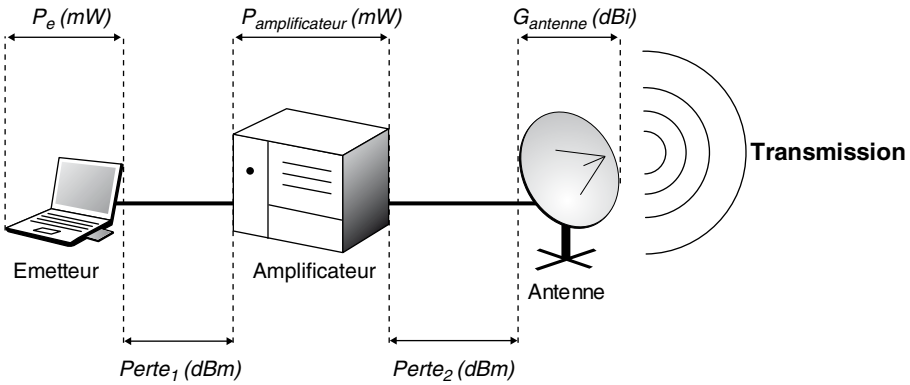


Figure 10.10
Calcul de la PIRE

Considérons une carte Wi-Fi 802.11 ayant une puissance d'émission de 30 mW. On voudrait se connecter par le biais d'un ordinateur portable à un point d'accès se trouvant à quelques kilomètres. La capacité de l'antenne interne de la carte n'autorisant une zone de couverture que de l'ordre d'une centaine de mètres, il est nécessaire de connecter une antenne à la carte. Prenons comme exemple une antenne de type parabole ayant un gain de 24 dBi reliée par un câble de 3 m dont la perte est de 2 dB/m. La perte totale est donc de 6 dB.

Pour trouver la PIRE, il faut que toutes les valeurs de la somme s'expriment en dBm. En appliquant la formule précédente, une puissance de 30 mW correspond à un gain de 14,77 dBm. La PIRE équivaut à 14,77 + 24 – (3 × 2), soit 32,77 dBm. Cela correspond à 1 892 mW, soit près de 20 fois la puissance maximale autorisée. Le déploiement dans ces conditions est illégal.

On voit donc que plus l'antenne est directive, plus la puissance doit être faible. Il n'empêche qu'avec des antennes directives, il est possible de couvrir des zones assez grandes et de relier un terminal à une antenne avec des distances importantes. Cette solution est parfois utilisée par des opérateurs pour relier des points hauts à des débits de 11 ou 54 Mbit/s.

IEEE 802.16

L'IEEE a mis en place le groupe de travail 802.16 pour proposer des standards de réseaux métropolitains dans la lignée des solutions développées pour les réseaux locaux et plus particulièrement de Wi-Fi.

Le groupe de travail 802.16 s'est d'abord préoccupé de la bande du spectre hertzien et a proposé l'utilisation de certaines bandes, comprises entre 2 et 11 GHz, dont les fréquences ne sont pas trop directives, et des plages situées entre 11 et 66 GHz, dont les fréquences sont hyperdirectives et demandent une visibilité directe des antennes.

Les standards IEEE 802.16 sont organisés en trois niveaux :

- Le niveau physique. Spécifie les fréquences, schémas de modulation, synchronisations, vitesses, techniques de découpage dans le temps (de type TDMA) et techniques de détection et de correction d'erreur, qui peuvent être choisies en option. La proposition de standard concerne la technique DAMA-TDMA (Demand Assignment Multiple Access-Time Division Multiple Access), qui correspond à une réservation dynamique de bande passante par l'intermédiaire de slots de temps. En d'autres termes, le temps est divisé en trames de longueur constante, elles-mêmes divisées en slots. Les slots sont alloués aux utilisateurs par des techniques de réservation. Dans le sens utilisateur vers réseau, l'allocation des slots est assez simple puisque la station de base sait ce qu'elle a à envoyer. Dans l'autre sens, le processus est plus complexe, puisque les stations sont indépendantes les unes des autres et que la communication entre les stations de base ne peut se faire qu'au travers de la station de base, via l'antenne de l'opérateur. Sur la voie allant de l'opérateur aux clients, deux modes sont proposés. Le mode A concerne les flux de type stream, c'est-à-dire les flux continus qui possèdent des points de synchronisation. Le mode B concerne les flots fondés sur les applications classiques du monde IP.
- Le niveau MAC. Situé au-dessus du niveau physique, il gère l'allocation des slots et utilise la méthode DAMA-TDMA.
- L'interface de communication avec les applications. Le niveau recherché est de type IP, mais la trame ATM peut aussi être émise sur la voie hertzienne directement dans les slots choisis par le niveau MAC. IP devenant de plus en plus le standard de référence, cette couche se concentre sur la gestion du niveau IP et l'encapsulation des paquets IP dans une trame adaptée à la tranche de temps. Au récepteur, les fragments sont réassemblés pour redonner le paquet IP.

Les standards 802.16 les plus importants sont les suivants :

- IEEE 802.16. Finalisé en décembre 2001, il concerne les bandes comprises entre 10 et 66 GHz, avec une vision directe entre les deux antennes pour des applications point-à-point.
- IEEE 802.16 2004. Révise et corrige quelques erreurs détectées dans les standards 802.16 et 802.16a et apporte des améliorations. C'est le standard que suivent les produits WiMAX fixe.
- IEEE 802.16a. Finalisé en janvier 2003, il complète le précédent pour la bande des 2 à 11 GHz. Ce standard s'adapte à des environnements multipoint et tient compte des impératifs des applications multimédias pour les acheminer.
- IEEE 802.16c. Amendement de 2002 au standard de base.
- IEEE 802.16e. Le standard est sorti en décembre 2005, avec pour objectif de permettre la mise en place des liaisons ADSL vers les mobiles. Les changements intercellulaires ou handovers sont pris en charge par le système. Le réseau sans fil donnant naissance au WiMAX mobile fonctionne dans une bande avec licence située en dessous des 6 GHz.

- IEEE 802.16m. Ce standard définit la nouvelle génération du WiMAX (WiMAX phase 2), qui a été acceptée comme membre de la famille 4G. Ce choix redonne un peu de vie au WiMAX.

Les produits WiMAX fixe et WiMAX mobile sont décrits à l'annexe I.

IEEE 802.22

Une nouvelle initiative soutenue par de nombreux industriels dans le domaine des réseaux régionaux concerne les WRAN (Wireless Regional Area Network).

Cette norme, dont l'étude a démarré en 2005, ne devrait être disponible que vers 2012. Elle a pour objectif d'utiliser le dividende numérique pour atteindre des portées de plusieurs dizaines de kilomètres et permettre de diffuser des applications de types télévision interactive, jeux vidéo interactifs ou vidéo à la demande sur des ordinateurs portables en mobilité.

Les techniques sous-jacentes sont très innovantes, avec l'utilisation de radios cognitives (que nous décrivons à la fin de ce chapitre), permettant de déterminer, pour un terminal donné, sa direction d'émission, sa puissance et la fréquence à utiliser. Cette solution devrait permettre de multiplier par dix l'utilisation spectrale.

Si l'on considère de surcroît que le dividende numérique va permettre de débloquer 200 MHz de bande passante en dessous de 1 GHz, c'est-à-dire pour les ondes pénétrant dans les bâtiments, comme la télévision, il est évident que cette nouvelle technologie régionale va concurrencer les opérateurs déjà installés. Une seule antenne devrait permettre, sur 20 à 30 kilomètres, de regrouper 30 000 télévisions interactives ou l'équivalent d'un million de téléphones portables, à condition, bien sûr, de disposer d'une très grande bande passante. Nous donnons quelques caractéristiques supplémentaires de ces réseaux à l'annexe I.

Les réseaux de mobiles

Les réseaux de mobiles se caractérisent par la mobilité du terminal. Pour réaliser cette mobilité, le réseau se compose de cellules, constituées par les espaces géographiques couverts par une antenne, et le système est capable de gérer des changements intercellulaires, c'est-à-dire le passage d'une cellule à une autre, ou encore le changement d'antenne.

Cette section examine les différentes générations de réseaux de mobiles, en partant de la première, entièrement analogique, pour atteindre la quatrième, totalement numérique et nativement IP.

Génération 1G

La première génération de réseaux de mobiles est apparue à la fin des années 1970. Elle définit un réseau cellulaire, c'est-à-dire composé de cellules, ou zones géographiques, limitées à quelques kilomètres, qui recouvrent le territoire de l'opérateur (*voir figure 10.11*). Ces cellules se superposent partiellement pour assurer une couverture

complète du territoire cible. Le mobile communique par le biais d'une interface radio avec l'antenne centrale, qui joue le rôle d'émetteur-récepteur de la cellule. Cette interface radio utilise des bandes de fréquences généralement spécifiques du pays dans lequel est implanté le réseau. L'émission des données sur l'interface radio est effectuée en analogique. Cette première génération ne pouvait avoir que relativement peu de succès, étant donné le fractionnement des marchés.

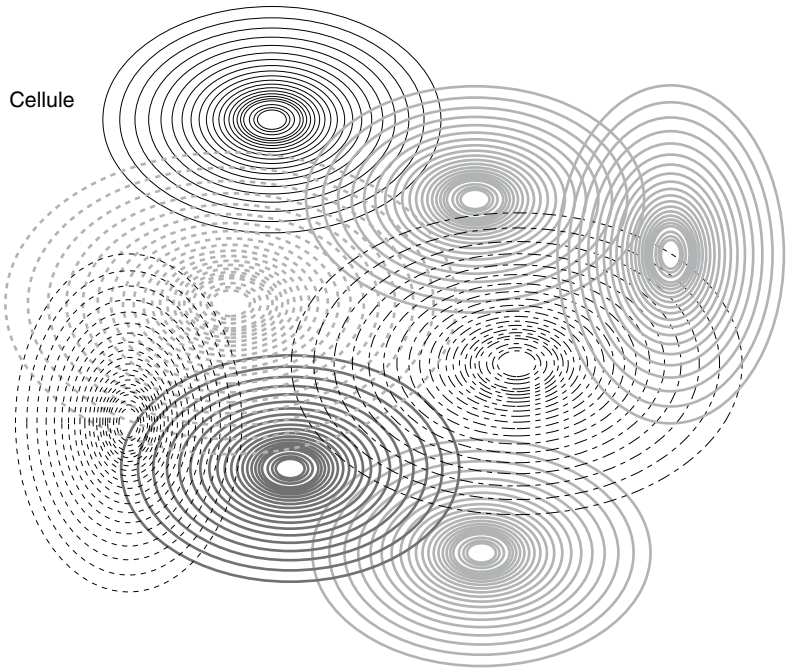


Figure 10.11
Réseau cellulaire

Les deux systèmes de première génération les plus développés proviennent des pays scandinaves. Il s'agit de NMT (Nordic Mobile Telecommunication), qui offre des fréquences de 450 puis 900 MHz et dessert 180 canaux depuis 1999, et d'AMPS (Advanced Mobile Phone System), qui utilise des bandes de fréquences comprises entre 800 et 900 MHz avec 832 canaux. Ce dernier système a donné naissance en Europe à l'ETACS (European Total Access Cellular System), qui utilise des bandes comprises entre 872 et 950 MHz.

La première génération utilise la technique d'accès FDMA (Frequency Division Multiple Access), qui consiste à donner à chaque utilisateur qui le demande une bande de fréquences dans la cellule où il se trouve afin de permettre l'émission et la réception des informations entre le mobile et l'antenne de la cellule. Lorsque le mobile sort de la portée de sa cellule, une autre bande de fréquences, qui correspond à la nouvelle cellule, lui est affectée. La bande précédente est libérée et réaffectée à un autre utilisateur. La

réutilisation des bandes de fréquences dans un maximum de cellules du réseau constitue l'un des problèmes majeurs posés par les systèmes cellulaires.

Comme pour les autres générations, la taille de la cellule dépend de la fréquence utilisée. Plus la fréquence est élevée, moins la portée est importante. Au départ, les fréquences utilisées allaient de 30 à 300 MHz dans les bandes UHF (Ultra-High Frequency) puis augmentaient dans les bandes VHF (Very High Frequency) de 300 MHz à 3 GHz. On utilise aujourd'hui des gammes de fréquences jusqu'à 20 GHz. Des fréquences encore plus élevées, atteignant 60 GHz, sont en cours d'expérimentation et vont donner lieu à des produits pour les réseaux personnels comme WiGig, des réseaux de type Wi-Fi mais pour de petites distances, que nous détaillons au chapitre 21. Les difficultés engendrées par de telles bandes proviennent de la grande directivité des ondes et d'un fort affaiblissement dans les environnements pollués. Leur portée est donc très faible et nécessite d'utiliser de toutes petites cellules, dites microcellules, voire des picocellules.

La largeur de la bande de fréquences utilisée dans la première génération dépend du système mais est généralement comprise entre 15 et 30 kHz. Les terminaux de cette génération ont connu une miniaturisation importante pour devenir réellement portables. Il a fallu résoudre le problème de la durée de vie des batteries, qui était très courte au départ et qui atteint aujourd'hui plusieurs jours.

Génération 2G

En 1982, la CEPT (Conférence européenne des Postes et Télécommunications) a décidé de normaliser un système de communication mobile dans la gamme des 890-915 MHz et 935-960 MHz pour l'ensemble de l'Europe. Deux ans plus tard, les premiers grands choix étaient faits, avec, en particulier, un système numérique. Le groupe spécial mobile, ou GSM, a finalisé en 1987 une première version comportant la définition d'une interface radio et le traitement de la parole téléphonique.

Avec une autre version dans la gamme des 1 800 MHz, le DCS 1800 (Digital Cellular System), la norme GSM a été finalisée au début de l'année 1990. Cette norme est complète et comprend tous les éléments nécessaires à un système de communication numérique avec les mobiles. Il existe d'autres normes pour cette deuxième génération, , comme l'IS-95 ou l'IS-136, mais elles sont fragmentaires et ne concernent généralement que l'interface radio.

Dans un système GSM, la station mobile comprend deux parties : l'équipement mobile, qui permet la communication radio, et le module d'identification, qui contient les caractéristiques identifiant l'abonné. Le réseau est découpé en cellules, qui possèdent chacune une station de base, ou BTS (Base Transceiver Station). Cette dernière s'occupe des transmissions radio sur la cellule. Associés à la station de base, des canaux de signalisation permettent aux mobiles de communiquer avec la BTS et *vice versa*. Chaque station de base est reliée à un contrôleur de station de base, ou BSC (Base Station Controller). Cette architecture est illustrée à la figure 10.12.

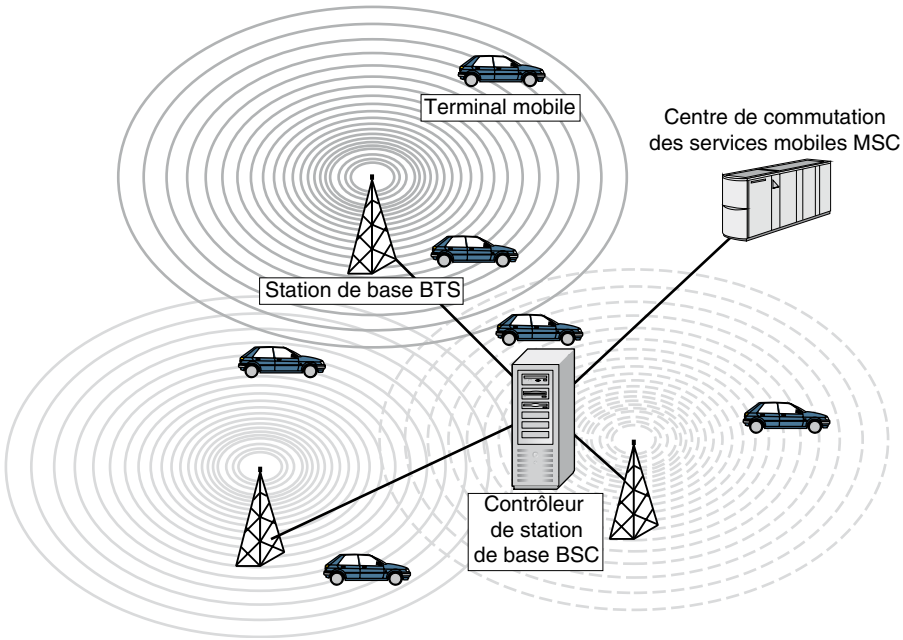


Figure 10.12
Architecture d'un réseau de mobiles

Le réseau lui-même contient un commutateur, ou MSC (Mobile services Switching Center), qui communique avec les différents systèmes radio, un enregistreur de localisation nominal, ou HLR (Home Location Register), qui est une base de données de gestion des mobiles, et un enregistreur de localisation des visiteurs, ou VLR (Visitor Location Register), qui est une base de données des visiteurs dans une cellule. Le système GSM comporte également des mécanismes de sécurité.

En ce qui concerne le mode d'accès, c'est la technique TDMA (Time Division Multiple Access), dans laquelle le temps est découpé en tranches, qui est employée. Une seule station peut accéder à une tranche donnée. Par canal radio, le découpage est effectué en huit tranches d'une durée de 0,57 ms. La parole est compressée sur une bande de 22,8 kHz, qui inclut un codage permettant la correction des erreurs. En Amérique du Nord, un système assez similaire, l'IS-54 (Interim Standard) a été développé. Il utilise également le TDMA. Sa vitesse de transmission peut atteindre 48,6 Kbit/s.

Les systèmes Télépoint, apparus avec la deuxième génération, constituent une autre possibilité de communication avec des récepteurs non reliés par câble. Dans ce cas, l'utilisateur peut accéder au réseau téléphonique avec un téléphone sans fil par l'intermédiaire d'une borne. Le rayon d'utilisation est souvent limité à une centaine de mètres. Le service Bi-Bop en France a fait partie de cette catégorie de réseau de communication local. La norme la plus utilisée est CT2 (Cordless Telephone of 2nd Generation), ou CAI (Common Air Interface). Cette norme, qui régit les transmissions numériques avec des combinés

sans fil, a été la première en Europe. Améliorée par les Canadiens sous le nom de CT2+, elle s'est vue ajouter des possibilités de gestion.

La norme DECT (Digital Enhanced Cordless Telecommunications) concerne plutôt les autocommutateurs téléphoniques, ou PABX (Private Automatic Branch eXchanger) sans fil. Dans quelques années, les autocommutateurs privés seront atteints par voie hertzienne. Les cellules seront alors très petites et les bandes assez facilement réutilisables à courte distance. Pour ces dernières normes, on parle de téléphonie mobile de proximité. Il faut rester sur la même borne durant toute la communication, ce qui implique de tout petits déplacements puisque les cellules sont minuscules.

Le réseau cœur du réseau de mobiles permet l'interconnexion des différents MSC, c'est-à-dire des commutateurs qui permettent aux contrôleurs de stations de base de communiquer entre eux. Dans la deuxième génération de mobiles, le réseau cœur est de type circuit. En d'autres termes, une communication entre deux machines s'effectue par un circuit. La différence avec un réseau de troisième génération réside dans le réseau cœur, qui passe d'une commutation de circuits à un transfert de paquets.

Un système intermédiaire, dit 2,5G, se place entre la deuxième et la troisième génération. Il consiste en un double réseau cœur incluant un réseau circuit pour la parole téléphonique et un réseau paquet pour le transfert des données. Le GPRS (General Packet Radio Service) puis EDGE (Enhanced Data for GSM Evolution) font partie de cette génération intermédiaire.

Génération 3G

La troisième génération s'est implantée au tournant des années 2000 avec un très fort déploiement à partir de 2005. Sa normalisation s'est effectuée principalement sous l'égide de l'UIT-T, sous le nom d'IMT 2000, et du 3GPP. La première ouverture a été celle de NTT DoCoMo au Japon en octobre 2001.

La différence la plus sensible avec la deuxième génération concerne l'introduction du mode paquet à l'exception de la parole téléphonique, qui reste très semblable à celle du GSM. Toutes les informations, en dehors de la parole, sont mises dans des paquets et transportées dans un réseau à transfert de paquets.

L'augmentation des débits est assez importante par rapport au GSM, qui plafonne à 9,6 Kbit/s, puisqu'elle atteint 384 Kbit/s dans les services commercialisés lors de la première génération de l'UMTS. Cependant, au démarrage de l'UMTS la partie du spectre dédiée à la troisième génération étant relativement faible, il ne fallait pas compter sur de très hauts débits en période fortement chargée.

Le codage numérique qui est utilisé pour le transport de la parole permet un débit de 8 Kbit/s. L'image animée est véhiculée par le biais d'une compression MPEG-2 ou MPEG-4. Plusieurs types de modulations ont été étudiés pour l'émission numérique du signal. Il s'agit d'extensions des modulations classiques en fréquence, en amplitude et en phase. L'accès au canal radio utilise les techniques FDMA, TDMA et CDMA.

FDMA et TDMA sont déjà utilisés dans la génération précédente et dans les réseaux satellite, mais avec l'inconvénient que la réutilisation des canaux radio dans des cellules

connexes peut donner lieu à un brouillage. La méthode principale pour la troisième génération est le CDMA. Les mobiles d'une même cellule se partagent un canal radio par des techniques d'étalement de spectre. Le système alloue un code unique à chaque client, ce code étant utilisé pour étaler le signal dans une très large bande passante, B, par rapport à la bande du signal utile, R. Plus le rapport B/R est important, plus le nombre d'utilisateurs potentiel augmente. L'avantage de cette méthode est la réutilisation des mêmes fréquences dans des cellules connexes.

La technique ATM a été adoptée dans un premier temps du fait de sa forte compatibilité avec le réseau fixe et pour la gestion des ressources. Aujourd'hui, on se dirige fortement vers des réseaux de type MPLS avec de la commutation Ethernet. La mobilité du terminal est assurée par des solutions normalisées par le 3GPP dans lesquelles l'intelligence est assez présente. Le débit des terminaux vers le réseau dans la première génération de l'UMTS reste relativement limité, avec 384 Kbit/s sur la voie montante, mais permet à l'utilisateur d'accéder à de premiers services multimédias.

Génération 3,5G

Une génération intermédiaire entre la 3G et la 4G s'est mise en place avec des extensions de l'UMTS et une augmentation des débits. Cette génération intermédiaire est illustrée par les solutions HSDPA, HSUPA et LTE. La commercialisation de HSDPA a démarré en 2006 et celle de HSUPA fin 2008.

HSDPA et HSUPA font entrer les mobiles dans l'univers des réseaux de données. Cette génération s'illustre par la mise en place de l'IMS (IP Multimedia Subsystem), que nous examinons en détail au chapitre 20. L'IMS est également classé au niveau terrestre comme faisant partie du NGN (Next Generation Network), qui représente la convergence fixe/mobile, dans laquelle les services sont accessibles aussi bien à partir de terminaux fixes que de terminaux mobiles.

La génération de l'IMS utilise de nombreux protocoles du monde Internet, dont le plus important est sûrement SIP (Session Initiation Protocol). La téléphonie devient de la téléphonie sur IP (ToIP).

Le LTE (Long Term Evolution), ou release 8 de l'UMTS, a démarré sa commercialisation au début de 2010 en Suède. C'est l'évolution la plus aboutie de l'UMTS et presque de la 4G. Cependant, elle reste classée en 3G+ du fait que la parole téléphonique n'est toujours pas en mode IP. C'est le passage au tout IP qui marque la 4G. Le débit crête du LTE peut atteindre 100 Mbit/s sur la voie descendante et 50 Mbit/s sur la voie montante.

La 3G a également introduit le principe du numéro unique. Le propriétaire de ce numéro peut l'utiliser sur tous les équipements, après, bien sûr, une authentification. En d'autres termes, l'utilisateur d'un équipement terminal porte avec lui son abonnement et l'utilise, avec les contraintes liées à l'équipement terminal, dans les conditions les plus diverses compatibles avec son abonnement. Une autre utilisation potentielle pour un individu muni de deux abonnements, un personnel et un professionnel, consiste à se faire appeler où qu'il soit dans le monde, sur l'un ou l'autre numéro. Selon la tonalité de la sonnerie, il peut savoir si l'on appelle son numéro privé ou celui de son entreprise.

Génération 4G

La quatrième génération est de nouveau une révolution pour les réseaux hertziens par sa totale compatibilité avec le monde IP, de telle sorte qu'il n'y a plus aucune différence entre un réseau fixe et un réseau de mobiles.

Toutes les applications sont traitées avec le protocole IP, même la parole téléphonique. Quoique l'on classifie parfois le LTE dans la quatrième génération, cette génération démarre avec le LTE Advanced. Les débits sont du même ordre de grandeur que dans le LTE. Les applications M2M (Machine to Machine) font partie de la 4G ainsi que toutes celles que l'on trouve aujourd'hui sur l'Internet fixe.

Le problème du manque de fréquences est résolu par l'utilisation de cellules de tailles différentes selon l'environnement et les débits demandés. Dans les zones très denses, il est possible d'utiliser des cellules de toute petite taille, capables d'apporter à chaque machine terminale un débit de plusieurs mégabits par seconde avec des débits crête beaucoup plus élevés.

Ces picocellules ont une portée de quelques dizaines de mètres au maximum. Pour des zones un peu moins denses, une ville avec moins de bureaux, par exemple, des microcellules de quelques centaines de mètres de diamètre sont adoptées. Des cellules plus grandes, dites cellules parapluie, se superposent aux précédentes pour résoudre les problèmes de grande mobilité.

La quatrième génération introduit à la fois le très haut débit et le « multi-homé », c'est-à-dire la possibilité de se connecter sur plusieurs réseaux simultanément.

Un même flot peut-être décomposé en plusieurs sous-flots transitant par des réseaux différents, afin d'augmenter la vitesse globale de la transmission. La quatrième génération peut également permettre à différents flots de partir chacun par son propre réseau. Le terminal doit donc être capable de détecter tous les réseaux qui sont autour de lui et de choisir pour chacune de ses applications le meilleur réseau à utiliser.

La radio cognitive et les avancées technologiques

Le mode du sans-fil progresse à une vitesse vertigineuse. On pensait avec les hauts débits relatifs de la 3G+ que l'on ne pourrait plus vraiment progresser. Il n'en est rien. On compte encore gagner entre 2010 et 2020 un ordre de grandeur de 1000 ! Là où les réseaux hertziens proposent actuellement des débits de 1 Mbit/s, on atteindra dans dix ans 1 Gbit/s. Cette augmentation prodigieuse à pour origine la radio cognitive et plusieurs autres avancées technologiques de premier plan.

Le premier concerne l'utilisation du spectre. Entre 0 et 20 GHz, il est d'environ 10 %. Ce spectre, que l'on disait saturé, l'est en fait très peu. Il est complètement licencié, c'est-à-dire que toutes les fréquences ont un propriétaire légal, mais les fréquences sont très souvent mal utilisées. La figure 10.13 illustre l'utilisation du spectre en cours de journée dans un cas standard. Certaines fréquences sont fortement utilisées, comme celles achetées par les opérateurs de télécommunications, qui les utilisent au mieux grâce à d'excellentes techniques de multiplexage, comme le CDMA.

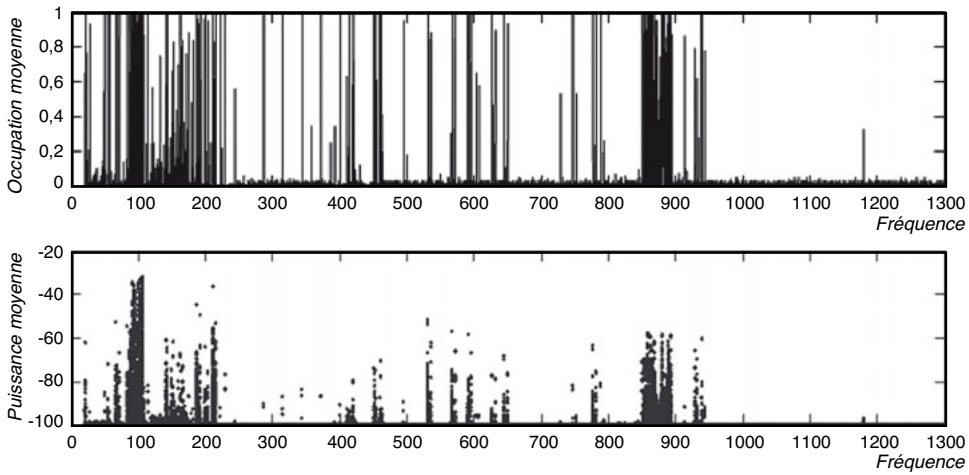


Figure 10.13

Utilisation des fréquences entre 0 et 1,3 GHertz

L'objectif de la radio cognitive est d'utiliser au mieux le spectre de fréquences en transmettant sur les fréquences non utilisées par leur possesseur. La réglementation est en cours de discussion aussi bien à l'intérieur de chaque pays que chez les organismes de normalisation comme l'IEEE (IEEE P1900).

L'idée de base est illustrée à la figure 10.14. Le point d'accès cognitif écoute la porteuse du signal primaire. Dès que celle-ci est libérée, il émet sur cette porteuse. Lorsque le signal primaire revient, le point d'accès cognitif s'arrête de transmettre. Ces techniques sont aujourd'hui au point, et de nombreux essais en ont montré l'efficacité. Il reste des points importants à améliorer, comme la présence de deux points d'accès cognitifs simultanément, qui entrent en compétition pour émettre en premier. Plusieurs propositions de techniques d'accès ont été déposées, mais aucune n'était normalisée au début de 2011.

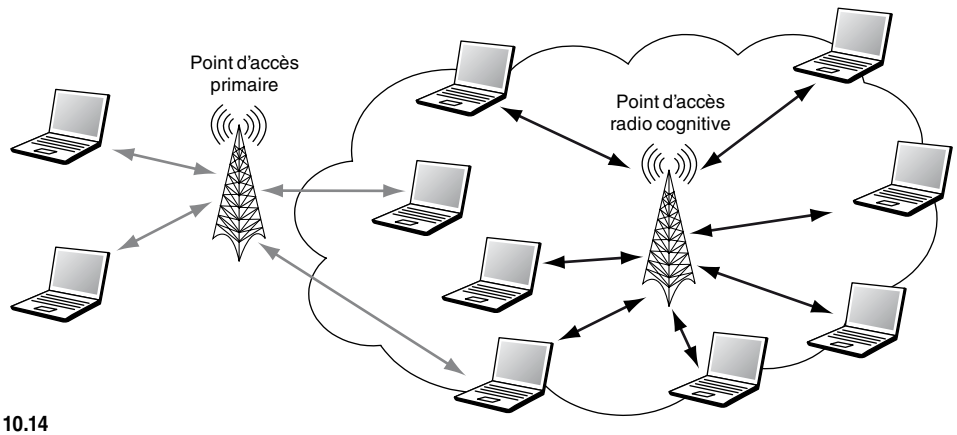


Figure 10.14

Exemple de points d'accès en radio cognitive

D'autres solutions vont permettre d'augmenter fortement les débits, comme les antennes directionnelles, ou *beamforming*. Ces antennes permettent d'émettre simultanément des flots différents dans plusieurs directions spatiales. L'avantage est bien sûr d'augmenter le débit en le multipliant par le nombre de directions. De plus, cette solution permet une bien meilleure réutilisation d'une même fréquence. La réutilisation des fréquences par des antennes directionnelles est illustrée à la figure 10.15.

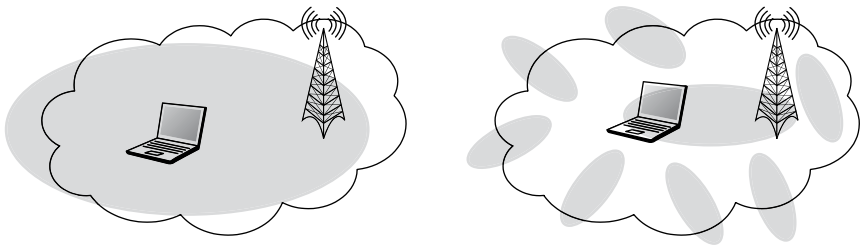


Figure 10.15

Réutilisation des fréquences par des antennes directionnelles

La boucle locale satellite

Trois catégories de systèmes satellitaires ont été définies sous les noms de LEOS, MEOS et GEOS (Low, Medium et Geostationary Earth Orbital Satellite). Les satellites sont situés respectivement à environ 1 000, 13 000 et 36 000 km de la Terre. Les deux premières catégories concernent les satellites défilants, et la dernière les satellites qui semblent fixes par rapport à la Terre.

Les distances à la Terre des différentes catégories de systèmes satellitaires sont illustrées à la figure 10.16. Lorsque les satellites sont défilants, il faut plusieurs satellites les uns derrière les autres pour couvrir un point de la Terre. C'est ce que l'on appelle une constellation.

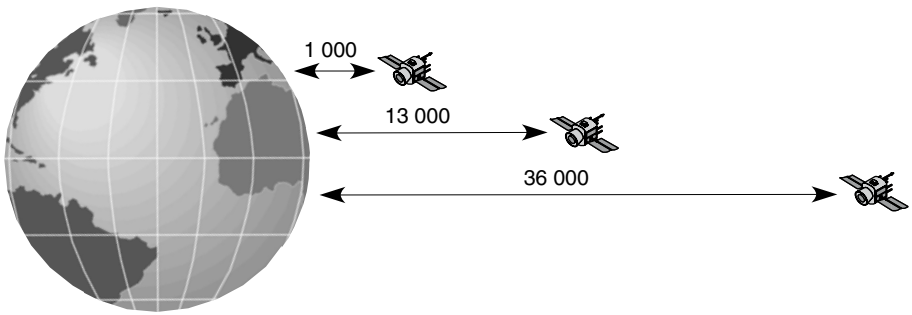


Figure 10.16

Distances à la Terre en kilomètre

La boucle locale satellite concerne l'accès d'un utilisateur, que ce soit une entreprise ou un particulier, au commutateur d'un opérateur employant un réseau terrestre. En d'autres termes, le satellite joue le rôle de boucle locale pour permettre à un utilisateur de se connecter à un opérateur. Cette boucle locale est destinée aux clients isolés ou qui n'ont pas la possibilité d'utiliser une boucle locale terrestre.

Les trois catégories de systèmes satellitaires peuvent jouer le rôle de boucle locale. Les LEOS adressent des terminaux relativement légers, ressemblant à des portables de type GSM, mais avec une antenne un peu plus grande. Les systèmes MEOS demandent des antennes plus importantes, qui peuvent exiger une certaine mobilité sur leur socle. Les systèmes GEOS demandent des antennes fixes très importantes.

La figure 10.17 illustre la taille du spot, c'est-à-dire la zone éclairée par une antenne située sur le satellite, que l'on peut obtenir à partir des différents types de satellites. Plus le satellite est près du sol, plus la taille du spot est petite. L'avantage offert par les satellites basse orbite est la réutilisation des fréquences, qui peut atteindre 4 000 pour une constellation de satellites située à 700 km du sol.

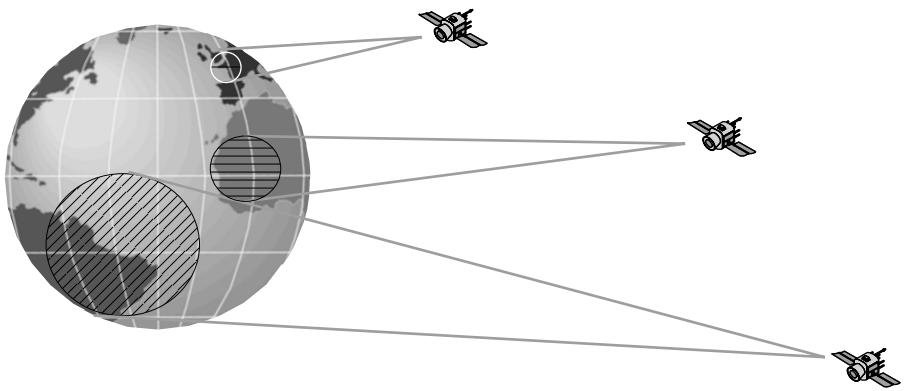


Figure 10.17

Taille des spots des différentes catégories de satellites

Les protocoles de la boucle locale satellite

La boucle locale satellite exige des trames pour permettre aux récepteurs de retrouver les débuts et les fins des paquets transportés. Les paquets, aujourd'hui essentiellement de type IP, sont encapsulés dans des trames, qui peuvent être de type HDLC (*voir l'annexe E*), soit de type ATM, soit encore de type Ethernet. Dans ces deux derniers cas, on parle de réseau satellite ATM ou Ethernet. Un commutateur ATM ou Ethernet peut se trouver dans le satellite.

Une difficulté rencontrée dans les protocoles de niveau trame (couche 2) concerne le nombre de trames qui peuvent être émises sans acquittement. Par exemple, si le protocole HDLC est utilisé, la limite maximale est de 128 trames, ce qui nécessite une longueur de

trame importante pour remplir un canal satellite de forte capacité. Nous verrons que des techniques spécifiques permettent de s'affranchir de cette limite. La solution ATM est encore fortement utilisée, car elle ne comporte pas cette limitation et s'adapte bien aux techniques en slots puisque la trame ATM est de longueur fixe.

Une autre particularité des boucles locales satellite vient du défilement des satellites lors de l'utilisation d'une constellation. Le client doit changer de satellite au fur et à mesure du passage des satellites au-dessus de sa tête. Ce changement s'appelle un handover satellite. Il est également possible que les satellites défilants aient plusieurs antennes et que le terminal de l'utilisateur ait à effectuer un handover intrasatellite.

Ces handovers peuvent être de différents types, appartenant à deux grandes catégories : les soft-handover et les hard-handover. Le soft-handover consiste à se connecter à la fois sur le satellite qui disparaît et sur celui qui apparaît. Le passage se fait alors en douceur. Dans un hard-handover, le passage s'effectue brutalement, la communication devant passer d'un satellite à l'autre sans recouvrement.

Conclusion

Devenue une réalité depuis 2004, la boucle locale radio s'est énormément étendue en quelques années. Les solutions sans fil proviennent des techniques Wi-Fi, WiMAX et WRAN. Les réseaux de mobiles sont devenus très concurrentiels dans ce domaine puisque leurs débits sont désormais comparables à ceux des réseaux sans fil.

La voie hertzienne est clairement une solution pour la boucle locale. Le principal problème qu'elle pose provient de la faible largeur de la bande passante disponible. Pour arriver à trouver des capacités importantes, il faut monter en fréquence et franchir les 20 GHz. Cependant, au-dessus de 20 GHz, la directivité, ajoutée à l'affaiblissement qui survient dès que les conditions ne sont pas parfaites, pose de nouveaux problèmes, à la fois techniques et de coût. De nouvelles solutions sont toutefois en train d'apparaître avec les antennes directives et la radio cognitive. Aussi est-il à peu près certain que la boucle locale sera à l'avenir fortement hertzienne et que les modems fixes ADSL utilisant les lignes téléphoniques seront remplacés par des modems ADSL mobiles.

Le réseau WiMAX était destiné à s'installer sur la boucle locale hertzienne. Malheureusement, pour de nombreuses raisons — opposition des opérateurs de mobiles, équipementiers sans ambition sur cette technologie… —, aucun déploiement n'a été effectué à l'échelle d'un pays. Cette technologie est donc restée marginale (quelques dizaines de milliers de connexions en France). L'IEEE a essayé de pousser une nouvelle génération, appelée WiMAX phase 2, mais ses chances de succès restent faibles du fait de l'arrivée du LTE (Long Term Evolution) et du LTE-Advanced, qui offrent les mêmes propriétés et, surtout, sont soutenus par les grands opérateurs.

La solution WRAN (Wireless Regional Area Network), ou Wi-RAN, devrait apporter une petite révolution en permettant, avec une seule antenne, de connecter des centaines de milliers de clients téléphoniques sur une portée de plusieurs dizaines de kilomètres.

Son déploiement d'une grande simplicité pourrait séduire des opérateurs entrants. La principale difficulté sera de récupérer des fréquences avec une largueur de bande importante et surtout sous les 1 GHz pour atteindre les portées nécessaires au transport de la télévision. Les deux axes privilégiés pour cela sont le dividende numérique et l'utilisation de la radio cognitive.

11

Les réseaux de domicile

Les réseaux de domicile forment une nouvelle catégorie de réseaux encore peu développée. Le domicile est vu par les opérateurs comme une étoile autour de la Home Gateway, qui est la « box » construite autour du modem ADSL. La nouvelle génération de réseaux de domicile devient un petit réseau d'entreprise, avec une centaine de connexions de matériels extrêmement divers provenant de trois mondes distincts : les télécommunications, l'électronique et l'informatique.

Parmi ces équipements, on trouve les téléphones avec et sans fil, offrant des fonctionnalités de vidéophonie, de téléphonie sur IP et de télévision. La haute définition et la parole de meilleure qualité que celle du GSM sont également disponibles.

Les industriels des équipements grand public de la maison proposent des télévisions, des consoles de jeu, des appareils photo et caméras ainsi que des machines à laver, réfrigérateurs, aspirateurs et futurs robots ménagers dotés d'adresses IP.

La difficulté majeure avec ces réseaux est de faire communiquer l'ensemble des équipements entre eux et avec l'extérieur. Nous détaillons dans ce chapitre les couches basses de leur architecture sous-jacente, ainsi que celles permettant à tous les équipements du domicile de s'échanger des informations.

La télésurveillance, les alarmes, les capteurs de présence forment une autre catégorie d'équipements qui doivent pouvoir être ajoutés aux réseaux de domicile pour pouvoir être jointes à distance. S'y ajoutent également les ampoules électriques et plus généralement tout ce qui est connecté au réseau électrique, comme les chaudières et pompes à chaleur.

Le but du réseau de domicile est de connecter tous les équipements du domicile pour leur permettre de communiquer avec l'extérieur et entre eux. Les problèmes à résoudre se divisent en deux grandes catégories : la connexion des équipements entre eux par le biais d'un réseau proposant un protocole acceptable par l'ensemble des machines et la gestion

des applications communes, qui, beaucoup plus qu'une connexion réseau, demandent un interfonctionnement.

Les couches basses de l'architecture

Les couches basses de l'architecture des réseaux de domicile, concernant les éléments physiques, les trames et les paquets, sont fondées essentiellement sur Ethernet, que ce soit sous forme hertzienne, courant porteur ou câblée. Ces trois supports se partagent en fait les connexions des équipements du domicile.

Les courants porteurs en ligne forment une catégorie importante des réseaux de domicile.

Le CPL

L'utilisation des courants porteurs en ligne, ou CPL, dans le domaine du domicile est aujourd'hui une réalité qui ne cesse d'attirer des clients. Les distances sont généralement assez faibles, de l'ordre de quelques mètres entre les différentes prises.

L'objectif est de réaliser sur l'ensemble des câbles électriques d'une même habitation un réseau partagé, de telle sorte qu'un message émis par un client par l'intermédiaire de sa prise électrique puisse être capté par l'ensemble des prises électriques de l'habitation. Le tableau électrique n'offrant qu'une faible protection contre la diffusion vers l'extérieur de l'habitation, il faut sécuriser les communications, comme dans les réseaux hertziens, où l'écoute est simple à réaliser.

Puisque le câble est partagé, une technique d'accès de type MAC est requise. La solution la plus souvent proposée est d'utiliser la norme Ethernet, qui permet le partage d'un câble commun. Cependant, contrairement à l'Ethernet classique, qui utilise la technique CSMA/CD comme méthode de partage, Ethernet sur courant porteur utilise la même technique que Wi-Fi c'est-à-dire le CSMA/CA. Il est en effet difficile avec la composante électrique d'écouter en même temps qu'on émet.

Le comportement de ces réseaux est similaire à celui de Wi-Fi : les performances se dégradent dès qu'une des stations subit un fort taux d'erreur en ligne l'obligeant à réduire sa vitesse d'émission. D'une vitesse brute annoncée de 200 Mbit/s, le standard CPL HomePlug AV peut chuter jusqu'à 0,9 Mbit/s.

Les principaux produits pour l'environnement du domicile proviennent de la technologie HomePlug avec les versions 1.0 turbo, Turbo et AV (Audio Video). Ces versions ont des débits bruts annoncés de 14, 80 et 200 Mbit/s. Comme nous l'avons indiqué, ces débits sont très fluctuants en fonction de l'environnement et peuvent chuter fortement, jusqu'à 1 Mbit/s.

La normalisation en cours s'effectue dans le groupe IEEE P1901 et prend pour base le HomePlug AV.

Dans le domicile, il est possible de mettre en place une passerelle entre le réseau CPL et les autres réseaux Ethernet. La difficulté principale de cette interconnexion réside dans

l'adéquation des classes de priorités entre les différents réseaux, qui ne sont pas toujours exactement positionnées de la même façon.

La sécurité de l'information qui transite sur ce réseau constitue également un problème. Le courant faible peut traverser le compteur électrique, même en présence de filtres spécialisés. Il faut donc chiffrer l'information avec une clé, par exemple la clé NEK (Network Encryption Key) de HomePlug, et implémenter cette clé sur l'ensemble des équipements au moyen d'un logiciel de configuration spécifique. Des équipements de type routeur, passerelle, gestion des NAT sont également indispensables. Ils sont très similaires à ceux des réseaux Wi-Fi.

Caractéristiques

La technologie CPL consiste à émettre des signaux sur le support physique qui transporte l'électricité. De nombreuses implémentations ont été effectuées depuis les années 1950, comme le relevé de compteur à distance et les applications de domotique à bas débit. Les communications CPL à haut débit sont beaucoup plus récentes.

Deux catégories de réseaux CPL doivent être distinguées : le CPL pour réaliser une communication sur la boucle locale et permettre à un utilisateur d'accéder à Internet à haut débit, d'une part, et la transmission de données sur un réseau électrique privé correspondant à un domicile, une entreprise ou au cabinet d'une profession libérale, d'autre part. La première catégorie n'a eu que peu de succès jusqu'à présent pour les hauts débits, compte tenu de la difficulté de traverser un ensemble d'équipements électriques ou de les contourner. Dans ce chapitre, nous ne nous intéressons qu'au CPL dans l'environnement privé.

Dans cet environnement, le câble électrique correspond à un support à accès multiple et en diffusion, c'est-à-dire qu'un émetteur connecté au câble voit son signal diffusé sur l'ensemble du câble. Le signal est en grande partie arrêté par le compteur électrique et le disjoncteur, mais pas suffisamment pour qu'il ne puisse être écouté chez les voisins. Des mesures de sécurité doivent donc être prises. Le câble électrique se comporte comme un réseau Ethernet, et plus précisément comme un réseau Wi-Fi. On retrouve donc exactement les caractéristiques d'un réseau Wi-Fi, avec sa technique d'accès et les difficultés d'y apporter de la qualité de service, une forte sécurité et des performances.

La technique d'accès CSMA/CA est en tout point identique à celle de Wi-Fi. La qualité de service est apportée par un ensemble de quatre classes de clients qui permettent, comme dans IEEE 802.11e, de privilégier certains flots par rapport à d'autres. La priorité s'exerce par le biais de temporisateurs de reprise plus ou moins longs en fonction de la classe de priorité. Cette solution n'est pas complètement efficace lorsque le réseau est saturé puisque les temporisateurs de reprise sont nombreux.

En fonction des interférences électriques, le débit brut peut décroître sans que l'utilisateur puisse le savoir, si ce n'est par le temps plus long nécessaire à la récupération d'un fichier. Le débit brut moyen est très difficile à estimer puisqu'il dépend du bipoint en communication. À chaque trame émise correspond une vitesse brute, de telle sorte qu'il faut faire une moyenne des débits bruts en tenant compte du temps de transmission de

chaque trame. Pour un réseau qui posséderait deux bipoints, c'est-à-dire quatre stations communiquant deux à deux, l'une à 100 Mbit/s et l'autre à 1 Mbit/s, il faut cent fois plus de temps pour émettre une trame entre le bipoint lent par rapport au bipoint rapide. En moyenne, le débit n'est donc que très légèrement supérieur à 1 Mbit/s. On peut estimer qu'un réseau CPL a un débit brut moyen à peu près égal à celui du bipoint le plus lent.

Pour éviter cet effondrement des performances, les dernières normalisations intègrent des technologies de partage, comme le TDMA, qui limitent fortement la chute de débit engendrée par les bipoints de mauvaise qualité.

Comme dans les réseaux Wi-Fi, le débit réel est très inférieur au débit brut. On peut estimer de façon très simplifiée que le débit réel est le tiers du débit brut. Si l'on prend l'exemple de la technologie HomePlug, qui possède trois générations, HP 1.0, HP Turbo et HP AV (Audio Vidéo), les débits bruts maximaux et les débits réels sont récapitulés au tableau 11.1.

Standard	Débit brut	Débit réel
HomePlug 1.0	14 Mbit/s	4,5 Mbit/s
HomePlug Turbo	85 Mbit/s	12 Mbit/s
HomePlug AV	180 Mbit/s	55 Mbit/s

TABLEAU 11.1 • Débits réels et bruts des réseaux HomePlug

Comme nous l'avons souligné, il faut ajouter une dégradation de la vitesse brute dès que le taux d'erreur sur les communications augmente. Dans le cas de HP 1.0, les vitesses brutes se dégradent de 14 à 12,83 Mbit/s, 10,16 Mbit/s, 8,36 Mbit/s, 6,35 Mbit/s, 4,04 Mbit/s, 2,67 Mbit/s, 0,9 Mbit/s. Comme le débit réel est très inférieur au débit brut, on s'aperçoit qu'il est possible d'avoir un réseau CPL débitant moins de 500 Kbit/s si l'une des stations travaille à la vitesse dégradée de 0,9 Mbit/s.

Le CPL met en œuvre une méthode très similaire à celle de Wi-Fi pour la transmission de données dans le domaine privé. Les contrôleurs Wi-Fi se positionnent pour prendre en charge les réseaux CPL. Lorsqu'une des deux solutions baisse en régime, l'autre prend le relais.

L'inconvénient principal des réseaux CPL provient d'une normalisation jusqu'à présent lente à s'établir, même si les choses semblent s'accélérer. Plusieurs groupes développent des spécifications distinctes. Les principaux de ces groupes sont les suivants :

- IEEE P1901
- Consortium HomePlug
- PLC Forum

La sécurité est une fonctionnalité essentielle pour mettre en œuvre un réseau CPL. Comme indiqué précédemment, les signaux peuvent traverser le compteur électrique, même en présence de filtres spécifiques. Pour éviter cet inconvénient, il suffit de chiffrer l'information de la même manière que dans Wi-Fi. De plus, le contrôleur peut contenir un serveur RADIUS pour identifier les demandes de connexion.

Fonctionnement

Dans le domicile, le signal numérique est émis vers les équipements d'extrémité entre 3 et 148 kHz pour les réseaux bas débit et entre 1 et 30 MHz pour les réseaux haut débit. Chaque équipement dispose de sa propre adresse et peut-être commandé par l'élément émetteur.

Du fait de son rayonnement électromagnétique, le câblage électrique fonctionne comme une antenne, de telle sorte que les interférences avec les ondes radio externes peuvent devenir importantes. Dans la zone des 1 à 30 MHz, qui nous intéresse ici, les interférences avec les radioamateurs et les DRM peuvent poser problème.

Les modems CPL utilisant l'OFDM permettent de gérer approximativement les interférences en n'utilisant pas les sous-bandes correspondant à des fréquences déjà utilisées par d'autres équipements. Une technique de *notching* a été mise au point pour éteindre et allumer les sous-bandes qui interfèrent avec d'autres émissions. En temps réel, un mécanisme d'analyse du niveau du rapport signal sur bruit permet de réaliser cet algorithme d'ajout et de retrait de certaines sous-bandes de l'OFDM.

Les bandes utilisées par les principaux produits sont indiquées au tableau 11.2.

Réseaux CPL	Bande de fréquences	Nbre de porteuses OFDM
HomePlug 1.0	4,49-20,7 MHz	76
HomePlug AV	2-28 MHz	917
DS2 45 Mbit/s	1,6-30 MHz	100
DS2 200 Mbit/s	2,46-11,725 et 13,8-22,8 MHz	2560
Spidcom	2-30 MHz	900

TABLEAU 11.2 • Bandes de fréquences et porteuses des réseaux CPL

Des expériences à des fréquences beaucoup plus élevées que 30 MHz, dans les bandes Wi-Fi à 2,4 et 5,15 GHz ont permis d'obtenir des débits de l'ordre du gigabit par seconde.

Plusieurs modes d'utilisation des réseaux CPL peuvent être envisagées : maître-esclave, pair-à-pair et centralisé. Le mode maître-esclave permet à un système central, situé sur le compteur électrique, de jouer le rôle de maître par rapport aux différentes branches de l'arbre composé des câbles électriques partant de ce centre. Le système central joue le rôle de pont entre les différents brins électriques. Le mode pair-à-pair correspond à une technologie Ethernet classique dans laquelle chaque émetteur peut aller directement à chaque récepteur. Le mode centralisé est une combinaison des deux précédents, dans lequel une station maître s'occupe de la gestion et du contrôle et met en place des communications dans le mode pair-à-pair.

La version AV de HomePlug utilise la solution centralisée. La station centralisée décide des tranches de temps accordées aux différentes stations communicant en pair-à-pair. Cette solution permet d'affecter les vitesses de communication pour chaque couple d'émetteur-récepteur.

Comme indiqué précédemment, la technique d'accès CSMA/CA est la même que dans Wi-Fi (*voir le chapitre 22*).

Une autre propriété importante des technologies CPL concerne l'adaptation des vitesses de transmission pour chaque station. Comme la vitesse de transmission entre un émetteur et un récepteur dépend de la qualité du support et de l'affaiblissement du signal, cette vitesse est tributaire de l'emplacement des deux stations en train de communiquer : si elles sont très éloignées et si du bruit électromagnétique perturbe le support, le débit peut être très bas.

Chaque couple de stations transmet à sa propre vitesse, comme une station Wi-Fi et son point d'accès. Pour déterminer la vitesse de transmission, chaque station possède une table « Tone Map » qui indique la meilleure vitesse de transmission par rapport aux autres stations du réseau. Cette table est mise à jour en un temps variant généralement de 10 ms à 1 s.

La figure 11.1 illustre, pour HomePlug 1.0, ce champ Tone Map, qui est transmis dans les en-têtes des trames de telle sorte que chaque station qui écoute le support puisse déterminer sa vitesse de transmission.

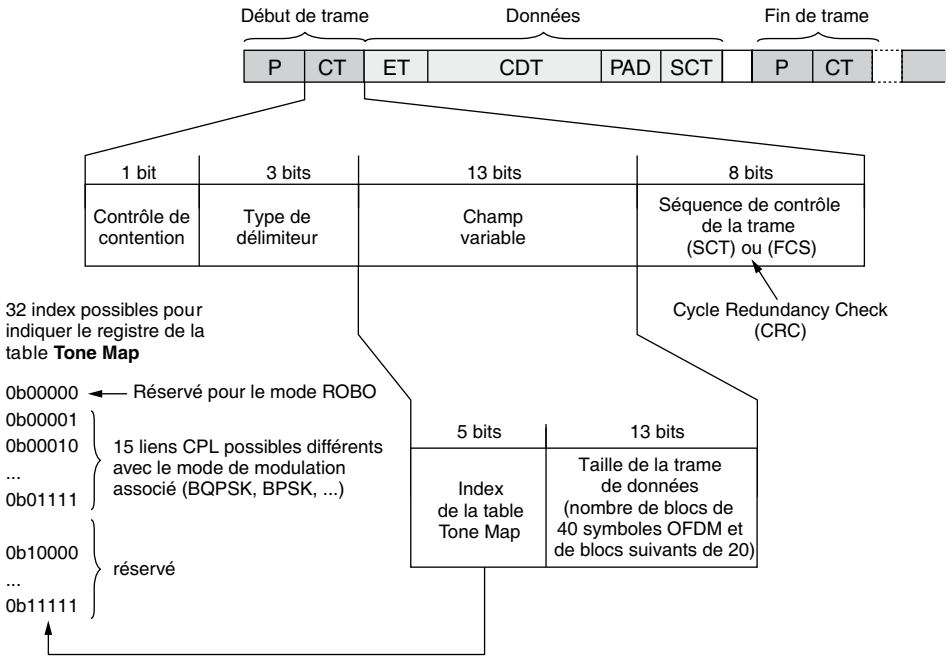


Figure 11.1

Le champ Tone Map dans HomePlug 1.0

Le champ d'indication de la vitesse sur 13 bits indique les 15 liaisons possibles ainsi que la modulation associée (DQPSK, DBPSK, etc.). Pour HomePlug AV, le nombre de liaisons est de 255 stations, et le champ tient sur 16 bits.

Le tableau 11.3 indique les différents débits de HomePlug 1.0 en fonction de la technique de modulation utilisée.

Technique de modulation	Paramètre de l'encodeur	FEC (taux de codage du code convolutionel)	Débit PHY (Mbit/s)
DQPSK	23/39 à 238/254	3/4	14,1
DQPSK	23/39 à 238/254	1/2	9,1
DQPSK	23/39 à 238/254	3/4	4,5
ROBO (DBPSK)	31/39 à 43/51	1/2	0,9

TABLEAU 11.3 • Débits du réseau HomePlug 1.0

L'inconvénient de cette solution est qu'elle ne permet pas de déterminer avec précision la capacité du réseau CPL. On peut estimer que le débit moyen du réseau est un peu supérieur au débit de la liaison la plus lente si les débits de chaque liaison sont à peu près équivalents.

Les versions à très haut débit, comme HomePlug AV, proposent des variantes du CSMA/CA permettant d'optimiser les débits. Les affectations du support se font en TDMA pour permettre en particulier le passage d'applications de streaming et des applications temps réel comme la parole téléphonique. Certains slots TDMA sont affectés à ces applications prioritaires et d'autres sont utilisés en CSMA/CA.

Les réseaux CPL introduisent des améliorations de la qualité de service par un système identique à celui d'IEEE 802.11e consistant à déterminer la taille de la fenêtre de contention. Plus la fenêtre est petite, plus la priorité est forte. Le choix de cette fenêtre est effectué au moment de l'exécution de l'algorithme de back-off, c'est-à-dire du tirage du temporisateur de reprise.

Comme le support physique n'est pas de bonne qualité, de nombreuses erreurs se produisent. Une reprise sur erreur étant nécessaire, les acquittements sont envoyés dès la réception d'un paquet. Les protocoles ARQ (Automatic Repeat reQuest) permettent d'effectuer la retransmission. Ils emploient pour cela des paquets d'acquittement positif et négatif ainsi que des paquets « fail », qui indiquent la non-réception du paquet pour cause de mémoire saturée ou de très mauvaise qualité du signal.

Globalement, les performances des réseaux CPL sont extrêmement variables. Malgré l'augmentation des débits bruts, le passage d'un canal de télévision haute définition n'est pas garanti sur la durée. C'est la raison pour laquelle dans le réseau de domicile on utilise un réseau maillé contenant à la fois le CPL et le Wi-Fi.

Sécurité

Comme indiqué précédemment, on retrouve en matière de sécurité les mêmes problématiques que celles rencontrées dans le monde Wi-Fi, atténuées toutefois par le fait qu'il faut pouvoir se connecter physiquement sur le médium électrique pour l'écouter, ce qui est beaucoup plus complexe à réaliser que l'écoute d'un signal radio. Cependant, les signaux véhiculés sur le câble peuvent traverser le compteur électrique et être captés par les voisins. Il faut donc se protéger des écoutes potentielles et des stations pirates à l'intérieur comme à l'extérieur du réseau.

Les attaques peuvent être du même genre que dans Wi-Fi : écoute, modification de l'information, utilisation non autorisée du support, etc.

Le chiffrement est une solution pour contrer les écoutes. Pour cela, il suffit que chaque station chiffre les trames émises avec une clé commune à l'ensemble des utilisateurs du réseau. Le réseau possède une clé de chiffrement, appelée NEK (Network Encryption Key), qui est transmise à l'ensemble des stations pour le chiffrement et le déchiffrement. Elle peut être transportée par deux moyens : une interface de configuration qui introduit la clé dans chaque station ou l'interface électrique, chaque équipement possédant une clé DEK (Default Encryption Key).

L'authentification des équipements entre eux s'effectue à l'aide de la clé NEK. En l'absence de cette clé, la communication n'est pas possible entre équipements non identifiés. Certains réseaux CPL peuvent avoir des fonctions plus évoluées en utilisant également l'adresse MAC pour l'authentification.

L'intégrité des échanges peut être assurée par une signature électronique, qui empêche un attaquant de modifier les informations transportées.

D'autres solutions, comme les contrôleurs ou l'utilisation de cartes à puce et de VPN, peuvent s'ajouter aux fonctions de sécurité proposées par les équipementiers.

Un contrôleur est un équipement par lequel transitent toutes les communications et qui contient un serveur d'authentification ainsi que des fonctions de sécurisation des communications. Un filtre applicatif peut contrôler les applications échangées et détruire certaines trames non reconnues. Le contrôleur peut accélérer certains flots et en ralentir d'autres, jusqu'à éliminer les trames non désirées. Le filtre applicatif peut également jouer un rôle pour la qualité de service en ralentissant les communications entre certains bipoints relativement lents.

L'inconvénient de ce système est qu'il implique une double transmission entre un point et un autre point, de l'émetteur vers le contrôleur et du contrôleur vers le destinataire. Cet intermédiaire peut ralentir le débit, mais il peut également, de façon assez inattendue, l'accélérer. En effet, si le bipoint émetteur-récepteur est éloigné, la vitesse peut être très faible du fait d'un fort affaiblissement. Si un contrôleur intermédiaire permet de retransmettre à une vitesse beaucoup plus grande, il y a un gain évident.

Les cartes à puce peuvent intégrer les mots de passe et les certificats nécessaires pour une authentification de plus haut niveau. Enfin, l'utilisation de VPN (Virtual Private Network) est recommandée lorsque la communication sort du réseau pour aller vers un site distant.

Les VLAN (Virtual LAN) permettent de définir des réseaux locaux virtuels et donc de séparer les trafics. En règle générale, cette séparation est réalisée par l'utilisation de plusieurs clés NEK. Les sous-réseaux virtuels peuvent être interconnectés entre eux par un pare-feu ou un contrôleur. Cette fonctionnalité permet, par exemple, d'intégrer un réseau CPL dans un réseau d'entreprise.

La normalisation

La normalisation des réseaux CPL est menée aujourd'hui principalement par l'IEEE. Plusieurs groupes ont été formés, dont le plus important est P1901.

L'IEEE a créé des groupes de travail pour normaliser les réseaux courant faible sur courant fort. Ces groupes sont les suivants :

- IEEE P1575 (Standard for Broadband over Power Line Hardware), qui s'occupe de la normalisation des installations et de la sécurité du réseau.
- IEEE P1775 (Powerline Communication Equipment-Electromagnetic Compatibility Requirements-Testing and Measurement Methods), qui s'est focalisé sur les rayonnements électromagnétiques et la compatibilité avec les autres équipements radio. Ce groupe a également édicté les mécanismes à utiliser pour effectuer des mesures et des tests sur ces réseaux électriques.
- IEEE P1901 (Draft Standard for Broadband over Power Line Networks Medium Access Control and Physical Layer Specifications), qui a pour objectif de réaliser une normalisation effective d'un réseau CPL. La tâche est difficile puisqu'il s'agit d'unifier l'ensemble des propositions actuelles vers une norme unique. Tous les principaux groupes qui ont travaillé dans le domaine sont présents, comme l'Alliance HomePlug, OPERA, UPA et CEPCA. Ce standard s'intéresse uniquement aux hauts débits, de l'ordre de 200 Mbit/s.

Un standard préliminaire a été approuvé à la fin de 2009 et publié au début de 2010. L'acceptation finale date de fin 2010. Deux niveaux physiques ont été définis, un utilisant une modulation OFDM, provenant de la technique HomePlug, et un second utilisant une modulation fondée sur les wavelets. Ces supports physiques sont optionnels. L'implémentation d'un seul support est acceptable, mais comme les deux solutions sont incompatibles, les utilisateurs doivent faire un choix.

Les principaux produits CPL

Les débits des principaux produits sont illustrés à la figure 11.2.

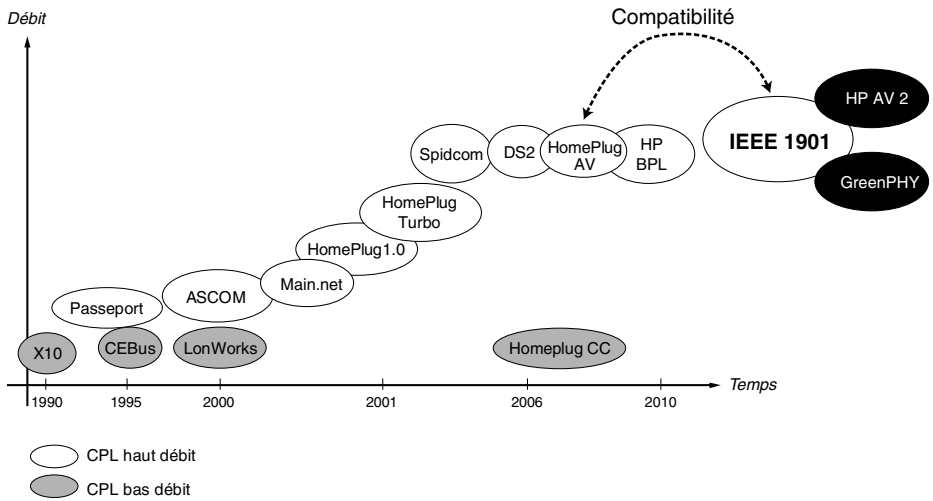


Figure 11.2

Débits des principaux produits CPL

HomePlug

Un réseau HomePlug est constitué de cartes coupleurs reliées aux prises de courant électrique. Une trame de type Ethernet est utilisée, mais avec plusieurs modifications afin de tenir compte des contraintes des réseaux électriques.

Nous retrouvons dans ce réseau des caractéristiques similaires à celles des réseaux hertziens, en particulier IEEE 802.11. Les cartes coupleurs s'adaptent à l'environnement électrique en adoptant quatre vitesses différentes. Si le bruit électromagnétique est trop important et perturbe la qualité de la communication, le système dégrade sa vitesse pour continuer à transmettre avec un taux d'erreur acceptable par l'utilisateur. La vitesse de base du réseau, de 14 Mbit/s, se dégrade par palier jusqu'à moins de 1 Mbit/s. Les cartes coupleurs se calent sur la vitesse correspondant au bipoint.

La structure de la trame HomePlug est illustrée à la figure 11.3. Des classes de clients travaillent suivant une priorité indiquée dans l'en-tête de la trame.

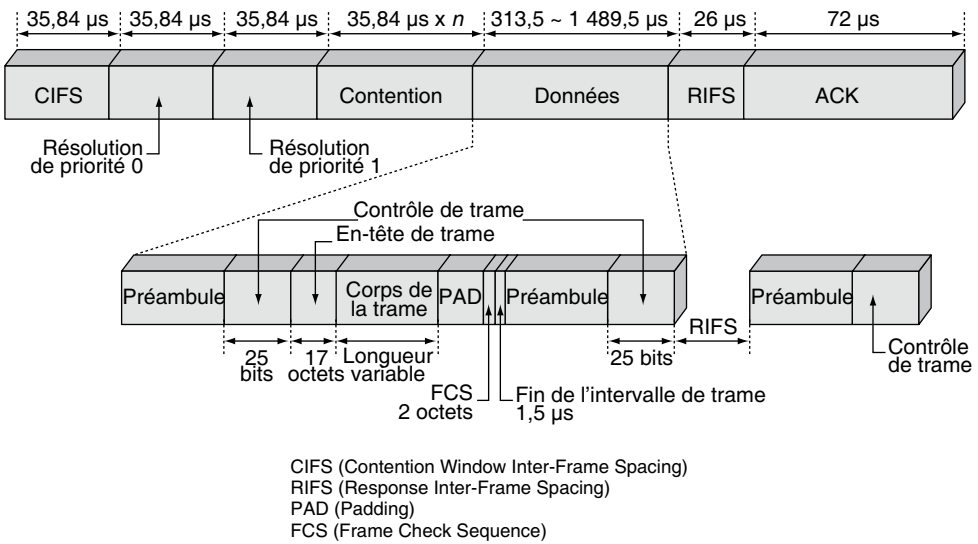


Figure 11.3

Structure de la trame HomePlug

Cette structure de trame est suffisamment complexe pour prendre en charge toutes les caractéristiques de ce réseau.

HomePlug AV est la dernière génération de la série et intègre de nouvelles améliorations sur le contrôle et la technique d'accès. En particulier, ce standard intègre un gestionnaire de connexion (Connection Manager) et un coordinateur central, qui rendent la gestion maître-esclave compatible avec les versions HomePlug précédentes. Ils optimisent en outre l'utilisation des bipoints ainsi que les tranches de temps provenant du TDMA introduites dans cette version.

La technologie physique est l'OFDM (Orthogonal Frequency Division Multiplexing), comme dans de nombreux réseaux hertziens, notamment IEEE 802.11a et g. La fréquence utilisée va de 1 à 30 MHz, avec 917 sous-bandes de fréquences. Suivant la qualité de la transmission sur une sous-bande particulière, la modulation varie pour aller d'une BPSK transportant un bit par sous-fréquence jusqu'à une 1024-QAM transportant 10 bits simultanément.

Les réseaux hertziens

L'utilisation des méthodes hertziennes s'est propagée avec Wi-Fi, mais de nombreux autres réseaux hertziens ont vu le jour, notamment UWB (Ultra Wide Band) et WiGig, le Wi-Fi personnel.

Ces réseaux étant présentés en détail aux chapitres 21 et 22, nous ne donnerons ici que des informations complémentaires utiles aux réseaux de domicile.

Wi-Fi

Wi-Fi est une excellente solution dans le domicile, mais il ne va pas sans un certain nombre de défauts, notamment en raison de son succès.

Dans une grande ville d'un pays développé, il est classique de détecter, en un point donné, une dizaine de réseaux Wi-Fi, voire beaucoup plus. Comme indiqué au chapitre 22, il n'est possible de choisir que trois fréquences réellement utilisables simultanément. Il existe donc de fortes interférences entre les réseaux Wi-Fi. De ce fait, il n'est pas rare, même avec un débit brut de 54 Mbit/s, qu'un utilisateur ne dispose que d'un débit très bas, en dessous de 1 Mbit/s, du fait d'interférences électromagnétiques.

De plus, certains utilisateurs sont équipés de plusieurs points d'accès, ce qui complique encore l'ingénierie à mettre en œuvre. Il faut dans ce cas modifier non seulement le plan de fréquences, mais la puissance d'émission, comme cela se fait dans les entreprises.

Une solution, qui pourrait devenir un standard dans les réseaux de domicile consiste à implanter Wi-Fi dans chaque prise de courant électrique ou au moins dans une prise de courant de chaque pièce. Cela permet de réduire la taille des cellules et de limiter leur puissance, mais ce n'est pas toujours possible avec les points d'accès bon marché.

Une autre solution pour obtenir un débit et une couverture convenables consiste à adopter l'IEEE 802.11n, qui offre un débit raisonnable, même en cas de forte demande, ou les réseaux mesh et les extensions des réseaux ad-hoc.

Du fait des interférences, il faut que les utilisateurs abaissent la puissance d'émission de leur point d'accès, ce qui présente l'inconvénient de réduire la portée. La solution à ce problème consiste à placer des bornes relais (ou bridges), qui communiquent entre elles en Wi-Fi ou par le biais du réseau électrique ou d'un réseau Ethernet spécifique. Les bornes relais servent à la fois de point d'accès et de relais, permettant aux clients de se connecter et de jouer le rôle d'un réseau mesh (*voir le chapitre 23*). En d'autres termes, dans le futur, les domiciles seront couverts par un ensemble de points d'accès reliés entre eux par des liaisons radio.

Le mode ad-hoc peut être adopté afin d'étendre le réseau de domicile en permettant à un équipement se trouvant hors de portée du point d'accès de se connecter en transitant par une ou deux machines intermédiaires.

UWB

L'Ultra Wide Band provient du groupe de travail IEEE 802.15.3. Cette solution offre un très haut débit, mais sur une courte distance : 480 Mbit/s de débit brut sur 3 mètres. En s'éloignant, le débit diminue pour passer à 120 Mbit/s sur 10 mètres en vue directe. Dans les faits, le débit est assez nettement inférieur et ne traverse pas les murs. Cette solution n'est donc pas complètement adaptée au domicile, sinon en disposant des répéteurs en grand nombre dans les différentes pièces.

Pour un produit complet, il est nécessaire d'incorporer les développements réalisés par la WiMedia Alliance qui intègrent différentes possibilités des couches hautes, regroupées parfois sous le nom de WiNET. Les couches hautes contiennent un protocole de reconnaissance de service et de mise en relation des machines terminales. La découverte de service est prise en charge par le standard UPnP (Universal Plug and Play), que nous détaillons un peu plus loin dans ce chapitre. La mise en relation des machines terminales est effectuée par un logiciel de négociation de profils entre machines permettant de définir un profil commun pour l'échange de données.

Comme pour les réseaux Wi-Fi, le débit réel d'une connexion UWB est assez difficile à déterminer. Il dépend de nombreux paramètres, tels que la distance entre les équipements qui communiquent, la puissance du signal, mais aussi les perturbations électromagnétiques externes. C'est une solution intéressante mais pas suffisamment universelle pour garantir la qualité de la communication entre deux équipements dans le domicile. En particulier, elle ne traverse pas les murs et demande donc des répéteurs dans toutes les pièces, ainsi qu'un moyen pour passer d'une pièce à l'autre. La principale restriction de cette solution est sa forte consommation électrique, qui dépasse celle de Wi-Fi.

Autres solutions

De nombreuses autres solutions pourraient être adaptées à l'univers de la maison, à commencer par un réseau Ethernet standard avec un câblage spécifique. Cette solution est utilisée par de nombreux particuliers en raison de son efficacité. Les domiciles neufs pourraient disposer directement d'un câblage Ethernet dans les murs, mais c'est rarement le cas.

Le réseau Ethernet peut aussi utiliser le câblage téléphonique du domicile. Cette solution n'est toutefois pas toujours satisfaisante, car ces câbles sont de très mauvaise qualité et sont perturbés par les courants de sonnerie.

Une technique potentiellement intéressante, appelée FSO (Free Space Optics), utilise l'infrarouge et est limitée à une pièce. Le réseau se sert de l'électricité et des ampoules pour la diffusion de l'infrarouge.

Un câblage en fibre optique peut être réalisé dans un domicile en continuité de celui d'un opérateur. Cette solution est examinée avec soin actuellement, mais son coût est

important, et elle demande la mise en place d'étoiles optiques supplémentaires, ce qui pose des problèmes d'atténuation du signal optique.

Plusieurs solutions pour raccorder des capteurs sont également envisagées, comme l'utilisation de ZigBee ou l'une des propositions du groupe 6LowPAN de l'IETF. L'implémentation de nombreux capteurs devrait permettre de suivre les personnes dans la maison afin d'éteindre ou allumer automatiquement les lumières, de déceler des effractions et de gérer des éléments de sécurité (capteur d'incendie) ou de confort (capteur de température).

Dernière solution en date, le WiGig, qui, porté par une alliance de nombreux grand constructeurs, la Gigabit Wireless Alliance, pourrait avoir son mot à dire, surtout par sa compatibilité Wi-Fi et son très haut débit de 6 Gbit/s.

En résumé, on peut voir le réseau de domicile comme un double réseau Wi-Fi- CPL, comme illustré à la figure 11.4. Ce réseau possède des bridges pour passer d'un réseau à l'autre et introduire le maillage. Si l'un des réseaux, ou une partie de réseau, pose problème on utilise l'autre.

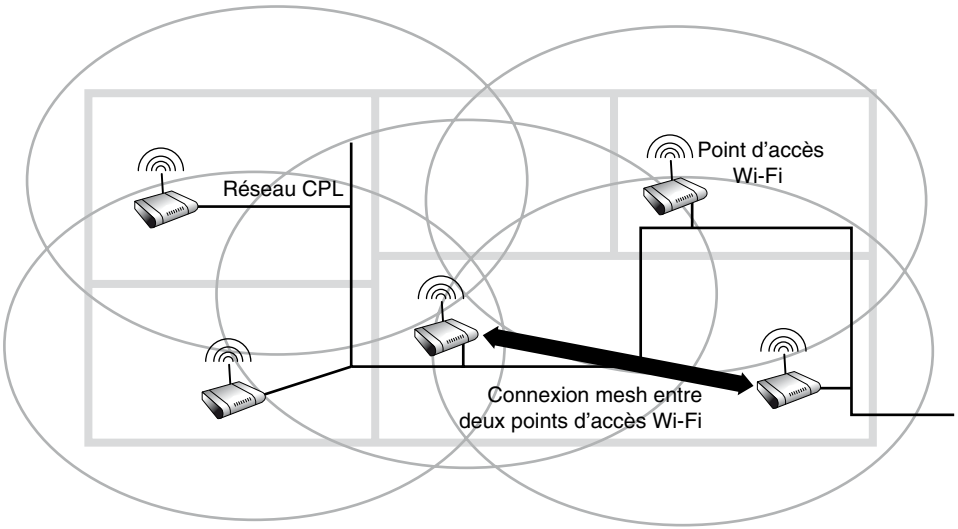


Figure 11.4

Réseau de domicile de nouvelle génération

Les accès

Les débits des accès au domicile ne cessent d'augmenter, depuis les modems ADSL et les InternetBox jusqu'aux accès en fibre optique, de type FTTH (Fiber to the Home). Ces accès utilisent la fibre optique et apportent le gigabit par seconde par utilisateur.

Pour des raisons de coût, l'arrivée de la fibre peut s'arrêter au trottoir avec FTTC (Fiber to the Curb) ou entrer dans le bâtiment avec FTTB (Fiber to the Building). Dans ces deux

derniers cas, la continuité s'effectue par le biais de câbles métalliques jusqu'à la porte de l'utilisateur.

La solution FTTH se développe énormément au niveau mondial. La structure de cette boucle locale est totalement différente de celle de la boucle ADSL sur câble métallique. Le signal est diffusé sur la fibre optique par des étoiles passives, ce qui donne un support physique multiaccès partagé, comme Ethernet. De ce fait, la capacité de la fibre optique est partagée par l'ensemble des utilisateurs. Lorsque des utilisateurs sont absents ou n'utilisent que peu leur accès, tout ce qui n'est pas utilisé est repris par les autres clients. En résumé, si un client se trouve seul à utiliser son accès optique, il dispose de toute la capacité du réseau.

Cette révolution de l'accès donne au réseau de domicile la puissance d'un réseau de très grande entreprise d'il y a cinq ans. Elle devrait permettre l'arrivée de nouveaux services à très haut débit, comme les murs de présence, le téléchargement de vidéos ou la diffusion de plusieurs canaux de télévision haute définition.

Même si la fibre optique n'arrive pas jusqu'au domicile, d'autres solutions, comme l'ADSL ou le VDSL, devraient être largement suffisantes pour irriguer le domicile. Ces technologies offrent des débits de 25 et 50 Mbit/s, largement acceptables pour prendre en charge toutes les applications moyen et haut débit. Les Home Gateways jouent ici un rôle capital. Si elles sont aujourd'hui optimisées pour le Triple ou le Quadruple-Play, elles devraient être dimensionnées pour les applications du domicile dans un avenir proche.

À la question de savoir quel équipement contrôlera le domicile, chacune des grandes catégories d'industriels apporte sa réponse : le monde des télécommunications pousse la Home Gateway, voire un serveur qui pourrait se trouver au niveau du DSLAM, tandis que celui de l'informatique verrait beaucoup mieux l'ordinateur personnel remplir ce rôle. Les enjeux sont très élevés, et des milliards de domiciles sont concernés à plus ou moins long terme.

Les couches supérieures de l'architecture

Les couches supérieures ont pour objectif de réaliser la communication entre les équipements du réseau de domicile entre eux. Les exemples les plus classiques concernent la télévision provenant de la Home Gateway à destination de l'un des écrans de la maison ou bien l'enregistrement d'un programme de télévision vers un DVD pouvant se trouver à l'autre bout du domicile.

Les applications de téléphonie présentent moins de difficulté du fait de leur faible débit. En revanche, elles demandent une gestion particulière de la mobilité en environnement de domicile.

En réalité, c'est la superposition de toutes ces applications, certaines à haut débit et avec des contraintes temps réel, d'autres avec des problèmes de consommation électrique, d'autres encore avec du multipoint et des débits importants, qui rend le réseau de domicile complexe à contrôler.

L'objectif des couches supérieures est de déterminer les profils qui doivent permettre de mettre deux machines en communication, en parlant le même langage et en proposant une qualité de service.

La figure 11.5 illustre certains des objets que l'on peut faire communiquer dans la maison.

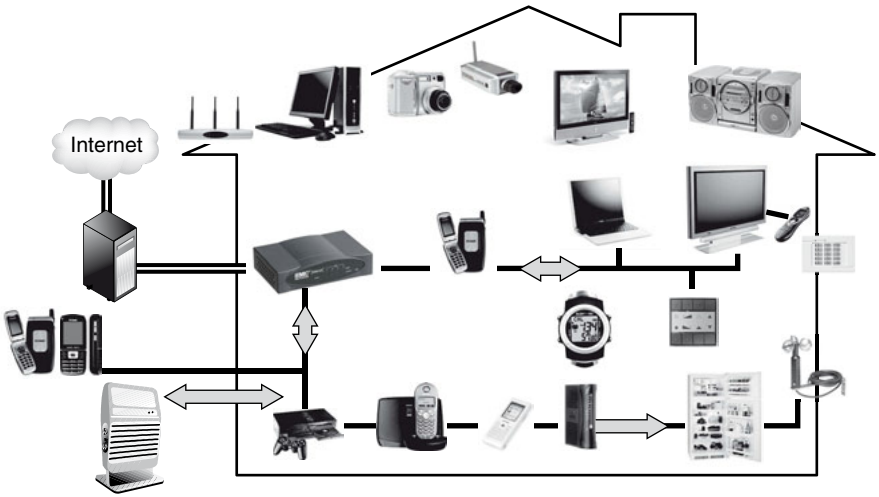


Figure 11.5

L'univers des objets à connecter dans un réseau de domicile

Ces objets à connecter viennent de trois univers différents :

- Télécommunications : équipements téléphoniques et terminaux multimédias mobiles (PDA, les SmartPhones, etc.). Ces objets ont une certaine intelligence, et leur système d'exploitation est capable de supporter des algorithmes de contrôle peu sophistiqués. Leur puissance est très variable, selon l'utilisation autre que téléphonique qui peut être faite de ces terminaux.
- Informatique : ordinateurs portables ou de bureau et plus généralement les équipements qui possèdent un système d'exploitation puissant, de la mémoire et une unité centrale pas trop limitée.
- Électronique grand public : appareils ménagers et électroniques, tels que télévisions, aspirateur, réfrigérateur, etc. Ces équipements disposent d'entrées-sorties analogiques, mais ils sont en train de devenir numériques, permettant leur connexion au réseau de domicile pour y envoyer et en recevoir des paquets IP.

La révolution dans le domaine des réseaux de domicile a pour objectif de faire communiquer toutes ces machines très différentes venant d'horizons distincts. Pour cela, toutes les machines devront devenir IP. Ainsi les télévisions deviennent-elles des ordinateurs et les ordinateurs des télévisions. Cette révolution est en cours, même si elle se fait encore peu sentir du fait principalement des coûts de ces équipements IP.

Les industriels du monde de l'informatique ont essayé de développer une technologie de découverte de service aux fonctionnalités minimales, notamment avec le standard UPnP (Universal Plug & Play). Cependant, la découverte de service, si elle est indispensable, n'est pas suffisante pour réaliser la communication. Il est nécessaire de mettre en place une véritable architecture de communication avec le média à utiliser, prenant en compte la vitesse et la qualité de service. Une telle architecture, dite DLNA (Digital Living Network Alliance), effectue un compromis entre l'ensemble des partenaires. Nous l'examinons en détail un peu plus loin dans ce chapitre.

L'architecture DLNA est cependant incomplète, car elle ne prend pas en compte la partie réseau à l'intérieur du domicile. Elle permet essentiellement de mettre d'accord des équipements en vu de communiquer. Pour gérer la qualité de service, la sécurité, la gestion de la mobilité ainsi que la maintenance du réseau de domicile, il faut aller plus loin sur la partie réseau proprement dite. Plusieurs consortiums se proposent d'aller dans ce sens, mais souvent avec des vues partielles. Citons notamment le DSL Forum et surtout HGI (Home Gateway Initiative), que nous détaillons plus loin.

UPnP

UPnP (Universal Plub & Play) est une technologie qui permet la communication des données entre n'importe quelle machine sous le contrôle d'un équipement du réseau domestique. Des DCP (Device Control Protocol) décrivent des méthodes normalisées pour l'interaction entre machines. Ces protocoles utilisent des techniques standards, comme UDP, TCP, HTTP, SSDP ou SOAP. Les descriptions sont effectuées en XML de façon à être totalement compatibles avec le monde Internet.

L'architecture UPnP spécifie six phases d'interaction, comme illustré à la figure 11.6 :

- L'adressage (Addressing), par laquelle les équipements obtiennent leur adresse IP.
- La découverte (Discovery), par laquelle les points de contrôle découvrent l'existence des équipements.
- La description (Description), par laquelle les points de contrôle apprennent à connaître les équipements et leurs services.

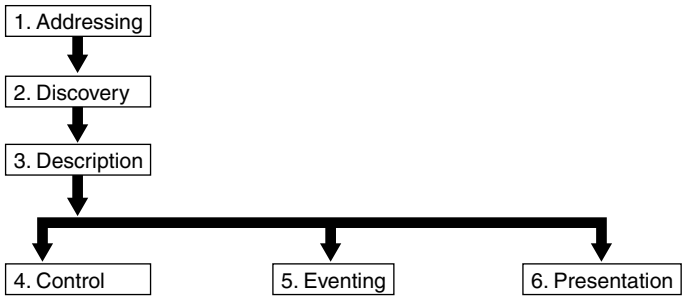


Figure 11.6

Les six phases d'interaction d'UPnP

- Le contrôle (Control), par laquelle les points de contrôle invoquent les actions à réaliser.
- La notification (Eventing), par laquelle les équipements peuvent notifier des contrôles.
- La présentation (Presentation), par laquelle les équipements peuvent présenter des pages Web aux points de contrôle pour obtenir les états et lancer des interactions.

UPnP est un bon début pour l'intercommunication entre des équipements différents, mais il reste insuffisant et peu sécurisé. En particulier, il ne définit pas le média à utiliser pour communiquer, ni le débit, ni la qualité de service nécessaire. C'est la raison de la mise en place de l'initiative DLNA, que nous allons examiner.

DLNA

L'architecture DLNA provient d'un consortium réunissant tous les grands acteurs des télécommunications, de l'électronique grand public et de l'informatique.

Le consortium comprend environ trois cents membres, dont vingt et un promoteurs (*promoter members*). L'objectif de ce consortium est de fournir les formats de base pour fournir l'interopérabilité des médias. Une de leur tâche importante est de développer des liaisons avec l'ensemble des organismes s'occupant de la normalisation des médias pour uniformiser les présentations et aboutir à un environnement commun, mais sans inventer de nouveaux standards.

DLNA doit également se préoccuper des tests de compatibilité entre les différentes piles protocolaires proposées par les industriels.

L'architecture de DLNA comporte six couches, comme l'illustre la figure 11.7.

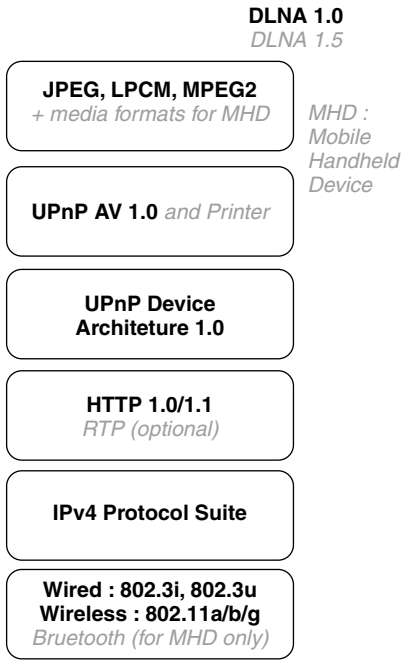


Figure 11.7
Les six couches de l'architecture DLNA

La couche la plus haute détermine les médias qui peuvent être utilisés entre deux équipements. Dans la version DLNA 1.5, les médias acceptables sont JPEG, LPCM et MPEG-2, ainsi que des médias destinés aux équipements d'extrémité mobiles, les MHD (Mobile Handheld Device).

De façon plus précise, les médias et leurs options sont indiqués au tableau 11.4.

Classe	Format de base	Formats optionnels
Image	JPEG	PNG, GIF, TIFF
Audio	LPCM	AAC, AC-3, ATRAC 3plus, MP3, WMA9
AV	MPEG-2	MPEG-1, MPEG-4, AVC, WMV9

TABLEAU 11.4 • Les médias de DLNA

Les couches 5 et 4 reprennent essentiellement UPnP comme technique de découverte des équipements. La couche 3 détermine les protocoles qui peuvent être utilisés entre les équipements d'extrémité. Le principale est HTTP, avec en option RTP.

La couche 2 décrit le protocole de niveau paquet. IPv4 a été choisi comme protocole de base. Le protocole IPv6 pourrait être utilisé en temps voulu.

La couche la plus basse se préoccupe des supports physique et hertzien pour permettre la communication. Les choix tournent autour d'Ethernet avec les Ethernet filaires et la technologie Wi-Fi dans la partie hertzienne. En complément pour les équipements mobiles, la norme Bluetooth a été ajoutée.

L'architecture DLNA est donc beaucoup plus complète que la simple découverte d'équipements. Elle est toutefois encore insuffisante dans les réseaux de domicile pour garantir une communication entre deux équipements avec qualité de service et sécurité.

Le groupe DLNA a fixé, en mars 2006, un certain nombre d'objectifs à atteindre. Ces directives ont pour objectif d'étendre la première génération de DLNA en y ajoutant les équipements d'impression et les mobiles. Les directives précédentes concernaient deux classes d'équipements, appelées DMS (Digital Media Server) et DMP (Digital Media Player). Avec la nouvelle génération, elles concernent douze classes.

Ces nouvelles possibilités sont les suivantes :

- Introduction de la possibilité d'imprimer sur le réseau vers un DMPr (Digital Media Printer), en particulier pour l'impression de photos.
- Possibilité de pousser (push) des images, de la vidéo ou du contenu audio d'un serveur vers un équipement de type Player. DLNA n'offre actuellement que la possibilité de tirer (pull) le média d'un serveur vers le Player. Cette solution permet de télécharger les images d'un appareil photo numérique vers un PC ou une télévision pour les visionner.
- Possibilité de contrôler la transmission vers un équipement mobile. Par exemple, donner la possibilité à un téléphone portable de transférer une chanson vers un équipement stéréo pour la diffuser.

- Prendre en charge la norme de codage AVC (MPEG-4). C'est le média d'interopérabilité par excellence pour la vidéo. Ce standard est effectivement conçu pour le stockage et le transfert optimisé de contenus vidéo.
- Prise en charge de la technologie Bluetooth.
- Prise en charge du protocole RTP, qui permet d'introduire une meilleure qualité de service applicative (*voir le chapitre 17*).
- Introduction de la qualité de service pour améliorer le transport des applications de type streaming.
- Prise en charge des téléchargements entre équipements mobiles et équipements audio/vidéo.

Modèle de compatibilité

Le consortium DLNA a développé un modèle de compatibilité entre équipements DLNA. Ce modèle est illustré à la figure 11.8. Il définit la compatibilité par le biais de tests de conformité et d'interopérabilité. Des outils de test automatiques ont été développés afin de permettre, entre autres, une certification de la partie UPnP.

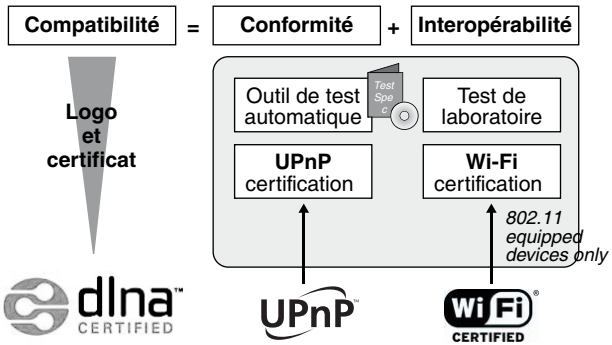


Figure 11.8
Modèle de compatibilité DLNA

Pour pouvoir entrer dans le réseau de domicile facilement, les équipements doivent posséder le sigle DLNA indiqué sur la figure. Malheureusement, les équipements DLNA sont assez nettement plus chers que les autres puisqu'ils incorporent un processeur, de la mémoire, des entrées-sorties, des codeurs, etc.

Comme indiqué précédemment, l'architecture DLNA n'est pas suffisante par elle-même pour garantir la traversée du réseau de domicile. Il faut y ajouter des fonctionnalités internes au réseau de communication lui-même. Les architectures de la section suivante visent à apporter ce complément.

Les autres architectures

Le DSL Forum compte approximativement deux cent cinquante membres, incluant des FAI, des opérateurs, des équipementiers et des industriels du logiciel. Son objectif est de définir une architecture de bout en bout permettant de garantir les communications entre le serveur se trouvant dans un réseau d'opérateur et la machine terminale de l'utilisateur. C'est donc beaucoup plus que le réseau de domicile qui est concerné.

Le DSL Forum se préoccupe en premier lieu de l'architecture et de la gestion des équipements d'extrémité.

L'architecture définie dans le document TR-069 vise l'autoconfiguration, le provisionnement de service dynamique, la gestion du logiciel et du firmware, le contrôle du statut des équipements et des liaisons ainsi que le monitoring de performance, la gestion des logs, le diagnostic, etc.

Pour cela, le Forum a défini un modèle de données commun pour la gestion des équipements et déterminé des modèles d'objets pour des applications comme la VoIP.

Un autre forum très important pour les réseaux de domicile provient du rassemblement d'un certain nombre d'opérateurs de télécommunications au sein du HGI (Home Gateway Initiative), parmi lesquels Orange, BT, DT, Belgacom, Telefonica, Telecom Italia, KPN, TeliaSonera et NTT. Cette initiative essentiellement européenne cherche à définir et normaliser par des spécifications industrielles des passerelles du réseau de domicile.

L'objectif du forum HGI est de spécifier un environnement résidentiel multiservice fondé sur une passerelle située entre l'InternetBox et les équipements résidentiels. La spécification HGI est fondée sur des standards existants. Son objectif est de les compléter afin que la normalisation du réseau de domicile soit complète. En particulier, la spécification est fondée sur les standards du DSL Forum, DLNA, OSGi, DVB, UPnP, ETSI et UMA.

La passerelle HGI devrait ainsi être au cœur du domicile et jouer le rôle de chef d'orchestre de ce réseau.

Conclusion

Le réseau de domicile est devenu un vrai réseau, au même titre que celui d'une petite entreprise d'aujourd'hui. Il faut à la fois gérer le réseau du point de vue des couches basses et des applications afin qu'elles puissent être atteintes de toutes les machines du domicile.

Nous n'avons pas détaillé dans ce chapitre les connexions qui devraient provenir des étiquettes électroniques et des réseaux de capteurs, mais ce sont des extensions qu'il faudra prendre en compte dans un avenir proche. Ces connexions devraient se développer énormément dans le domicile pour introduire de nouveaux paramètres, comme la température extérieure sur la porte de sortie ou la possibilité de retrouver ses livres à l'intérieur de la maison. Dans ce dernier exemple, il suffirait de saisir le nom du livre recherché pour qu'une géolocalisation soit possible au travers d'une étiquette électronique associée et une triangularisation pour obtenir l'emplacement géographique.

D'autres développements sont en cours pour étendre le réseau de domicile. La première extension concerne les « extensions » du domicile, comme la voiture ou la maison de campagne. L'utilisateur doit pouvoir bénéficier dans sa voiture des mêmes services que chez lui. De même, les extensions vers la chambre d'hôtel ou le bureau semblent naturelles. Cependant, ces extensions posent de nouveaux problèmes, surtout si la mobilité est un paramètre supplémentaire à prendre en compte. C'est dans cet objectif que des groupes de travail spécifiques, comme VANET (Vehicular Ad hoc Networks), ont été mis sur pied par l'IETF.

Partie IV

Les architectures réseau

Les architectures de réseaux s'intéressent à la façon dont les messages sont transportés d'une extrémité à l'autre du réseau au travers des différentes couches. L'architecture dépend fortement du niveau auquel il faut remonter dans les nœuds intermédiaires.

Nous allons dans cette partie commencer par les architectures de bas niveau pour aller jusqu'au niveau paquet.

12

Les réseaux optiques

Les réseaux optiques permettent de transporter des signaux sous forme optique et non électrique, à la différence des réseaux classiques. Les avantages de l'optique sont nombreux, notamment parce que les signaux sont mieux préservés, puisqu'ils ne sont pas perturbés par les bruits électromagnétiques, et que les vitesses sont très importantes.

Ce chapitre examine les techniques de transport de signaux sur la fibre optique puis le multiplexage en longueur d'onde, qui permet une augmentation très importante des capacités d'une fibre optique, et enfin les techniques de transport des trames.

La fibre optique

Considérée comme le support permettant les plus hauts débits, la fibre optique est une technologie aujourd'hui complètement maîtrisée. Dans les fils métalliques, on transmet les informations par l'intermédiaire d'un 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 se développe.

Une connexion optique nécessite un émetteur et un récepteur. Différents types de composants sont envisageables. La figure 12.1 illustre la structure d'une liaison par fibre optique. Les informations numériques sont modulées par un émetteur de lumière, qui peut être :

- une diode électroluminescente (DEL) qui ne comporte pas de cavité laser ;
- une diode laser (DL) ;
- un laser modulé.

Le phénomène de dispersion est moins important si l'on utilise un laser, lequel offre une puissance optique supérieure aux DEL mais à un coût plus important. De plus, la durée de vie d'un laser est inférieure à celle d'une diode électroluminescente.

Le faisceau lumineux est véhiculé à l'intérieur d'une fibre optique. Cette dernière est constituée d'un guide cylindrique d'un diamètre compris entre 100 et 300 microns (μm), recouvert d'isolant.

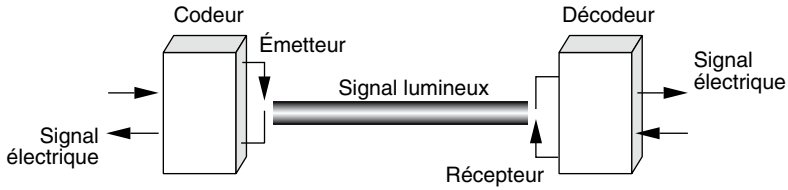


Figure 12.1

Liaison par fibre optique

On distingue deux types de récepteurs :

- les diodes PIN ;
- les diodes à avalanche.

Les composants extrémité, émetteurs et récepteurs, limitent actuellement les vitesses que l'on peut atteindre sur les fibres.

Les principaux avantages apportés par la fibre optique sont les suivants :

- Très large bande passante, de l'ordre de 1 GHz pour 1 km, qui permet le multiplexage sur un même support de très nombreux canaux, comme le téléphone, la télévision, etc.
- Faible encombrement.
- Grande légèreté, le poids d'un câble optique par unité de longueur, de l'ordre de quelques grammes au kilomètre, étant environ neuf fois plus faible que celui d'un câble conventionnel. Le rayon de courbure peut descendre en dessous de 1 cm.
- Très faible atténuation, qui permet d'envisager un espacement important des points de régénération des signaux transmis. Le pas de régénération est supérieur à 10 km, alors que, sur du câble coaxial, il est de l'ordre de 2 à 3 km. Un système en fibre optique débitant plusieurs gigabits par seconde utilisé sur une longueur d'onde de 0,85 μm présente un affaiblissement de 3 dB/km, ce qui donne un pas de régénération de près de 50 km.
- Excellente qualité de la transmission. Une liaison par faisceau lumineux est, par exemple, insensible aux orages, aux étincelles et au bruit électromagnétique. Cette immunité au bruit est un des principaux avantages de la fibre optique, laquelle est particulièrement recommandée dans un mauvais environnement électromagnétique. Le câblage des ateliers et des environnements industriels peut ainsi être effectué en fibre optique.
- Bonne résistance à la chaleur et au froid.
- Matière première bon marché, la silice.
- Absence de rayonnement, ce qui rend son emploi particulièrement intéressant pour les applications militaires. Une tentative d'intrusion sur la fibre optique peut être aisément détectée par l'affaiblissement de l'énergie lumineuse en réception.

La fibre optique présente toutefois quelques difficultés d'emploi, notamment les suivantes :

- Difficultés de raccordement aussi bien entre deux fibres qu'entre une fibre et le module d'émission ou de réception. En laboratoire, on peut réaliser des connexions pour lesquelles les pertes sont inférieures à 0,2 dB. Sur le terrain, il faut faire appel à des connecteurs amovibles, qui demandent un ajustement précis et occasionnent des pertes supérieures à 1 dB. De ce fait, lorsqu'on veut ajouter une connexion à un support en fibre optique, il faut couper la fibre optique et ajouter des connecteurs très délicats à placer. Le passage lumineux électrique (*voir figure 12.2*) que l'on ajoute fait perdre les avantages de faible atténuation et de bonne qualité de la transmission.

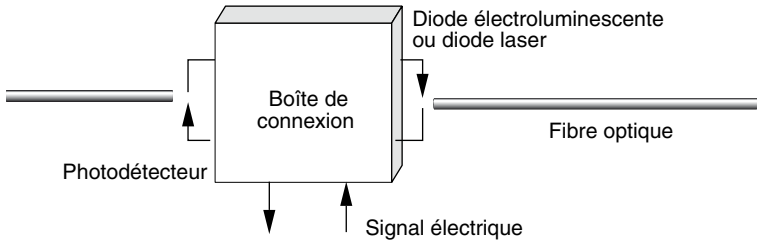


Figure 12.2

Raccordements à une fibre optique

- Dérivations difficiles à réaliser, l'affaiblissement qui en découle dépassant souvent 5 dB. Ces dérivations sont pourtant nécessaires puisque les composants extrémité de l'accès optique sont le plus souvent actifs et engendrent une panne définitive du réseau en cas de défaillance (*voir figure 12.3*).

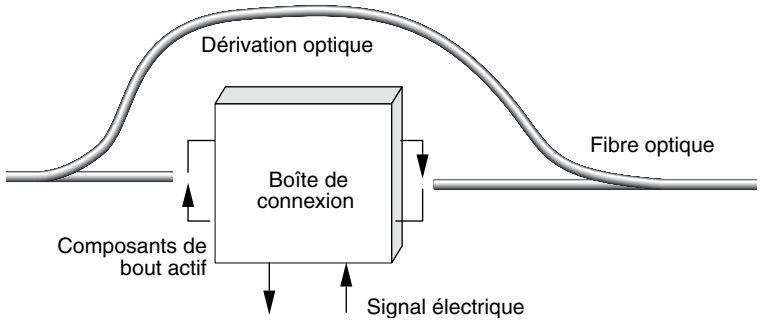


Figure 12.3

Dérivation en fibre optique

- Le multiplexage en longueur d'onde, qui consiste à faire transiter dans une même fibre plusieurs longueurs d'onde en parallèle ou encore ce que l'on peut appeler plusieurs couleurs en même temps. On trouve facilement sur le marché des multiplexages en longueur d'onde jusqu'à une centaine de couleurs. La limite actuelle est de l'ordre de mille

longueurs d'onde sur une même fibre optique. Avec mille longueurs d'onde, la fibre est totalement remplie, et de nouveaux progrès ne pourront être effectués que si une découverte importante est réalisée pour augmenter encore le nombre de longueurs d'onde.

Il existe plusieurs types de fibres :

- les fibres multimodes à saut d'indice ;
- les fibres multimodes à gradient d'indice ;
- les fibres monomodes, au diamètre très petit.

Les fibres multimodes à saut d'indice ont une bande passante allant jusqu'à 100 MHz sur 1 km et celles à gradient d'indice jusqu'à 1 GHz sur 1 km. Les fibres monomodes offrent la plus grande capacité d'information potentielle, de l'ordre de 100 GHz/km, et les meilleurs débits, mais ce sont aussi les plus complexes à réaliser. On utilise généralement des câbles optiques contenant plusieurs fibres. L'isolant entourant les fibres évite les problèmes de diaphonie entre les différentes fibres.

La fibre optique est particulièrement adaptée aux liaisons point-à-point numériques. On peut réaliser des liaisons multipoint en utilisant des coupleurs optiques ou des étoiles optiques.

Le monde de la fibre optique est toujours en pleine évolution. De nombreuses recherches sont en cours, dont certaines ont déjà abouti. On réalise notamment des commutateurs de paquets optiques, dont l'utilisation pourrait se révéler particulièrement intéressante à l'avenir pour augmenter encore la souplesse de commutation dans la fibre optique.

Les coûts du matériel et de l'installation freinent cependant son emploi dans les réseaux d'accès, même si elle est devenue le médium physique le plus répandu dans les cœurs de réseau. Son insensibilité aux perturbations électriques rend son utilisation nécessaire dans certains environnements fortement perturbés ou dans des situations spécifiques, comme le câblage d'une entreprise souhaitant qu'aucun rayonnement ne puisse être détecté à distance à partir des câbles. En effet, il est possible de détecter les signaux dans un câble métallique à l'aide d'équipements *ad hoc*, du fait du rayonnement des ondes électriques qui circulent dans le câble.

Le multiplexage en longueur d'onde

Sur les câbles métalliques, et notamment le câble coaxial, on utilise de plus en plus un multiplexage en fréquence pour faire transiter plusieurs canaux en parallèle sur des fréquences différentes. Si l'on veut reprendre cette idée dans la fibre optique et réaliser le passage de plusieurs signaux lumineux simultanément, il faut faire appel à un multiplexage en longueur d'onde. Aujourd'hui, de nombreux composants extrémité adaptés offrent cette possibilité.

Les débits peuvent atteindre de la sorte 10 Gbit/s sur une seule longueur d'onde, avec une montée en puissance prévue bientôt à 40 Gbit/s, voire 160 Gbit/s. Des vitesses encore plus grandes ont déjà été obtenues en laboratoire. Une fibre à 128 longueurs d'onde d'un débit de 10 Gbit/s offre un débit total de 1,28 Tbit/s. Cela représente approximativement

60 millions de voix téléphoniques transitant en même temps sur le support physique. En d'autres termes, l'ensemble de la population française peut téléphoner à 60 millions de personnes en même temps en n'utilisant qu'une seule fibre optique.

Architecture des réseaux optiques

Les réseaux optiques s'appuient sur le multiplexage en longueur d'onde, qui consiste, comme expliqué à la section précédente, à diviser le spectre optique en plusieurs sous-canaux, chaque sous-canal étant associé à une longueur d'onde. Cette technique est aussi appelée WDM (Wavelength Division Multiplexing), DWDM (Dense WDM), lorsque le nombre de longueurs d'onde dépasse la vingtaine, puis u-DWDM (ultra-Dense WDM) pour plus de 200 longueurs d'onde.

Un cas particulier a été mis au point avec CWDM (Coarse WDM) pour réduire le coût du multiplexage en longueur d'onde en ayant une séparation entre les longueurs d'onde beaucoup plus importante. Cette solution réduit énormément le coût des composants optiques mais diminue également le nombre de longueurs d'onde à moins d'une vingtaine, ce qui est largement suffisant dans les environnements métropolitains.

La figure 12.4 illustre un réseau de communication utilisant le multiplexage en longueur d'onde. Le chemin d'un nœud à un autre peut-être entièrement optique ou passer par des commutateurs optoélectroniques.

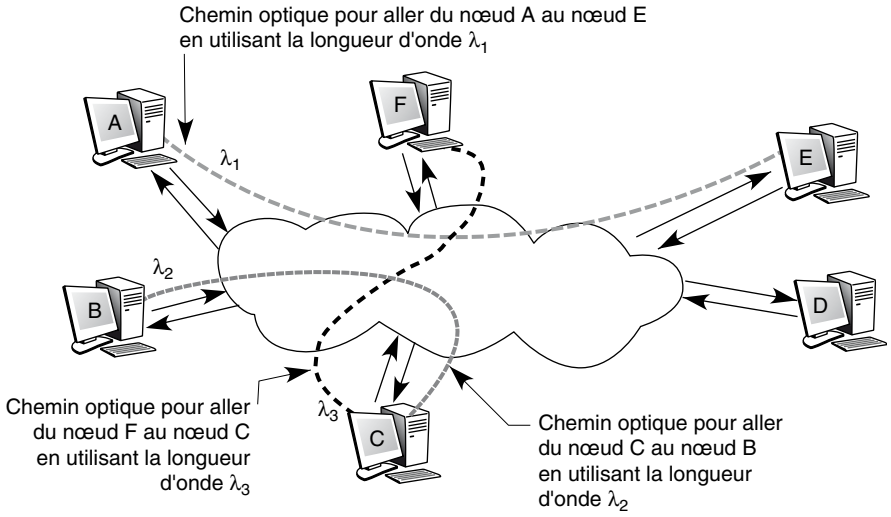


Figure 12.4

Multiplexage en longueur d'onde dans un réseau optique

Sur chaque longueur d'onde, un autre niveau d'optoélectronique peut être utilisé, soit par un multiplexage en fréquence, et dans ce cas la bande passante est de nouveau subdivisée entre plusieurs stations (Subcarrier Multiplexing), soit par un multiplexage temporel, ou TDM (Time Division Multiplexing).

Les réseaux optiques à multiplexage en longueur d'onde peuvent être regroupés en deux sous-catégories :

- les réseaux à diffusion ;
- les réseaux à routage en longueur d'onde.

Chacune de ces sous-catégories peut être à saut unique (single-hop) ou à saut multiple (multi-hop).

Les réseaux à diffusion

Dans les réseaux à diffusion, chaque station de réception reçoit l'ensemble des signaux envoyés par les émetteurs. L'acheminement des signaux s'effectue de façon passive. Chaque station peut émettre sur une longueur d'onde distincte. Le récepteur reçoit le signal désiré en se plaçant sur la bonne longueur d'onde. Les deux topologies les plus classiques sont l'étoile et le bus, comme illustré aux figures 12.5 et 12.6. Dans les deux cas, chaque station émet vers le centre, qui effectue un multiplexage en longueur d'onde de l'ensemble des flots qui lui parvient.

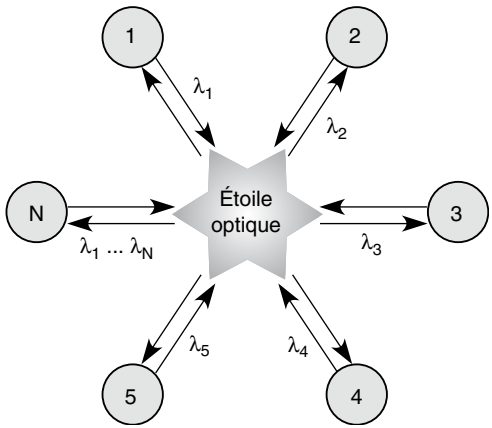


Figure 12.5
Topologie en étoile

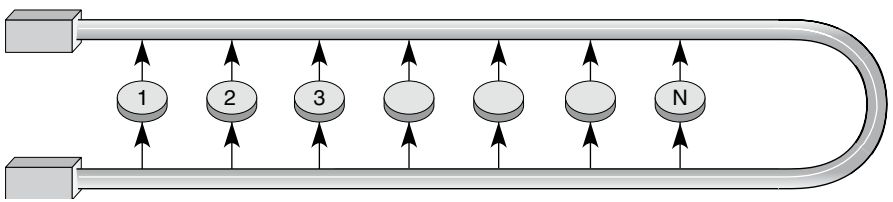


Figure 12.6
Topologie en bus

Lorsque l'ensemble des signaux arrive directement à l'ensemble des stations sans repasser par des formes électriques, le réseau est dit à saut unique (single-hop). C'est le cas des deux structures illustrées aux figures 12.6 et 12.7. S'il faut passer par des étapes intermédiaires pour effectuer un routage, nous avons des réseaux à sauts multiples (multi-hop), comme ceux décrits aux figures 12.8 et 12.9.

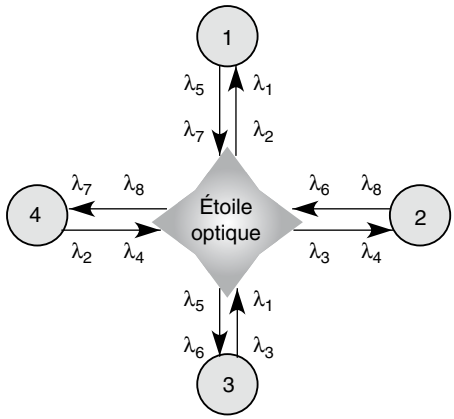


Figure 12.7

Architecture de réseau en étoile à sauts multiples

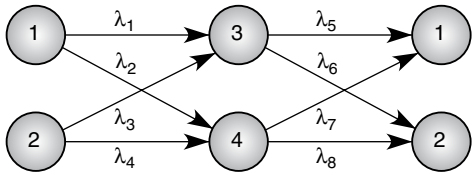


Figure 12.8

Architecture de réseau Shufflenet à sauts multiples

Le Lambdanet de Bellcore est un exemple d'un réseau à diffusion et à saut unique. La difficulté de ce type de réseau est de disposer de longueurs d'onde en nombre suffisant et de récepteurs équipés des composants capables de s'adapter aux variations rapides de longueur d'onde des signaux optiques. Compte tenu de cette difficulté majeure, des réseaux à diffusion et sauts multiples ont été développés par plusieurs sociétés. Dans ces réseaux, l'émetteur et le récepteur ne disposent généralement que de deux longueurs d'onde. Pour aller d'un port d'entrée à un port de sortie, l'information est routée sous la forme d'un paquet de données. Comme la commutation s'effectue dans un nœud intermédiaire, il y a passage par un élément électronique, qui constitue un point fragile à sécuriser.

La figure 12.8 montre que, pour passer du nœud 1 au nœud 2, il faut émettre, par exemple, sur la longueur d'onde 2 vers le nœud 4, qui retransmet sur la longueur d'onde 8 vers le nœud 2, ou émettre sur la longueur d'onde 1 vers le nœud 3, qui retransmet vers la

station 2 sur la longueur d'onde 6. On voit que deux chemins sont possibles, ce qui sécurise le processus de communication.

Les réseaux à routage en longueur d'onde

L'idée à la base des réseaux à routage en longueur d'onde consiste à réutiliser au maximum les mêmes longueurs d'onde. La figure 12.9 illustre un nœud d'un réseau à routage en longueur d'onde dans lequel de mêmes longueurs d'onde sont utilisées à plusieurs reprises.

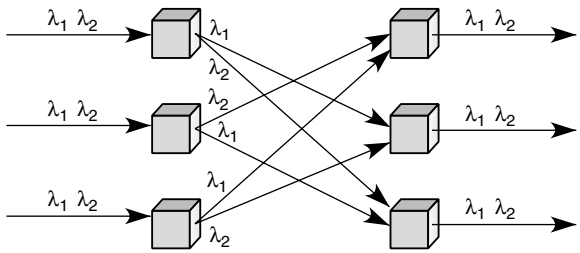


Figure 12.9

Nœud de base d'un réseau à routage en longueur d'onde

Cette architecture correspond à un routage fixe sur les longueurs d'onde. On peut également développer des réseaux à routage en longueur d'onde avec des routages dynamiques dans le temps. À cet effet, il faut insérer des commutateurs optiques ou optoélectroniques, suivant la technologie utilisée, entre les ports d'émission et de réception. Un exemple de cette technique est illustré à la figure 12.10.

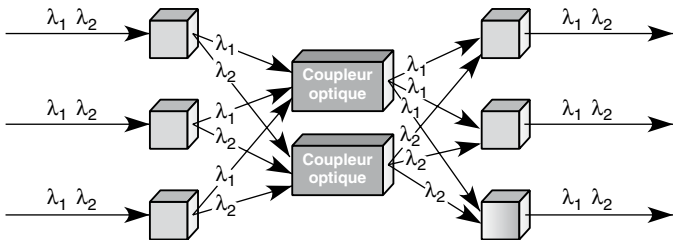


Figure 12.10

Routage dynamique

De nombreuses recherches ont encore lieu dans le domaine de l'optique pour optimiser l'utilisation des longueurs d'onde. Cette technique permet d'atteindre des débits particulièrement élevés, qui se comptent en térabits par seconde. Les difficultés proviennent des coûts encore élevés du multiplexage en longueur d'onde et surtout des commutateurs optiques. Lorsqu'on veut minimiser le coût ou augmenter la portée, il faut utiliser des commutateurs optoélectroniques. Une certaine fragilité est alors visible à chaque passage d'un

environnement lumineux à un environnement électrique. Des progrès considérables doivent encore être réalisés pour réamplifier les signaux de façon optique et régler pratiquement instantanément les coupleurs d'émission ou de réception sur la bonne longueur d'onde.

Les commutateurs optiques

Les commutateurs optiques permettent d'interconnecter des liaisons optiques entre elles. À des fibres optiques entrantes correspondent des fibres optiques sortantes. Si le commutateur utilise une partie électrique, le commutateur est dit optoélectronique et non plus uniquement optique. Ces commutateurs se fondent sur l'interconnexion de commutateurs élémentaires, c'est-à-dire de commutateurs qui possèdent deux portes d'entrée et deux portes de sortie, comme illustré à la figure 12.11. Montés en série, ces commutateurs élémentaires permettent de réaliser de grands commutateurs. La conception de ces équipements pose cependant de nombreux problèmes.

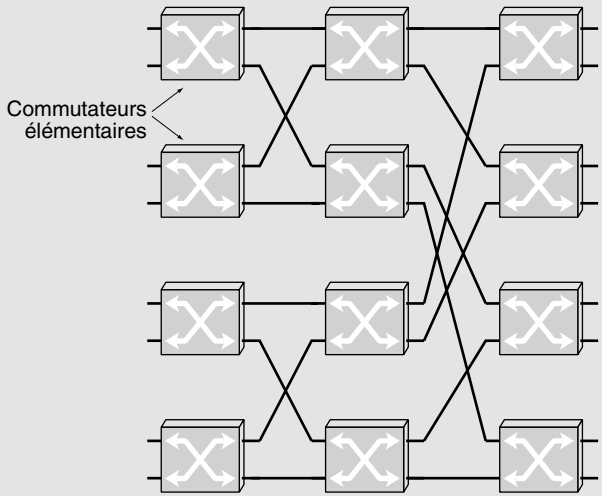


Figure 12.11

Fonctionnement d'un commutateur optique ou optoélectronique

Ces commutateurs, ou MIN (Multistage Interconnection Network), peuvent être de deux types : soit le signal est transformé en signal électrique, soit le signal est commuté en optique. Le premier cas a été présenté en détail au chapitre 4, traitant des routeurs et des commutateurs. Dans la seconde catégorie, on distingue les deux techniques suivantes :

- décisions de contrôle et de routage effectuées électriquement ;
- commutation tout optique.

La commutation de circuits reste plus facile à implémenter que la commutation de paquets, les décisions de contrôle et de routage étant beaucoup plus simples dans ce cas. Dans une commutation de paquets, à l'arrivée de chaque paquet, il faut prendre plusieurs décisions de contrôle et de routage, qui demandent plusieurs centaines de picosecondes dans le meilleur des cas. Actuellement, on sait gérer les collisions potentielles de signaux optiques lorsqu'un croisement de chemins est nécessaire. La technique tout optique reste encore aujourd'hui expérimentale.

Une autre technologie se développe. Située entre la commutation de circuits et la commutation de paquets, elle provient de la commutation de *bursts* (burst-switching). Cette commutation consiste à commuter un ensemble de paquets émis les uns derrière les autres, sans perte de temps entre chaque paquet. Cette émission revient à mettre en place un circuit le temps du pic de trafic. Ce temps peut aller d'une fraction de seconde à quelques secondes. L'idée est évidemment de simplifier la commutation de paquets en utilisant l'équivalent d'un long paquet, constitué de l'ensemble des paquets d'un burst, mais aussi de gagner en utilisation des ressources par rapport à une commutation de circuits, dans laquelle le circuit est parfois mal utilisé.

Un point sensible de ce système concerne la commande des commutateurs. Comment les configurer pour traiter les différents flots de façon différenciée, ou encore comment appliquer à chaque flot la priorité ou la sécurité qui a été négociée par l'utilisateur avec l'opérateur du réseau au début de la connexion ? Pour cela, un réseau de signalisation doit être ajouté au réseau de fibre optique. Ce réseau de signalisation, dit hors bande, c'est-à-dire utilisant une capacité de transport distincte de celle dévolue aux flots utilisateur, est de plus en plus souvent constitué d'un réseau IP. À chaque commutateur optique correspond un routeur IP, par lequel transitent les commandes arrivant dans des paquets IP.

Les commutations par burst et par paquet

Les réseaux optiques que nous avons décrits jusqu'ici utilisent essentiellement une commutation en longueur d'onde. Les paquets utilisent un circuit construit entre un point d'entrée et un point de sortie soit en utilisant la même longueur d'onde tout le long du chemin, soit en changeant de longueur d'onde dans certains nœuds intermédiaires. Cette solution de type circuit n'est pas très efficace pour le transport des données. En effet, les débits qui transitent dans les circuits correspondent à la superposition des débits provenant de groupes d'utilisateurs multiplexés et se présentent donc sous une forme très irrégulière. Les débits transportés par les réseaux sont de surcroît de plus en plus variables dans le temps. De plus, la proportion du débit représentée par la parole téléphonique est en diminution, ce qui enlève encore un peu plus de régularité au trafic que les opérateurs ont à traiter lorsqu'il n'y a que des conversations téléphoniques à transporter.

Pour éviter cette mauvaise utilisation, on a développé des réseaux optiques capables de commuter non plus des longueurs d'onde mais des paquets. Les paquets sont commutés dans un commutateur optique vers une porte de sortie où on leur attribue une couleur disponible pour les émettre. L'inconvénient de cette solution est le nombre de paquets, qui se comptent en milliard par seconde, à traiter dans de gros commutateurs. Le coût de traitement optique étant très important, il est aujourd'hui difficile d'imaginer la date de sortie de tels commutateurs.

Une autre idée s'est développée, consistant à trouver le moyen de traiter de très gros paquets, appelés *bursts*. La commutation par burst n'est rien d'autre qu'une commutation de paquets avec de très gros paquets. À la vitesse de plusieurs gigabits par seconde, la commutation d'un burst peut demander un temps de l'ordre de quelques dizaines à quelques centaines de microsecondes. À une vitesse de 10 Gbit/s, un burst de 100 µs

correspond à 1 Mbit de données. On rassemble donc les données à transporter en paquets de l'ordre de 1 Mbit, puis on met en place un circuit pendant le temps de la transmission.

Appelée OBS (Optical Burst Switching), cette technique devrait bientôt être proposée par quelques équipementiers spécialisés dans la fibre optique. Plusieurs solutions pour réaliser la commutation par burst ont été testées sous les noms de TAG (Tell And Go), TAW (Tell And Wait), JIT (Just In Time) et JET (Just Enough Time).

Dans le TAG (*voir figure 12.12*), lorsque le burst est prêt à être envoyé, un message d'établissement de connexion, ou message SETUP, est émis dans le réseau. Ce message SETUP ouvre le circuit, lequel se referme après le passage du dernier octet du burst. Pour que cette solution soit acceptable, il faut que le réseau soit très peu chargé et que les temps de mise en place du circuit soient négligeables.

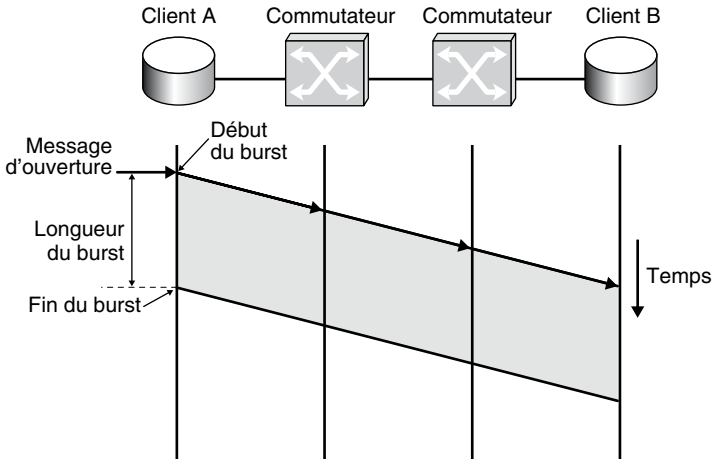


Figure 12.12

Commutation par burst TAG

Dans le TAW (*voir figure 12.13*), un message SETUP prend le temps nécessaire pour mettre en place le circuit puis envoie un message de confirmation d'ouverture avant que le burst soit émis. Cette méthode est acceptable si le temps d'ouverture du circuit est négligeable par rapport au temps de transmission du burst.

Les méthodes JIT et JET permettent toutes deux de s'approcher d'un fonctionnement optimal. Le message d'établissement SETUP est émis avec un temps d'avance sur le burst lui-même de telle sorte que le circuit soit ouvert au moment exact où le burst se présente (*voir figure 12.14*).

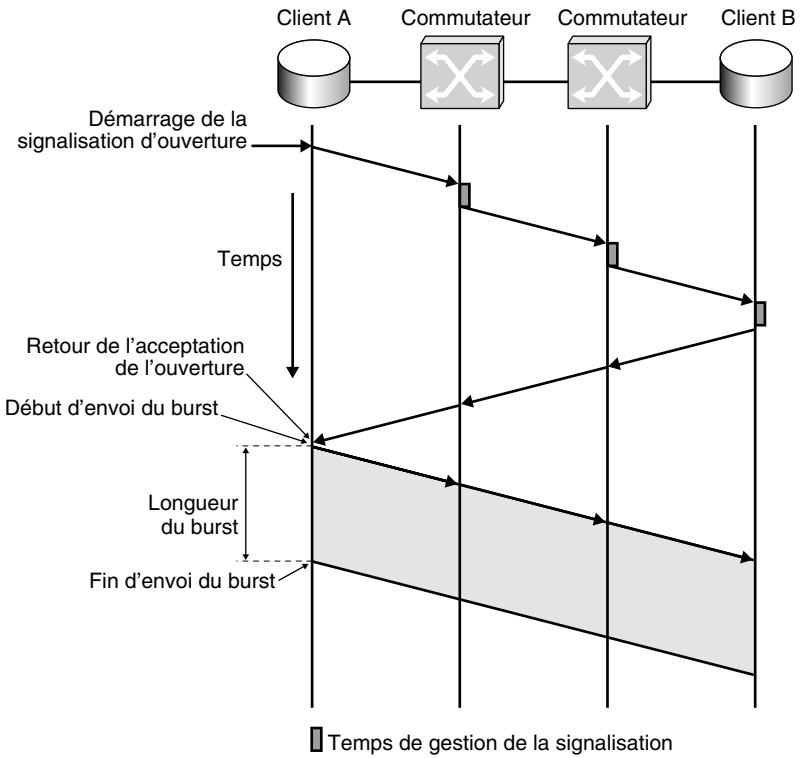


Figure 12.13

Commutation par burst TAW

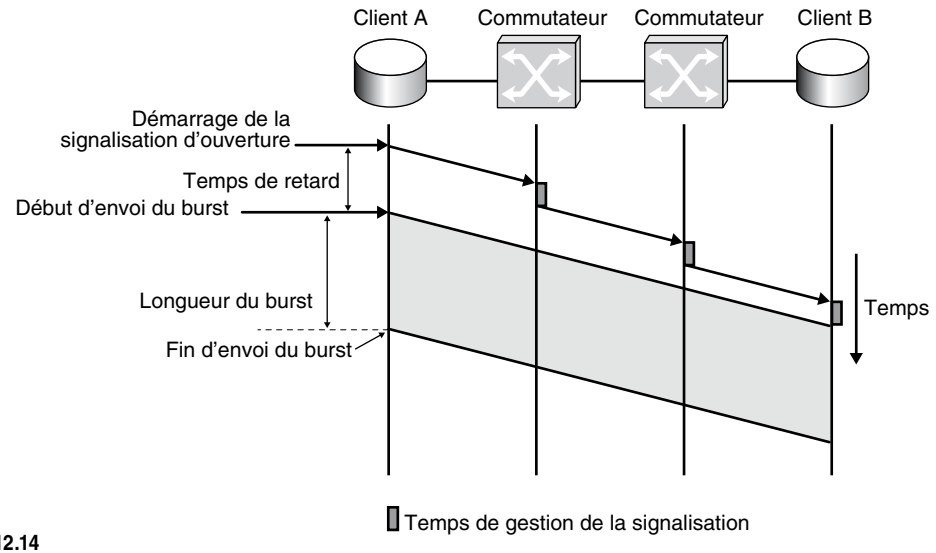


Figure 12.14

Commutation par burst JIT et JEN

La difficulté de cette méthode est de déterminer le temps de latence avant le départ du burst. Plusieurs propositions ont été effectuées pour limiter ce temps au minimum, les deux techniques JIT et JET se distinguant par ce calcul. Il faut à tout prix éviter la destruction du burst par manque de réservation dans un nœud intermédiaire, comme l'illustre la figure 12.15.

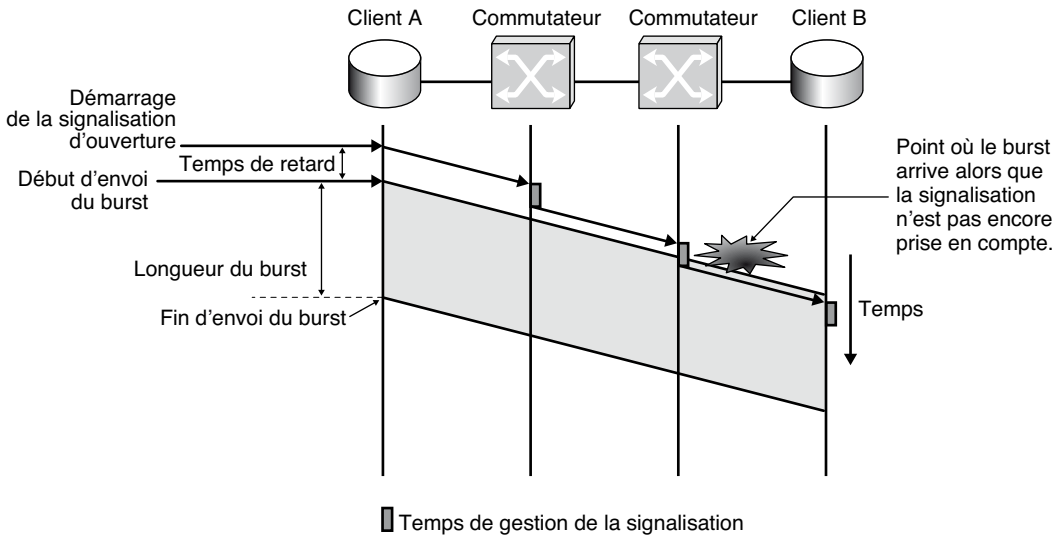


Figure 12.15

Destruction du burst par manque de réservation

La commutation de paquets optiques devrait succéder à la commutation de burst en diminuant le burst jusqu'à la taille d'un paquet. La difficulté reste toujours l'impossibilité ou presque de mémoriser un paquet optique. On peut tout au plus utiliser un rouleau de câble optique pour mémoriser un paquet, mais il est impossible d'aller plus loin. La difficulté sera donc d'ouvrir une voie de communication pour le passage d'un paquet optique. Seule une signalisation extrêmement rapide sera capable de réaliser ce type de transfert.

Signalisation et GMPLS

La commutation par burst demande une forte signalisation pour mettre en place et détruire des circuits plusieurs milliers de fois par seconde. Si plusieurs centaines de milliers de circuits doivent être édifiées et détruits en parallèle, cela exige un système de signalisation capable de traiter des ouvertures et fermetures qui se comptent en centaines de millions chaque seconde. C'est la raison pour laquelle l'OBS pourrait avoir du mal à percer sur le marché des commutateurs optiques de grande taille.

Pour le moment, la solution retenue par beaucoup de grands opérateurs pour leur réseau et plus particulièrement leur cœur de réseau optique est GMPLS (Generalized

MultiProtocol Label Switching), que nous étudions en détail au chapitre 15 avec le protocole MPLS. L'idée principale à la base de cette adoption est la bonne granularité du conduit devant transporter les paquets d'une même communication d'une entrée à une sortie du réseau et la performance des plans de contrôle et de gestion associés. Un plan de contrôle ou de gestion est en fait un réseau spécialisé dans le transport des données de contrôle ou de gestion. Le plan de contrôle est aussi appelé réseau de signalisation. Les protocoles associés à la signalisation sont détaillés au chapitre 26.

Dans le cadre du réseau GMPLS, des protocoles classiques sont utilisés, comme les routages OSPF, IS-IS et la réservation RSVP. Mais ces protocoles sont complétés par des options souvent appelées TE (Trafic Engineering), qui permettent d'ouvrir les meilleurs chemins possibles et d'effectuer des réservations qui sont calculées par de l'ingénierie de trafic.

La figure 12.16 illustre les évolutions du plan de transport et du plan de contrôle/gestion depuis les années 1970. Jusqu'à l'année 2030, le plan de contrôle/gestion était centralisé autour d'un nœud central pour devenir de plus en plus distribué. GMPLS décrit un plan de gestion permettant de définir les granularités des conduits et un plan de contrôle utilisant les protocoles IP et les techniques de contrôle par politique (*voir le chapitre 26*).

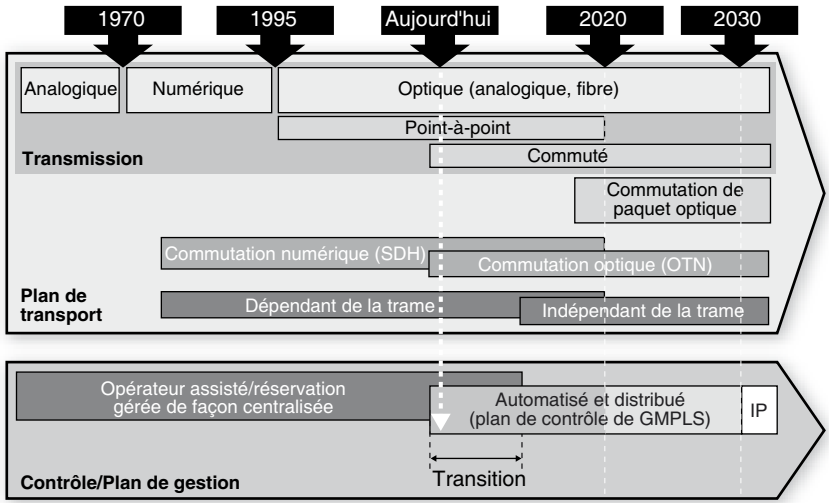


Figure 12.16

Étapes d'introduction du contrôle et de la gestion dans les réseaux optiques

Conclusion

Les réseaux optiques répondent bien aux demandes d'augmentation des débits des utilisateurs. L'utilisation d'un grand nombre de longueurs d'onde, à des vitesses pouvant atteindre 40, 100 puis 160 Gbit/s, permet de satisfaire aisément la demande actuelle. Le potentiel de croissance des débits devrait permettre de suivre facilement la demande. Cependant, la surcapacité, qui aura été fondamentalement utilisée entre les années 2000 et 2010, ne devrait plus être de mise après 2010, date à laquelle les méthodes de contrôle réactives pour établir des communications devraient être de plus en plus utilisées.

Tous les cœurs de réseau utilisent de la fibre optique. Il reste encore d'importants progrès à accomplir pour arriver à un réseau tout optique, dans lequel les signaux sous forme lumineuse seraient transportés de bout en bout sous la forme de paquets.

13

Les réseaux de niveau physique

Une interface désigne un point situé entre deux équipements. Deux grandes catégories d'interfaces sont classiquement définies : les interfaces UNI (User Network Interface), situées entre l'équipement utilisateur et le réseau, et les interfaces NNI (Network Node Interface), situées entre deux nœuds d'un même réseau ou de réseaux distincts. L'interface détermine comment les données traversent le point de passage entre les deux équipements.

Ce chapitre se penche sur les interfaces des réseaux de niveau physique et détaille notamment les suivantes :

- SONET (Synchronous Network) et SDH (Synchronous Digital Hierarchy), définies au départ pour transporter un grand nombre de communications téléphoniques sur un même support physique.
- POS (Packet over SONET), où les communications téléphoniques sont remplacées par des paquets.
- G.709 OTN (Optical Transport Network), qui détermine la dernière génération d'interfaces d'accès sur les réseaux optiques.
- RPR (Resilient Packet Ring), qui définit une nouvelle génération de réseaux de niveau physique et une interface, de même type que SONET/SDH, associée au monde Ethernet.
- MPLS-TP (Transport Profil), qui remplace les interfaces synchrones du type SONET par une interface asynchrone.

Les équipements de communication ont accompagné la diffusion massive du téléphone. Avec l'apparition de la hiérarchie plésiochrone, définissant la capacité des lignes physiques à transporter un grand nombre de communications téléphoniques simultanées, il a fallu déterminer des techniques d'accès définissant le multiplexage des communications. Ces techniques n'étant quasiment plus utilisées, nous les décrivons à l'annexe J. En revanche, nous présentons en détail la hiérarchie synchrone SONET, améliorée par SDH, qui a la même fonction mais d'une façon plus moderne. Le transport des paquets s'effectue sur cette hiérarchie grâce à la technologie PoS (Packet over SONET). Cette hiérarchie est toujours très utilisée car la technologie SONET/SDH permet une reconfiguration du réseau en cas de panne.

Un standard important a été défini par l'UIT-T avec OTN (Optical Transport Network), MPLS-TP (Tranport Profile) et RPR (Resilient Packet Ring), pour l'utilisation d'une trame semblable à celle d'Ethernet dans le cadre de la norme IEEE 802.17.

Enfin, nous examinerons la solution proposée dans le cadre de MPLS-TP, qui propose de remplacer la norme synchrone SONET par un système complètement asynchrone mais capable de retrouver la synchronisation en bout de course.

Les interfaces avec le niveau physique

Le niveau physique représente le premier niveau de la hiérarchie du modèle de référence. Ce niveau s'occupe de transporter les éléments binaires sur des supports physiques variés. Pour accéder à un support, il faut utiliser une interface d'accès.

La figure 13.1 illustre l'ensemble des interfaces de la couche physique avec un support physique, qui est ici de la fibre optique, pour y faire transiter des paquets IP. On voit sur la droite de la figure qu'on peut encapsuler un paquet IP dans une trame ATM, ou tout du moins un fragment du paquet IP puisque la trame ATM est de taille limitée. Ensuite, la trame ATM peut être émise directement sur une fibre optique, si la vitesse est suffisamment basse pour qu'il n'y ait pas besoin de synchronisation d'horloge, ou encapsulée dans une trame SONET/SDH avant d'être acheminée sur la fibre optique. Cette solution a été fortement utilisée au début des années 2000, mais, aujourd'hui, la trame ATM est remplacée par la trame Ethernet, comme nous allons le voir.

Une deuxième solution, également en voie de disparition, consiste à utiliser la trame HDLC ou la trame PPP (Point-to-Point Protocol) pour réaliser cette encapsulation. Pour permettre la synchronisation des horloges, les trames HDLC et PPP sont elles-mêmes encapsulées dans une trame SONET/SDH avant d'être transmises sur la fibre optique.

En allant vers la gauche de la figure, on voit la technique la plus classique aujourd'hui : le paquet IP est encapsulé dans une trame Ethernet, GbE (1 Gbit/s), 10GbE (10 Gbit/s) et 100GbE (100 Gbit/s). Ces trames sont soit véhiculées directement sur la fibre optique, soit transmises par l'intermédiaire de SONET/SDH suivant la vitesse, l'éloignement des stations, soit encore en utilisant le Profile Transport de MPLS-TP.

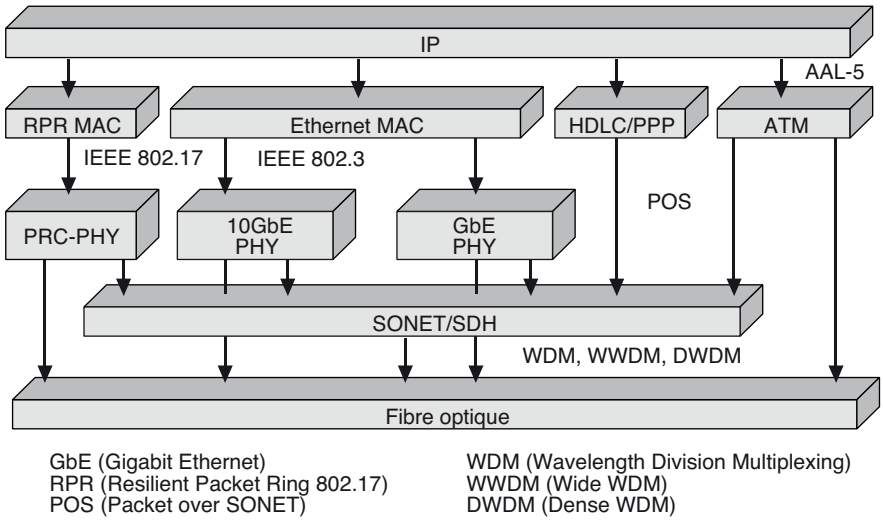


Figure 13.1

Interfaces sur fibre optique

La partie gauche de la figure montre la technique compatible avec Ethernet, dans laquelle les préambules des trames Ethernet sont augmentés pour donner le temps d'effectuer la synchronisation des horloges. Cette solution, standardisée sous le nom IEEE 802.17 est une excellente solution sur les réseaux métropolitains..

Les trois trames utilisées sur l'interface physique sont PPP, ATM et Ethernet. Lorsqu'on examine les standards, on note souvent, même si ce n'est pas une obligation, que le niveau physique est lui-même découpé en deux : le niveau PM (Physical Medium), le sous-niveau le plus bas du niveau physique, qui est responsable du transport de l'information sur le support physique et de la synchronisation bit, et le niveau TC (Transmission Convergence), le sous-niveau haut du niveau physique, qui est responsable de l'adaptation au support physique des éléments binaires provenant des trames.

Les fonctions de l'interface d'accès au sous-niveau TC sont notamment les suivantes :

- adaptation de débit ;
- protection de l'en-tête ;
- délimitation des trames ;
- adaptation aux systèmes de transmission ;
- génération et récupération de la trame.

L'adaptation de débit consiste à ajuster les différents flux d'information à la bande passante de la liaison physique. Pour cela, on peut ajouter des trames vides, dites de bourrage sur un système de type SONET. Une autre solution consiste à insérer des octets de bourrage lorsque aucune transmission de trame n'est en cours. Le nombre d'octets de bourrage dépend de l'intervalle de temps entre deux trames.

SONET (Synchronous Optical Network)

Issue d'une proposition de Bellcore (Bell Communication Research), SONET est une technique de transport entre deux nœuds, qui définit l'interface adoptée pour le NNI (Network Node Interface). Elle ne concernait au départ que l'interconnexion des réseaux téléphoniques des grands opérateurs, PTT, *carrier,* etc. Toute la difficulté de la normalisation a consisté à trouver un compromis entre les intérêts américains, européens et japonais pour permettre l'interconnexion des différents réseaux d'opérateur et des réseaux nationaux.

La hiérarchie des débits étant différente sur les trois continents, il a fallu s'entendre sur un niveau de base. C'est finalement le débit de 51,84 Mbit/s qui a été retenu et qui forme le premier niveau, appelé STS-1 (Synchronous Transport Signal, level 1). Les niveaux situés au-dessus du niveau 1, appelés STS-N, sont des multiples du niveau de base.

SONET décrit la composition d'une trame synchrone émise toutes les 125 µs. La longueur de cette trame dépend du débit de l'interface. Ses diverses valeurs sont classées au tableau 13.1 suivant la rapidité du support optique, ou OC (Optical Carrier).

OC-1	51,84 Mbit/s	OC-24	1 244,16 Mbit/s
OC-3	155,52 Mbit/s	OC-36	1 866,24 Mbit/s
OC-9	466,56 Mbit/s	OC-48	2 488,32 Mbit/s
OC-12	622,08 Mbit/s	OC-96	4 976,64 Mbit/s
OC-18	933,12 Mbit/s	OC-192	9 953,28 Mbit/s

TABLEAU 13.1 • Valeurs de la trame SONET en fonction de la rapidité du support optique

Comme illustré à la figure 13.2, la trame SONET comprend dans les trois premiers octets de chaque rangée des informations de synchronisation et de supervision. Les cellules sont émises dans la trame. L'instant de début de l'envoi d'une cellule ne correspond pas forcément au début de la trame mais peut se situer n'importe où dans la trame. Des bits de supervision précèdent ce début de sorte que l'on ne perde pas de temps pour l'émission d'une cellule.

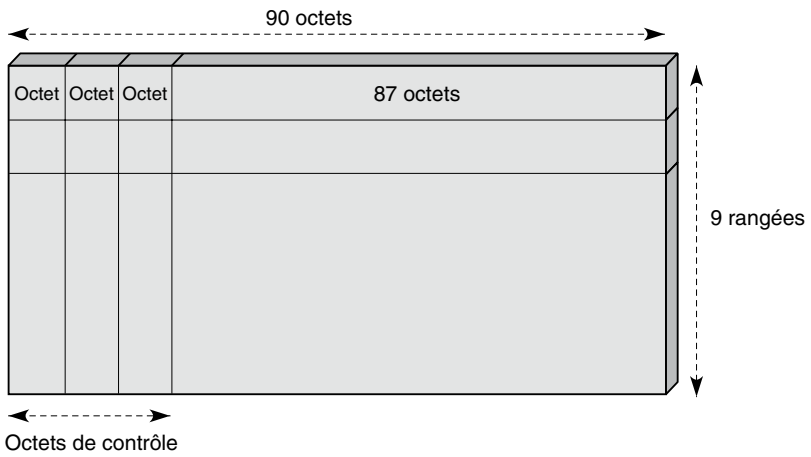


Figure 13.2
Trame SONET de base

Lorsque les signaux à transporter arrivent dans le coupleur SONET, ils ne sont pas copiés directement tels quels mais inclus dans un container virtuel (Virtual Container). Ce remplissage est appelé adaptation. Les trames SONET et SDH comportent plusieurs types de containers virtuels, appelés VC-N (Virtual Container de niveau N). À ces containers, il faut ajouter des informations de supervision situées dans les octets de début de chaque rangée. En ajoutant ces informations supplémentaires, on définit une unité administrative, ou AU-N (Administrative Unit-N).

Les niveaux supérieurs comptent toujours neuf rangées, mais il y a *n* fois 90 octets par rangée pour le niveau *N*. La trame du niveau *N* de la hiérarchie SONET est illustrée à la figure 13.3.

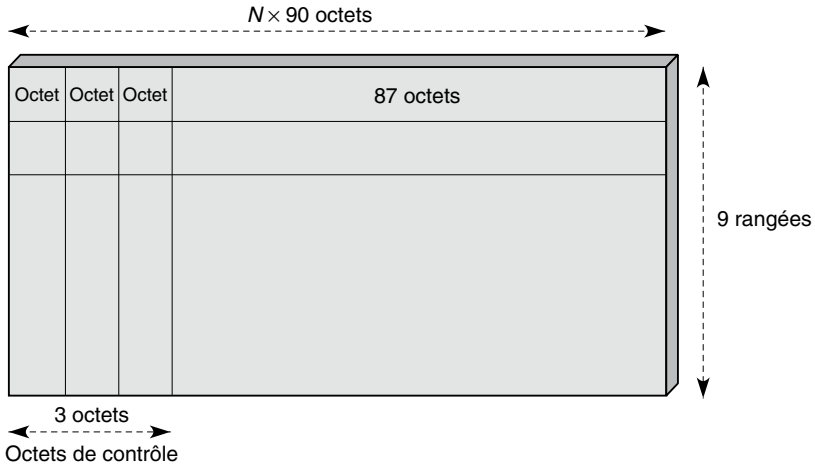


Figure 13.3
Trame SONET STS-N

Le standard SONET est utilisé pour transporter des trames (niveau trame), voire des paquets (niveau paquet) mais, bien sûr, encapsulés dans une trame à très haute vitesse. La trame SONET possède les débits respectivement de 155 Mbit/s, 622 Mbit/s, 2,488 Gbit/s et 9,953 Gbit/s pour l'OC3, l'OC12, l'OC48 et l'OC192. Cela permet de transporter n'importe quel type de trames à haute vitesse que ce soit ATM, Ethernet, IP encapsulé dans une trame, ou toute autre entité.

Une caractéristique très importante de SONET est de fiabiliser la communication en cas de rupture ou de panne de l'un de ses composants. Les réseaux SONET que l'on trouve dans les métropoles ont une topologie en boucle. Deux chemins sont ainsi disponibles pour aller d'un point à un autre, en particulier de l'utilisateur au réseau cœur de l'opérateur. SONET permet la modification de ce chemin en 50 ms. Lors d'une rupture de la communication dans un sens de la boucle, la reconfiguration peut s'effectuer en un temps occasionnant une coupure quasiment indétectable pour les deux personnes en train de se parler. Cette capacité de reconfiguration est un des atouts majeurs des structures SONET/SDH. Nous reviendrons sur les topologies en boucle de SONET/SDH à la fin de ce chapitre pour les comparer à celles provenant du monde Ethernet.

SDH (Synchronous Digital Hierarchy)

La recommandation SDH a été normalisée par l'UIT-T (G.707 et G.708) :

- G.707 : Synchronous Digital Bit Rate ;
- G.708 : Network Node Interface for the Synchronous Digital Hierarchy.

On retrouve dans SDH les débits à 155, 622, 2 488 Mbit/s et 9 953 Mbit/s de SONET.

Le temps de base correspond toujours à 8 000 trames par seconde, chaque trame étant composée de neuf fois 270 octets. Au total, cela fait 155,520 Mbit/s. La structure de la trame synchrone SDH est illustrée à la figure 13.4.

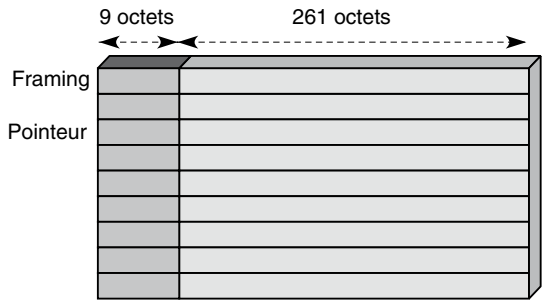


Figure 13.4
Trame SDH

L'information transportée est indiquée par un pointeur qui se situe dans la zone de supervision de la trame. Lorsque la quantité d'information à transporter est supérieure à la zone disponible dans la trame SDH, elle continue dans la trame suivante, la fin étant indiquée par un pointeur de fin.

La figure 13.5 montre comment un flux à 140 Mbit/s peut être transporté sur une liaison SDH à 155 Mbit/s (un débit de 140 Mbit/s représente 8 fois 261 octets plus 100 octets, ce qui correspond à la partie grisée de la figure 13.5).

Les cellules ATM sont transportées dans la trame SDH dès que possible. Il ne faut perdre qu'un minimum de temps lors de la transmission sur chaque liaison pour éviter que la variance du temps de réponse de la cellule n'augmente trop.

La figure 13.6 illustre le transport de cellules sur une liaison SDH de base : les cellules se trouvent n'importe où, et elles sont signalées dans la zone SOH ou dans la trame car aucun temps ne doit être perdu à attendre un slot particulier.

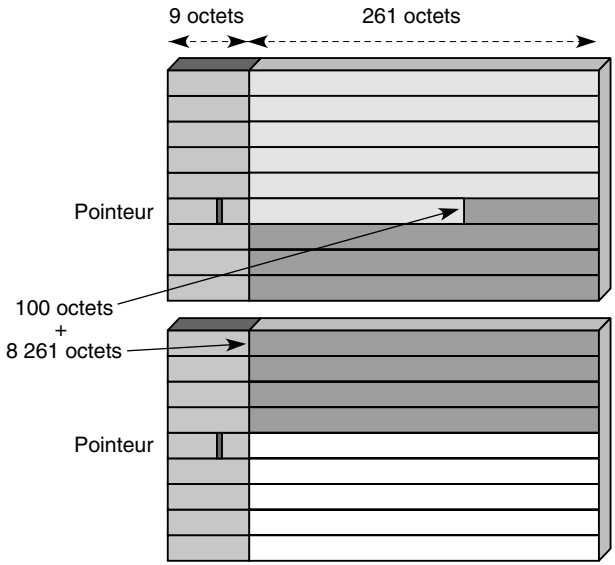


Figure 13.5

Transport d'un flux SDH à 140 Mbit/s

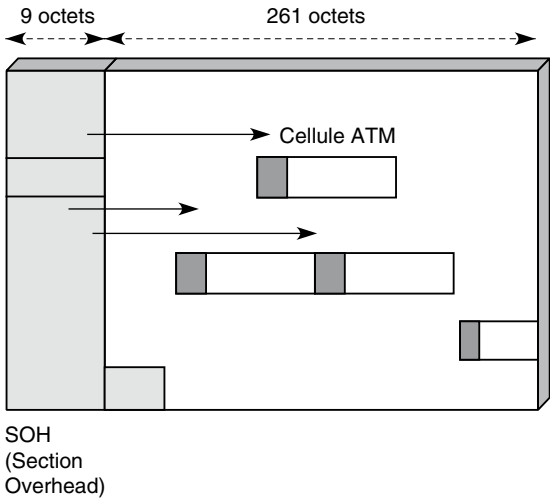


Figure 13.6

Transport de cellules ATM sur une liaison SDH

La trame de base de SDH est appelée STM-1 (Synchronous Transport Module, niveau 1). Elle est équivalente au STS-4 de la recommandation SONET. La hiérarchie SDH de l'UIT-T est récapitulée au tableau 13.2.

STM-1	155,52 Mbit/s	STM-12	1 866,24 Mbit/s
STM-3	466,56 Mbit/s	STM-16	2 488,32 Mbit/s
STM-4	622,08 Mbit/s	STM-32	4 976,64 Mbit/s
STM-6	933,12 Mbit/s	STM-64	9 953,28 Mbit/s
STM-8	1 244,16 Mbit/s	STM-256	39 813,12 Mbit/s

TABLEAU 13.2 • Hiérarchie SDH de l'UIT-T

Les signaux à transporter proviennent de liaisons, qui peuvent être synchrones ou asynchrones. Pour un transport plus aisé, on les accumule dans un container virtuel VC (Virtual Container), comme nous l'avons déjà vu pour la recommandation SONET. Ce packaging est appelé *adaptation*. Il existe différents containers virtuels pour chaque type de signal à transmettre.

Les liaisons SDH utilisées par les opérateurs sont au nombre de cinq, correspondant aux STM-1, STM-4, STM-16, STM-64 et STM-256. La trame de base est multipliée par 4 pour aller au niveau suivant. Cela correspond à des débits de 622 Mbit/s, 2,488 Gbit/s, 9,953 Gbit/s et 39 813 Gbit/s. Les containers virtuels pour ces niveaux sont les VC-4, VC-16, VC-64 et VC-256. Le transport de ces containers sur les trames STM-4 STM-16, STM-64 et STM-256 s'effectue par un multiplexage temporel, comme illustré à la figure 13.7, dans laquelle 4 trames VC-4 sont découpées et entrelacées octet par octet.

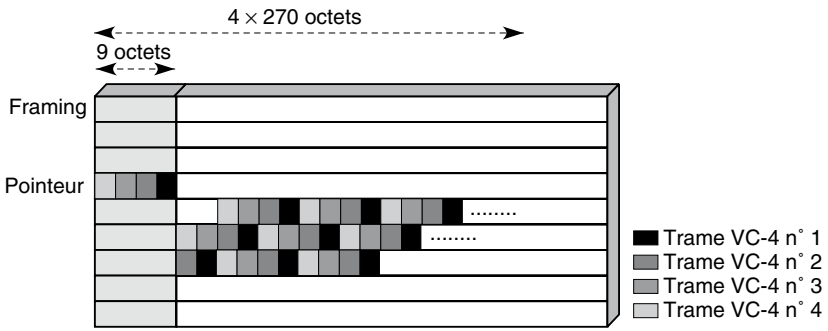


Figure 13.7

Multiplexage de containers VC-4 sur une trame STM-4

Comme dans SONET, le contenu du container avec les pointeurs forme une unité administrative, ou AU (Administrative Unit). Les unités administratives sont de plusieurs niveaux : AU-1, AU-4, AU-16, AU-64 et AU-256. Le niveau STM-16 est formé à partir de quatre STM-4, qui sont entrecroisés sur le support physique. Les niveaux supérieurs utilisent les mêmes entrecroisements.

En Europe, l'ETSI a défini des formats européens sous les noms de C-12, C-3 et C-4, qui correspondent à des valeurs de containers. Des formats intermédiaires, appelés TU

(Tributary Unit) et TUG (Tributary Unit Groups), complètent la hiérarchie. Cette hiérarchie quelque peu complexe est illustrée à la figure 13.8.

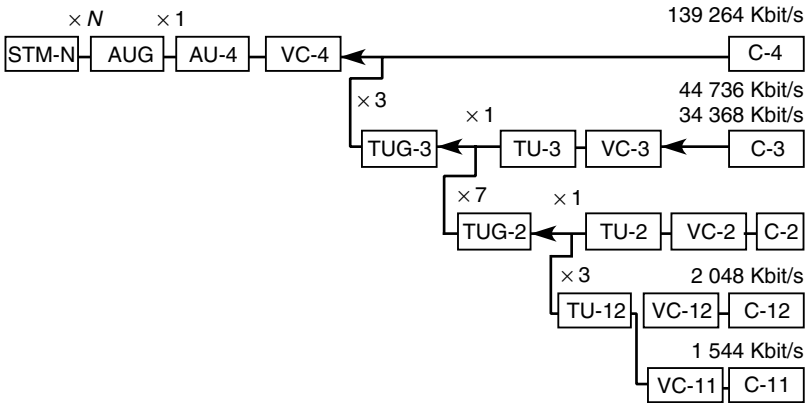


Figure 13.8

Hiérarchie SDH de l'ETSI

PoS (Packet over SONET) et EoS (Ethernet over SONET))

Comme expliqué précédemment, l'interface SONET a été choisie au départ par l'UIT-T pour interconnecter les réseaux téléphoniques. Cette interface détermine un temps de 125 µs entre l'émission de deux trames. La trame SONET est une sorte de wagon, que l'on peut remplir par des octets ou des trames et plus généralement par des containers. La technique générale de transport de paquets sur SONET/SDH s'appelle PoS. Elle est aujourd'hui largement utilisée pour acheminer directement à haute vitesse des paquets de tout type sur un support SONET/SDH.

L'interface IP over SONET devrait s'appeler IP/PPP-HDLC Over SONET. Pour formater le flot de paquets IP en trames, on utilise le protocole PPP, qui fournit un protocole d'encapsulation, un contrôle d'erreur et un protocole d'ouverture de la connexion. Les trames PPP peuvent être remplacées par des trames HDLC suivant la RFC 1662. PPP est décrit dans la RFC 1661.

La figure 13.9 illustre la structure de la trame IP over SONET encapsulant le paquet IP.

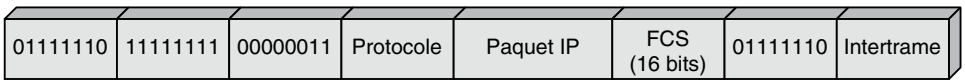


Figure 13.9

Format de la trame IP over SONET

Les routeurs ou les commutateurs doivent être capables de traiter les débits permis par SONET/SDH (155 Mbit/s, 622 Mbit/s, 2,5 Gbit/s, 10 Gbit/s, 40 Gbit/s et bientôt 160 Gbit/s). Comme les paquets IP sont de plus en plus souvent encapsulés dans une trame Ethernet, SONET est utilisé pour transporter ce type de trame à l'intérieur de sa

zone de données. On obtient la technique Ethernet over SONET (EoS). L'avantage de cette solution est de permettre une synchronisation des trames Ethernet. Véhiculer de la parole téléphonique sous IP et l'encapsuler dans SONET devient très facile sur de longues distances. L'encapsulation des trames Ethernet s'effectue par une méthode d'encapsulation de blocs appelée Generic Framing Procedure pour permettre justement à des flots bas débit de se positionner aux bons endroits à l'intérieur de la trame SONET.

SONET est également utilisé pour le transport de l'Ethernet 10 Gbit/s (10GbE) en encapsulant les trames Ethernet afin de permettre au 10GbE d'atteindre de longues distances. Il s'agit bien sûr d'Ethernet commuté.

L'interface OTN (Optical Transport Network)

Comme expliqué précédemment, la norme SONET/SDH a été introduite pour transporter de la parole téléphonique, et il a fallu de nombreuses adaptations pour le transport des trames et paquets de type IP, ATM, Ethernet ou autres. Le successeur de SONET/SDH a été mis en chantier et normalisé début 2002 par l'UIT-T sous le nom d'OTN (Optical Transport Network). Son rôle est de faire transiter des paquets sur des liaisons à 2,5, 10, 40 et 160 Gbit/s. La recommandation correspondante porte le numéro G.709.

La figure 13.10 illustre le nouveau format de la trame synchrone OTN.

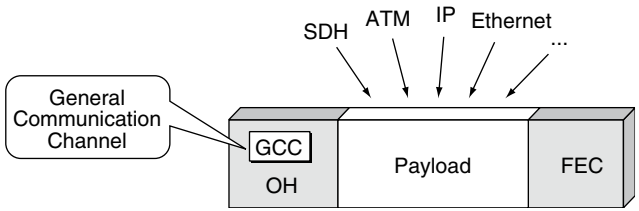


Figure 13.10

Format de la trame OTN

Tous les types de trames doivent pouvoir être transportées de façon transparente dans la trame OTM, sans qu'elles aient besoin d'être modifiées. Un champ est prévu pour ajouter un FEC (Forward Error Correction) afin d'effectuer les corrections nécessaires pour atteindre un taux d'erreur déterminé.

L'interface OTN est constituée de plusieurs niveaux. En partant de la fibre optique on trouve les couches suivantes :

- OTS (Optical Transmission Section), qui prend en charge la transmission du signal optique en vérifiant son intégrité.
- OMS (Optical Multiplex Section), qui prend en charge les fonctionnalités permettant de réaliser un multiplexage en longueur d'onde.
- OCh (Optical Channel), qui est le niveau de bout en bout du signal optique. Ce niveau permet la modification de la connexion et le reroutage, ainsi que les fonctions de maintenance de la connexion.
- DW (Digital Wrapper), qui correspond à l'enveloppe numérique.

Le niveau Digital Wrapper est lui-même décomposé en trois sous-niveaux :

- OTUk (Optical Transport Unit), qui donne la possibilité d'adopter une correction utilisant un FEC.
- ODUk (Optical Data Unit), qui gère la connectivité indépendamment des clients et offre une protection et une gestion de cette connectivité.
- OPUk (Optical Payload Unit), qui indique une correspondance entre le signal et le type de client.

L'architecture globale d'OTN est illustrée à la figure 13.11.

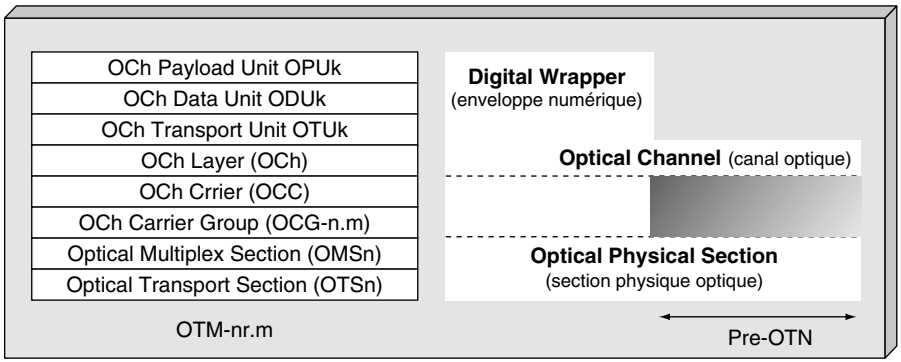


Figure 13.11

Structure en couches de l'architecture OTN

La figure 13.12 illustre les différentes entités de transport sur l'interface OTH (Optical Transport Hierachy) et la figure 13.13 la structure de la trame et les débits de l'interface OTN.

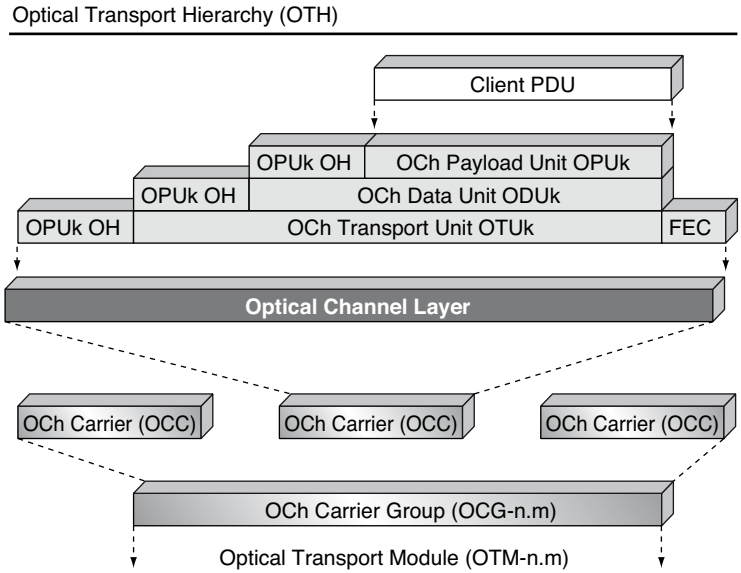
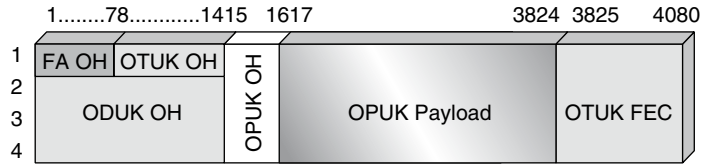


Figure 13.12

Entités de transport de la hiérarchie OTH



OPU			ODU			OTU		
k = 1	k = 2	k = 3	k = 1	k = 2	k = 3	k = 1	k = 2	k = 3
48,971	12,191	3,035	48,971	12,191	3,035	48,971	48,971	3,035
20,420	82,028	329,489	20,420	82,028	329,489	20,420	20,420	329,489
2 488,320	9 995,277	40 150,519	2 498,775	10 037,274	40 319,219	2 666 057	10 709,225	43 018,413

OPU (Optical Packet Unit) ODU (Optical Data Unit) OTU (Optical Transport Unit)

Figure 13.13

Structure de la trame et débits de l'interface OTN

MPLS-TP

Nous nous intéressons dans cette section à la partie interface physique de MPLS-TP (Transport Profile). Il est à noter que le mot « transport » ne se réfère pas au niveau:message (couche 4, ou transport) du modèle de référence, mais au transport des éléments binaires sur le niveau physique (couche 1). Cependant, MPLS-TP rassemble l'ensemble des spécifications pour réaliser un réseau MPLS, allant de la signalisation à la commutation en passant par le système de gestion et nous le retrouverons quand nous traiterons de MPLS (*voir le chapitre 15*).

L'interface qui nous intéresse ici a pour objectif de remplacer l'interface synchronisée SONET par une interface asynchrone de type paquet. Le but est de réduire les coûts en remplaçant une interface synchrone assez complexe par une interface asynchrone beaucoup plus simple. La difficulté est de récupérer la synchronisation à l'extrémité du réseau. MPLS-TP ajoute également des techniques de redondance afin d'offrir une disponibilité forte et, comme SONET, une reconfiguration dans des temps ne gênant pas la parole téléphonique.

Parmi les redondances possibles, citons notamment les techniques 1:1, 1+1, N:1, N,M,O :

- 1:1 : un chemin doit être secouru par un deuxième chemin.
- 1+1 : le flot a ouvert deux chemins, avec la possibilité, en cas de panne d'un chemin, de continuer à offrir une qualité de service acceptable tout en n'utilisant qu'un seul chemin.
- N:1 : N chemins ont en commun un chemin de secours.
- N+1 : N + 1 chemins sont ouverts par le flot, avec la possibilité que si l'un de ces N + 1 flots tombe en panne la qualité de service reste acceptable en n'utilisant que les N chemins ;
- N,M,O : N chemins sont secourus par M chemins, qui, eux-mêmes, sont secourus par O chemins. Beaucoup de possibilités sont offertes en permettant ou non de faire circuler des flots sur les chemins de secours qui sont moins prioritaires.

Nous reviendrons en détail sur ce standard au chapitre 15.

RPR (Resilient Packet Ring)

Les réseaux Ethernet présentent généralement une topologie sous forme de bus ou d'arbre, qui ne facilite pas les reconfigurations en cas de panne. Quand il est possible d'utiliser une méthode commutée, la boucle est une meilleure technologie, et c'est pourquoi elle a été choisie par de nombreux réseaux métropolitains, notamment SONET/SDH.

RPR propose une nouvelle solution de réseau métropolitain en boucle permettant de réagir rapidement en cas de panne d'un tronçon de la boucle et d'offrir de très hauts débits, allant jusqu'à 10 Gbit/s par boucle. Son avantage sur SONET/SDH réside dans son prix de revient beaucoup plus bas, du fait des composants utilisés.

Limitations de SONET et d'Ethernet dans les techniques de boucle

SONET est essentiellement conçu pour des communications point-à-point en commutation de type circuit, comme la parole téléphonique. La figure 13.14 illustre l'accès d'une station vers les autres stations. On peut constater que SONET permet d'aller directement de l'émetteur au récepteur. Chaque circuit se voit allouer une capacité de transmission déterminée. Si la quantité d'information à émettre est inférieure à la valeur allouée, ce qui n'est pas utilisé est perdu.

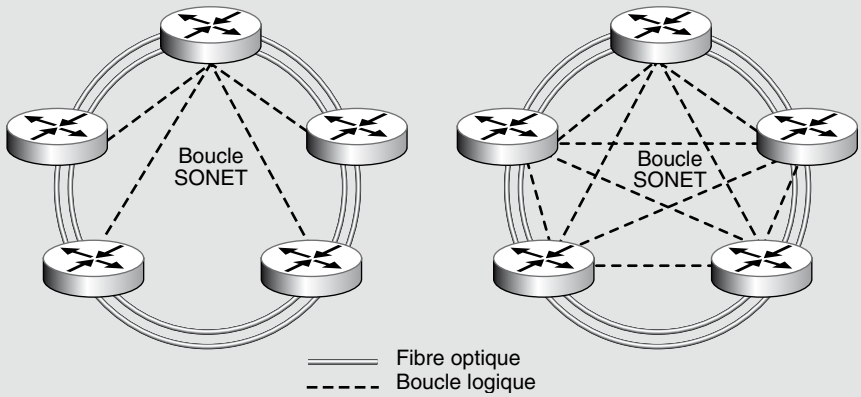


Figure 13.14

Topologie de SONET

SONET n'est donc pas adapté aux transferts de trames asynchrones et irrégulières. De plus, les applications multipoint ne sont pas prises en compte de façon intrinsèque car il faut autant de circuits que de points à atteindre. Pour protéger SONET contre les incidents et permettre une reconfiguration simple, la bande passante réellement utilisée est de l'ordre de 50 %. À l'inverse, Ethernet est bien adapté aux flots asynchrones et aux applications multipoint mais très mal aux flots synchrones.

La figure 13.15 illustre la topologie en anneau qu'il est possible de mettre en place dans Ethernet. On transmet la trame Ethernet d'un nœud vers un autre nœud. Lorsqu'on atteint le dernier commutateur de la chaîne, la trame repart vers l'origine sur une ligne qui va en sens contraire.

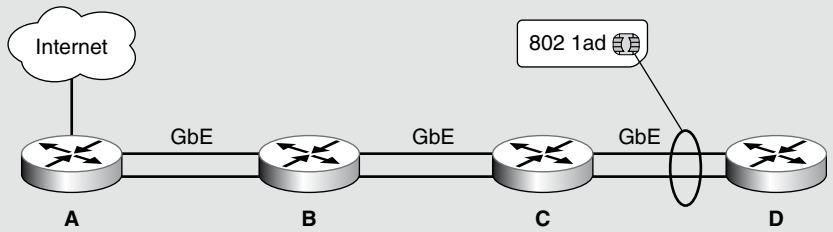


Figure 13.15
Boucle Ethernet

Les techniques Ethernet utilisent l'algorithme du Spanning-Tree, présenté en détail au chapitre 6, pour réaliser le routage des trames. Cet algorithme est trop lent pour la reconfiguration lors de la circulation de paroles téléphoniques. En effet, il faut compter un minimum de 500 ms pour remettre en place le nouveau routage, contre 50 ms au maximum pour une boucle SONET. C'est la raison de l'adoption dans RPR d'une solution en boucle, mais avec une technique de transfert dans les nœuds qui ne provient pas de la commutation, à la différence de SONET.

La méthode d'accès à la boucle doit être capable de gérer les milliers d'utilisateurs d'une boucle métropolitaine sans perte de temps sur la boucle. Avec la nouvelle technique d'accès partagée au support physique bien adaptée au monde métropolitain et aux réseaux de grande capacité possédant des milliers de clients, il est possible d'obtenir des réseaux métropolitains à temps de reconfiguration court et acceptable pour les voies de communication téléphoniques à tarifs compétitifs.

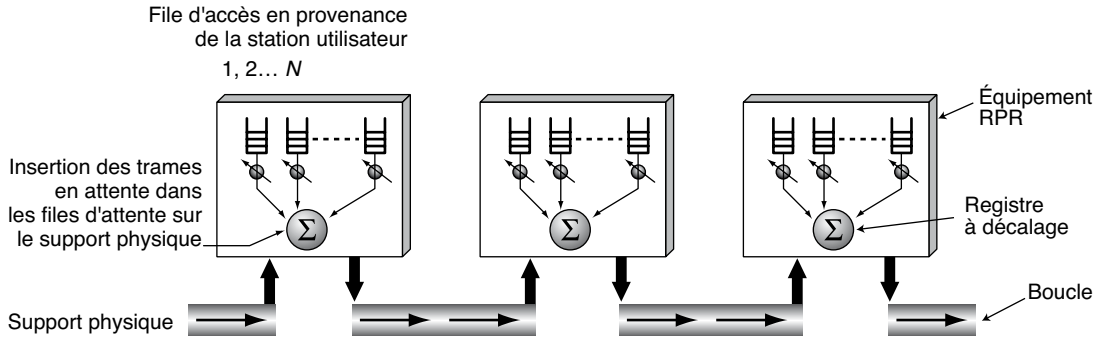


Figure 13.16
Boucle fonctionnelle de la technique RPR

Le nœud du réseau RPR n'est pas un commutateur mais un équipement d'insertion de paquets, comme nous allons le voir. Les paquets vont d'un équipement RPR à un autre. Ils forment un flux de paquets transitant sur la boucle à laquelle sont connectés les équipements RPR. Un équipement RPR possède *N* files d'attente correspondant à des niveaux de priorité. La file prioritaire est servie jusqu'à ce qu'elle soit vide, après quoi la file 2 prend le relais, et ainsi de suite. Le service s'effectue de la façon suivante : lorsqu'un

équipement RPR veut émettre sur la boucle, il met le paquet arrivant de la boucle dans un registre à décalage, qui n'est autre qu'une mémoire supplémentaire dans laquelle les éléments binaires entrent par un côté et ressortent par l'autre ; il émet alors le paquet en attente dans la file d'attente puis le paquet mis en attente dans le registre à décalage. Cette solution est schématisée à la figure 13.16.

Tant que la boucle est pleine, c'est-à-dire tant que les registres d'insertion sont utilisés, une station ne peut plus émettre. Il faut donc enlever une trame, et c'est ce que l'on fait lorsque la trame revient à son émetteur. Un nœud a pour cela trois fonctions : ADD, qui insère une trame lorsque cela est possible, DROP, pour prélever une trame qui a fini son tour de boucle, et PASS, pour laisser passer une trame dans le registre.

Le multicast est inhérent à la technologie des registres à décalage puisque le nœud émetteur n'envoie qu'une seule trame, qui est recopiée en cas de diffusion à l'ensemble des nœuds de transfert lors du parcours du message. La topologie utilisée est en boucle, mais, pour des raisons de reconfigurabilité, elle est doublée par deux boucles contrarotatives. Cette boucle est illustrée à la figure 13.17.

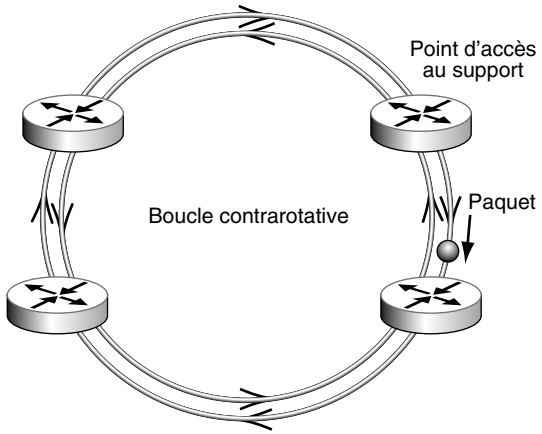


Figure 13.17

Boucle contrarotative de RPR

Le support physique peut être de différents types entre deux nœuds si nécessaire.

La reconfiguration RPR

L'un des points fort de l'architecture RPR réside dans sa reconfigurabilité en moins de 50 ms, qui permet de prendre en compte des voies téléphoniques. Cette reconfiguration s'effectue en inversant le sens de la communication sur la boucle. Lorsque la double fibre optique est coupée (*voir figure 13.18*), des interrupteurs sont déclenchés dans les nœuds entourant la fibre optique coupée. Ces interrupteurs permettent de refaire une boucle unique en remplacement de la double boucle.

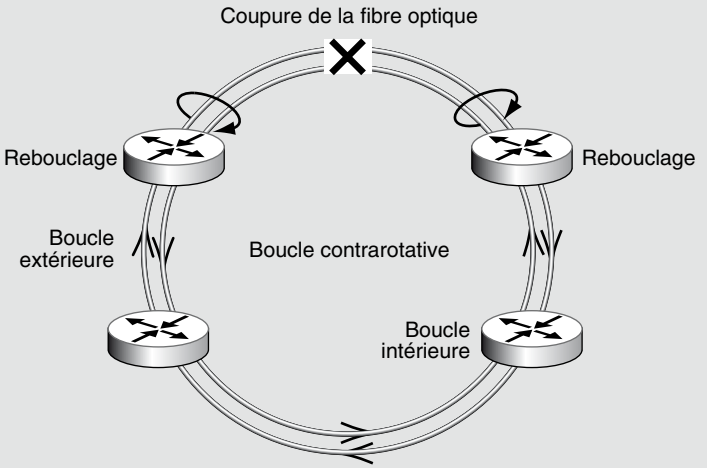


Figure 13.18
Double boucle contrarotative de RPR

Un autre avantage de la topologie en boucle est qu'elle permet d'implémenter un algorithme d'accès attribuant des droits égaux à tous les utilisateurs. La technique d'accès par registre permet à chaque utilisateur d'obtenir le débit maximal disponible sur le réseau sans se restreindre à la valeur du circuit ouvert, à la différence de SONET.

Si une application demande une diffusion ou un multipoint, le support en boucle permet de prendre aisément en compte cette demande puisque la trame émise sur la boucle est prélevée par l'émetteur après un tour de boucle. Les stations participant au multipoint ont donc toute latitude pour prélever une copie au passage.

La différence entre la boucle RPR et la boucle SONET est illustrée à la figure 13.19. Dans le cas de SONET, les trames sont émises sur un circuit allant directement de l'émetteur au récepteur et dont la capacité a été réservée à l'avance. Dans RPR, les trames sont émises sur la boucle avec un débit au moins égal au débit de la boucle divisé par le nombre de stations connectées, voire davantage si toutes les stations ne sont pas actives. Les ressources sont totalement partagées par l'ensemble des utilisateurs.

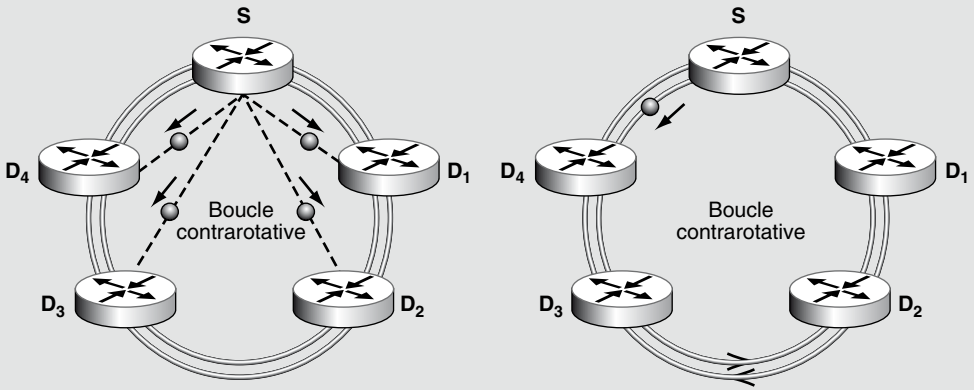


Figure 13.19
Comparaison des boucles SONET (à gauche) et RPR

En comparaison des techniques de type circuit, dans lesquelles il faut souvent attendre un mois en moyenne pour pouvoir disposer du circuit, RPR se distingue par la rapidité avec laquelle il est possible d'offrir une capacité de transmission à un utilisateur. Dans SONET, il faut activer des mécanismes de réservation de slots déterminés pour arriver à la capacité de transmission réclamée par l'utilisateur. Dans RPR, étant donné que le trafic d'un nœud est connu à l'avance, l'opérateur sait immédiatement si le débit demandé est acceptable pour l'infrastructure du réseau.

Même si SONET permet d'effectuer la réservation de ressources par le biais d'un automate, la mise en place du circuit et son optimisation réclament du temps et des logiciels d'ingénierie de trafic.

Les applications de RPR

RPR permet de mettre en place de nombreux services, à commencer par ceux d'un fournisseur de services métropolitains, parfois appelé MSP (Metro Service Provider), ILEC (Incumbent Local Exchange Carrier), CLEC (Competitive Local Exchange Carrier) ou BLEC (Building Local Exchange Carrier). Il peut en outre remplacer les opérateurs de modems câble ou ADSL dont la fonction est de proposer des accès haut débit à Internet, car la technologie RPR est parfaitement adaptée à cette demande. La figure 13.20 illustre ce que pourrait être un tel réseau métropolitain.

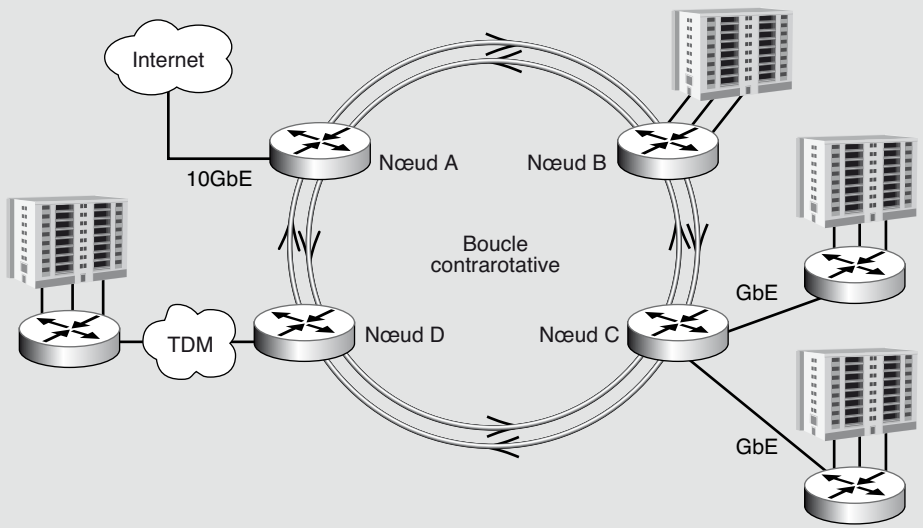


Figure 13.20

Réseau métropolitain à base de technologie RPR

Grâce à RPR, chaque utilisateur se voit attribuer un débit variable, dont la borne maximale est connue, ce qui garantit une très grande souplesse d'exploitation. Un SLA (Service Level Agreement) peut être négocié pour le débit et le temps de transit dans le réseau. Un temps de reconfiguration de moins de 50 ms est acceptable puisque aucune station ne peut monopoliser la bande passante. De plus, la technologie RPR étant très proche d'Ethernet, un couplage avec les réseaux Ethernet des entreprises est simple à mettre en œuvre, quel que soit le débit, qui peut aller de 10 Mbit/s à 10 Gbit/s.

IEEE 802.17

Le groupe de normalisation de RPR est l'IEEE 802.17, chargé d'introduire les concepts Ethernet dans les réseaux métropolitains et étendus. Plus de 300 sociétés participent à cette normalisation. Le protocole IEEE 802.17 doit être parfaitement compatible avec les protocoles 802.1D, 802.1Q et 802.1f. La trame émise sur le support physique étant du même type que la trame Ethernet, la compatibilité avec Ethernet est complète. Le groupe de travail IEEE 802.17b a été monté pour encore améliorer la première norme en permettant une meilleure réutilisation des trames RPR.

L'utilisation intensive de la trame Ethernet semble une solution simple permettant de faire baisser les prix des connexions à des niveaux impossibles à atteindre avec les technologies de type SONET.

Conclusion

Les interfaces d'accès aux réseaux de transport de données permettent de déterminer les performances du réseau. La trame utilisée par l'interface a une implication directe à la fois sur l'équipement terminal et sur le réseau. L'interface dominante pour les hauts débits est depuis de nombreuses années SONET/SDH, qui apporte à la fois des vitesses de transmission importantes et une sécurisation de l'interface par la possibilité de reconfigurer les boucles SONET en moins de 50 ms. Cependant, le coût de cette interface est élevé. Du fait qu'elle n'est pas associée directement à une structure de trame de niveau 2, il faut en effet encapsuler cette trame de niveau 2 dans la trame SONET.

L'arrivée de technologies telles que MPLS-TP et RPR a pour objectif de diminuer le coût de l'interface en utilisant des techniques classiques, déjà largement utilisées dans les réseaux locaux. Une autre solution, représentée par OTN, vise à trouver une interface universelle pour accéder à un réseau de fibre optique. La problématique de l'interface unique est toutefois loin d'être résolue, et l'on s'oriente plutôt aujourd'hui vers un choix d'interface correspondant au type d'équipement terminal à connecter et de réseau à traverser.

14

Les réseaux Ethernet et ATM

La trame Ethernet ne cesse de gagner du terrain par rapport à la trame ATM, au point de dominer désormais complètement le monde des réseaux.

C'est la raison pour laquelle nous avons relégué à l'annexe K les techniques du Relais de trames et les compléments de la solution ATM.

Les modes partagé et commuté

Ethernet fonctionne selon deux modes très différents mais totalement compatibles, le mode partagé et le mode commuté, qui permettent tous deux de transporter des trames Ethernet.

Le mode partagé indique que le support physique est partagé entre les terminaux munis de cartes Ethernet. Dans ce mode, deux stations qui émettraient en même temps verraient leurs signaux entrer en collision. Dans le mode commuté, les terminaux sont connectés à un commutateur, et il ne peut y avoir de collision puisque le terminal est seul sur la liaison connectée au commutateur. Le commutateur émet vers la station sur la même liaison mais en full-duplex, c'est-à-dire en parallèle mais dans l'autre sens.

La figure 14.1 illustre ces deux techniques avec cinq stations terminales.

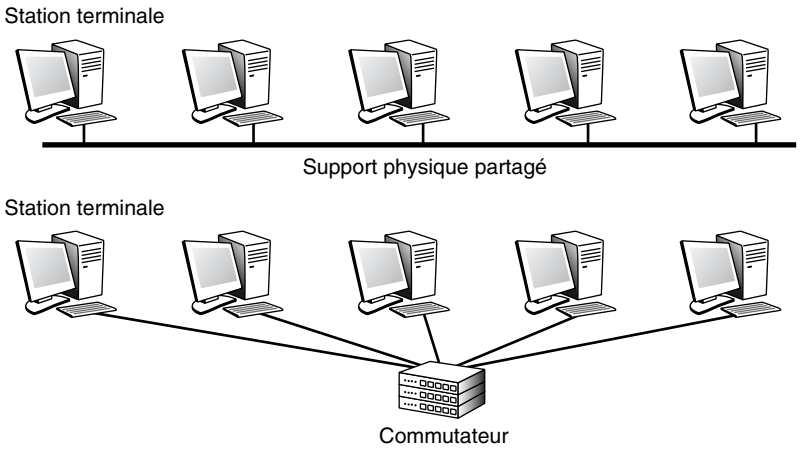


Figure 14.1

Comparaison des techniques partagées et commutées

Les principaux avantages et inconvénients des deux modes sont les suivants :

- Il n'y a pas de collision en mode commuté, mais les trames doivent être mémorisées dans les commutateurs, ce qui demande un contrôle de flux.
- Pour connecter une station en commutation, il faut deux coupleurs et un commutateur, tandis que pour connecter une station en mode partagé, un seul coupleur est suffisant. La technique partagée est donc moins chère à mettre en œuvre.
- La technique commutée autorise des liaisons sans contrainte de distance, tandis que la méthode partagée s'accompagne d'une limitation forte de la distance pour résoudre le problème du partage du support physique.

Les réseaux Ethernet partagés

Les réseaux Ethernet partagés mettent en œuvre une technique d'accès au support physique normalisée par le groupe de travail IEEE 802.3 sous le nom d'accès MAC (Medium Access Control). MAC utilise une technique générale appelée accès aléatoire.

Née de recherches effectuées au début des années 1970 sur les techniques d'accès aléatoire, la norme IEEE 802.3, qui a donné ensuite naissance à la norme ISO 8802.3, décrit la technique d'accès à un réseau local Ethernet partagé. C'est la société Xerox qui en a développé la première les prototypes.

On peut caractériser les réseaux Ethernet partagés par la technique d'accès CSMA/CD, dont le débit varie de 1 à 10, 100 et 1 000 Mbit/s. Au-delà, à la vitesse de 10 000 Mbit/s, seule la solution commutée est acceptable pour des raisons de distance, comme nous le verrons.

Avant d'entrer plus avant dans les détails des différents produits Ethernet commercialisés, indiquons les différents noms empruntés par les réseaux Ethernet partagés :

- Cheapernet. Ethernet partagé qui utilise un câble fin (thin cable) mais en conservant les mêmes capacités de transmission.
- Starlan. Réseau partagé utilisant la technique d'accès CSMA/CD mais sur une topologie très différente et à des vitesses de 1 Mbit/s pour la première génération, 10 Mbit/s pour la deuxième et 100 Mbit/s pour la troisième.
- Fast Ethernet. Nom des réseaux à 100 Mbit/s.
- Gigabit Ethernet, ou GbE. Correspond à la capacité de 1 000 Mbit/s. Il est à noter que le 10GbE (10 000 Mbit/s), solution pour réseaux métropolitains, n'existe qu'en mode commuté.

Dans les faits, le nombre de réseaux Ethernet partagés normalisés est impressionnant. L'encadré ci-dessous en dresse la liste en utilisant la nomenclature IEEE.

Les réseaux Ethernet partagés normalisés

Le groupe de travail indique la technique utilisée : IEEE 802.3 correspond à CSMA/CD ; IEEE 802.3 Fast Ethernet à une extension de CSMA/CD, IEEE 802.9 à une interface CSMA/CD à laquelle on ajoute des canaux B ; IEEE 802.11 à un Ethernet par voie hertzienne, etc. Viennent ensuite la vitesse puis la modulation ou non (base = bande de base et broad = broadband) et enfin un élément complémentaire, qui, à l'origine, était la longueur d'un brin et s'est transformé en type de support physique :

- IEEE 802.3 10Base5 (câble coaxial blindé jaune) ;
- IEEE 802.3 10Base2 (Cheapernet, câble coaxial non blindé brun, Thin Ethernet) ;
- IEEE 802.3 10Broad36 (Ethernet large bande, câble coaxial CATV);
- IEEE 802.3 1Base5 (Starlan à 1 Mbit/s) ;
- IEEE 802.3 10BaseT, Twisted-Pair (paires de fils torsadées) ;
- IEEE 802.3 10BaseF, Fiber Optic (fibre optique) :
  - 10BaseFL, Fiber Link;
  - 10BaseFB, Fiber Backbone;
  - 10BaseFP, Fiber Passive ;
- IEEE 802.3 100BaseT, Twisted-Pair ou encore Fast Ethernet (100 Mbit/s en CSMA/CD) :
  - 100BaseTX ;
  - 100BaseT4 ;
  - 100BaseFX ;
- IEEE 802.3 1000BaseCX (deux paires torsadées de 150 Ω) ;
- IEEE 802.3 1000BaseLX (paire de fibre optique avec une longueur d'onde élevée) ;
- IEEE 802.3 1000BaseSX (paire de fibre optique avec une longueur d'onde courte) ;
- IEEE 802.3 1000BaseT (quatre paires de catégorie 5 UTP) ;
- IEEE 802.9 10BaseM (multimédia) ;
- IEEE 802.11 10BaseX (hertzien).

La norme IEEE 802.12 définit le réseau local 100VG AnyLAN, qui est compatible avec Ethernet. La compatibilité correspond à l'utilisation d'une même structure de trame que dans Ethernet. La technique d'accès, en revanche, n'est pas compatible avec le CSMA/CD, comme nous le verrons à la fin de ce chapitre.

L'architecture de communication classique d'un réseau Ethernet partagé comporte comme épine dorsale un réseau Ethernet sur lequel sont connectés des réseaux locaux de type capillaire.

La figure 14.2 illustre l'architecture générale d'un environnement Ethernet partagé d'entreprise.

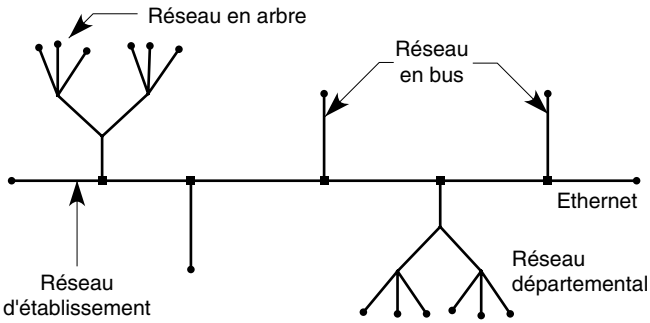


Figure 14.2

Architecture d'un réseau Ethernet partagé d'entreprise

Les réseaux capillaires peuvent être formés à partir du câblage partant du répartiteur d'étage. De plus en plus souvent, les nouveaux bâtiments sont précâblés selon une structure identique à celle du réseau téléphonique à partir du répartiteur d'étage.

Les caractéristiques des câblages utilisés sont les suivantes :

- Câblage banalisé. Un même câble peut être utilisé pour raccorder un combiné téléphonique ou un terminal informatique.
- Câblage non banalisé. Le câble mis en place pour les communications des postes de travail informatiques est différent de celui pour la connexion des combinés téléphoniques.

Caractéristiques

Les caractéristiques des réseaux Ethernet partagés sont décrites dans la norme ISO 8802.3 10Base5.

La topologie d'un réseau Ethernet comprend des brins de 500 m au maximum, interconnectés les uns aux autres par des répéteurs. Ces répéteurs sont des éléments actifs qui récupèrent un signal et le retransmettent après régénération. Les raccordements des matériels informatiques peuvent s'effectuer tous les 2,5 m, ce qui permet jusqu'à 200 connexions par brin. Dans de nombreux produits, les spécifications indiquent que le signal ne doit jamais traverser plus de deux répéteurs et qu'un seul peut être éloigné. La régénération du signal s'effectue une fois franchie une ligne d'une portée de 1 000 m. La longueur maximale est de 2,5 km, correspondant à trois brins de 500 m et un répéteur éloigné (*voir figure 14.3*). Cette limitation de la distance à 2,5 km n'est cependant pas une

caractéristique de la norme. Nous verrons un peu plus loin que l'on peut s'affranchir de ces contraintes de trois répéteurs et atteindre une distance totale de l'ordre de 5 km.

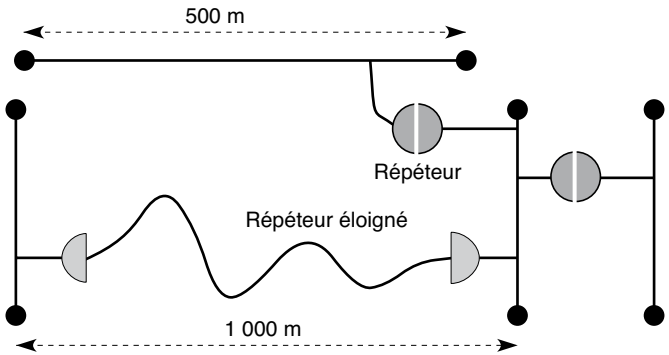


Figure 14.3
Topologie d'Ethernet

La seule contrainte à prendre en compte est le temps maximal qui s'écoule entre l'émission et la réception du signal dans le coupleur le plus éloigné. Ce temps ne doit pas excéder une valeur de 25,6 µs. En effet, lors d'une collision, le temps avant réémission est un multiple de 51,2 µs. Pour éviter une nouvelle collision entre deux trames réémises sur des tranches de temps différentes, il doit s'écouler au maximum 51,2 µs entre le moment de l'émission et celui de l'écoute de la collision. Le temps aller est au maximum de 25,6 µs, si la collision s'effectue juste avant l'arrivée du signal distant. Il faut également 25,6 µs pour remonter la collision jusqu'à la station initiale (*voir figure 14.4*). De plus, la longueur d'une trame doit être au minimum égale au temps aller-retour de façon que l'émetteur puisse enregistrer une collision. Cette longueur minimale est de 64 octets. On retrouve bien 51,2 µs de temps minimal de propagation en remarquant que 64 octets équivalent à 512 bits, qui, à la vitesse de 10 Mbit/s, requièrent un temps d'émission de 51,2 µs.

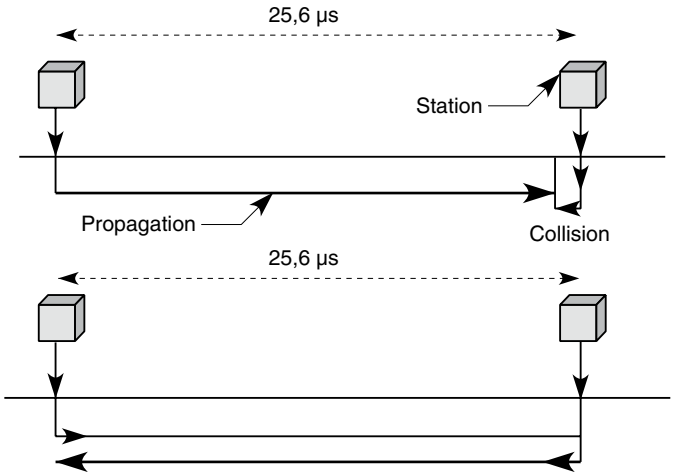


Figure 14.4
Temps maximal entre émission et réception d'une collision

Tout réseau pour lequel le temps aller-retour est inférieur à 51,2 µs est susceptible d'utiliser la norme IEEE 802.3. La vitesse de propagation sur un câble coaxial étant approximativement de 200 000 km/s, la portée maximale sur un même câble est de 5 km environ. Dans la topologie de base, une grande partie du temps de propagation est perdue dans les répéteurs. Pour atteindre des distances supérieures à 4 km, certains câblages utilisent des étoiles optiques passives, qui permettent de diffuser le signal vers plusieurs brins Ethernet sans perte de temps. Dans ce cas, la déperdition d'énergie sur l'étoile optique pouvant atteindre plusieurs décibels, il n'est pas possible d'en émettre plus de deux ou trois en série. On obtient alors la topologie illustrée à la figure 14.5.

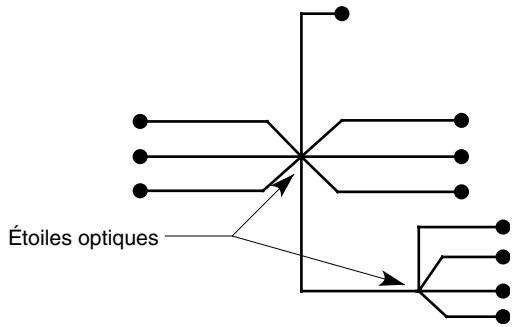


Figure 14.5

Topologie Ethernet avec étoiles optiques

La technique d'accès au support de transmission choisie par Ethernet est l'accès aléatoire avec détection de la porteuse de type persistant. Si le module d'émission-réception détecte la présence d'autres émissions sur le câble, le coupleur Ethernet ne peut émettre de trame.

Si une collision se produit, le module d'émission-réception émet un signal pour interrompre la collision et initialiser la procédure de retransmission. L'interruption de la collision intervient après l'envoi d'une séquence binaire, appelée séquence de bourrage (*jam*), qui vérifie que la durée de la collision est suffisante pour être remarquée par toutes les stations en transmission impliquées dans la collision.

Il est nécessaire de définir plusieurs paramètres pour expliquer la procédure de reprise sur une collision. Le temps aller-retour maximal correspond au temps qui s'écoule entre les deux points les plus éloignés du réseau local, à partir de l'émission d'une trame jusqu'au retour d'un signal de collision. Cette valeur est de 51,2 µs ou de 512 temps d'émission d'un bit, ou encore 512 temps élémentaires. La séquence de bourrage dure 48 temps élémentaires. Ethernet définit encore une « tranche de temps », qui est le temps minimal avant retransmission (51,2 µs). Le temps avant retransmission dépend également du nombre n de collisions déjà effectuées. Le délai aléatoire de retransmission dans Ethernet est un multiple de la tranche de temps $r \leftrightarrow 51{,}2$ µs, où r est un nombre aléatoire tel que $0 \leq r < 2^k$, où $k = \min(n,10)$ et n est le nombre de collisions déjà effectuées. Si, au bout de 16 essais, la trame est encore en collision, l'émetteur abandonne sa transmission. Une reprise s'effectue à partir des protocoles de niveaux supérieurs.

Lorsque deux trames entrent en collision pour la première fois, elles ont une chance sur deux d'entrer de nouveau en collision : $r = 1$ ou 0. Bien que l'algorithme de retransmission, ou de back-off, ne semble pas optimal, c'est la technique qui donne les meilleurs résultats, car il vaut mieux essayer de remplir le support de transmission plutôt que d'attendre des temps trop longs et de perdre en débit.

Un calcul simple montre que les temps de retransmission, après une dizaine de collisions successives, ne représentent que quelques millisecondes, c'est-à-dire un temps encore très court. CSMA/CD étant une technique probabiliste, il est difficile de cerner le temps qui s'écoule entre l'arrivée de la trame dans le coupleur de l'émetteur et le départ de la trame du coupleur récepteur jusqu'au destinataire. Ce temps dépend du nombre de collisions, ainsi que, indirectement, du nombre de stations, de la charge du réseau et de la distance moyenne entre deux stations. Plus le temps de propagation est important, plus le risque de collision augmente.

Tous les calculs rapportés ici se réfèrent à un réseau Ethernet à 10 Mbit/s. Si nous augmentons la vitesse du réseau en multipliant par 10 son débit (100 Mbit/s), la distance maximale entre les deux stations les plus éloignées est également divisée par 10, et ainsi de suite, de telle sorte que nous obtenons en gardant la même longueur minimale de la trame :

- 10 Mbit/s $\Rightarrow$ 5 km
- 100 Mbit/s $\Rightarrow$ 500 m
- 1 Gbit/s $\Rightarrow$ 50 m
- 10 Gbit/s $\Rightarrow$ 5 m

Ces distances s'entendent sans l'existence de répéteurs ou de hubs, qui demandent un certain temps de traversée et diminuent d'autant la distance maximale. Pour contrer ce problème, deux solutions peuvent être mises en œuvre : augmenter la taille de la trame Ethernet ou passer à la commutation. Le réseau Ethernet 1 Gbit/s utilise une trame minimale de 512 octets, qui lui permet de revenir à une distance maximale de 400 m. Le réseau à 10 Gbit/s n'utilise que la commutation.

Performance d'un réseau Ethernet 10 Mbit/s

De nombreuses courbes de performances montrent le débit réel en fonction du débit offert, c'est-à-dire le débit provenant des nouvelles trames additionné du débit provoqué par les retransmissions. La figure 14.6 illustre le débit réel en fonction du débit offert.

On peut montrer qu'un dysfonctionnement se produit dès que le débit offert dépasse une certaine limite, en raison de collisions de plus en plus nombreuses. Pour éviter ce type de problème sur un réseau Ethernet, il faut que le débit instantané soit inférieur à 5 Mbit/s. Pour obtenir cette valeur maximale, on limite le nombre de stations à plusieurs centaines de PC ou à plusieurs dizaines de postes de travail. Ce sont les chiffres le plus souvent cités.

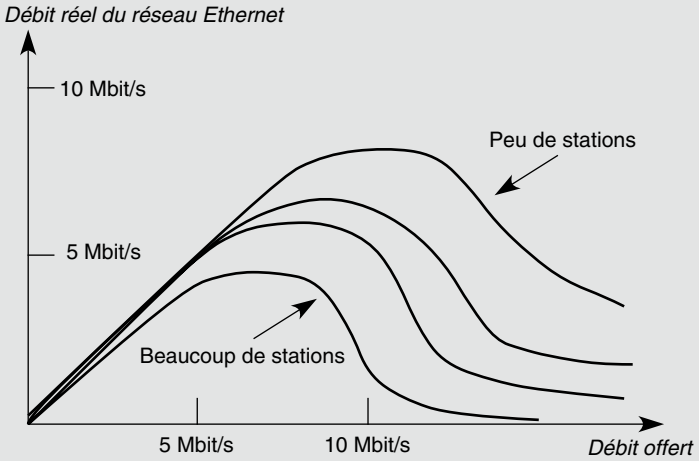


Figure 14.6

Performance du réseau Ethernet

Pour résoudre les problèmes de débit, une solution consiste à réaliser un ensemble de réseaux Ethernet interconnectés par des passerelles. À la différence du répéteur, la passerelle est un organe intelligent, capable de sélectionner les trames qui doivent être émises vers les réseaux suivants. La passerelle doit gérer un adressage. Elle limite de ce fait le débit sur chaque réseau. On obtient dans ce cas des topologies sans contrainte de distance. La passerelle peut être de différents types. Il s'agit d'un pont lorsqu'on a uniquement un problème d'adresse physique à résoudre. On parle alors de pont filtrant pour filtrer les trames qui passent. Les trames destinées à une station située sur le même réseau sont stoppées, tandis que les autres trames sont réémises vers le réseau suivant.

L'exemple traité sur 10 Mbit/s est également valable pour l'ensemble des technologies Ethernet à plus haut débit. La solution pour ne pas tomber sur des problèmes de saturation est naturellement de passer à la gamme supérieure dès que nécessaire. Comme, au-delà de 1 Gbit/s, le contrôle des débits devient complexe, les réseaux Ethernet à 10 Gbit/s et 100 Gbit/s n'existent plus en partagé : ils n'utilisent que la commutation.

L'accès aléatoire

L'accès aléatoire, qui consiste à émettre à un instant totalement aléatoire, s'appuie sur la méthode aloha. Cette dernière tient son nom d'une expérience effectuée sur un réseau reliant les diverses îles de l'archipel hawaïen au début des années 1970. Dans cette méthode, lorsqu'un coupleur a de l'information à transmettre, il l'envoie, sans se préoccuper des autres usagers. S'il y a collision, c'est-à-dire superposition des signaux de deux ou plusieurs utilisateurs, les signaux deviennent indéchiffrables et sont perdus. Ils sont retransmis ultérieurement, comme illustré à la figure 14.7, sur laquelle les coupleurs 1, 2 et 3 entrent en collision. Le coupleur 1 retransmet sa trame en premier parce qu'il a tiré le plus petit temporisateur. Ensuite, le coupleur 2 émet, et ses signaux entrent en collision avec le coupleur 1. Tous deux retirent un temps aléatoire de retransmission. Le coupleur 3

vient écouter alors que les coupleurs 1 et 2 sont silencieux, de telle sorte que la trame du coupleur 3 passe avec succès. La technique aloha est à l'origine de toutes les méthodes d'accès aléatoire.

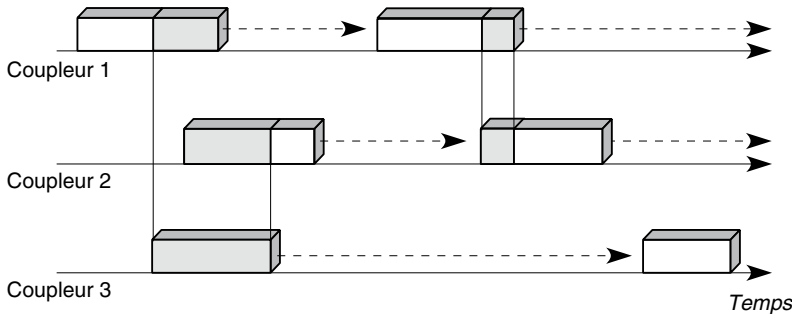


Figure 14.7

Principe de fonctionnement de l'aloha pur

Outre son extrême simplicité, l'aloha a l'avantage de ne nécessiter aucune synchronisation et d'être complètement décentralisé. Son principal inconvénient réside dans la perte d'informations résultant d'une collision et dans son manque d'efficacité, puisque la transmission des trames en collision n'est pas interrompue.

Le débit d'un tel système devient très faible dès que le nombre de coupleurs augmente. On peut démontrer mathématiquement que si le nombre de stations tend vers l'infini, le débit devient nul. À partir d'un certain moment, le système n'est plus stable. Afin de diminuer la probabilité de conflit entre les usagers, diverses améliorations de cette technique ont été proposées (*voir encadré*).

Slotted aloha, ou aloha en tranches

Une amélioration de la technique aloha a consisté à découper le temps en tranches de temps, ou slots, et à n'autoriser l'émission de trames qu'en début de tranche, le temps de transmission d'une trame demandant exactement une tranche de temps. De la sorte, il n'y a pas de collision si une seule trame transmet en début de tranche. En revanche, si plusieurs trames commencent à émettre en début de tranche, les émissions de trames se superposent tout le long du slot. Dans ce dernier cas, il y a retransmission après un temps aléatoire.

Cette méthode améliore le débit pendant la période de démarrage mais reste instable. De plus, on constate un coût supplémentaire provenant d'une complication des appareils, puisque toutes les émissions doivent être synchronisées.

CSMA, ou l'accès aléatoire avec écoute de la porteuse

La technique CSMA (Carrier Sense Multiple Access) consiste à écouter le canal avant d'émettre. Si le coupleur détecte un signal sur la ligne, il diffère son émission à une date ultérieure. Cela réduit considérablement les risques de collision, sans toutefois les

supprimer complètement. Si, durant le temps de propagation entre le couple de stations les plus éloignées (période de vulnérabilité), un coupleur ne détecte pas l'émission d'une trame, il peut y avoir superposition de signaux. De ce fait, il faut réémettre ultérieurement les trames perdues.

De nombreuses variantes de cette technique ont été proposées, qui diffèrent par trois caractéristiques :

- La stratégie suivie par le coupleur après détection de l'état du canal.
- La manière dont les collisions sont détectées.
- La politique de retransmission des messages après collision.

Ses principales variantes sont les suivantes :

- CSMA non persistant. Le coupleur écoute le canal lorsqu'une trame est prête à être envoyée. Si le canal est libre, le coupleur émet. Dans le cas contraire, il recommence le même processus après un délai aléatoire.
- CSMA persistant. Un coupleur prêt à émettre écoute préalablement le canal et transmet s'il est libre. S'il détecte l'occupation de la porteuse, il continue à écouter jusqu'à ce que le canal soit libre et émet à ce moment-là. Cette technique permet de perdre moins de temps que dans le cas précédent, mais elle a l'inconvénient d'augmenter la probabilité de collision, puisque les trames qui s'accumulent pendant la période occupée sont toutes transmises en même temps.
- CSMA p-persistant. L'algorithme est le même que précédemment, mais, lorsque le canal devient libre, le coupleur émet avec la probabilité p. En d'autres termes, le coupleur diffère son émission avec la probabilité 1 – p. Cet algorithme réduit la probabilité de collision. En supposant que deux terminaux souhaitent émettre, la collision est inéluctable dans le cas standard. Avec ce nouvel algorithme, il y a une probabilité 1 – p que chaque terminal ne transmette pas, ce qui évite la collision. En revanche, il augmente le temps avant transmission, puisqu'un terminal peut choisir de ne pas émettre, avec une probabilité 1 – p, alors que le canal est libre.
- CSMA/CD (Carrier Sense Multiple Access/Collision Detection). Cette technique d'accès aléatoire normalisée par le groupe de travail IEEE 802.3 est actuellement la plus utilisée. À l'écoute préalable du réseau s'ajoute l'écoute pendant la transmission. Un coupleur prêt à émettre ayant détecté le canal libre transmet et continue à écouter le canal. Le coupleur persiste à écouter, ce qui est parfois indiqué par le sigle CSMA/CD persistant. S'il se produit une collision, il interrompt dès que possible sa transmission et envoie des signaux spéciaux, appelés bits de bourrage, afin que tous les coupleurs soient prévenus de la collision. Il tente de nouveau son émission ultérieurement suivant un algorithme que nous présenterons ultérieurement.

  La figure 14.8 illustre le CSMA/CD. Dans cet exemple, les coupleurs 2 et 3 tentent d'émettre pendant que le coupleur 1 émet sa propre trame. Les coupleurs 2 et 3 se mettent à l'écoute et émettent en même temps, au délai de propagation près, dès la fin de la trame Ethernet émise par le coupleur 1. Une collision s'ensuit. Comme les coupleurs 2 et 3 continuent d'écouter le support physique, ils se rendent compte de la collision,

arrêtent leur transmission et tirent un temps aléatoire pour démarrer le processus de retransmission.

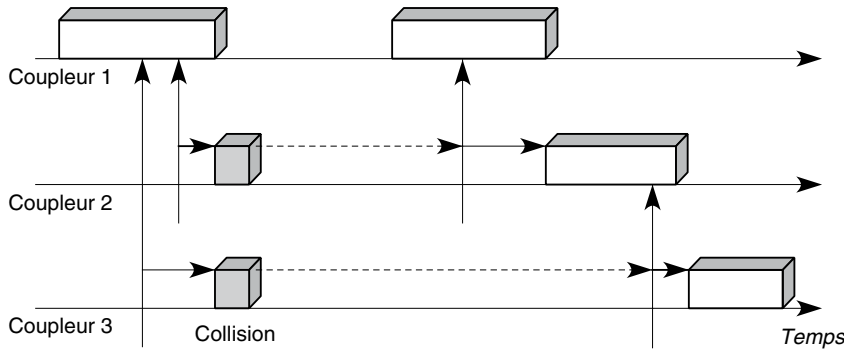


Figure 14.8

Principe de fonctionnement du CSMA/CD

Le CSMA/CD engendre un gain d'efficacité par rapport aux autres techniques d'accès aléatoire car il y a détection immédiate des collisions et interruption de la transmission en cours. Les coupleurs émetteurs reconnaissent une collision en comparant le signal émis avec celui qui passe sur la ligne. Les collisions ne sont donc plus reconnues par absence d'acquittement mais par détection d'interférences. Cette méthode de détection des conflits est relativement simple, mais elle nécessite des techniques de codage suffisamment performantes pour reconnaître facilement une superposition de signaux. On utilise généralement pour cela des techniques de codage différentiel, tel le code Manchester différentiel.

- CSMA/CA. Moins connu que le CSMA/CD, l'accès CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) commence à être fortement utilisée dans les réseaux Wi-Fi, c'est-à-dire les réseaux Ethernet sans fil IEEE 802.11 (*voir le chapitre 24*). C'est une variante du CSMA/CD, qui permet à la méthode CSMA de fonctionner lorsque la détection des collisions n'est pas possible, comme dans le hertzien. Son principe de fonctionnement consiste à résoudre la contention avant que les données soient transmises en utilisant des accusés de réception et des temporisateurs.

  Les coupleurs désirant émettre testent le canal à plusieurs reprises afin de s'assurer qu'aucune activité n'est détectée. Tout message reçu doit être immédiatement acquitté par le récepteur. L'envoi de nouveaux messages n'a lieu qu'après un certain délai, de façon à garantir un transport sans perte d'information. Le non-retour d'un accusé de réception, au bout d'un intervalle de temps prédéterminé, permet de détecter s'il y a eu collision. Cette stratégie rend non seulement possible l'implémentation d'un mécanisme d'acquittement au niveau trame mais présente l'avantage d'être simple et économique, puisqu'elle ne nécessite pas de circuit de détection de collision, contrairement au CSMA/CD.

Il existe diverses techniques de CSMA avec résolution des collisions, parmi lesquelles le CSMA/CR (Carrier Sense Multiple Access/Collision Resolution). Certaines variantes du CSMA utilisent par ailleurs des mécanismes de priorité pouvant entrer sous ce vocable, qui évitent les collisions par des niveaux de priorité distincts, associés aux différentes stations connectées au réseau.

Les réseaux Ethernet commutés

Nous avons décrit en détail à la section précédente les techniques utilisées dans les réseaux Ethernet partagés, dans lesquels un même câble est partagé par plusieurs machines.

L'autre solution mise en œuvre dans les réseaux Ethernet est la commutation. Dans ce cas, le support physique n'est pas partagé, deux machines s'échangeant des trames Ethernet sur une liaison. Cette solution change totalement la donne, puisqu'il n'y a plus de collision.

La commutation Ethernet, ou Ethernet FDSE (Full Duplex Switched Ethernet), est née au début des années 1990. Avant l'arrivée de l'Ethernet commuté, les réseaux Ethernet partagés étaient découpés en sous-réseaux partagés autonomes, reliés entre eux par des ponts. De ce fait, on multipliait le trafic par le nombre de sous-réseaux.

Les ponts ne sont en fait que des commutateurs Ethernet qui mémorisent les trames et les réémettent vers d'autres réseaux Ethernet. En poursuivant cette logique à l'extrême, on peut découper le réseau jusqu'à n'avoir qu'une seule station par réseau Ethernet. On obtient alors la commutation Ethernet.

Le réseau Ethernet FDSE est un réseau particulièrement simple puisqu'il n'y a que deux stations : celle que l'on veut connecter au réseau et le commutateur de raccordement. On dispose donc d'un Ethernet par terminal relié directement au commutateur.

En commutation, chaque carte Ethernet est reliée directement à un commutateur Ethernet, lequel se charge de rediriger les trames dans la bonne direction. La commutation demande une référence qui, *a priori,* n'existe pas dans le monde Ethernet, aucun paquet de supervision n'ouvrant le chemin en posant des références. Le mot de commutateur peut donc être considéré comme inexact puisqu'il n'y a pas de référence. Cependant, il est possible de parler de commutation, si l'on considère l'adresse du destinataire comme une référence. Le chemin est alors déterminé par la suite de références égale à l'adresse du destinataire sur 6 octets. Pour réaliser cette commutation de bout en bout, chaque commutateur doit avoir la possibilité de déterminer la liaison de sortie en fonction de la référence, c'est-à-dire de la valeur de l'adresse du récepteur.

Cette technique de commutation peut présenter les difficultés suivantes :

- Gestion des adresses de tous les coupleurs raccordés au réseau. Les techniques de VLAN, que nous examinons en détail au chapitre 25, permettent de résoudre ce problème.
- Gestion des congestions éventuelles au sein d'un commutateur.

Du fait de la seconde difficulté, il faut mettre en place des techniques de contrôle susceptibles de prendre en charge, sur les liaisons entre commutateurs, les trames provenant simultanément de tous les coupleurs Ethernet. On retrouve là les caractéristiques des

architectures des réseaux de commutation. La limitation de distance n'existant plus, on peut réaliser des réseaux en commutation Ethernet à la taille de la planète.

L'environnement Ethernet s'impose actuellement par sa simplicité de mise en œuvre tant que le réseau reste de taille limitée. C'est une solution réseau qui présente l'avantage de s'appuyer sur l'existant, à savoir les cartes Ethernet présentes dans toutes mes machines terminales et les divers réseaux Ethernet que de nombreuses entreprises ont mis en place pour créer leurs réseaux locaux.

L'inconvénient de la commutation de niveau trame réside dans l'adressage de niveau 2, qui correspond à l'adressage plat d'Ethernet. L'adressage plat, ou absolu, ne permet pas de connaître l'emplacement géographique d'une carte Ethernet d'après sa valeur. Dès que le réseau comporte un grand nombre de postes, ce qui est le cas si l'on accepte une mobilité des terminaux, par exemple, la mise à jour des tables de commutation (look-up table) devient quasi impossible puisqu'il n'existe pas de normalisation pour l'automatisation de cette fonction pour un grand réseau. La commutation Ethernet que nous avons vue au chapitre 6 n'est utilisable que dans de petits réseaux.

La limitation des performances de l'environnement Ethernet est due au partage du support physique par l'ensemble des cartes Ethernet. Pour remédier à cet inconvénient, on peut augmenter la vitesse de base en passant au 100 Mbit/s ou au 1 Gbit/s. Une autre solution consiste à commuter les trames Ethernet. Le premier pas vers la commutation consiste, comme nous l'avons vu, à couper les réseaux Ethernet en petits tronçons et à les relier entre eux par un pont. Le rôle du pont est de filtrer les trames en ne laissant passer que celles destinées à un réseau Ethernet autre que celui d'où provient la trame. De ce fait, on limite le nombre de cartes Ethernet qui se partagent un même réseau. Pour que cette solution soit viable, le trafic doit être relativement local.

Dans la commutation, suivant l'adresse, le commutateur achemine la trame vers un autre commutateur ou vers une carte Ethernet. La capacité disponible par terminal est de 10 Mbit/s, 100 Mbit/s ou 1 Gbit/s, voire 10 Gbit/s et même 40 et 100 Gbit/s. Toute la difficulté réside dans la complexité des réseaux à commutation de trames Ethernet, avec les problèmes d'ouverture des chemins et de contrôle de flux qu'ils posent.

Une seconde solution de commutation Ethernet se répand rapidement au travers des techniques MPLS et Ethernet Carrier Grade. Il s'agit de réseaux Ethernet destinés aux opérateurs de télécommunications. Dans le premier cas, on ajoute une nouvelle zone dans la trame Ethernet pour porter la référence qui n'est plus l'adresse Ethernet de destination. Dans le second cas, on utilise le champ VLAN (Virtual LAN) que nous allons voir pour introduire un chemin. Ces deux solutions sont explicitées dans la suite.

Ethernet pour les entreprises

Nous décrivons dans cette section les réseaux Ethernet d'entreprise. Nous traiterons plus loin des réseaux Ethernet des opérateurs.

Le premier exemple de réseaux Ethernet à 10 Mbit/s est important car il conditionne les réseaux Ethernet suivants. Dès que toutes les cartes d'un réseau assurent le 100 Mbit/s, le

réseau possède automatiquement cette vitesse. En revanche, tant qu'il reste dans le réseau une carte à 10 Mbit/s, même si ce 10 Mbit/s n'est quasiment plus utilisé, le réseau tourne à 10 Mbit/s.

Les réseaux Ethernet 10/100 Mbit/s

Les réseaux Ethernet à 10 Mbit/s ont été les premiers à être introduits sur le marché. Ils sont aujourd'hui remplacés par les réseaux à 10/100 Mbit/s, qui s'adaptent automatiquement aux 100 Mbit/s dès qu'il n'existe plus de carte Ethernet à 10 Mbit/s sur le réseau. Cet encadré examine les différents produits de l'Ethernet partagé à 10/100 Mbit/s.

Cheapernet

Cheapernet est un réseau local Ethernet partagé utilisant un câble coaxial particulier, normalisé sous le vocable 10Base2/100Base2.. Le câble coaxial utilisé n'est plus le câble jaune blindé mais un câble fin de couleur brune non blindé, aussi appelé *thin cable* ou câble RG-58. Ce câble a une moindre résistance au bruit électromagnétique et induit un affaiblissement plus important du signal.

Nous ne traitons dans la suite que le cas de l'Ethernet 10 Mbit/s. Le cas 100 Mbit/s s'en déduit en divisant par 10 les valeurs obtenues. Les brins de l'Ethernet 10 Mbit/s sont limités à 185 m. Les répéteurs sont de type Ethernet et travaillent à 10 Mbit/s. La longueur totale peut atteindre 925 ou 1 540 m suivant les versions. Les contraintes sont les mêmes que pour le réseau Ethernet en ce qui concerne le temps aller-retour. En revanche, pour obtenir une qualité comparable, il faut limiter la distance sans répéteur. La longueur maximale a ici moins d'importance, car le réseau Cheapernet est un réseau capillaire permettant d'aller jusqu'à l'utilisateur final à moindre coût.

Starlan

Né d'une étude d'AT&T sur la qualité du câblage téléphonique à partir du répartiteur d'étage, le réseau Starlan répond à une tout autre nécessité que le réseau Cheapernet. Sur les réseaux capillaires de l'entreprise, des débits de 1 Mbit/s étaient acceptables dans les années 1980. L'arrivée de Starlan correspondait à la volonté d'utiliser cette infrastructure capillaire, c'est-à-dire le câblage téléphonique, à partir du répartiteur d'étage (*voir figure 14.9*).

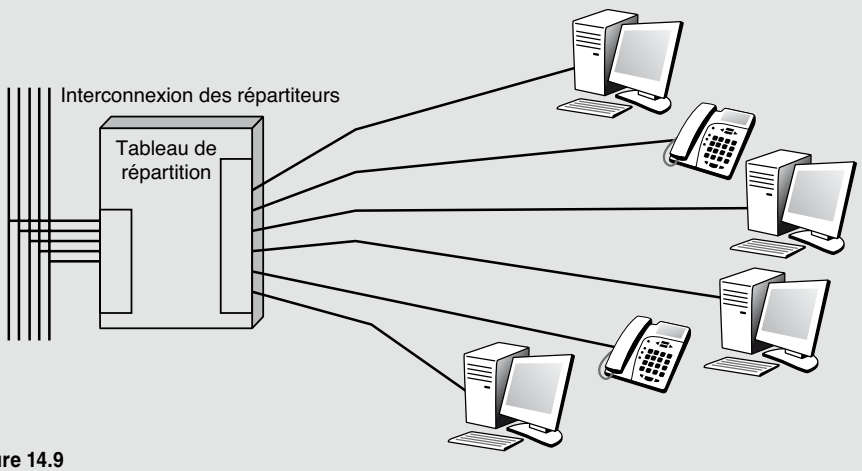


Figure 14.9
Câblage à partir du répartiteur d'étage

Comme les câbles à partir du répartiteur d'étage ne permettaient guère qu'un débit de 1 Mbit/s, on a repris la technique Ethernet en l'adaptant à un câblage en étoile à une vitesse de 1 Mbit/s. C'est toujours la méthode d'accès CSMA/CD qui est utilisée sur un réseau en étoile actif, comme celui illustré à la figure 14.10. La vitesse de 1 Mbit/s a rapidement été remplacée par une solution à 10 Mbit/s.

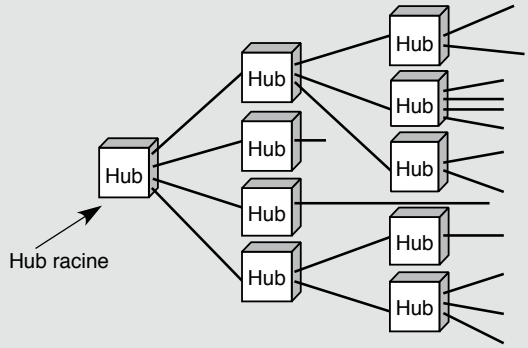


Figure 14.10
Architecture d'un réseau Starlan

Étant donné le grand nombre d'entreprises qui ont renouvelé leur câblage avec des paires de fils de qualité, le Starlan à 10 Mbit/s a rencontré un succès massif. Les réseaux Starlan à 10 Mbit/s portent aussi le nom d'Ethernet 10 Mbit/s sur paires de fils torsadées pour bien indiquer que le coupleur est le même que celui des réseaux Ethernet sur câble coaxial à 10 Mbit/s. La double vitesse 10/100 s'est imposée dans les années 1990. Nous ne traitons dans la suite que le cas de base à 1 Mbit/s, mais le cas de 10 Mbit/s s'en déduit facilement.

La norme Starlan IEEE 802.3 1Base5 permet de disposer d'un maximum de cinq nœuds, ou hubs, successifs à partir du nœud de base inclus. Entre deux nœuds, une distance maximale de 250 m est permise. Dans la réalité, on retrouve exactement les mêmes contraintes que dans le réseau Ethernet, c'est-à-dire un temps aller-retour maximal de 512 µs entre les deux points les plus éloignés. Pour le réseau local Starlan à 10 Mbit/s, on retrouve la valeur de 51,2 µs.

Le hub est un nœud actif capable de régénérer les signaux reçus vers l'ensemble des lignes de sortie, de telle sorte qu'il y ait diffusion. Le hub permet de raccorder les équipements terminaux situés aux extrémités des branches Starlan.

Classiquement, à chaque équipement correspond une prise de connexion Starlan. Cependant, pour ajouter un terminal supplémentaire dans un bureau, il faudrait tirer un câble depuis le répartiteur d'étage ou le sous-répartiteur le plus proche, à condition qu'existe encore une sortie possible. Une solution de rechange consiste à placer sur une même prise plusieurs machines connectées en série, comme illustré la figure 14.11.

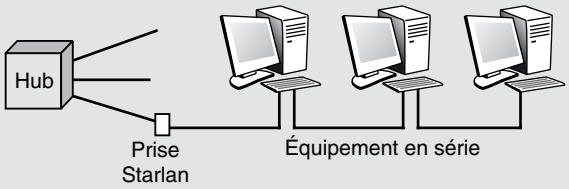


Figure 14.11
Équipements en série connectés sur une prise Starlan unique

Le Fast Ethernet 100 Mbit/s

Fast Ethernet est la dénomination de l'extension à 100 Mbit/s du réseau Ethernet à 10 Mbit/s. C'est le groupe de travail IEEE 802.3u qui en est à l'origine. La technique d'accès est la même que dans la version Ethernet 10 Mbit/s, mais à une vitesse multipliée par 10. Les trames transportées sont identiques. Cette augmentation de vitesse peut se heurter au système de câblage et à la possibilité ou non d'y faire transiter des débits aussi importants.

C'est la raison pour laquelle trois sous-normes ont été proposées pour le 100 Mbit/s :

- IEEE 802.3 100BaseTX, qui requiert deux paires non blindées (UTP) de catégorie 5 ou deux paires blindées (STP) de type 1.
- IEEE 802.3 100BaseT4, qui requiert quatre paires non blindées (UTP) de catégories 3, 4 et 5.
- IEEE 802.3 100BaseFX, qui requiert deux fibres optiques.

La distance maximale entre les deux points les plus éloignés est fortement réduite par rapport à la version à 10 Mbit/s. La longueur minimale de la trame étant toujours de 64 octets, le temps de transmission est de 5,12 µs. On en déduit que la distance maximale qui peut être parcourue dans ce laps de temps est de l'ordre de 1 000 m, ce qui représente pour le réseau Fast Ethernet une longueur maximale d'approximativement 500 m. Comme le temps de traversée des hubs est relativement important, la plupart des constructeurs limitent la distance maximale à 210 m pour le Fast Ethernet. Le temps entre deux trames, ou intergap, est réduit à 0,96 µs.

Cette solution a l'avantage d'offrir une bonne compatibilité avec la version à 10 Mbit/s, qui permet de relier sur un même hub des stations à 10 Mbit/s et à 100 Mbit/s. Le coût de connexion du 100 Mbit/s est aujourd'hui le même que celui de l'Ethernet classique, dix fois moins rapide.

Les réseaux Fast Ethernet servent souvent de réseaux d'interconnexion de réseaux Ethernet 10 Mbit/s. La distance relativement limitée couverte par le Fast Ethernet ne lui permet toutefois pas d'« arroser » une entreprise un peu grande. Le Gigabit Ethernet, que nous détaillons ci-après, ne résout pas davantage ce problème dans sa version partagée. En revanche, la version commutée n'ayant plus de contrainte de distance, le Gigabit Ethernet commuté est une des solutions d'interconnexion des réseaux Fast Ethernet.

Une autre solution pour étendre la couverture du réseau Ethernet consiste à relier des Fast Ethernet par des ponts destinés à filtrer les trames à l'aide de l'adresse MAC. Ces ponts ayant les mêmes fonctionnalités que les commutateurs, on trouve aujourd'hui dans les grandes entreprises des réseaux à transfert de trames Ethernet qui utilisent des commutateurs Ethernet. Nous examinons ces architectures ultérieurement dans ce chapitre.

Le Gigabit Ethernet (GbE)

Le Gigabit Ethernet, ou GbE, est une évolution du standard Ethernet. Plusieurs améliorations ont été apportées pour cela au Fast Ethernet à 100 Mbit/s.

L'interface à nouveau modifiée s'appelle GMII (Gigabit Media Independent Interface). Elle comporte un chemin de données sur 8 bits, au lieu de 4 dans la version moins puissante. Les émetteurs-récepteurs travaillent avec une horloge cadencée à 125 MHz. Le codage adopté provient des produits Fibre Channel pour atteindre le gigabit par seconde. Un seul type de répéteur est désormais accepté dans cette nouvelle version.

Les différentes solutions normalisées sont les suivantes :

- 1000BaseCX, à deux paires torsadées de 150 Ω ;
- 1000BaseLX, à une paire de fibre optique de longueur d'onde élevée ;
- 1000BaseSX, à une paire de fibre optique de longueur d'onde courte ;
- 1000BaseT, à quatre paires de catégorie 5 UTP.

La technique d'accès au support physique, le CSMA/CD, est également modifiée. Pour être compatible avec les autres versions d'Ethernet, ce qui est un principe de base, la taille de la trame émise doit se situer entre 64 et 1 500 octets. Les 64 octets, c'est-à-dire 512 bits, correspondent à un temps d'émission de 512 ns. Ce temps de 512 ns représente la distance maximale du support pour qu'une station en émission ne se déconnecte pas avant d'avoir reçu un éventuel signal de collision. Cela représente 100 m pour un aller-retour. Si aucun hub n'est installé sur le réseau, la longueur maximale du support physique est de 50 m. Dans les faits, avec un hub de rattachement et des portions de câble jusqu'aux coupleurs, la distance maximale est ramenée à quelques mètres. Pour éviter cette distance trop courte, les normalisateurs ont augmenté artificiellement la longueur de la trame pour la porter à 512 octets. Si la longueur de la trame à transmettre est inférieure à 512 octets, le coupleur ajoute des octets de bourrage qui sont ensuite enlevés par le coupleur récepteur.

S'il s'agit d'une bonne solution pour agrandir le réseau Gigabit, le débit utile est toutefois très faible si toutes les trames à transmettre ont une longueur de 64 octets, un huitième de la bande passante étant utilisé dans ce cas. C'est en particulier le cas pour transporter de la téléphonie sur IP (ToIP), où les octets utiles de téléphonie sont au nombre de 16. Dans ce cas, il faut effectuer un bourrage des trames de 64 octets.

Le Gigabit Ethernet accepte les répéteurs ou les hubs lorsqu'il y a plusieurs directions possibles. Dans ce dernier cas, un message entrant est recopié sur toutes les lignes de sortie. La figure 14.12 illustre un répéteur Gigabit correspondant à la norme IEEE 802.3z. Les différentes solutions du Gigabit Ethernet peuvent s'interconnecter par l'intermédiaire d'un répéteur ou d'un hub.

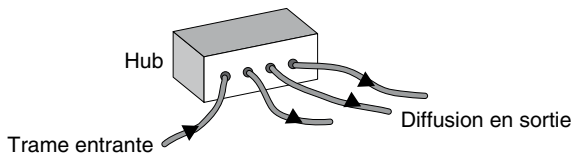


Figure 14.12
Hub Gigabit Ethernet

Le Gigabit Ethernet fonctionne également en mode commuté, dans une configuration full-duplex. On peut, par ce moyen, interconnecter des Gigabit Ethernet entre eux ou des Fast Ethernet et des Ethernet classiques.

Des routeurs Gigabit sont également disponibles lorsqu'on remonte jusqu'à la couche réseau IP. Dans ce cas, il faut récupérer le paquet IP pour effectuer un routage en utilisant l'adresse IP qui se trouve dans le paquet à transporter à l'intérieur de la trame Ethernet. La figure 14.13 illustre une interconnexion de deux réseaux commutés par un routeur Gigabit.

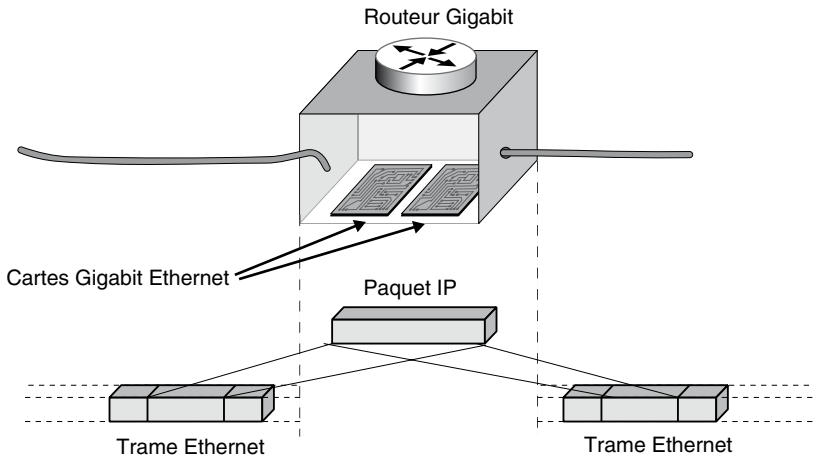


Figure 14.13

Interconnexion de deux réseaux Ethernet commutés par un routeur

La gestion du réseau Gigabit, comme celle des réseaux Ethernet plus anciens, est assurée par des techniques classiques, essentiellement SNMP (Simple Network Management Protocol). La MIB (Management Information Base) du Gigabit Ethernet est détaillée dans le standard IEEE 802.3z.

Le 10 Gigabit Ethernet (10GbE)

Le 10Gigabit Ethernet, ou 10GbE, est une évolution du standard Ethernet qui n'est surpassée que par la version 100GbE (100 Gbit/s). Cette technique est fortement utilisée dans les réseaux métropolitains et d'opérateurs. Il s'agit d'une solution assez simple, car il suffit de multiplexer dix réseaux GbE pour multiplier la vitesse par dix.

Le 10 Gigabit Ethernet, ou 10GbE a été normalisé par le groupe de travail IEEE 802.3ae, dans l'objectif de proposer deux types de solutions, toutes deux en full-duplex et en commutation. La distance va de 65 m avec des fibres multimodes jusqu'à 40 km avec de la fibre optique monomode. Les deux types d'interfaces proposées sont LAN-PHY et WAN-PHY.

Le groupe IEEE 802.3ae a normalisé dans le LAN PHY un flux à la vitesse de 10,312 5 Gbit/s avec un codage 64B/66B. L'interface WAN-PHY utilise le même codage, mais avec une compatibilité avec les interfaces SONET OC-192 et SDH STM-64.

L'architecture proposée par ce groupe de travail est illustrée à la figure 14.14.

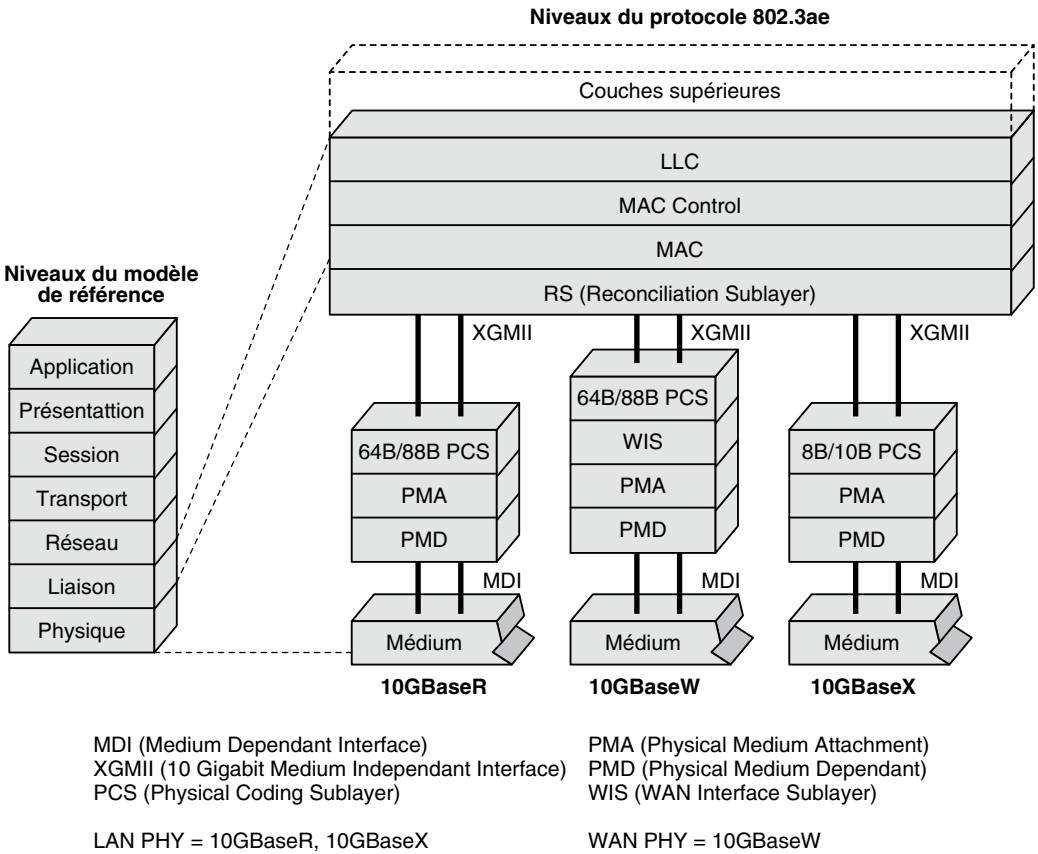


Figure 14.14

Architecture des réseaux 10GbE

Le groupe de travail de l'IEEE incorpore une interface compatible SONET mais qui reste Ethernet. Comme expliqué précédemment, cette interface implique l'existence d'un support physique 10GbE, appelé WAN PHY, qui équivaut au support SONET/SDH de type OC-192 ou STM-64. L'avantage de cette compatibilité est de permettre de reprendre tout l'environnement de gestion et de maintenance ainsi que la fiabilisation de SONET/SDH. Cette solution a été défendue par la 10GEA (10 Gigabit Ethernet Alliance).

Le 100 Gigabit Ethernet (100GbE)

Le 100 Gigabit Ethernet, ou 100GbE, est la dernière évolution du standard Ethernet. Cette solution a été proposée par le NG Ethernet Forum, dont l'objectif est de définir l'environnement Ethernet de nouvelle génération *(http://www.ng-ethernet.com/)*. Le standard a été finalisé et voté en juin 2010 par le groupe IEEE 802.3ba, d'ailleurs avec une version à 40 Gbit/s (40GbE).

Les 40GbE et 100GbE sont des extensions naturelles en mode commuté du 10GbE. Il utilise une technologie CWDM (Coarse WDM) avec 10 et 25 longueurs d'onde (*voir chapitre 12*). Plusieurs niveaux physiques ont été normalisés qui doivent être choisis en fonction de la distance à atteindre. Les principaux niveaux sont :

- sur câble métallique : 10 mètres à 40 Gbit/s
- sur fibre multimode : 100 mètres à 100 Gbit/s
- sur fibre monomode : 40 kilomètres à 100 Gbit/s.

Ethernet pour les opérateurs

Ethernet devenant le standard de transport des paquets IP, du fait de la forte coopération entre IP et Ethernet, tous les opérateurs implémentent Ethernet à la place d'ATM. La solution Ethernet est tout à fait compatible avec MPLS puisque l'Ethernet commuté utilise un shim-label, ou référence, au fonctionnement classique, entrant parfaitement dans ce cadre. L'autre solution pour les opérateurs provient de l'Ethernet Carrier Grade.

Les solutions Ethernet actuelles permettent de mettre en place cette technologie dans de nombreux contextes, allant du réseau métropolitain au réseau étendu. Les débits vont de 1 à 100 Gbit/s. Les options les plus importantes concernent les solutions suivantes :

- Les réseaux virtuels Ethernet, pour que l'utilisateur ait l'impression que le réseau distant est relié au réseau de l'entreprise par un réseau local Ethernet.
- Les réseaux métropolitains, avec la poussée du MEF (Metropolitan Ethernet Forum).
- La possibilité de gérer des boucles haut débit à forte fiabilité, comme sur SONET, avec la norme RPR (Resilient Packet Ring), normalisée par le groupe de travail IEEE 802.17. Cette solution a été présentée au chapitre 13.
- MPLS Ethernet Forwarding, que nous examinerons au chapitre suivant.
- Ethernet Carrier Grade.

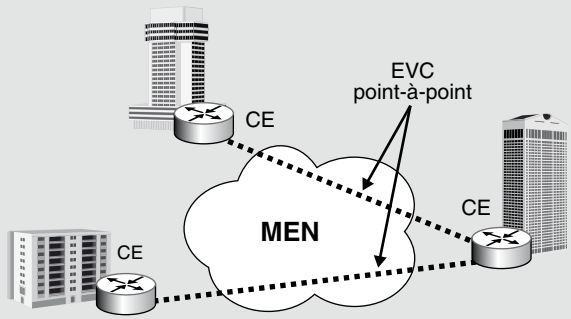
Les connexions virtuelles Ethernet

La figure 14.15 illustre un réseau d'opérateur Ethernet utilisant un réseau privé virtuel Ethernet construit à partir d'EVC (Ethernet Virtual Connection). Grâce à cette solution, les VPN-IP ou MPLS sont parfaitement compatibles avec le monde Ethernet.

Un EVC peut être soit point-à-point, soit point-à-multipoint, soit encore multipoint-à-multipoint. Un réseau privé virtuel Ethernet peut donc avoir toutes les propriétés des VPN classiques mais avec une efficacité supérieure, puisque le système se trouve au niveau 2, et à un coût bien inférieur grâce aux matériels Ethernet utilisés.

Figure 14.15

Réseau privé virtuel Ethernet à base d'EVC



CE (Customer Equipment) : équipement client
MEN (Metropolitan Ethernet Network)

Nous présenterons les solutions sous-jacentes de VLAN (Virtual LAN) au chapitre 25 étant donné leur importance dans les réseaux d'entreprise et d'opérateur.

Les réseaux Ethernet MEF

Les réseaux MEF (Metropolitan Ethernet Forum) sont connus depuis longtemps. Ils ont pour objectif d'interconnecter les réseaux d'entreprise dans une même métropole à très haut débit. Les techniques utilisées ont été décrites au chapitre 14. Elles utilisent les réseaux Ethernet commutés à 1, 10, 40 et 100 Gbit/s.

Pour réaliser de la téléphonie sur IP et des services nécessitant des contraintes temporelles fortes, les réseaux d'opérateurs Ethernet permettent d'introduire des priorités, à cette différence près que le champ IEEE 802.1p, qui sert à l'introduction de ces priorités, n'a que 3 bits. Ces 3 bits ne permettent que 8 niveaux de priorités, à comparer aux 14 niveaux définis par l'IETF pour les services DiffServ.

Les niveaux de priorités proposés par le MEF sont les suivants :

- 802.1p-6 DiffServ Expedited Forwarding.
- 802.1p-5/4/3 DiffServ Assured Forwarding.
- 802.1p-5, qui présente la perte la plus faible.
- 802.1p-3, qui présente la perte la plus forte.
- 802.1p-2 DiffServ Best Effort.

Dans l'environnement Ethernet, le contrôle de flux est généralement un problème délicat. Diverses propositions ont été faites pour l'améliorer. En particulier, les méthodes de backpressure proposent l'envoi de messages de contrôle de la part des commutateurs surchargés, qui permettent aux commutateurs connexes de stopper leur émission vers le nœud congestionné pendant un temps indiqué dans la primitive de contrôle.

Le choix effectué par le MEF est un contrôle de type relais de trames, où l'on retrouve exactement les mêmes paramètres :

- CIR (Committed Information Rate)
- CBS (Committed Burst Size)
- PIR (Peak Information Rate)

- MBS (Maximum Burst Size)

Ces différentes propositions montrent que le monde Ethernet est en train de grignoter petit à petit des parts de marché et devrait devenir la technologie numéro un des opérateurs de réseau dans un avenir qui se rapproche.

Ethernet Carrier Grade

Ethernet a été conçu pour les applications informatiques, non pour les applications multimédias. Pour se mettre à niveau et entrer dans le domaine du multimédia, l'environnement Ethernet a donc dû se transformer. On parle d'Ethernet Carrier Grade, c'est-à-dire acceptable pour les opérateurs de télécommunications avec les outils de contrôle et de gestion nécessaires dans ce cas. Cette mutation concerne essentiellement l'Ethernet commuté.

L'Ethernet Carrier Grade doit posséder des fonctionnalités que l'on trouve dans les réseaux de télécommunications, notamment les suivantes :

- La fiabilité, qui permet de n'avoir que très peu de pannes. Le temps moyen entre pannes, ou MTBF (Mean Time Between Failure), doit être d'au moins 50 000 heures.
- La disponibilité, qui doit atteindre les valeurs classiques pour la téléphonie, c'est-à-dire être en état de marche 99,999 % du temps. Cette valeur est loin d'être atteinte par les réseaux Ethernet classiques, qui sont plutôt à 99,9 % du temps.
- La protection et la restauration. Lorsqu'une panne se produit, le système doit pouvoir se remettre en marche au bout d'un temps maximal de 50 ms. Cette durée provient de la téléphonie, qui n'accepte des coupures que sur des intervalles de temps inférieurs à cette valeur. Les réseaux SONET, par exemple, atteignent cette valeur de temps de reconfiguration. Les solutions sont généralement la redondance, totale ou partielle, qui permet de mettre en route un autre chemin, prévu à l'avance, en cas de coupure.
- L'optimisation des performances par un monitoring actif ou passif. Les performances ne sont pas toutes homogènes lorsque les flots de paquets varient. Il faut donc adapter les flots pour qu'ils puissent transiter sans problème.
- Le réseau doit pouvoir accepter les SLA (Service Level Agreement). Le SLA est une notion typique d'un réseau d'opérateur lorsqu'un client veut négocier une garantie de service. Le SLA est déterminé par une partie technique, le SLS (Service Level Specification), et une partie administrative dans laquelle sont négociées les pénalités si le système ne donne pas satisfaction.
- La gestion est aussi une fonctionnalité importante des réseaux d'opérateurs. En particulier, des systèmes de détection de pannes et des signalisations doivent être disponibles pour que le réseau soit en état de marche.

Du point de vue technique, l'Ethernet Carrier Grade est une extension de la technologie VLAN. Un VLAN est un réseau local dans lequel les machines peuvent se trouver en des points très éloignés. L'objectif est de faire fonctionner ce réseau comme si tous les points étaient géographiquement proches les uns des autres pour former un réseau local. Un VLAN peut avoir plusieurs utilisateurs. Chaque trame Ethernet est émise en diffusion à

l'ensemble des machines du VLAN. Les tables qui effectuent le routage des trames sont fixes et peuvent être vues comme des tables de commutation dans lesquelles les adresses des destinataires sont des références.

Lorsque le VLAN n'a que deux points, l'émission d'une trame Ethernet d'un point vers l'autre s'apparente à une commutation sur un chemin. C'est cette vision qui a été retenue dans l'Ethernet Carrier Grade. On forme des chemins en déterminant des VLAN. Le chemin est unique et simple si le VLAN n'a que deux point et en multipoint s'il y a plus de deux points.

Le problème de cette solution vient de la taille limitée de la zone VLAN, qui n'autorise que douze éléments binaires. Cela convenait dans le cadre d'un réseau d'entreprise avec une commutation Ethernet standard, mais devenait tout à fait insuffisant dans le cadre de l'Ethernet Carrier Grade, qui vise les réseaux d'opérateurs. Il a donc fallu augmenter la taille du champ VLAN.

On peut subdiviser l'Ethernet Carrier Grade en plusieurs solutions d'extension de la zone VLAN, toutes décrites à la figure 14.16. La solution la plus classique consiste à utiliser la norme IEEE 802.1ad, qui est connue sous plusieurs nom : Ethernet PB (Provider Bridge), QiQ (Q in Q) ou VLAN en cascade. La norme IEEE 802.1ah, aussi connue sous les noms de MiM (MAC-in-MAC) ou PBB (Provider Backbone Bridge). La solution la plus avancée est appelée PBT (Provider Backbone Transport), ou encore PW over PBT (pseudowire). Elle permet de revenir pour le transport à une solution classique dans laquelle les trames Ethernet sont commutées suivant une succession de références correspondant à MPLS-SL (Service Label).

Sur la figure 14.16, ces solutions sont comparées à la solution MPLS PW PBT, qui utilise à la fois la solution PBT et la solution MPLS.

Considérons dans un premier temps la technologie Ethernet PB (Provider Bride). Le fournisseur d'accès Internet ajoute un numéro de VLAN à celui du client. Il y a donc deux numéros de VLAN : le C-VID (Customer-VLAN ID) et le S-VID (Service- VLAN ID). Le pont du fournisseur de service permet d'étendre la notion de VLAN au réseau de l'opérateur sans détruire le VLAN de l'utilisateur. Cette solution permet de définir les diffusions à effectuer dans le réseau de l'opérateur. Comme le champ de la trame Ethernet, dans lequel le numéro de VLAN est indiqué, possède une longueur de 12 bits, cela permet de définir jusqu'à 4 094 entités du réseau de l'opérateur. Ces entités peuvent être des services, des tunnels ou des domaines de diffusion. Cependant, si 4 094 est une valeur suffisante en entreprise, elle reste très inférieure aux besoins d'un opérateur. Des implémentations jouent sur une translation de référence pour agrandir le domaine, mais cela augmente la complexité de gestion de l'ensemble. Cette solution ne convient donc pas aux réseaux importants.

La solution proposée par le groupe IEEE 802.1ah PBB (Provider Backbone Bridge) améliore la précédente en commutant le trafic de trames sur l'adresse MAC. Cette solution, dite MIM (MAC-in-MAC), encapsule l'adresse MAC du client dans une adresse MAC de l'opérateur. Cela permet à l'opérateur cœur de ne connaître que ses adresses MAC. Dans le réseau PBB, la correspondance des adresses MAC utilisateur et MAC réseau n'est connue que par les nœuds de bord, évitant l'explosion des adresses MAC.

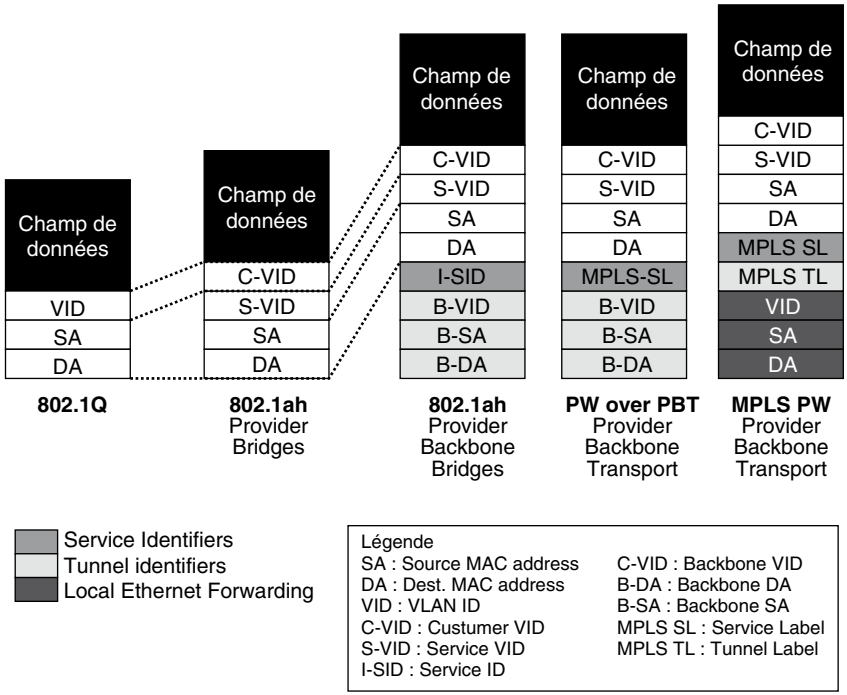


Figure 14.16

Technologies de l'Ethernet Carrier Grade

La troisième solution, appelée PBT (Provider Backbone Transport), est assez proche de la technique MPLS, tout en fournissant les propriétés nécessaires au Carrier Grade, comme un taux d'indisponibilité de moins de 50 ms. Il s'agit en quelque sorte d'un tunnel MPLS secouru. Le tunnel PBT est créé comme un tunnel MPLS, avec les références correspondant aux extrémités du réseau. Les numéros de VLAN client et serveur sont encapsulés dans le tunnel MPLS, lequel peut lui-même posséder une différentiation en VLAN opérateur. La référence réelle est donc de 24 bits + 48 bits, soit 72 bits.

La dernière solution est celle du service PS (pseudowire) de MPLS. Dans ce cas, les VLAN utilisateur et opérateur sont encapsulés dans un tunnel de service MPLS, qui peut lui-même être encapsulé dans un tunnel de transport MPLS. Cette solution provient de l'encapsulation de tunnels dans MPLS.

La technologie Ethernet Carrier Grade intéresse de nombreux opérateurs. L'avenir dira quelle sera la solution gagnante. Mais il est d'ores et déjà certain que l'encapsulation de VLAN dans des VLAN sera présente dans chacune d'elles.

Les extensions d'Ethernet

Ethernet est à la fois une norme ancienne et une norme du futur : ancienne, par les techniques de réseau local, et du futur, grâce à la commutation et à son application aux réseaux métropolitains et étendus mais aussi à la boucle locale, aux réseaux électriques, sans fil, etc.

Ethernet dans la boucle locale

La boucle locale consiste à relier les utilisateurs au premier nœud, routeur ou commutateur, de l'opérateur chez lequel le client possède un abonnement. Les solutions à haut débit se partagent entre l'ATM et Ethernet mais depuis 2010 toutes les nouvelles connexions sont Ethernet.

On comprend tout de suite l'intérêt de cette solution, qui offre une continuité avec la machine terminale, laquelle possède généralement une carte Ethernet. L'équipement terminal est la plupart du temps connecté par Ethernet au modem *x*DSL ou câble haut débit. Pourquoi changer de technologie, c'est-à-dire décapsuler le paquet IP qui a été introduit dans une trame Ethernet pour le mettre dans une trame ATM ? Les solutions les plus simples auraient été soit de mettre directement une carte ATM dans le PC, soit d'utiliser des modems Ethernet à la place de modems ATM.

Le groupe de travail EFM (Ethernet in the First Mile) a proposé pour cela la norme IEEE 802.3ah, qui comporte trois types de topologies et de supports physiques :

- point-à-point en paires torsadées à une vitesse de 10 Mbit/s sur une distance de 750 m ;
- point-à-point en fibre optique à une vitesse de 1 Gbit/s sur une distance de 10 km ;
- point-à-multipoint en fibre optique à une vitesse de 1 Gbit/s sur une distance de 10 km.

La norme précise les procédures d'administration et de maintenance pour les extrémités et la ligne elle-même. Ces procédures permettent de faire remonter les pannes et de monitorer les paramètres de la liaison.

Le VDSL (Very high bit rate DSL), équivalent des modems *x*DSL pour les hautes vitesses, est également compatible avec Ethernet et offre une continuité complète à haut débit du poste de travail émetteur jusqu'au poste de travail récepteur par le biais de modems EFM.

PoE (Power over Ethernet)

Un inconvénient majeur des équipements réseau, et des équipements Ethernet en particulier, vient de la nécessité de les alimenter électriquement. En cas de coupure de courant, le réseau s'arrête et peut mettre en difficulté l'entreprise. Une solution qui s'impose de plus en plus est l'auto-alimentation des équipements réseau par l'intermédiaire du câblage lui-même.

Le groupe de travail IEEE 802.3af propose d'alimenter électriquement les équipements Ethernet par le câble Ethernet lui-même. Les équipements peuvent être aussi bien des commutateurs du réseau que des points d'accès Wi-Fi ou d'autres équipements réseau qui se branchent sur une prise Ethernet. L'avantage de cette solution est de sécuriser les alimentations électriques des serveurs raccordés au réseau électrique et donc tous les autres équipements raccordés au serveur.

Les sources électriques peuvent être de deux types : end-span, dans lequel un serveur particulier dessert l'ensemble du réseau, et mid-span, où plusieurs équipements se partagent l'alimentation des autres équipements réseau. Les fils métalliques peuvent être de catégorie 3 avec 4 fils ou 5/6 avec 8 fils, c'est-à-dire quatre paires de fils. Deux solutions sont utilisées pour transporter le 48 volts vers les équipements qui en ont besoin : soit l'alimentation utilise deux paires tandis que les deux autres paires sont dédiées aux données, soit les paires sont mixtes lorsqu'il n'y a que deux paires, l'électricité et le courant étant portés sur des fréquences différentes.

La solution PoE est illustrée à la figure 14.17, où plusieurs équipements réseau (téléphone IP, point d'accès, accès Bluetooth, webcam) sont directement alimentés au travers d'Ethernet. L'équipement UPS (Uninterruptable Power Supply) peut être ajouté pour éviter les coupures de courant.

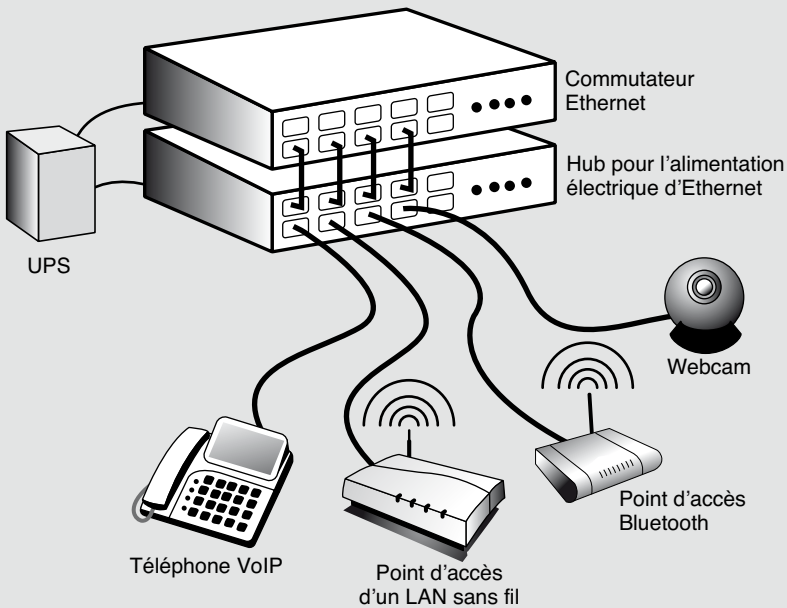


Figure 14.17

Architecture de l'alimentation électrique PoE

Une autre vision d'Ethernet est le transport des trames directement sur les câbles électriques. Cette solution se développe fortement dans le cadre de la domotique, où les particuliers peuvent connecter directement leur carte coupleur Ethernet sur leurs nombreuses prises électriques (*voir le chapitre 11*).

La commutation de cellules

L'ATM introduit une technique de commutation utilisant un circuit virtuel pour acheminer les cellules, qui ne sont autres que des trames ATM, d'une extrémité à l'autre du réseau.

La commutation de cellules est une commutation de trames assez particulière, puisque toutes les trames sont de longueur constante, cette longueur étant toute petite. La cellule est formée d'exactement 53 octets, comprenant 5 octets d'en-tête et 48 octets de données.

La cellule ATM est une trame et non un paquet. Pour retrouver le début et la fin de cette trame lors d'une transmission, il suffit de compter jusqu'à 424 bits pour déterminer la fin de la trame, le bit suivant correspondant nécessairement au début de la trame suivante. La

difficulté de cette méthode de transmission, que nous préciserons plus loin, concerne la resynchronisation lorsqu'une erreur se produit et que le comptage des éléments binaires est perturbé.

Circuit virtuel et conduit virtuel

Le champ suivant contient la référence composée de l'identificateur de voie virtuelle et de l'identificateur de conduit virtuel, VCI/VPI (Virtual Channel Identifier/Virtual Path Identifier). Le rôle des conduits virtuels est de fournir des connexions semi-permanentes.

Le circuit virtuel (VC), la connexion de circuit virtuel (VCC), le conduit virtuel (VP) et la connexion de conduit virtuel (VPC) se définissent comme suit :

- Le circuit virtuel, ou VC (Virtual Channel), est un terme générique utilisé pour décrire la capacité de communication pour le transport des cellules ATM. Un identificateur de circuit virtuel, ou VCI, classiquement appelé référence de commutation, est affecté à une liaison de VC qui transporte des cellules ATM entre deux nœuds ATM. Le nœud ATM, dans lequel la valeur VCI est traduite, s'appelle aussi un commutateur ATM.
- La connexion de circuit virtuel, ou VCC (Virtual Channel Connection), définit la connexion de bout en bout entre les deux points d'accès à la couche AAL. Une VCC est composée de la concaténation d'un ou plusieurs VC.
- Le conduit virtuel, ou VP (Virtual Path), est un faisceau de VC. Tous les VC d'un faisceau ont les mêmes nœuds extrémité.
- La connexion de conduit virtuel, ou VPC (Virtual Path Connection), est composée de la concaténation d'un ou plusieurs VP. Le nœud ATM est alors appelé un brasseur.

La figure 14.18 illustre la hiérarchie VP/VC et la figure 14.19 des exemples de VPC et de VCC. Le parcours d'une connexion VPC est établi par un routage de l'acheminement dans les brasseurs intermédiaires (A, B et C pour VP1 à la figure 14.19).

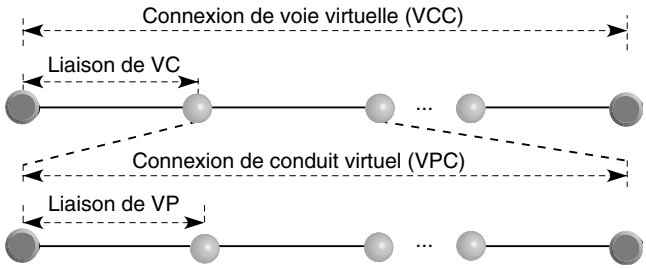


Figure 14.18

Hiérarchie de liaison des VC, VCC, VP et VPC

Les nœuds de la partie supérieure de la figure 14.19 sont des commutateurs. Les brasseurs ne participent pas à l'administration de la bande passante des conduits virtuels.

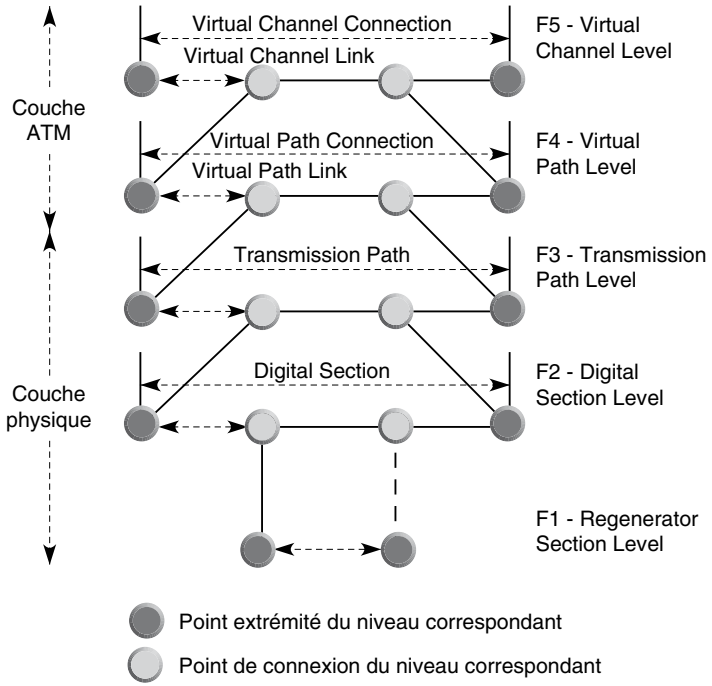


Figure 14.19

Brasseurs et commutateurs ATM

L'architecture en couches de l'ATM

Les réseaux à commutation de cellules suivent les principes d'une nouvelle architecture, où les fonctionnalités ne sont pas regroupées aux mêmes niveaux que dans le modèle de référence.

La couche physique de ce nouveau modèle correspond à la couche physique du modèle de référence, mais avec une différence importante : la couche physique regroupe les bits par 424 pour retrouver directement la structure de la trame. La couche physique effectue donc un transport 424 bits par 424 bits et non bit par bit. Cette propriété permet à la couche du dessus d'appartenir au niveau trame puisque le début et la fin du bloc de données ont été déterminés par la couche physique. Nous verrons que la troisième couche du modèle ATM est de niveau message, avec également des différences importantes. L'architecture ATM est illustrée à la figure 14.20.

Le rôle de ce nouveau modèle, dit modèle UIT-T, est de prendre en charge les applications multimédias, c'est-à-dire la superposition de la voix, des données et de l'image. Le modèle de référence de l'ISO n'était bâti que pour les applications de données et correspondait donc à l'architecture des réseaux d'ordinateurs.

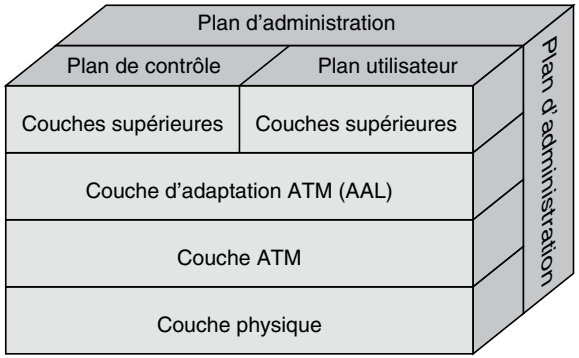


Figure 14.20

Architecture ATM (modèle de référence UIT-T)

Le modèle UIT-T ne s'intéresse qu'au transport de bout en bout de l'information, et non à son traitement aux extrémités du réseau. Il est constitué de trois couches : la couche prenant en charge le transport des cellules sur un support physique, la couche se préoccupant de l'acheminement des cellules de bout en bout et la couche chargée de l'interface avec les couches supérieures et regroupant les cellules pour les délivrer à l'utilisateur.

La couche la plus basse concerne les protocoles de niveau physique dépendant du médium, ou PMD (Physical Medium Dependent). Cette couche PMD est elle-même divisée en deux sous-couches :

- La couche TC (Transmission Convergence), chargée du découplage du taux de transmission des cellules, de la génération et de la vérification de la zone de détection d'erreur de l'en-tête, le HEC, de la délimitation des cellules, de l'adaptation de la vitesse de transmission et de la génération et de la récupération des cellules sur le support physique.
- La couche PM (Physical Medium), chargée de la transmission sur le support physique et des problèmes d'horloge.

Le protocole PMD décrit la façon dont les cellules sont émises sur le support physique. Plusieurs solutions ont été définies pour cela, dont les plus couramment implémentées reposent sur l'utilisation de SONET (Synchronous Optical NETwork) et de SDH (Synchronous Digital Hierarchy), normalisées par l'UIT-T. SONET décrit la structure d'une trame synchrone émise toutes les 125 µs. La longueur de cette trame dépend de la vitesse de l'interface. Les diverses valeurs des connexions SONET sont classées suivant la rapidité du support optique, ou OC (Optical Carrier).

La deuxième couche est celle de l'ATM proprement dite. Cette couche gère le transport de bout en bout de la cellule.

Enfin, la couche AAL (ATM Adaptation Layer), ou couche d'adaptation à l'ATM, se charge de l'interface avec les couches supérieures. Cet étage est lui-même subdivisé en deux niveaux, l'un prenant en compte les problèmes liés directement à l'interfonctionnement

avec la couche du dessus, et l'autre ceux concernant la fragmentation et le réassemblage des messages en cellules. Dans cette couche AAL, quatre classes de services (A, B, C et D) ont été définies. Elles sont décrites au tableau 14.1. À ces quatre classes de services correspondaient quatre classes de protocoles, numérotées de 1 à 4. Cette subdivision en quatre classes de protocole a été modifiée en 1993 par le regroupement des classes 3 et 4 et par l'ajout d'une nouvelle classe de protocoles, la classe 5, qui définit un transport de données simplifié.

	Classe A	Classe B	Classe C	Classe D
Synchro. source récepteur	Forte		Faible	
Flux	Constant	Variable		
Type de connexion	Orienté connexion			Sans connexion

TABLEAU 14.1 • Classes de services de la couche AAL

La première classe de services correspond à une émulation de circuit, la deuxième au transport d'une application synchrone mais dont le débit est variable, la troisième à un transfert de données en mode avec connexion et la dernière à un transfert de données en mode sans connexion.

L'annexe K décrit les protocoles associés à ces différentes classes.

Conclusion

Les réseaux Ethernet dominent le marché des réseaux d'entreprise depuis de nombreuses années. Ces réseaux ne font qu'accentuer leur avance, et, bientôt, pratiquement 100 % des réseaux d'entreprise seront Ethernet.

Face à un tel succès, le groupe de travail 802 de l'IEEE multiplie les offensives vers d'autres directions, comme les réseaux sans fil, pour lesquels l'Ethernet sans fil est devenu le principal standard.

Des réseaux métropolitains Ethernet sont déjà commercialisés, et leur succès ne fait aucun doute. Les réseaux d'opérateurs sont également en train de passer à la technologie Ethernet. Plusieurs solutions existent pour cela, dont MPLS Ethernet Forwarding et l'Ethernet Carrier Grade.

15

MPLS et GMPLS

MPLS (MultiProtocol Label-Switching)

MPLS est une norme proposée par l'IETF, l'organisme de normalisation d'Internet, pour l'ensemble des architectures et des protocoles de haut niveau, dont il ne reste aujourd'hui que le protocole IP. Les nœuds de transfert spécifiques utilisés dans MPLS sont appelés LSR (Label Switch Router). Les LSR se comportent comme des commutateurs pour les flots de données utilisateur et comme des routeurs pour la signalisation. Pour acheminer les trames utilisateur, on utilise des références, ou *labels*. À une référence d'entrée correspond une référence de sortie. La succession des références définit le chemin suivi par l'ensemble des trames contenant les paquets du flot IP.

Toute trame utilisée en commutation, ou label-switching, peut être utilisée dans un réseau MPLS. La référence est placée dans un champ spécifique de la trame ou dans un champ ajouté dans ce but.

Les LSR remplacent les routeurs en travaillant soit en mode routeur, pour tracer le chemin par la signalisation, soit en mode commutation, pour toutes les trames qui suivent le chemin tracé. Le chemin est déterminé par le mode IP et donc par un algorithme de routage d'Internet.

La solution de routage-commutation de cette technique est illustrée aux figures 15.1 et 15.2. La première suppose que la trame du niveau trame est ATM et la suivante que la trame du niveau paquet est Ethernet. Il faut noter que, dans le cas de la solution ATM, le paquet IP à transporter est découpé dans la couche AAL (ATM Adaptation Layer) en 48 octets pour être encapsulé dans la trame ATM. Cette étape n'existe pas dans le monde Ethernet, et c'est une des raisons pour laquelle on préfère très largement commuter des trames Ethernet qu'ATM.

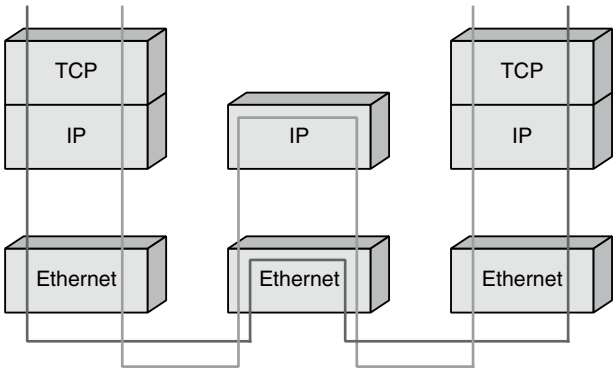


Figure 15.1
TCP/IP sur ATM en MPLS

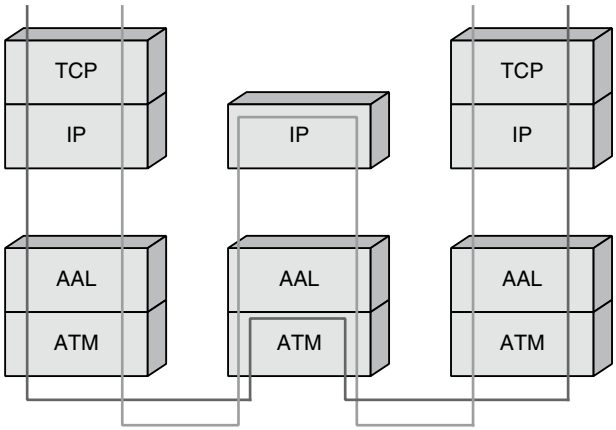


Figure 15.2
Architecture d'un environnement IP sur Ethernet

Cette architecture est dictée par l'environnement Ethernet, qui brille par sa simplicité de mise en œuvre. Elle a l'avantage de s'appuyer sur l'existant, les coupleurs et les divers réseaux Ethernet, que de nombreuses sociétés ont mis en place pour créer leurs réseaux locaux.

Puisque les données produites au format IP, IPX ou autre sont placées dans des trames Ethernet afin d'être transportées dans l'environnement local, il est tentant de commuter directement les trames Ethernet d'un réseau local vers un autre. Comme tous les réseaux de l'environnement Ethernet sont compatibles et parlent le même langage, les machines émettant des trames Ethernet peuvent s'interconnecter facilement. On peut ainsi réaliser des réseaux extrêmement complexes avec des segments partagés sur les parties locales, des liaisons commutées sur les longues distances ou entre les commutateurs Ethernet et des passages par des routeurs lorsqu'une remontée jusqu'au niveau IP est exigée.

Caractéristiques

MPLS est l'aboutissement logique de toutes les propositions qui ont été faites dans les années 1990. L'idée de l'IETF a été de rassembler les propositions en une norme commune pour transporter des paquets IP sur des sous-réseaux travaillant en mode commuté. Les nœuds sont des routeurs-commutateurs, ou LSR (Label Switch Router), capables de remonter soit au niveau IP pour effectuer un routage, soit au niveau trame pour effectuer une commutation.

Les caractéristiques les plus importantes de la norme MPLS sont les suivantes :

- Spécification des mécanismes pour transporter des flots de paquets IP avec diverses granularités des flots entre deux points, deux machines ou deux applications. La granularité désigne la grosseur du flot, qui peut intégrer plus ou moins de flots utilisateur.
- Indépendance du niveau trame et du niveau paquet, bien que seul le transport de paquets IP soit réellement pris en compte.
- Mise en relation de l'adresse IP du destinataire avec une référence d'entrée dans le réseau.
- Reconnaissance par les routeurs de bord des protocoles de routage de type OSPF et de signalisation comme RSVP.
- Utilisation de différents types de trames.

Quelques propriétés supplémentaires méritent d'être soulignées :

- Ouverture du chemin fondée sur la topologie, bien que d'autres possibilités soient également définies dans la norme.
- Assignation des références faite par l'aval, c'est-à-dire à la demande d'un nœud qui émet un message dans la direction de l'émetteur.
- Granularité variable des références.
- Stock de références géré selon la méthode « dernier arrivé premier servi ».
- Possibilité de hiérarchiser les demandes.
- Utilisation d'un temporisateur TTL.
- Encapsulation d'une référence dans la trame incluant un TTL et une qualité de service.

Un avantage apporté par le protocole MPLS est la possibilité, illustrée à la figure 15.3, de transporter les paquets IP sur plusieurs types de réseaux commutés. Il est ainsi possible de passer d'un réseau ATM à un réseau Ethernet. En d'autres termes, il peut s'agir de n'importe quel type de trame, à partir du moment où une référence peut y être incluse. Nous verrons plus loin comment ajouter une référence lorsque la trame ne le prévoit pas. L'avantage de cette solution est la migration simple d'anciennes technologies vers de nouvelles, comme d'ATM à Ethernet, assez simplement.

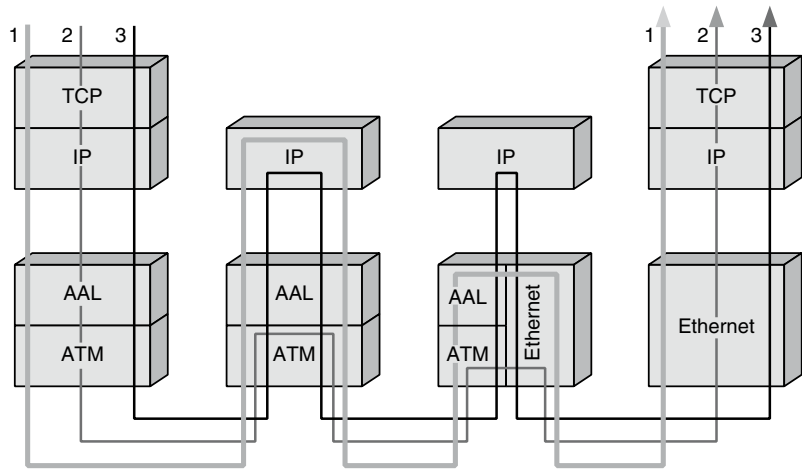


Figure 15.3

Réseau MPLS avec des sous-réseaux distincts

Fonctionnement

La transmission des données s'effectue sur des chemins, nommés LSP (Label Switched Path). Un LSP est une suite de références partant de la source et allant jusqu'à la destination. Les LSP sont établis avant la transmission des données (control-driven) ou à la détection d'un flot qui souhaite traverser le réseau (data-driven).

Les références incluses dans les trames sont distribuées en utilisant un protocole de signalisation. Le plus important de ces protocoles est LDP (Label Distribution Protocol), mais on utilise aussi RSVP (Resource reSerVation Protocol), éventuellement associé à un protocole de routage, comme BGP (Border Gateway Protocol) ou OSPF. Les trames acheminant les paquets IP transportent les références de nœud en nœud.

LSR et LER

Les nœuds qui participent à MPLS sont classifiés en LER (Label Edge Router) et LSR. Un LSR est un routeur dans le cœur du réseau qui participe à la mise en place du chemin par lequel les trames sont acheminées. Un LER est un nœud d'accès au réseau MPLS. Un LER peut avoir des ports multiples permettant d'accéder à plusieurs réseaux distincts, chacun pouvant avoir sa propre technique de commutation. Les LER jouent un rôle important dans la mise en place des références.

LSR

Un équipement qui effectue une commutation sur une référence s'appelle un LSR. Les tables de commutation LSFT (Label Switching Forwarding Table) consistent en un ensemble de références d'entrée auxquelles correspondent des ports de sortie. À une référence d'entrée peuvent correspondre plusieurs ports de sortie pour tenir compte des adresses multipoint.

Les tables de commutation peuvent être plus complexes. À une référence d'entrée peuvent correspondre le port de sortie du nœud dans une première sous-entrée mais aussi, dans une deuxième sous-entrée, un deuxième port de sortie correspondant à la file de sortie du prochain nœud qui sera traversé, et ainsi de suite. De la sorte, à une référence peuvent correspondre un ensemble de ports de sortie qui seront empruntés lors de l'acheminement du paquet.

Les tables de commutation peuvent être spécifiques de chaque port d'entrée d'un LSR et regrouper des informations supplémentaires, comme une qualité de service ou une demande spécifique de ressources.

FEC (Forwarding Equivalence Class)

Dans MPLS, le routage s'effectue par l'intermédiaire de classes d'équivalence, appelées FEC. Une classe représente un flot ou un ensemble de flots ayant les mêmes propriétés, notamment le même préfixe dans l'adresse IP. Toutes les trames d'une FEC sont traitées de la même manière dans les nœuds du réseau MPLS. Les trames sont introduites dans une FEC au nœud d'entrée et ne peuvent plus être distinguées à l'intérieur de la classe des autres flots.

Une FEC peut être bâtie de différentes façons. Elle peut avoir une adresse de destination bien déterminée, un même préfixe d'adresse, une même classe de service, etc. Chaque LSR possède une table de commutation qui indique les références associées aux FEC. Toutes les trames d'une même FEC sont transmises sur la même interface de sortie. Cette table de commutation est appelée LIB (Label Information Base).

Les références utilisées par les FEC peuvent être regroupées de deux façons :

- Par plate-forme : les valeurs des références sont uniques sur l'ensemble des LSR d'un domaine, et les références sont distribuées sur un ensemble commun géré par un nœud particulier.
- Par interface : les références sont gérées par interface, et une même valeur de référence peut se retrouver sur deux interfaces différentes.

MPLS et les références

Une référence en entrée permet donc de déterminer la FEC par laquelle transite le flot. Cette solution ressemble à la notion de conduit virtuel dans le monde ATM, où les circuits virtuels sont multiplexés. Ici, nous avons un multiplexage de tous les circuits virtuels à l'intérieur d'une FEC, de telle sorte que, dans ce conduit, nous ne puissions plus distinguer les circuits virtuels.

Le LSR examine la référence et envoie la trame dans la direction indiquée. On voit bien ainsi le rôle capital joué par les LER, qui assignent aux flots de paquets des références qui permettent de commuter les trames sur le bon circuit virtuel. La référence n'a de signification que localement, puisqu'il y a modification de sa valeur sur la liaison suivante.

Une fois le paquet classifié dans une FEC, une référence est assignée à la trame qui va le transporter. Cette référence détermine le point de sortie par le chaînage des références. Dans le cas des trames classiques, comme LAP-F du relais de trames ou ATM, la référence est positionnée dans le DLCI (Data Link Connection Identifier) ou dans le VPI/VCI.

La signalisation nécessaire pour déposer la valeur des références le long du chemin déterminé pour une FEC peut être gérée soit à chaque flot (data-driven), soit par un environnement de contrôle indépendant des flots utilisateur. Cette dernière solution est préférable dans le cas de grands réseaux du fait de ses capacités de passage à l'échelle.

Les références peuvent être distribuées pour :

- un routage unicast vers une destination particulière ;
- une gestion du trafic, ou TE (Traffic Engineering) ;
- un multicast ;
- un réseau privé virtuel ;
- une qualité de service.

Le format de la référence MPLS est illustré à la figure 15.4. La référence est encapsulée dans l'en-tête de niveau trame du champ normalisé pour transporter la référence ou juste entre l'en-tête de niveau trame et l'en-tête de niveau paquet.

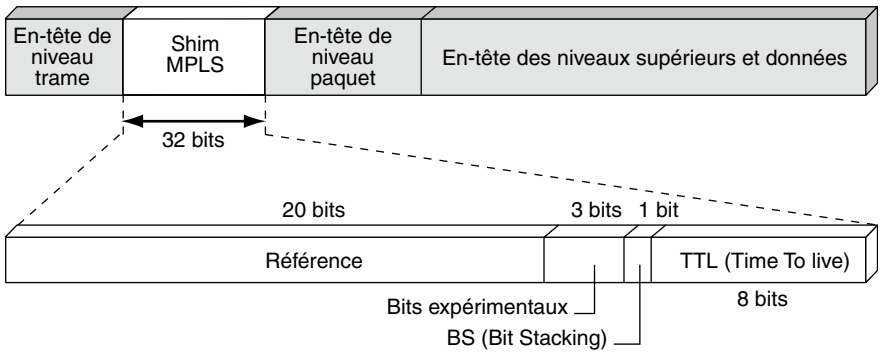


Figure 15.4

Format générique d'une référence dans MPLS

Les figures 15.5 et 15.6 illustrent la mise en place de la référence dans le cas d'ATM et la figure 15.7 concerne le cas où la trame n'est pas conçue au départ pour un label-switching, comme la trame PPP.

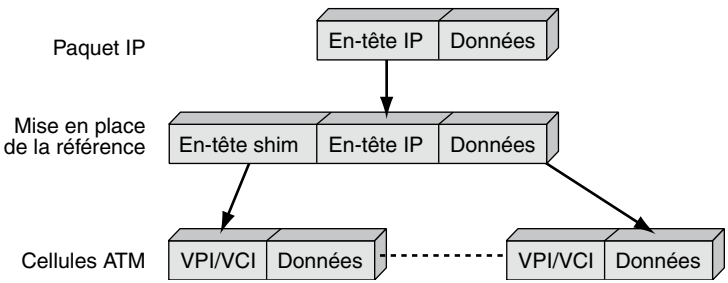


Figure 15.5

Mise en place des références dans l'ATM

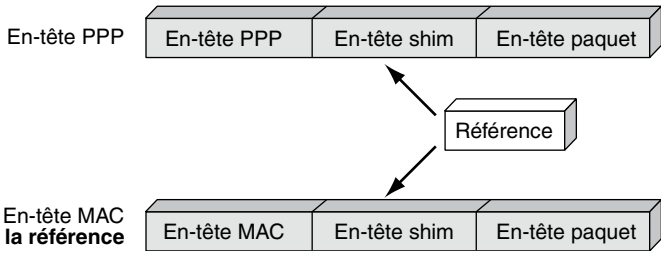


Figure 15.6

Mise en place des références dans la trame PPP

Distribution des références

MPLS normalise plusieurs méthodes pour réaliser la distribution des références. La distribution indique que chaque nœud possède ses propres références et qu'il doit les mettre en correspondance avec les références de ses voisins.

Les méthodes de distribution des références sont les suivantes :

- Topology-based, ou fondée sur la topologie, qui utilise les messages destinés à la gestion du routage, comme OSPF et BGP.
- Request-based, ou fondée sur le flot, qui utilise une requête de demande d'ouverture d'un chemin pour un flot IP. C'est le cas de RSVP.
- Traffic-based, ou fondée sur le trafic : à la réception d'un paquet, une référence est assignée à la trame qui le transporte.

Les méthodes fondées sur la topologie et sur le flot correspondent à un contrôle (control-based), tandis que celle fondée sur le trafic correspond à des données.

Les protocoles de routage, dont IGP (Interior Gateway Protocol), ont été améliorés pour transporter une référence supplémentaire. Le protocole OSPF a été complété par une prise en compte des débits sur les liaisons : OSPF-TE (Traffic Engineering). De même le protocole RSVP comporte une version associée à MPLS qui lui permet de transporter une référence. La version la plus aboutie est RSVP-TE (Traffic Engineering), qui permet l'ouverture de chemins en tenant compte des ressources du réseau.

L'IETF a également normalisé un nouveau protocole de signalisation, LDP (Label Distribution Protocol), pour gérer la distribution des références. Des extensions de ce protocole, comme CR-LDP (Constraint-based Routing-LDP), permettent de choisir les routes suivies par les clients des FEC avec une qualité de service prédéfinie.

Les principaux protocoles de signalisation sont les suivants :

- LDP, qui fait correspondre des adresses IP unicast et des références.
- RSVP-TE et CR-LDP, qui ouvrent des routes avec une qualité de service.
- PIM (Protocol Independent Multicast), qui fait correspondre des adresses IP multicast et des références associées.
- BGP, qui est utilisé pour déterminer des références dans le cadre de réseaux privés virtuels.

LSP (Label Switched Path)

Un domaine MPLS est déterminé par un ensemble de nœuds MPLS sur lesquels sont déterminés des FEC. Les LSP sont les chemins déterminés par les références positionnées par la signalisation. Les LSP sont déterminés sur un domaine avant l'arrivée des données dans le cas le plus classique. Deux options sont utilisées à cette fin :

- Le routage saut par saut (hop-by-hop). Dans ce cas, les LSR sélectionnent les prochains sauts indépendamment les uns des autres. Le LSR utilise pour cela un protocole de routage comme OSPF.
- Le routage explicite, identique au routage par la source. Le LER d'entrée du domaine MPLS spécifie la liste des nœuds par lesquels la signalisation a été routée, le choix de cette route pouvant avoir été contraint par des demandes de qualité de service.

Le chemin suivi par les trames dans un sens de la communication peut être différent dans l'autre sens.

Agrégation de flots

Les flots provenant de différentes interfaces peuvent être rassemblés et commutés sur une même référence s'ils vont vers la même direction de sortie. Cela correspond à une agrégation de flots. Cette technique est déjà exploitée sur les réseaux ATM, dans lesquels un conduit peut agréger plusieurs flots venant de différents nœuds d'entrée vers un point commun, où les flots sont désagrégés.

L'agrégation de flots a pour objectif d'éviter l'explosion du nombre de références à utiliser ou, ce qui est équivalent, d'empêcher les tables de commutation de devenir trop importantes.

Signalisation

Comme expliqué précédemment, plusieurs mécanismes de distribution des références, appelée signalisation, peuvent être implémentés dans les nœuds d'un réseau MPLS, notamment les suivants :

- Demande de référence : un LSR émet une demande de référence à ses voisins vers l'aval (downstream), qu'il peut lier à la valeur d'une FEC. Ce mécanisme peut être utilisé de nœud en nœud jusqu'au nœud de sortie du réseau MPLS.
- Correspondance de référence : en réponse à une demande de référence d'un nœud amont, un LSR envoie une référence provenant d'un mécanisme de correspondance connu déjà mise en place pour aller jusqu'au nœud de sortie.

La figure 15.7 donne une illustration de ces deux mécanismes.

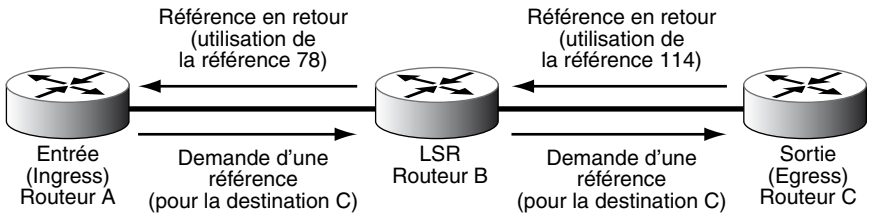


Figure 15.7

Mécanismes de signalisation de MPLS

LDP (Label Distribution Protocol)

LDP est le protocole de distribution des références qui tend à devenir le standard le plus utilisé dans MPLS. Ce protocole tient compte des adresses unicast et multicast. Le routage est explicite et est géré par les nœuds de sortie. Les échanges s'effectuent sous le protocole TCP pour assurer une qualité acceptable.

Deux classes de messages sont acceptées, celle des messages adjacents et celle des messages indiquant les références. La première permet d'interroger les nœuds qui peuvent être atteints directement à partir du nœud origine. La seconde classe de messages transmet les valeurs de la référence lorsqu'il y a accord entre les nœuds adjacents. Ces messages sont encodés sous la forme classique, qui permet de décrire un objet : on indique dans un premier champ le type d'objet, dans un deuxième la longueur totale du message décrivant l'objet et dans un troisième la valeur de l'objet. Cet encodage s'appelle TLV (Type Length Value).

Le routage s'effectue, comme nous l'avons vu, par des classes d'équivalence, ou FEC. Une classe représente une destination ou un ensemble de destinations ayant le même préfixe dans l'adresse IP. De ce fait, un paquet qui a une destination donnée appartient à une classe et suit une route commune avec les autres paquets de cette classe. Cela définit un arbre, dont la racine est le destinataire et dont les feuilles sont les émetteurs. Les paquets n'ont plus qu'à suivre l'arbre jusqu'à la racine, les flots se superposant petit à petit en allant vers la racine. Cette solution permet de ne pas utiliser trop de références différentes.

La granularité des références, c'est-à-dire la taille des flots qui utilisent une même référence, résulte de la taille des classes d'équivalence : s'il y en a peu, les flots sont importants, et la granularité est forte ; s'il y en a beaucoup, les flots sont faibles, et la granularité est fine. Par exemple, une destination peut correspondre à un réseau important, dans lequel toutes les adresses ont un préfixe commun. La destination peut aussi correspondre à une application particulière sur une machine donnée, ce qui donne une forte granularité. Ce dernier cas est illustré à la figure 15.8, dans laquelle le récepteur est la machine 1 et la FEC est déterminée par l'arbre dont les feuilles sont les machines terminales 1, 2 et 3. La classe d'équivalence, en descendant l'arbre à partir de 1, commence par les références 28 puis 47 et se continue par les branches 77 puis 13 puis 36. À partir de 2, les références 53 puis 156 sont utilisées pour aller vers la racine. À partir de 3, ce sont les références 134 et 197 qui sont utilisées. Toutes les références que nous venons de citer appartiennent à la même classe d'équivalence.

Dans cet exemple, les terminaux 1, 2 et 3 souhaitent émettre un flux de paquets IP vers la station terminale 4. Pour cela la station 1 émet ses trames (encapsulant les paquets IP) avec la référence 28, qui est commutée vers la référence 47 puis commutée vers les références 77 puis 13 puis 36. Le flot partant de la station 2 est commuté de 53 en 156 puis en 77, 13 et 36. Enfin, le troisième flot, partant de la station 3, est commuté à partir des valeurs 134 puis 197, 13 et 36. On voit que l'agrégation s'effectue sur les deux premiers flots avec la seule valeur 77 et que les trois flux sont agrégés sur les valeurs 13 et 36. La station 4 aurait pu être remplacée par un sous-réseau, ce qui aurait certainement permis d'agréger beaucoup plus de flux et d'avoir une granularité moins fine.

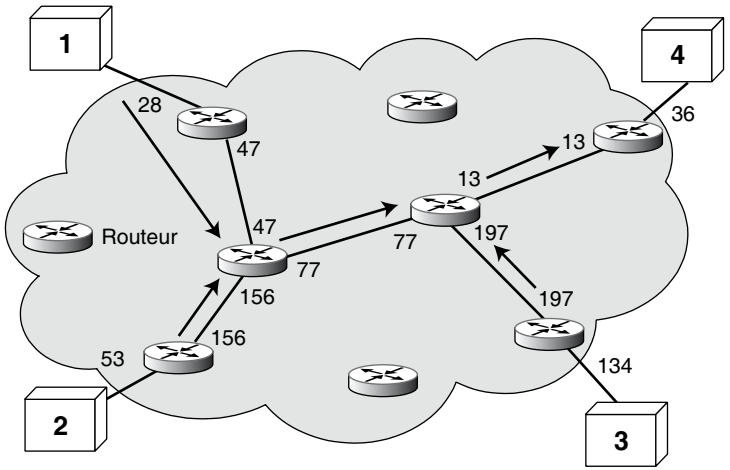


Figure 15.8

Classes d'équivalence (FEC) dans un réseau MPLS

Un problème posé par les tables de routage impliquant les FEC est celui des boucles potentielles, c'est-à-dire d'un possible retour à une station qui a déjà vu passer la trame. Si le routage utilise un protocole comme OSPF, on évite les boucles en utilisant un message d'information.

Le protocole LDP comprend les messages suivants :

- Message de découverte (discovery message), qui annonce et maintient la présence d'un LSR dans le réseau.
- Message de session (session message), qui établit, maintient et termine des sessions entre des ports LDP.
- Message d'avertissement (advertisement message), qui crée, maintient et détruit la correspondance entre les références et les FEC.
- Message de notification (notification message), qui donne des informations d'erreur ou de problème.

Les tables de commutation peuvent être construites et contrôlées de différentes façons. Les protocoles de routage d'Internet, tels que OSPF, BGP, PIM, etc., sont généralement utilisés à cet effet. Il faut leur ajouter des procédures pour faire correspondre les références et les classes d'équivalence FEC.

Nous avons indiqué que la distribution des références s'effectuait par l'aval en remontant vers la station d'émission. En réalité, il est indiqué dans la norme MPLS que la distribution des références peut s'effectuer par l'aval (downstream) ou par l'amont (upstream). Dans le premier cas, le destinataire indique aux nœuds amont la valeur de la référence à mettre dans la table de commutation. Dans le second cas, le paquet arrive avec une référence, et le nœud met à jour sa table de commutation.

Dans la distribution amont (upstream), un nœud aval envoie la valeur de la référence qu'il souhaite recevoir pour commuter un paquet sur une FEC. Ce sont les nœuds situés le plus en aval qui déclenchent le processus et indiquent les destinataires et leur granularité. Les modifications s'effectuent lors de la réception d'une trame ou par l'intermédiaire d'informations de supervision.

La distribution des identificateurs peut s'effectuer par l'intermédiaire des protocoles RSVP-TE ou PIM.

Les piles de références

Le mécanisme de piles de références de MPLS permet à un LSP de transiter par des nœuds non-MPLS ou par des domaines hiérarchiques. Pour cela, la zone portant la référence peut stocker non plus une valeur mais une pile de valeurs, c'est-à-dire une pile de références. Suivant le niveau de la hiérarchie de références on utilise la référence de la hiérarchie correspondante dans la pile.

Les piles de références permettent de réaliser des tunnels, dans lesquels sont regroupées les références d'un même niveau de la hiérarchie. À la sortie du tunnel, on revient à la hiérarchie juste en dessous, comme illustré à la figure 15.9. Sur cette figure, le flot partant de la station 1 est commuté sur les valeurs 28 puis 53. Au nœud A, une pile de références est créée avec l'ajout de la référence 156, qui est utilisée dans le nœud suivant pour commuter sur les valeurs 77 puis 197. Le nœud B permet la sortie du tunnel en utilisant de nouveau la référence 53 après avoir dépilé les références. On voit qu'entre le nœud A et le nœud B un tunnel est constitué, qui, à une référence d'entrée 53, fait correspondre une référence de sortie 13.

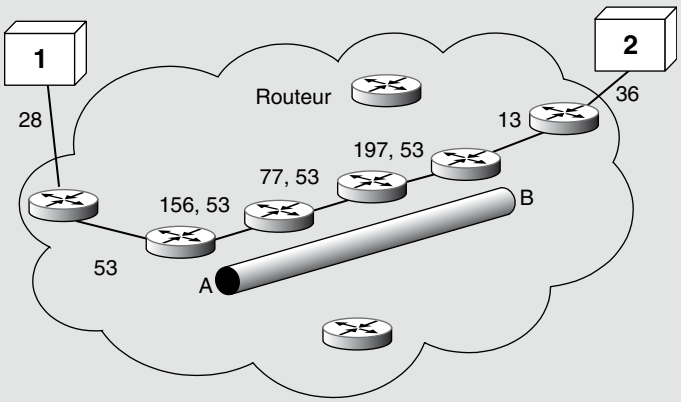


Figure 15.9

Tunnel MPLS réalisé grâce à une pile de références

L'ingénierie de trafic

Il est difficile de réaliser une ingénierie du trafic dans Internet du fait que le protocole BGP n'utilise que des informations de topologie du réseau. L'IETF a introduit dans l'architecture MPLS un routage à base de contrainte et un protocole de routage interne à état des liens étendu afin de réaliser une ingénierie de trafic efficace.

Comme nous l'avons vu, chaque trame encapsulant un paquet IP qui entre dans le réseau MPLS se voit ajouter par le LSR d'entrée, ou Ingress LSR, une référence au niveau de l'en-tête permettant d'acheminer la trame dans le réseau. Les chemins sont préalablement ouverts par un protocole de réservation de ressources, RSVP ou LDP. À la sortie du réseau, la référence ajoutée à l'en-tête de la trame est supprimée par le LSR de sortie, ou Egress LSR.

Des attributs permettant de contrôler les ressources attribuées à ces chemins sont associés au LSP, qui est le chemin construit entre le LSR d'entrée et le LSR de sortie. Ces attributs sont récapitulés au tableau 15.1. Ils concernent essentiellement la bande passante nécessaire au chemin, son niveau de priorité, son aspect dynamique, par l'intermédiaire du protocole utilisé pour son ouverture, et sa flexibilité en cas de panne.

Attribut	Description
Bande passante	Besoins minimaux de bande passante à réserver sur le chemin du LSP
Attribut de chemin	Indique si le chemin du LSP doit être spécifié manuellement ou dynamiquement par l'algorithme CBR (Constraint-Based Routing).
Priorité de démarrage	Le LSP le plus prioritaire se voit allouer une ressource demandée par plusieurs LSP.
Priorité de préemption	Indique si une ressource d'un LSP peut lui être retirée pour être attribuée à un autre LSP plus prioritaire.
Affinité ou couleur	Exprime des spécifications administratives.
Adaptabilité	Indique si le chemin d'un LSP doit être modifié pour avoir un chemin optimal.
Flexibilité	Indique si le LSP doit être rerouté en cas de panne sur le chemin du LSP.

TABLEAU 15.1 • Attributs des chemins LSP dans un réseau MPLS

L'algorithme CR (Constraint-based Routing)

L'algorithme CR est appliqué lors de l'ouverture du chemin ou de sa réouverture si le chemin est dynamique.

En plus des contraintes de topologie utilisées par les algorithmes de routage classiques, l'algorithme CR calcule les routes en fonction de contraintes de bande passante ou administratives. Les chemins calculés par le protocole CR ne sont pas forcément les plus courts. En effet, le chemin le plus court peut ne pas satisfaire la capacité de bande passante demandée par le LSP. Le LSP peut donc emprunter un autre chemin, plus lent mais disposant de la capacité de bande passante demandée. De la sorte, le trafic est distribué de manière plus uniforme sur le réseau.

L'algorithme CR peut s'effectuer en temps réel ou non. Dans le premier cas, le nombre de LSP à traverser est calculé à des instants quelconques par les routeurs sur la base d'informations locales. Dans le second cas, un serveur se charge, à partir d'informations recueillies sur tout le réseau, de calculer les chemins périodiquement et de reconfigurer automatiquement les routeurs avec les nouveaux chemins calculés.

Le protocole de routage est nécessaire pour le transport des informations de routage. Dans le cas de l'algorithme CR, le protocole de routage doit transporter, en plus des informations de topologie, des contraintes telles que les besoins en bande passante. La propagation de ces informations se fait plus fréquemment que dans le cas d'un IGP standard, puisqu'il y a plus de facteurs susceptibles de changer. Pour ne pas surcharger le réseau, il faut toutefois veiller que la fréquence de propagation des informations ne soit pas trop importante. Un compromis doit être trouvé entre le besoin d'actualiser les informations et celui d'éviter les propagations excessives.

La conception d'un système MPLS pour l'ingénierie de trafic nécessite de parcourir les étapes suivantes :

1. **Définition de l'étendue géographique du système MPLS.** Dépend de la politique administrative et de l'architecture du réseau.
2. **Définition des routeurs membres du système MPLS.** Il s'agit de définir les LSR d'entrée, de transit et de sortie du système MPLS. Pour diverses raisons, ce dernier ne contient pas nécessairement tous les routeurs du réseau, notamment si un routeur n'est pas assez puissant ou s'il n'est pas sécurisé.
3. **Définition de la hiérarchie du système MPLS.** Deux cas sont possibles : connecter tous les LSR du système MPLS et créer un seul niveau de hiérarchie formant un grand système MPLS ou diviser le réseau en plusieurs niveaux de hiérarchie. Dans ce dernier cas, les LSR de premier et deuxième niveau de la hiérarchie, qui forment le cœur du réseau, sont fortement maillés.
4. **Définition des besoins en bande passante des LSP.** Les besoins en bande passante peuvent être définis par la matrice de trafic de bout en bout, qui n'est pas toujours disponible, ou par un calcul statistique fondé sur l'exploitation des LSP et la mise à jour régulière de cette information en observant constamment leur trafic.
5. **Définition des chemins des LSP.** Les chemins sont généralement calculés de manière dynamique par un CR temps réel. Lorsqu'il se révèle difficile de réaliser ce calcul en temps réel, on peut utiliser un algorithme CR non-temps réel.
6. **Définition des priorités des LSP.** On peut attribuer la plus haute priorité à des LSP devant écouler un trafic volumineux. Cela permet d'emprunter les chemins les plus courts et d'éviter de surcharger un grand nombre de liens dans le réseau, tout en offrant une stabilité du routage et une meilleure utilisation des ressources.
7. **Définition du nombre de chemins parallèles entre deux extrémités quelconques.** On peut configurer plusieurs chemins en parallèle ayant des routes physiquement différentes. Cela garantit une distribution de la charge du trafic plus uniforme. L'idée sous-jacente est de définir des LSP de petite taille en vue d'une meilleure flexibilité du routage. Cette flexibilité est la première motivation des LSP parallèles.
8. **Définition de l'affinité des LSP et des liens.** Des couleurs peuvent être attribuées aux LSP et aux liens en fonction de contraintes administratives. Ces couleurs servent à déterminer les chemins à choisir pour les LSP.

9. **Définition des attributs d'adaptation et de flexibilité.** Selon l'évolution du comportement du réseau, il est possible de trouver des chemins optimaux pour les LSP déjà calculés. L'administrateur réseau peut accepter ou refuser une nouvelle optimisation des LSP. Il ne faut pas que cette dernière soit trop fréquente, car elle pourrait introduire une instabilité du routage. Il faut aussi prévoir des mécanismes de reroutage des LSP en cas de panne d'un LSR.

L'exploitation d'un réseau MPLS suit les étapes énumérées ci-dessous :

1. **Recueil des données statistiques en utilisant les LSP au démarrage du système.** L'objectif de cette étape est de calculer le taux de trafic entre chaque paire de routeurs. Les méthodes statistiques existantes permettent de calculer le taux de trafic à l'entrée et à la sortie d'une interface mais pas celui allant vers une destination particulière. La construction de la matrice de trafic de bout en bout est effectuée par estimation, ce qui rend l'ingénierie de trafic difficile et peu efficace. L'utilisation des LSP au démarrage d'un système MPLS donne précisément le taux de trafic entre deux extrémités quelconques en fonction des destinations.
2. **Exploitation des LSP avec les contraintes de bande passante définies à l'étape précédente.** L'étape 1 ci-dessus ayant permis de connaître les besoins en bande passante de chaque LSP, cette information est utilisée par l'algorithme CR pour recalculer les LSP avec leur besoin réel en bande passante.
3. **Mise à jour périodique des bandes passantes des LSP.** Une mise à jour périodique des bandes passantes des LSP est nécessaire pour assurer l'évolution et l'adaptation du réseau au changement du trafic dans le réseau.
4. **Exécution de l'algorithme CR en temps réel.** Pour une utilisation efficace des liens, l'algorithme CR doit être exécuté sur un serveur spécialisé. Calculé sur un serveur disposant de toutes les informations de topologie et d'attributs de tous les LSP, cet algorithme peut permettre d'atteindre le temps réel. L'algorithme propose des LSP ayant de meilleures performances comparées à celles des LSP déjà ouverts. L'algorithme CR doit pouvoir s'exécuter en temps réel pour tenir compte d'une panne d'un LSP. L'algorithme peut alors déterminer rapidement un nouveau LSP capable d'écouler le trafic en attente.

La qualité de service

Nous venons de voir que MPLS permettait de faire de l'ingénierie et d'effectuer des calculs pour déterminer les ressources à affecter à un chemin lorsque le système est relativement statique. Si le système est dynamique, des chemins doivent s'ouvrir et se fermer pour satisfaire à des contraintes qui s'expriment sur des laps de temps plus courts. L'idée de base est d'ouvrir les chemins grâce à un algorithme tenant compte des ressources. Nous avons déjà examiné la proposition CR-LDP. Cet algorithme ayant été partiellement abandonné, un autre algorithme, RSVP-TE, a pris une place de choix parmi les équipementiers.

Dans CR-LDP, les deux ports qui doivent communiquer s'échangent leur ensemble de références pour établir la connexion. Dans RSVP-TE, il n'y a pas de négociation de

références. C'est le plan de gestion qui prend à sa charge cette négociation. Pour de très grands réseaux, la mise en place du chemin avec LDP peut nécessiter des ressources considérables, ce qui explique son échec pour le moment.

CR-LDP peut spécifier la route à partir de la source par un champ de type TLV et RSVP-TE par le biais de l'objet « explicit route ». Les deux protocoles envoient une réponse au nœud d'entrée pour indiquer le succès ou l'échec de l'ouverture du chemin.

Les tableaux 15.2 et 15.3 récapitulent respectivement les similitudes et différences entre les deux techniques.

Caracteristique	CR-LDP	RSVP-TE	Commentaire
Initialisation de l'ouverture	Message LABEL_REQUEST	RSVP-TE Message PATH contenant l'objet LABEL_REQUEST	
Ouverture	DIFF-SERV_PSC TLV	Objet DIFFSERV_PSC	Les deux contiennent l'information correspondant au DSCP (DiffServ Code Point) inclus dans le message de demande d'ouverture.
Accepte les LSP point-à-multipoint	Non	Non	En attente d'une RFC
Possibilité d'un routage par la source	Transporté pa la liste TLV de EXPLICIT_ROUTE	Transporté par l'objet EXPLICIT_ROUTE	Spécifie le chemin à suivre.

TABLEAU 15.2 • Similitudes entre RSVP-TE et CR–LDP

Caracteristique	CR-LDP	RSVP-TE	Commentaire
Étape de développement	Le plus jeune mais non utilisé aujourd'hui	Le plus ancien, avec des ajouts pour tenir compte des divers réseaux disponibles dans MPLS	Certains objets de RSVP ont été modifiés pour être utilisés dans MPLS.
Signalisation	UDP pour la découverte et TCP pour la session	Paquets IP ou encapsulation dans UDP pour l'échange de messages	Pas de détection de panne déterministe avec RSVP-TE. Un problème sur TCP peut avoir un impact catastrophique sur les chemins dans CR-LDP.
État de la connexion	Hard State	Soft State	Le Soft State ne passe généralement pas l'échelle. RSVP prend en charge l'agrégation des messages de rafraîchissement.
Fiabilité	Défini pour prendre en charge la plupart des techniques trame, comme ATM, le relais de trames ou Ethernet.	Tunneling à travers le réseau ATM qui doit être configuré manuellement.	

TABLEAU 15.3 • Différences entre RSVP-TE et CR–LDP

MPLS-TP

Le protocole MPLS est aujourd'hui unanimement choisi pour le cœur des réseaux d'opérateurs. Cependant, MPLS est complexe, et la compatibilité entre équipementiers n'est en général pas assurée. Le manque d'un système de gestion est également flagrant. De plus, l'IETF souhaite s'étendre vers la périphérie et proposer aux opérateurs une solution plus simple à configurer et moins cher. Pour y arriver, le groupe de travail MPLS-TP (Transport Profile) a été mis en chantier et devient disponible en 2011.

La différence entre le standard de base MPLS et la nouvelle génération MPLS-TP est illustrée à la figure 15.10 : MPLS-TP est un sous ensemble de MPLS en enlevant des options, en particulier sur la signalisation. En revanche, MPLS-TP contient un nouvel environnement de gestion dit OAM (Operation and Maintenance) et une protection de la partie transport sur le support physique que nous avons détaillée au chapitre 13.

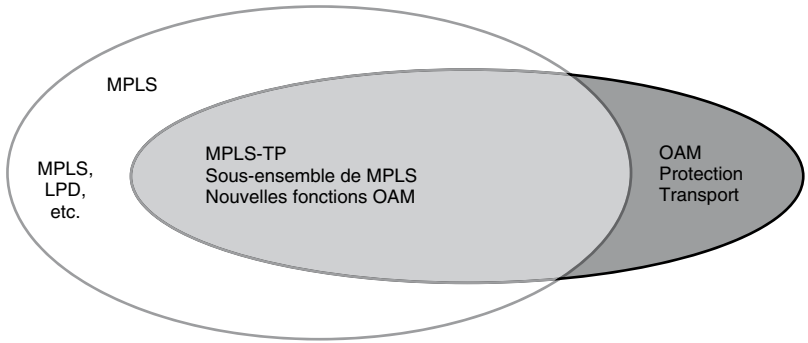


Figure 15.10

Les différences entre MPLS et MPLS-TP

Les fonctionnalités de MPLS-TP peuvent être résumées de la façon suivante :

- MPLS est repris pour la partie commutation avec une simplification au niveau de la mise en place des LSP :
- une architecture de pseudowire (émulation d'un niveau 2 en mode connexion, c'est-à-dire émulation d'un câble) dit PWE3 (pseudowire emulation edge-to-edge) ;
- utilisation du plan de contrôle, statique ou dynamique, provenant de GMPLS qui est décrit dans la suite de ce chapitre ;
- des fonctionnalités de gestion provenant d'un environnement OAM ;
- des procédures permettant d'augmenter la fiabilité et la disponibilité pour obtenir des performances du même ordre que celles de SONET ;
- utilisation d'un ensemble de fonctions de gestion provenant d'un protocole dit Generic Associated Channel (G-ACh) ;
- introduction du multipoint.

Un point très important concerne la normalisation. À l'IETF s'est ajoutée l'UIT-T afin d'aboutir à une norme rassemblant à la fois les télécommunications et l'informatique. Cette convergence est illustrée à la figure 15.11. La partie haute de l'architecture est conservée, mais de façon simplifiée. La partie basse, concernant le transport des éléments binaires, est intégrée à MPLS-TP par la solution OTN poussée par l'UIT-T (*voir le chapitre 13*). Enfin, la synchronisation que l'on trouve dans SONET ainsi que la fiabilité et la disponibilité sont repris dans MPLS-TP.

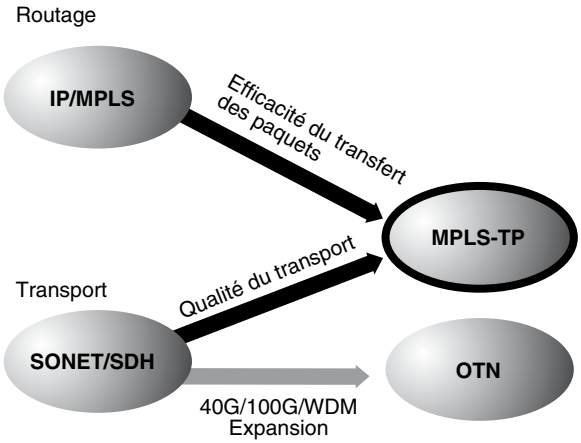


Figure 15.11

La convergence entre l'IETF et l'UIT-T

La figure 15.12 détaille davantage cette convergence. La normalisation de base a été effectuée par l'IETF et reprise ensuite par l'UIT-T sous le nom T-MPLS afin d'ajouter la fonction de transport des éléments binaires. Ce standard intermédiaire a été repris par l'IETF pour le conforter dans la version MPLS-TP en parallèle du travail d'amélioration de T-MPLS par l'UIT-T.

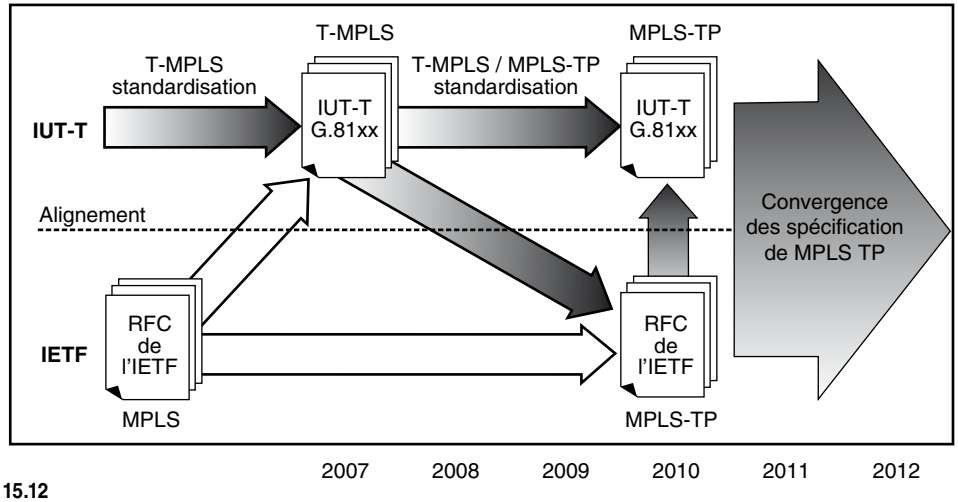


Figure 15.12

Le processus de normalisation de MPLS-TP

MPLS-TP est le grand standard que tous les opérateurs attendaient. Il s'applique aussi bien à l'intérieur du réseau qu'à la périphérie, par exemple pour connecter des réseaux d'accès utilisateur ou des réseaux d'accès d'antennes 3G et 4G.

GMPLS (Generalized MPLS)

Comme son nom l'indique, GMPLS est une généralisation du protocole MPLS. Cette généralisation est assez simple à expliquer, puisque tout ce qui peut jouer le rôle d'une référence — numéro d'une longueur d'onde, numéro d'un slot, etc. — peut entrer dans GMPLS. La structure de GMPLS est toutefois plus complexe qu'il n'y paraît, et une gestion globale est nécessaire pour arriver à bien contrôler cet environnement. GMPLS apporte aussi un plan de supervision qui devient un standard même pour la version simplifiée de MPLS : MPLS-TP.

Les extensions de MPLS

Au niveau trame (couche 2, ou liaison), MPLS ne travaille que sur des structures de trame de niveau 2 : c'est ce qu'on appelle le L2S (Level 2 Switching). Des extensions permettent toutefois d'introduire des références sur d'autres supports, comme le numéro d'une tranche de temps dans un partage temporel ou un numéro de longueur d'onde sur une fibre optique.

Les principales possibilités d'extension de MPLS sont les suivantes :

- PSC (Packet Switching Capable), pour les paquets capables de recevoir une référence. On pourrait imaginer un paquet IPv6 avec le flow-label comme référence, mais cette solution n'est pas acceptable en l'état, car un paquet ne peut être transmis directement sur un support physique : il faut l'encapsuler dans une trame. C'est généralement la trame PPP qui sert de transporteur.
- L2SC (Level 2 Switching Capable), qui correspond au label-switching utilisé dans la norme MPLS.
- TDMC (Time Division Multiplexing Capable), qui introduit la référence en tant que slot dans un multiplexage temporel. Toutes les techniques qui comportent une structure sous forme de trame avec des slots à l'intérieur font partie de cette classe. En particulier, toutes les techniques hertziennes avec division temporelle s'intègrent dans GMPLS.
- LSC (Lambda Switching Capable), qui prend le numéro de la longueur d'onde à l'intérieur d'une fibre optique comme référence de commutation. Cette technique a été la première extension de MPLS sous le nom de MPλS.
- FSC (Fiber Switching Capable), qui prend le numéro d'une fibre optique parmi un faisceau de fibres optiques comme référence de commutation. Dans un faisceau, les fibres sont numérotées de 1 à n, n correspondant au nombre de fibres optiques.

Le tableau 15.4 récapitule les techniques de transfert offertes par un réseau GMPLS.

Domaine de transfert	Type de trafic	Type de transfert	Exemple de station	Nomenclature
Trame	ATM, Ethernet	Utilisation de références	Commutateur ATM ou Ethernet	L2SC (Layer 2 Switching Capable)
Paquet	IP	Routage	Routage IP	PSC (Packet Switching Capable)
Temps	TDM/SONET	Slot de temps se répétant par cycle	Brasseur et commutateur	TDMC (Time Division Multiplexing Capable)
Longueur d'onde	Transparent	Lambda	DWDM	LSC (Lambda Switching Capable)
Espace physique	Transparent	Fibre optique	OXC (Optical Cross Connect)	FSC (Fiber Switching Capable)

TABLEAU 15.4 • Techniques de transfert de GMPLS

D'autres extensions sont imaginables, comme l'association d'un code dans une communication, que ce soit dans un CDMA ou dans une transmission quelconque. Par ces extensions, il est possible de faire correspondre en entrée et en sortie des références qui ne proviennent pas de la même technologie. En revanche, les différentes solutions ne donnent pas forcément des débits identiques. Par exemple, si l'on choisit comme référence une tranche avec un numéro bien déterminé d'un multiplex temporel hertzien, qui risque de donner au mieux quelques mégabits par seconde, il est difficile de lui faire correspondre en sortie une longueur d'onde d'une fibre optique qui peut avoir une capacité de 10 Gbit/s. Une hiérarchisation des supports est donc nécessaire.

Hiérarchie des supports

La figure 15.13 illustre une hiérarchie possible entre les supports qui peuvent être utilisés dans GMPLS. Dans cette figure, un flot de paquets IP donne naissance à un PSC, lui-même intégré dans un L2SC de type FEC, c'est-à-dire rassemblant plusieurs flots IP ayant une propriété commune, comme un même LSR de sortie.

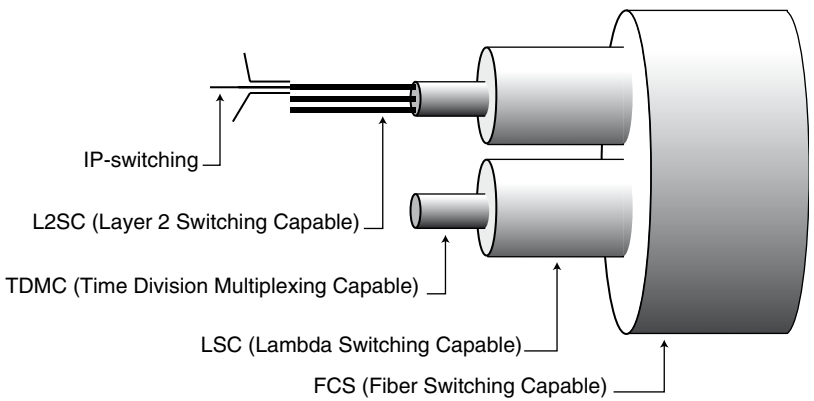


Figure 15.13

Hiérarchie des techniques de transfert dans GMPLS

Les flots de niveau L2CS peuvent eux-mêmes être encapsulés dans un slot d'une technique de type SONET/SDH. En continuant dans la hiérarchie, les flots TDMC peuvent être à leur tour multiplexés dans une même longueur d'onde, c'est-à-dire dans un LSC. En continuant la hiérarchie pour arriver au plus haut niveau, les longueurs d'onde peuvent elles-mêmes être intégrées dans une fibre particulière d'un faisceau de fibre optique.

Réseau overlay

Une autre caractéristique importante des réseaux MPLS et GMPS est de travailler en réseau overlay, c'est-à-dire en une hiérarchie de réseaux, comme illustré à la figure 15.14, où trois niveaux sont représentés.

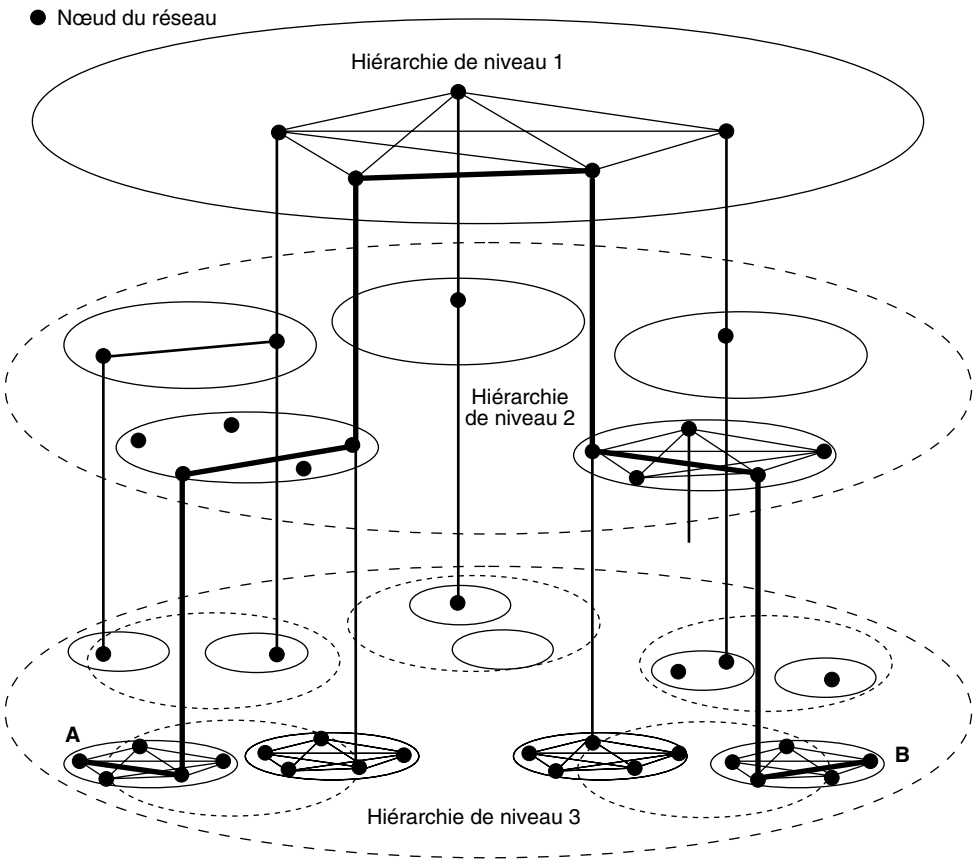


Figure 15.14

Hiérarchie de réseau à trois niveaux

Si l'on suppose, pour simplifier, que le réseau global ne comprend que deux niveaux de hiérarchie, comme illustré à la figure 15.15, chaque nœud du réseau overlay dessert un

réseau du niveau sous-jacent. Pour aller d'un point à un autre, de A à D par exemple, le paquet doit être envoyé par le réseau local au nœud d'entrée du réseau overlay, c'est-à-dire de A à B sur la figure, puis transmis dans le réseau overlay de B à C et enfin dans le réseau local d'arrivée de C à D.

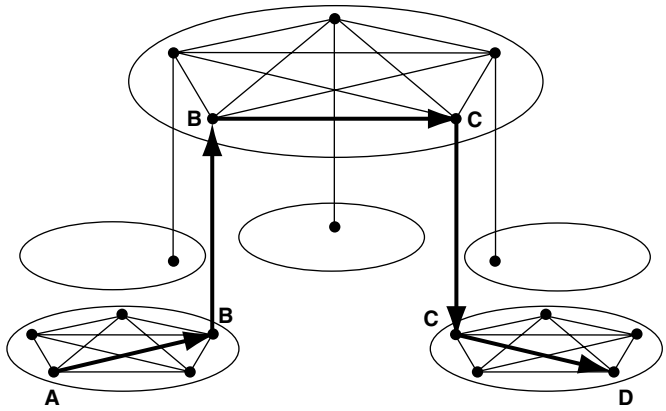


Figure 15.15

Fonctionnement d'un réseau overlay

Si les différents niveaux de la hiérarchie comportent des réseaux maillés, qui permettent d'aller directement d'un point à un autre dans le réseau, on voit que cette solution de réseau permet de limiter le nombre de nœuds à traverser. Dans le cas de la figure 15.16, pour aller de A à D, l'on ne passe que par deux nœuds intermédiaires, alors que si tous les nœuds du réseau avaient été au même niveau, il aurait fallu peut-être une dizaine de sauts.

La structure hiérarchique des supports de transmission de GMPLS permet de mettre en place ce type de réseau. On peut, par exemple, dans un cas simple, avoir des domaines MPLS de niveau 2 interconnectés par un réseau overlay utilisant une longueur d'onde sur une fibre optique. Ce réseau overlay relie les points des domaines de base choisis pour faire partie du réseau overlay.

Pour ouvrir des chemins sur des réseaux différents les uns des autres, un ensemble de protocoles de contrôle et de surveillance est nécessaire. Un premier problème posé par le routage dans les réseaux overlay concerne le contrôle de la connectivité, qui est pris en charge par des messages de type HELLO, envoyés régulièrement sur toutes les interfaces. Chaque HELLO doit être acquitté explicitement. Lorsque aucun ACK n'est reçu, la ligne est considérée comme étant en panne. Dans le cas de GMPLS sur fibre optique, il n'est pas possible d'envoyer des messages HELLO. Le contrôle de la connectivité doit donc se faire par un nouveau protocole.

Un second problème posé par les réseaux overlay provient de l'impossibilité pour des nœuds de même niveau mais n'appartenant pas au même domaine de se transmettre directement des messages de contrôle. Il faut passer par un réseau de niveau supérieur, lequel peut ne pas être capable d'interpréter les messages des niveaux inférieurs. Il n'y a donc pas de vision globale du réseau.

Contrôle et gestion de MPLS

Pour améliorer le contrôle et la gestion, il est nécessaire de bien séparer les plans utilisateur, gestion et contrôle, surtout si le réseau est complexe. Cela vaut encore davantage dans les réseaux utilisant de la fibre optique.

Comme pour l'ATM, on distingue trois plans dans GMPLS :

- Le plan utilisateur, qui est chargé de transporter les données utilisateur d'une extrémité à l'autre.
- Le plan de contrôle, destiné à mettre en place les circuits virtuels puis à les détruire à la fin de la transmission ou à les maintenir si nécessaire.
- Le plan de gestion, qui transporte les messages nécessaires à la gestion du réseau.

Les groupes de travail de GMPLS ont développé une telle architecture pour permettre de contrôler par un plan spécifique l'ensemble des composants du réseau.

Pour s'adapter au protocole GMPLS, les protocoles de signalisation (RSVP-TE, CR-LDP) et les protocoles de routage (OSPF-TE, IS-IS-TE) ont été étendus. Un nouveau protocole de gestion, appelé LMP (Link Management Protocol), a été introduit pour gérer les plans utilisateur et de contrôle. LMP est un protocole IP qui contient des extensions pour RSVP-TE et CR-LDP.

Le tableau 15.5 récapitule les propriétés de ces protocoles et leurs extensions dans le cadre de GMPLS.

Protocole	Description
Routage (OSPF-TE, IS-IS-TE)	Destiné à la découverte automatique de la topologie du réseau et à la mesure de la disponibilité des ressources (bande passante, type de protection). Les principales améliorations sont les suivantes : - Indication du type de protection (1+1, 1:1, non protégé, trafic en plus). 1+1 indique qu'un chemin de secours est ouvert en permanence, 1:1 qu'en cas de panne un chemin de secours est prévu mais sans réservation de ressource. - Implémentation de lignes de dérivation pour améliorer le passage à l'échelle. - Acceptation et indication de liaisons qui n'ont pas d'adresse IP; utilisation d'une identification Link ID. - Identité des interfaces d'entrée et de sortie (interface ID). - Découverte d'un chemin pour un back-up utilisant un chemin différent du chemin primaire (shared-risk link group).
Signalisation (RSVP-TE, CR-LDP)	Destiné à la mise en place des chemins par une ingénierie de trafic. Les principales améliorations sont les suivantes : - Échange des références avec des réseaux non paquet (référence généralisée). - Établissement de chemin LSP bidirectionnel. - Signalisation pour l'ouverture d'un chemin de back-up. - Proposition de références suggérées. - Accepte la commutation de longueur d'onde.
LMP (Link Management Protocol)	Inclut les extensions suivantes : - Control Channel Management : établit, lors de la négociation, les paramètres de la liaison, tels la fréquence d'émission des messages KEEP_ALIVE et HELLO. - Link Connectivity Verification : permet de s'assurer de la connectivité physique entre les nœuds voisins grâce à des messages de type PING. - Link Property Correlation : détermine les mécanismes de protection. - Fault Isolation : isole les fautes simples ou multiples du domaine optique.

TABLEAU 15.5 • Propriétés et extensions des protocoles de GMPLS

Les différentes couches que nous avons examinées forment l'architecture dite multicouche de GMPLS : trame, slot temporel, longueur d'onde, ensemble de longueurs d'onde, fibre optique, groupe de fibre optique.

Plan de contrôle de GMPLS

Une des difficultés rencontrées pour établir des LSP est de trouver le meilleur chemin, en tenant compte des multiples couches de l'architecture. Par exemple, il est possible d'ouvrir une liaison optique reliant deux commutateurs optiques et traversant plusieurs autres commutateurs de façon totalement transparente. De ce fait, cette liaison, souvent appelée TE-Link, est vue comme une liaison à un saut. L'optimisation du chemin à ouvrir a donc tout intérêt à passer par des TE-Link du plus bas niveau possible.

L'architecture du plan de contrôle permettant de réaliser l'ouverture des LSP est illustrée à la figure 15.16. Cette architecture contient les couches basses de l'architecture GMPLS, avec les différentes possibilités de transporter les paquets IP de contrôle sur les différentes commutations acceptées par GMPLS. Les paquets IP sont routés par des protocoles de routage de type OSPF-TE, c'est-à-dire en tenant compte de l'ingénierie de trafic. Une fois le chemin déterminé, une réservation est réalisée, essentiellement par le protocole RSVP-TE. D'autres possibilités, comme CR-LDP ou BGP, peuvent être employées, mais elles n'ont pas encore rencontré le même succès que RSVP-TE.

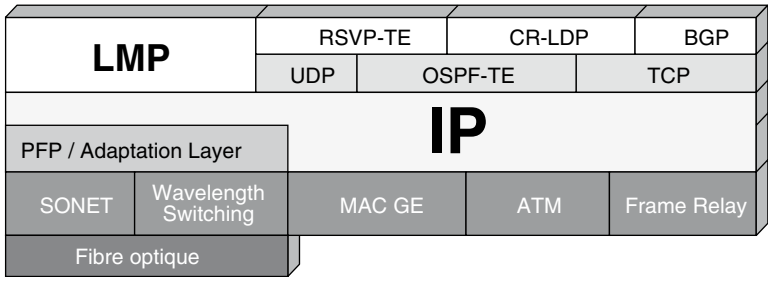


Figure 15.16

Architecture de GMPLS

Le plan de contrôle de GMPLS demandera encore de nombreux développements et de tests avant d'être vraiment optimisé. Il est aujourd'hui surtout utilisé pour la partie optique, mais comme il n'y a pas de mémoire tampon dans les nœuds, les ouvertures et fermetures doivent se faire à la volée.

À une mise en place des LSP devant se faire plusieurs heures à l'avance et souvent de façon manuelle devrait succéder un processus automatique permettant d'ouvrir et de fermer les LSP quasiment instantanément au fur et à mesure des demandes.

Conclusion

Les réseaux MPLS et GMPS sont promis à un bel avenir. Tous les grands opérateurs ont investi dans cette direction, non sans une certaine appréhension quant à la complexité globale de cette nouvelle architecture, qui peut être vue comme un compromis entre un grand nombre d'architectures différentes. La proposition MPLS-TP est la solution à ces problèmes et devrait devenir la très grande norme des réseaux d'opérateurs.

Le plan utilisateur semble bien conçu et permet d'optimiser assez facilement la mise en place du réseau et son ingénierie, notamment pour ce qui concerne la qualité de service, la maintenance et la gestion.

MPLS a aussi été retenu pour réaliser des réseaux privés virtuels grâce à ses chemins qu'il est relativement facile de protéger. Nous examinons ces solutions de VPN au chapitre 25.

16

Les réseaux IP : architecture

IP est un sigle très connu dans le domaine des réseaux. Il correspond à l'architecture développée pour le réseau Internet. Au sens strict, IP (Internet Protocol) est un protocole de niveau paquet. Au-dessus de ce protocole, au niveau message, deux protocoles lui sont associés : TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

Ce chapitre décrit l'architecture générale des réseaux IP et les protocoles qui permettent à cet environnement de gérer les problèmes d'adressage et de routage et plus généralement tous les protocoles associés au protocole IP et se trouvant dans le niveau paquet.

L'architecture IP

L'architecture IP repose sur l'utilisation obligatoire du protocole IP, qui a pour fonctions de base l'adressage et le routage des paquets IP. Le niveau IP correspond exactement au niveau paquet de l'architecture du modèle de référence.

Au-dessus d'IP, deux protocoles ont été choisis, TCP et UDP, que nous avons introduits au chapitre 8. Ces protocoles correspondent au niveau message du modèle de référence. En fait, ils intègrent une session élémentaire, grâce à laquelle TCP et UDP prennent en charge les fonctionnalités des couches 4 (transport) et 5 (session).

La principale différence entre eux réside dans leur mode, avec connexion pour TCP et sans connexion pour UDP. Le protocole TCP est très complet et garantit une bonne qualité de service, en particulier sur le taux d'erreur des paquets transportés. En revanche, UDP est un protocole sans connexion, qui supporte des applications moins contraignantes en matière de qualité de service.

La couche qui se trouve au-dessus de TCP-UDP regroupe les fonctionnalités des couches 6 et 7 du modèle de référence et représente essentiellement le niveau application.

L'architecture TCP/IP est illustrée à la figure 16.1. Elle contient trois niveaux : le niveau paquet, le niveau message et un niveau reprenant les fonctionnalités des couches supérieures.

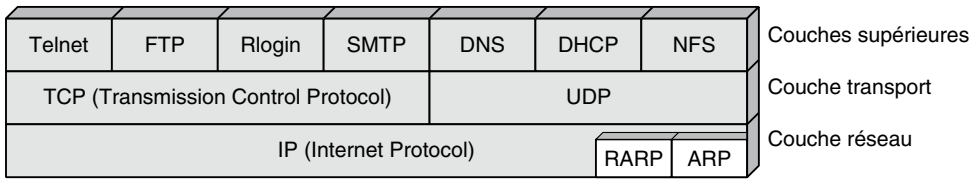


Figure 16.1

Architecture TCP/IP

Internet

À la fin des années 1960, le Département américain de la Défense décide de réaliser un grand réseau à partir d'une multitude de petits réseaux, tous différents, qui commencent à foisonner un peu partout en Amérique du Nord. Il a fallu trouver le moyen de faire coexister ces réseaux et de leur donner une visibilité extérieure, la même pour tous les utilisateurs. D'où l'appellation d'*InterNetwork* (interréseau), abrégée en Internet, donnée à ce réseau de réseaux.

L'architecture Internet se fonde sur une idée simple : demander à tous les réseaux qui veulent en faire partie de transporter un type unique de paquet, d'un format déterminé par le protocole IP. De plus, ce paquet IP doit transporter une adresse définie avec suffisamment de généralité pour pouvoir identifier chacun des ordinateurs et des terminaux dispersés à travers le monde. Cette architecture est illustrée à la figure 16.2.

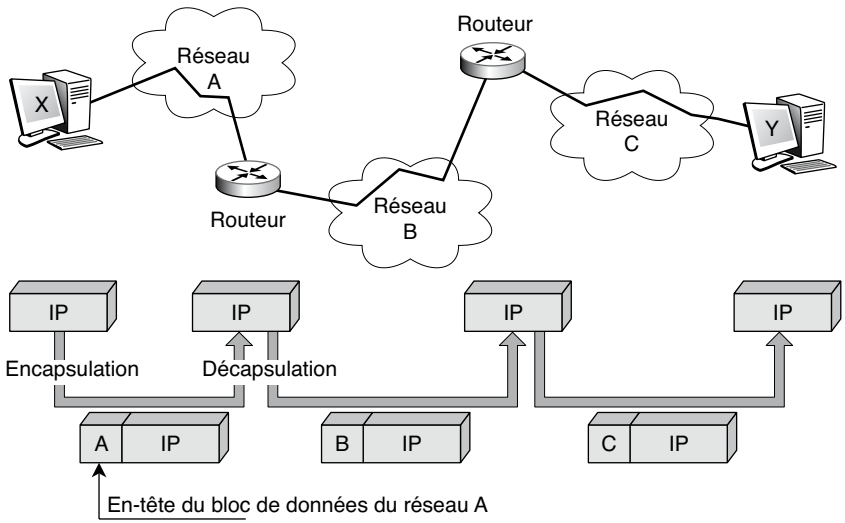


Figure 16.2

Architecture d'Internet

L'utilisateur qui souhaite émettre sur cet inter réseau doit ranger ses données dans des paquets IP, qui sont remis au premier réseau à traverser. Ce premier réseau encapsule le paquet IP dans sa propre structure de paquet, le paquet A, qui circule sous cette forme jusqu'à une porte de sortie, où il est décapsulé de façon à récupérer le paquet IP. L'adresse IP est examinée pour situer, grâce à un algorithme de routage, le prochain réseau à traverser, et ainsi de suite jusqu'à arriver au terminal de destination.

Pour compléter le protocole IP, la Défense américaine a ajouté le protocole TCP, qui précise la nature de l'interface avec l'utilisateur. Ce protocole détermine en outre la façon de transformer un flux d'octets en un paquet IP, tout en assurant une qualité du transport de ce paquet IP. Les deux protocoles, assemblés sous le sigle TCP/IP, se présentent sous la forme d'une architecture en couches. Ils correspondent respectivement au niveau paquet et au niveau message du modèle de référence.

Le modèle Internet se complète par une troisième couche, appelée niveau application, qui regroupe les différents protocoles sur lesquels se construisent les services Internet. La messagerie électronique (SMTP), le transfert de fichiers (FTP), le transfert de pages hypermédias, le transfert de bases de données distribuées (World-Wide Web), etc., sont quelques-uns de ces services. La figure 16.3 illustre les trois couches de l'architecture Internet.

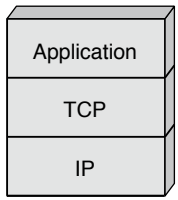


Figure 16.3

Les trois couches de l'architecture Internet

Les paquets IP sont indépendants les uns des autres et sont routés individuellement dans le réseau par les équipements interconnectant les sous-réseaux, les routeurs. La qualité de service proposée par le protocole IP est très faible et n'offre aucune détection de paquets perdus ni de possibilité de reprise sur erreur.

Le protocole TCP regroupe les fonctionnalités du niveau message du modèle de référence. C'est un protocole assez complexe, qui comporte de nombreuses options permettant de résoudre tous les problèmes de perte de paquet dans les niveaux inférieurs. En particulier, un fragment perdu peut être récupéré par retransmission sur le flot d'octets. Le protocole TCP utilise un mode avec connexion.

La souplesse de l'architecture Internet peut parfois être un défaut, dans la mesure où l'optimisation globale du réseau est effectuée sous-réseau par sous-réseau, par une succession d'optimisations locales. Cela ne permet pas une homogénéité des fonctions dans les différents sous-réseaux traversés. Une autre caractéristique importante de cette architecture est de situer tout le système de commande, c'est-à-dire l'intelligence et le contrôle du réseau, dans la machine terminale, ne laissant quasiment rien dans le réseau, tout au moins dans la version actuelle, IPv4, du protocole IP. L'intelligence de contrôle se trouve dans le logiciel TCP du PC connecté au réseau.

C'est le protocole TCP qui se charge d'envoyer plus ou moins de paquets en fonction de l'occupation du réseau. Une fenêtre de contrôle précise le nombre maximal de fragments non acquittés pouvant être émis. La fenêtre de contrôle de TCP augmente ou diminue le trafic suivant le temps nécessaire pour effectuer un aller-retour. Plus ce temps augmente, plus on considère le réseau congestionné, et plus le débit d'émission doit diminuer pour combattre la saturation. En contrepartie, le coût de l'infrastructure est extrêmement bas, aucune intelligence ne se trouvant dans le réseau. Le service rendu par le réseau des réseaux correspond à une qualité appelée best-effort, qui signifie que le réseau fait de son mieux pour écouler le trafic. En d'autres termes, la qualité de service n'est pas assurée.

La nouvelle génération du protocole IP, le protocole IPv6, introduit des fonctionnalités inédites, qui rendent les nœuds du réseau plus intelligents. Les routeurs de nouvelle génération sont dotés d'algorithmes de gestion de la qualité de service, qui leur permettent d'assurer un transport capable de répondre à des contraintes temporelles ou à des pertes de paquets. On attend l'arrivée d'IPv6 depuis une dizaine d'années, mais c'est toujours IPv4 qui régente le monde IP. La raison à cela est qu'à chaque nouveau besoin réalisable avec IPv6, IPv4 a été capable de trouver les algorithmes nécessaires pour faire aussi bien.

Dans IPv4, chaque nouveau client est traité de la même façon que ceux qui sont déjà connectés, les ressources étant équitablement distribuées entre tous les utilisateurs. Les politiques d'allocation de ressources des réseaux des opérateurs de télécommunications sont totalement différentes, puisque, sur ces réseaux, un client qui possède déjà une certaine qualité de service ne subit aucune pénalité du fait de l'arrivée d'un nouveau client. Comme nous le verrons, la solution aujourd'hui préconisée dans l'environnement Internet consiste à favoriser les clients ayant des exigences de temps réel, au moyen de protocoles adaptés, utilisant des niveaux de priorité.

Le protocole IP existe depuis trente ans, mais il est resté presque confidentiel pendant vingt ans avant de décoller, moins par ses propriétés que du fait de l'échec des protocoles liés directement au modèle de référence, trop nombreux et souvent incompatibles. L'essor du monde IP vient de la simplicité de son protocole, comportant très peu d'options, et de sa gratuité.

Fonctionnement des réseaux TCP/IP

La plupart des réseaux sont des entités indépendantes, mises en place pour rendre service à une population restreinte. Les utilisateurs choisissent des réseaux adaptés à leurs besoins spécifiques, car il est impossible de trouver une technologie satisfaisant tous les types de besoins. Dans cet environnement de base, les utilisateurs qui ne sont pas connectés au même réseau ne peuvent pas communiquer. Internet est le résultat de l'interconnexion de ces différents réseaux physiques par des routeurs. Les interfaces d'accès doivent respecter pour cela certaines conventions. C'est un exemple d'interconnexion de systèmes ouverts.

Pour obtenir l'interfonctionnement de différents réseaux, la présence du protocole IP est obligatoire dans les nœuds qui assurent le routage entre les réseaux. Globalement, Internet est un réseau à transfert de paquets. Ces paquets traversent un ou plusieurs sous-réseaux pour atteindre leur destination, sauf bien sûr si l'émetteur se trouve dans le même

sous-réseau que le récepteur. Les paquets sont routés dans des passerelles situées dans les nœuds d'interconnexion. Ces passerelles sont des routeurs. De façon plus précise, les routeurs transfèrent des paquets d'une entrée vers une sortie, en déterminant pour chaque paquet la meilleure route à suivre.

Internet est un réseau routé, par opposition aux réseaux X.25 ou ATM, qui sont des réseaux commutés. Dans un réseau routé, chaque paquet suit sa propre route, qui est à chaque instant optimisée, tandis que, dans un réseau commuté, la route est toujours la même.

Les problèmes posés par la synchronisation

L'architecture IP, utilisant le routage et le service best-effort, présente une difficulté : le synchronisme. En effet, le temps de traversée d'un paquet est relativement aléatoire. Il dépend du nombre de paquets en attente dans les lignes de sortie des nœuds et du nombre de retransmissions correspondant à des erreurs en ligne. Le fait de transporter des applications temps réel avec des synchronisations fortes, comme la parole temps réel, pose des problèmes complexes, qui ne peuvent être résolus que dans certains cas. Si l'on suppose qu'une conversation téléphonique interactive entre deux individus accepte une latence de 600 ms aller-retour, il est possible de resynchroniser les octets à la sortie, si le temps total de paquétisation-dépaquétisation et de traversée du réseau est effectivement inférieur à 300 ms dans chaque sens.

La resynchronisation qu'il est possible d'obtenir est illustrée à la figure 16.4. Il faut déterminer un temps maximal de traversée du réseau et effectuer une resynchronisation sur cette valeur. Le logiciel des terminaux informatiques, que l'on peut qualifier d'intelligent, permet de gérer ces problèmes temporels si le temps de traversée du réseau est borné. Ensuite se pose la question de savoir si le temps maximal de traversée est acceptable par l'application. Ce temps maximal de traversée du réseau doit être inférieur à 28 ms si des échos existent aux extrémités et égal au plus à 300 ms s'il y a interactivité et à plusieurs secondes, voire dizaines de secondes si l'application est monodirectionnelle, comme la vidéo à la demande ou la diffusion de programmes radio.

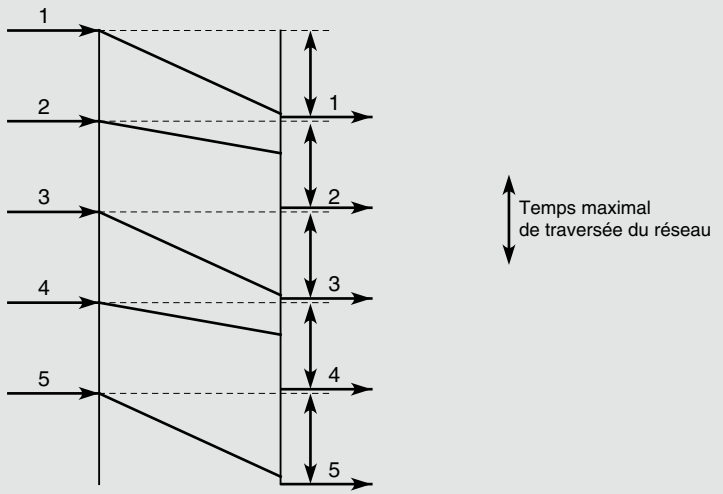


Figure 16.4
Resynchronisation d'une application isochrone

Il est évident que si le terminal est non intelligent et analogique, la reconstruction du flux synchrone est impossible dans un réseau à transfert de paquets. De plus, il est nécessaire de mettre en place des protocoles permettant un contrôle plus strict de l'information isochrone en cas de saturation. De ce fait, le réseau Internet a des difficultés à transporter des données isochrones, au moins jusqu'à l'arrivée de la nouvelle génération, qui a été conçue dans l'esprit du multimédia.

L'adressage IPv4 et IPv6

Comme Internet est un réseau de réseaux, l'adressage y est particulièrement important. Cette section donne un premier aperçu des problèmes d'adressage au travers du protocole IP de première génération IPv4 et de la nouvelle génération IPv6.

Les machines d'Internet ont une adresse IPv4 représentée sur un entier de 32 bits. L'adresse est constituée de deux parties : un identificateur de réseau et un identificateur de la machine pour ce réseau. Il existe quatre classes d'adresses, chacune permettant de coder un nombre différent de réseaux et de machines :

- classe A : 128 réseaux et 16 777 216 hôtes (7 bits pour les réseaux et 24 pour les hôtes) ;
- classe B : 16 384 réseaux et 65 535 hôtes (14 bits pour les réseaux et 16 pour les hôtes) ;
- classe C : 2 097 152 réseaux et 256 hôtes (21 bits pour les réseaux et 8 pour les hôtes) ;
- classe D : adresses de groupe (28 bits pour les hôtes appartenant à un même groupe).

Ces adresses sont détaillées à la figure 16.5.

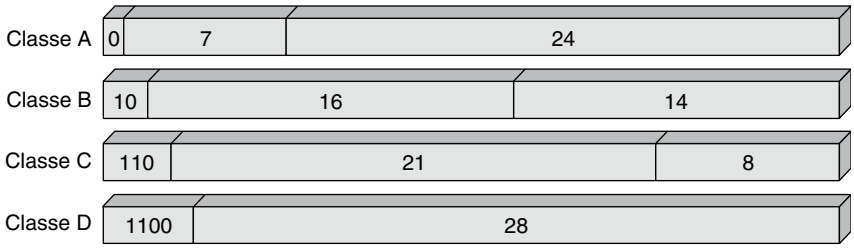


Figure 16.5
Classes d'adresses d'IPv4

Les adresses IP ont été définies pour être traitées rapidement. Les routeurs qui effectuent le routage en se fondant sur le numéro de réseau sont dépendants de cette structure. Un hôte relié à plusieurs réseaux a plusieurs adresses IP. En réalité, une adresse n'identifie pas simplement une machine mais une connexion à un réseau.

Pour assurer l'unicité des numéros de réseau, les adresses Internet sont attribuées par un organisme central, le NIC (Network Information Center). On peut également définir ses propres adresses si l'on n'est pas connecté à Internet. Il est toutefois vivement conseillé d'obtenir une adresse officielle pour garantir l'interopérabilité dans le futur.

Comme l'adressage d'IPv4 est quelque peu limité, il a fallu proposer une extension pour couvrir les besoins des années 2 000. Cette extension d'adresse est souvent présentée comme la raison d'être de la nouvelle version d'IP, alors qu'il ne s'agit que d'une raison parmi d'autres.

L'adresse IPv6 tient sur 16 octets. Le nombre d'adresses potentielles autorisées par IPv6 dépasse 10^{23} pour chaque mètre carré de la surface terrestre. La difficulté d'utilisation de cette immense réserve d'adresses réside dans la représentation et l'utilisation rationnelle de ces 128 bits. La représentation s'effectue par groupe de 16 bits et se présente sous la forme suivante :

123 : FCBA : 1024 : AB23 : 0 : 0 : 24 : FEDC

Des séries d'adresses égales à 0 peuvent être abrégées par le signe ::, qui ne peut apparaître qu'une seule fois dans l'adresse. En effet, ce signe n'indiquant pas le nombre de 0 successifs, pour déduire ce nombre en examinant l'adresse, les autres séries ne peuvent pas être abrégées.

L'adressage IPv6 est hiérarchique. Une allocation des adresses (c'est-à-dire une répartition entre les potentiels utilisateurs) a été proposée, dont le tableau 16.1 fournit le détail.

Adresse	Premiers bits de l'adresse	Caractéristiques
0 :: /8	0000 0000	Réservé
100 :: /8	0000 0001	Non assigné
200 :: /7	0000 0001	Adresse ISO
400 :: /7)	0000 010	Adresse Novell (IPX)
600 :: /7	0000 011	Non assigné
800 :: /5	0000 1	Non assigné
1000 :: /4	0001	Non assigné
2000 :: /3	001	Non assigné
4000 :: /3	010	Aadresses des fournisseurs de services
6000 :: /3	011	Non assigné
8000 :: /3	100	Adresses géographiques d'utilisateurs
A000 :: /3	101	Non assigné
C000 ::/3	110	Non assigné
E000 :: /4	1110	Non assigné
F000 :: /5	1111 0	Non assigné
F800 :: /6	1111 10	Non assigné
FC00 :: /7	1111 110	Non assigné
FE00 :: /9	1111 1110 0	Non assigné
FE80 :: /10	1111 1110 10	Adresses de liaisons locales
FEC0 :: /10	1111 1110 11	Adresses de sites locaux
FF00 :: /8	1111 1111	Adresse de multipoint

TABLEAU 16.1 • Allocation des adresses IPv6

Les protocoles de résolution d'adresses ARP et RARP

Les adresses IP sont attribuées indépendamment des adresses matérielles des machines. Pour envoyer un datagramme sur Internet, le logiciel réseau doit convertir l'adresse IP en une adresse physique, utilisée pour transmettre la trame.

La résolution d'adresse désigne la détermination de l'adresse d'un équipement à partir de l'adresse de ce même équipement à un autre niveau protocolaire. On résout, par exemple, une adresse IP en une adresse Ethernet ou en une adresse ATM.

C'est le protocole ARP (Address Resolution Protocol) qui effectue cette traduction entre le monde IP et Ethernet en s'appuyant sur le réseau physique. ARP permet aux machines de résoudre les adresses sans utiliser de table statique répertoriant toutes les adresses des deux mondes. Une machine utilise ARP pour déterminer l'adresse physique du destinataire en diffusant dans le sous-réseau une requête ARP contenant l'adresse IP à traduire. La machine possédant l'adresse IP concernée répond en renvoyant son adresse physique. Pour rendre ARP plus performant, chaque machine tient à jour en mémoire une table des adresses résolues et réduit ainsi le nombre d'émissions en mode diffusion.

Au moment de son initialisation (*bootstrap*), une machine sans mémoire de masse (*diskless*) doit contacter son serveur pour déterminer son adresse IP et pouvoir utiliser les services TCP/IP. Le protocole RARP (Reverse ARP) permet à une machine d'utiliser son adresse physique pour déterminer son adresse logique sur Internet. Le mécanisme RARP permet à un calculateur de se faire identifier comme cible en diffusant sur le réseau une requête RARP. Les serveurs recevant le message examinent leur table et répondent. Une fois l'adresse IP obtenue, la machine la stocke en mémoire vive et n'utilise plus RARP jusqu'à ce qu'elle soit réinitialisée.

Le protocole ARP s'appuie sur le réseau physique afin d'effectuer la traduction d'adresse. Pour déterminer l'adresse physique du destinataire, une machine diffuse sur le sous-réseau une requête ARP qui contient l'adresse IP à traduire. La machine possédant l'adresse IP concernée répond en renvoyant son adresse physique. Ce processus est illustré à la figure 16.6.

De façon inverse, une station qui se connecte au réseau peut connaître sa propre adresse physique sans avoir d'adresse IP. Au moment de son initialisation, la machine contacte son serveur afin de déterminer son adresse IP et de pouvoir utiliser les services TCP/IP. Le protocole RARP lui permet d'utiliser son adresse physique pour obtenir son adresse logique sur Internet. Par le biais du mécanisme RARP, une station peut se faire identifier comme cible en diffusant sur le réseau une requête RARP. Les serveurs recevant le message examinent leur table et répondent. Une fois l'adresse IP obtenue, la machine la stocke en mémoire vive et n'utilise plus RARP jusqu'à ce qu'elle soit réinitialisée.

Dans IPv6, les protocoles ARP et RARP sont remplacés par un protocole de découverte des voisins, appelé ND (Neighbor Discovery), qui est un sous-ensemble du protocole de contrôle ICMP (Internet Control Message Protocol), présenté en détail au chapitre 17.

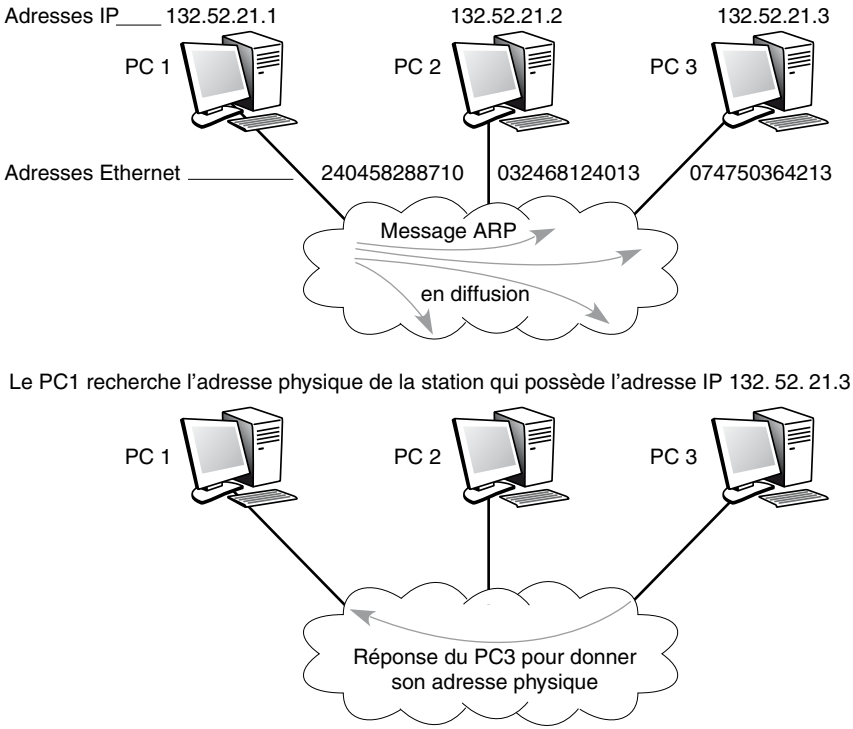


Figure 16.6

Fonctionnement du protocole ARP

DNS (Domain Name System)

Nous avons vu que les structures d'adresses étaient complexes à manipuler, car elles se présentent sous forme de groupes de chiffres décimaux de type *abc* : *def:ghi:jkl*, avec une valeur maximale de 255 pour chacun des quatre groupes. Les adresses IPv6 tiennent sur 8 groupes de 4 chiffres décimaux. La saisie de telles adresses dans le corps d'un message deviendrait vite insupportable. C'est la raison pour laquelle l'adressage utilise une structure hiérarchique complètement différente, beaucoup plus simple à manipuler et à mémoriser.

Le rôle du DNS est de permettre la mise en correspondance des adresses physiques dans le réseau et des adresses logiques. La structure logique est hiérarchique et utilise au plus haut niveau des domaines caractérisant principalement les pays, qui sont indiqués par deux lettres, comme *fr* pour la France, et des domaines fonctionnels comme :

- com : organisations commerciales ;
- edu : institutions académiques ;
- org : organisations, institutionnelles ou non ;
- gov : gouvernement américain ;
- mil : organisations militaires américaines ;

- net : opérateurs de réseau ;
- int : entités internationales.

À l'intérieur de ces grands domaines, on trouve des sous-domaines, qui correspondent à de grandes entreprises ou à d'importantes institutions. Par exemple, *rp* représente le nom de l'équipe travaillant dans le domaine des réseaux et des performances du laboratoire LIP6 de l'Université Paris VI, ce qui donne l'adresse *rp.lip6.fr* pour le personnel de cette équipe au sein du laboratoire.

Pour réaliser cette opération de traduction, le monde IP utilise des serveurs de noms, c'est-à-dire des serveurs pouvant répondre à des requêtes de résolution de nom ou encore être capables d'effectuer la traduction d'un nom en une adresse. Les serveurs de noms d'Internet sont les serveurs DNS. Ces serveurs sont hiérarchiques. Lorsqu'il faut retrouver l'adresse physique IP d'un utilisateur, les serveurs qui gèrent le DNS s'envoient des requêtes de façon à remonter suffisamment dans la hiérarchie pour trouver l'adresse physique du correspondant. Ces requêtes sont effectuées par l'intermédiaire de petits messages, qui portent la question et la réponse en retour.

La figure 16.7 illustre le fonctionnement du DNS. Le client *guy.pujolle@reseau.lip6.fr* veut envoyer un message à *xyz.xyz@systeme.lip6.fr.* Pour déterminer l'adresse IP de *xyz.xyz@systeme.lip6.fr,* une requête est émise par le PC de Guy Pujolle, qui interroge le serveur de noms du domaine *réseau.lip6.fr.* Si celui-ci a en mémoire la correspondance, il répond au PC. Dans le cas contraire, la requête remonte dans la hiérarchie et atteint le serveur de noms de *lip6.fr,* qui, de nouveau, peut répondre positivement s'il connaît la correspondance. Dans le cas contraire, la requête est acheminée vers le serveur de noms de *systeme.lip6.fr,* qui connaît la correspondance. C'est donc lui qui répond au PC de départ.

Le format d'une requête DNS est illustré à la figure 16.8.

Les deux premiers octets contiennent une référence. Le client choisit une valeur à placer dans ce champ, et le serveur répond en utilisant la même valeur, de sorte que le client reconnaisse sa demande. Les deux octets suivants contiennent les bits de contrôle. Ces derniers indiquent si le message est une requête du client ou une réponse du serveur, si une demande à un autre site doit être effectuée, si le message a été tronqué par manque de place, si le message de réponse provient du serveur de noms responsable ou non de l'adresse demandée, etc. Pour le récepteur qui répond, un code de réponse est également inclus dans ce champ.

Les six possibilités suivantes ont été définies :

- 0 : pas d'erreur.
- 1 : la question est formatée de façon illégale.
- 2 : le serveur ne sait pas répondre.
- 3 : le nom demandé n'existe pas.
- 4 : le serveur n'accepte pas la demande.
- 5 : le serveur refuse de répondre.

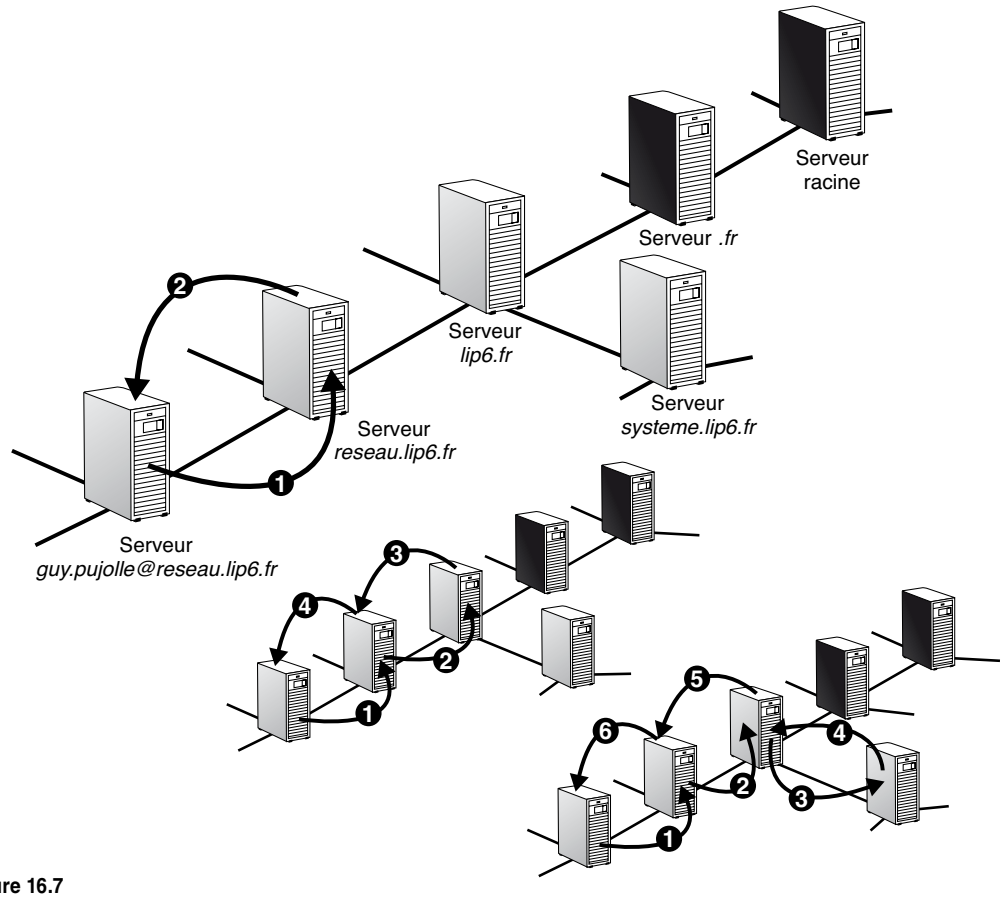


Figure 16.7

Fonctionnement du DNS

Identifier *(identificateur)*	Control *(contrôle)*
Number of Questions *(nombre de questions)*	Number of Answers *(nombre de réponses)*
Number of Authorities *(nombre d'autorités)*	Nombre de champs supplémentaires
Question *(question)*	
Answer *(réponse)*	
Authority *(autorité)*	
Additional *(champ supplémentaire)*	

Figure 16.8

Format d'une requête DNS

La plupart des requêtes n'effectuent qu'une demande à la fois. La forme de ce type de requête est illustrée à la figure 16.9. Dans la zone Question, le contenu doit être interprété de la façon suivante : 6 indique que 6 caractères suivent ; après les 6 caractères de réseau, 4 désigne les 4 caractères de *lip6,* 2 les deux caractères de *fr* et enfin 0 la fin du champ.

Le champ Autorité permet aux serveurs qui ont autorité sur le nom demandé de se faire connaître. La zone Champs supplémentaires permet de transporter des informations sur le temps pendant lequel la réponse à la question est valide.

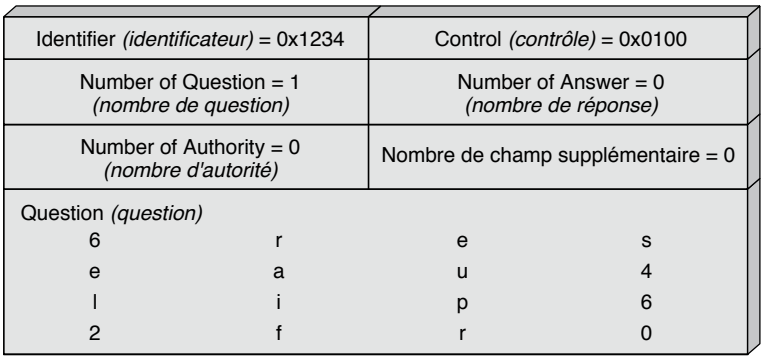


Figure 16.9

Requête DNS avec une seule demande

Le routage IP

Un environnement Internet résulte de l'interconnexion de réseaux physiques par des routeurs. Chaque routeur est connecté directement à deux ou plusieurs réseaux, les hôtes étant généralement connectés à un seul réseau, mais cela n'est pas obligatoire.

Il existe plusieurs types de routages :

- Routage direct. C'est le cas si les deux machines qui veulent communiquer sont rattachées au même réseau et ont donc le même numéro de réseau IP. Il peut s'agir de deux hôtes ou d'un routeur et d'un hôte. Il suffit, pour effectuer le transport du paquet IP, de déterminer l'adresse physique du destinataire et d'encapsuler le datagramme dans une trame avant de l'envoyer sur le réseau.
- Routage indirect. Dans ce cas, le routage est plus complexe car il faut déterminer le routeur auquel les datagrammes doivent être envoyés. Ces derniers peuvent ainsi être transmis de routeur en routeur jusqu'à ce qu'ils atteignent l'hôte destinataire. La fonction de routage se fonde principalement sur les tables de routage. Le routage est effectué à partir du numéro de réseau de l'adresse IP de l'hôte de destination. La table contient, pour chaque numéro de réseau à atteindre, l'adresse IP du routeur auquel envoyer le datagramme. Elle peut également comprendre une adresse de routeur par défaut et l'indication de routage direct. La difficulté du routage provient de l'initialisation et de la mise à jour des tables de routage.

- Le subnetting. Cette technique d'adressage et de routage normalisée permet de gérer plusieurs réseaux physiques à partir d'une même adresse IP d'Internet. Le principe du subnetting consiste à diviser la partie numéro d'hôte d'une adresse IP en numéro de sous-réseau et numéro d'hôte. En dehors du site, les adresses sont interprétées sans qu'il soit tenu compte du subnetting, le découpage n'étant connu et traité que de l'intérieur. Le redécoupage du numéro d'hôte permet de choisir librement le nombre de machines en fonction du nombre de réseaux sur le site. Au niveau conceptuel, les techniques d'adressage et de routage sont les mêmes. Au niveau physique, on utilise un masque d'adresse.

Le réseau Internet s'est tellement étendu qu'il a dû être scindé en systèmes autonomes pour en faciliter la gestion. On appelle système autonome (AS) un ensemble de routeurs et de réseaux reliés les uns aux autres, administrés par une même organisation et s'échangeant des paquets par le biais d'un même protocole de routage.

Le protocole de routage partagé par tous les routeurs d'un système autonome est appelé protocole de routage intérieur, ou IRP (Interior Routing Protocol). Un protocole intérieur n'a pas besoin d'être implémenté à l'extérieur du système autonome. De ce fait, on peut choisir son algorithme de routage de façon à optimiser le routage intérieur. Les protocoles intérieurs sont également appelés IGP (Interior Gateway Protocol).

Lorsqu'un réseau Internet comporte plusieurs systèmes autonomes reliés entre eux, il faut faire appel à un protocole de routage extérieur, ou ERP (Exterior Routing Protocol). Les protocoles ERP doivent avoir une connaissance des divers AS pour accomplir leur tâche. Les protocoles ERP sont également appelés EGP (Exterior Gateway Protocol).

La figure 16.10 donne un exemple de systèmes autonomes avec des protocoles IRP interconnectés par un ERP.

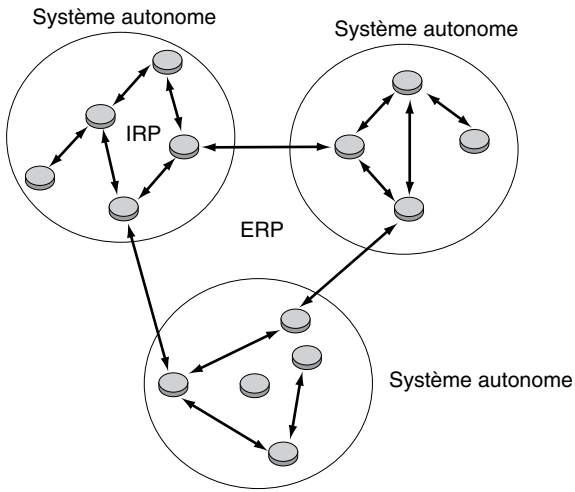


Figure 16.10

Protocoles de routage intérieur et extérieur

Les algorithmes de routage

Un algorithme de routage est un procédé permettant de déterminer le routage des paquets dans un nœud. Pour chaque nœud d'un réseau, l'algorithme détermine une table de routage, qui, à chaque destination, fait correspondre une ligne de sortie. L'algorithme doit mener à un routage cohérent, c'est-à-dire sans boucle. Cela signifie qu'il ne faut pas qu'un nœud route un paquet vers un autre nœud qui pourrait lui renvoyer le paquet.

On distingue trois grandes catégories d'algorithmes de routage :

- à vecteur de distance (distance-vector routing) ;
- à état des liens (link state routing) ;
- à vecteur de chemin (path-vector routing).

Les algorithmes de routage à vecteur de distance requièrent que chaque nœud s'échange des informations entre voisins, c'est-à-dire entre nœuds directement connectés. De ce fait, chaque nœud peut maintenir à jour une table en y ajoutant des informations sur tous ses voisins. Cette table donne la distance à laquelle se trouvent chaque nœud et chaque réseau à atteindre. Première à avoir été mise en œuvre dans le réseau ARPAnet, cette technique devient vite lourde lorsque le nombre de nœuds augmente puisqu'il faut transporter beaucoup d'informations de nœud en nœud. RIP (Routing Information Protocol) est le meilleur exemple de protocole utilisant un vecteur de distance.

Dans ce type d'algorithme, chaque routeur diffuse à ses voisins un vecteur listant chaque réseau qu'il peut atteindre avec la métrique associée, c'est-à-dire le nombre de sauts. Chaque routeur peut donc bâtir une table de routage avec les informations reçues de ses voisins mais n'a aucune idée de l'identité des routeurs qui se trouvent sur la route sélectionnée. De ce fait, l'utilisation de cette solution pose de nombreux problèmes pour les protocoles de routage extérieurs. Il est en effet supposé que tous les routeurs utilisent la même métrique, ce qui peut ne pas être le cas entre systèmes autonomes. De plus, un système autonome peut avoir des raisons particulières de se comporter différemment d'un autre système autonome. En particulier, si un système autonome a besoin de déterminer par quel autre système autonome vont passer ses messages, pour des raisons de sécurité par exemple, il ne peut pas le savoir.

Les algorithmes à état des liens avaient au départ pour objectif de pallier les défauts du routage par vecteur de distance. Quand un routeur est initialisé, il doit définir le coût de chacun de ses liens connectés à un autre nœud. Le nœud diffuse ensuite l'information à l'ensemble des nœuds du système autonome, et donc pas seulement à ses voisins. À partir de l'ensemble de ces informations, les nœuds peuvent effectuer un calcul leur permettant d'obtenir une table de routage indiquant le coût nécessaire pour atteindre chaque destination. Lorsqu'un routeur reçoit des informations qui modifient sa table de routage, il en avertit tous les routeurs intervenant dans sa configuration. Comme chaque nœud possède la topologie du réseau et les coûts de chaque lien, le routage peut être vu comme centralisé dans chaque nœud. Le protocole OSPF (Open Shortest Path First) met en œuvre cette technique, qui correspond à la deuxième génération de protocoles Internet.

Les algorithmes à état des liens règlent les problèmes évoqués précédemment pour le routage extérieur mais en soulèvent d'autres. Les divers systèmes autonomes peuvent avoir des métriques différentes ainsi que des restrictions spécifiques, de telle sorte qu'il ne soit pas possible d'obtenir un routage cohérent. La diffusion de l'ensemble des informations nécessaires à l'ensemble des systèmes autonomes peut par ailleurs devenir rapidement ingérable.

L'objectif des algorithmes à vecteur de chemin est de pallier les insuffisances des deux premières catégories en se dispensant des métriques et en cherchant à savoir quel réseau peut être atteint par quel nœud et quels systèmes autonomes doivent être traversés pour cela. Cette approche est très différente de celle par vecteur de distance puisque les vecteurs de chemin ne prennent pas en compte les distances ni les coûts. De plus, du fait que chaque information de routage liste tous les systèmes autonomes qui doivent être traversés pour arriver au routeur destinataire, l'approche par vecteur de chemin est beaucoup plus dirigée vers les systèmes de routage extérieurs. Le protocole BGP (Border Gateway Protocol) appartient à cette catégorie.

RIP (Routing Information Protocol)

RIP est le protocole le plus utilisé dans l'environnement TCP/IP pour router les paquets entre les passerelles du réseau Internet. C'est un protocole IGP (Interior Gateway Protocol), qui utilise un algorithme permettant de trouver le chemin le plus court.

Par chemin, on entend le nombre de nœuds traversés, qui doit être compris entre 1 et 15. La valeur 16 indique une impossibilité. En d'autres termes, si le chemin pour aller d'un point à un autre du réseau Internet est supérieur à 15, la connexion ne peut être mise en place. Les messages RIP permettant de dresser les tables de routage sont envoyés approximativement toutes les 30 secondes. Si un message RIP n'est pas parvenu à son voisin au bout de trois minutes, ce dernier considère que le lien n'est plus valide, le nombre de liens étant supérieur à 15. Le protocole RIP se fonde sur une diffusion périodique des états du réseau d'un routeur vers ses voisins. La version RIP2 comporte un routage par sous-réseau, l'authentification des messages, la transmission multipoint, etc.

Un exemple d'implémentation de cet algorithme est donné au chapitre 8 avec le routage distribué.

OSPF

OSPF fait partie de la deuxième génération de protocoles de routage. Beaucoup plus complexe que RIP, mais au prix de performances supérieures, il utilise une base de données distribuée, qui garde en mémoire l'état des liens. Ces informations forment une description de la topologie du réseau et de l'état des nœuds, qui permet de définir l'algorithme de routage par un calcul des chemins les plus courts.

L'algorithme OSPF permet, à partir d'un nœud, de calculer le chemin le plus court, avec les contraintes indiquées dans les contenus associés à chaque lien. Les routeurs OSPF communiquent entre eux par l'intermédiaire du protocole OSPF, placé au-dessus d'IP. Regardons maintenant ce protocole de façon un peu plus détaillée.

L'hypothèse de départ pour les protocoles à état des liens est que chaque nœud est capable de détecter l'état du lien avec ses voisins (marche ou arrêt) et le coût de ce lien. Il faut donner à chaque nœud suffisamment d'informations pour lui permettre de trouver la route la moins chère vers toutes les destinations. Chaque nœud doit donc avoir la connaissance de ses voisins. Si chaque nœud à la connaissance des autres nœuds, une carte complète du réseau peut être dressée. Un algorithme se fondant sur l'état des voisins nécessite deux mécanismes : la dissémination fiable des informations sur l'état des liens et le calcul des routes par sommation des connaissances accumulées sur l'état des liens.

Une première solution consiste à réaliser une inondation fiable des informations, de façon à s'assurer que chaque nœud reçoit sa copie des informations de la part de tous les autres nœuds. En fait, chaque nœud inonde ses voisins, qui, à leur tour, inondent leurs propres voisins. Plus précisément, chaque nœud crée ses propres paquets de mise à jour, appelés LSP (Link-State Packet), contenant les informations suivantes :

- Identité du nœud qui crée le LSP.
- Liste des nœuds voisins avec le coût du lien associé.
- Numéro de séquence.
- Temporisateur (Time To Live) pour ce message.

Les deux premières informations sont nécessaires au calcul des routes. Les deux dernières ont pour objectif de rendre fiable l'inondation. Le numéro de séquence permet de mettre dans l'ordre les informations qui auraient été reçues dans le désordre. Le protocole possède des éléments de détection d'erreur et de retransmission.

Le calcul de la route s'effectue après réception de l'ensemble des informations sur les liens. À partir de la carte complète du réseau et des coûts des liens, il est possible de calculer la meilleure route. Le calcul est effectué en utilisant l'algorithme de Dijkstra sur le chemin le plus court.

Dans le sigle OSPF (Open Shortest Path First), le mot Open indique que l'algorithme est ouvert et pris en charge par l'IETF. En utilisant les mécanismes indiqués ci-dessus, le protocole OSPF ajoute les propriétés supplémentaires suivantes :

- Authentification des messages de routage. Des dysfonctionnements peuvent conduire à des catastrophes. Par exemple, un nœud qui, à la suite de la réception de messages erronés, volontairement ou non, ou de messages d'un attaquant modifiant sa table de routage, calcule une table de routage dans laquelle tous les nœuds peuvent être atteints à un coût nul reçoit automatiquement tous les paquets du réseau. Ces dysfonctionnements peuvent être évités en authentifiant les émetteurs des messages. Les premières versions d'OSPF possédaient un mot de passe d'authentification sur 8 octets. Les dernières versions possèdent des authentifications beaucoup plus fortes.
- Nouvelle hiérarchie. Cette hiérarchie doit permettre un meilleur passage à l'échelle. OSPF introduit un niveau de hiérarchie supplémentaire en partitionnant les domaines en ères (areas). Cela signifie qu'un routeur à l'intérieur d'un domaine n'a pas besoin de savoir comment atteindre tous les réseaux du domaine. Il suffit qu'il sache comment atteindre la bonne ère. Cela entraîne une réduction des informations qui doivent être transmises et stockées.

Il y a plusieurs types de messages OSPF, mais ils utilisent tous le même en-tête, qui est illustré à la figure 16.11.

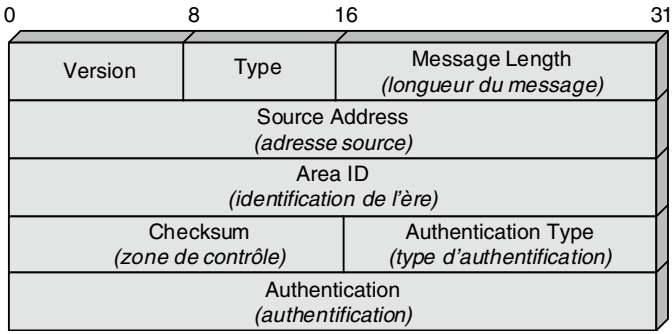


Figure 16.11
Format de l'en-tête OSPF

La version en cours est la 2. Cinq types ont été définis avec des valeurs de 1 à 5. L'adresse source indique l'émetteur du message. L'identification de l'ère indique l'ère dans laquelle se trouve le nœud émetteur. Le type d'authentification porte la valeur 0 s'il n'y a pas d'authentification, 1 en cas d'authentification par mot de passe et 2 si une technique d'authentification est mise en œuvre et décrite dans les 4 octets suivants.

Les cinq types de messages comportent le message Hello comme type 1. Ce message est envoyé par un nœud à ses voisins pour leur indiquer qu'il est toujours présent et non en panne. Les quatre autres types servent à envoyer des informations telles que des requêtes, des envois ou des acquittements des messages LSP. Ces messages transportent principalement des LSA (Link-State Advertisement), c'est-à-dire des informations sur l'état des liens. Un message OSPF peut contenir plusieurs LSA.

La figure 16.12 illustre un message OSPF de type 1 portant un LSA.

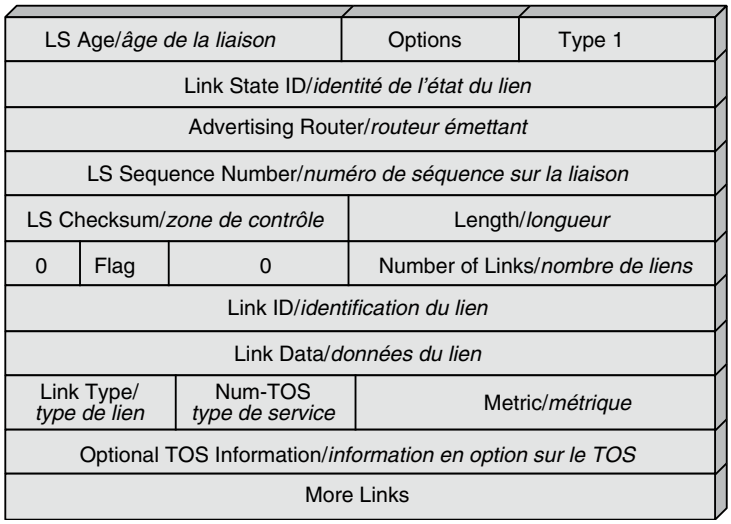


Figure 16.12
Message OSPF portant un LSA

Ce type indique le coût des liens entre les routeurs. Le type 2 est utilisé pour indiquer les réseaux auxquels l'émetteur est connecté. Les types 3 et 4 se préoccupent de l'indication des ères. À la figure 18.13, le champ LS Age est l'équivalent du temporisateur TTL (Time To Live), si ce n'est que le compteur augmente jusqu'à une certaine valeur prédéfinie, alors que le TTL descend jusqu'à 0.

Le type est ici le type 1. Les deux champs Link State ID et LS sequence number sont identiques et transportent l'identificateur du routeur qui émet le message. La raison de ce double champ est de vérifier l'identité du routeur par deux moyens différents. Le numéro de séquence permet de reséquencer les messages reçus. Le LS Checksum permet de vérifier la correction du message. Il prend en compte les informations à partir du champ Option. Le champ longueur indique la longueur totale du message. Ce sont ensuite des informations sur le LSA qui sont transportées : Link ID identifiant chaque lien, informations à propos du lien (Link Data) et métrique.

Le champ TOS (Type Of Service) permet à l'algorithme OSPF de choisir la meilleure route possible en fonction du type de service. Il peut donc y avoir plusieurs métriques qui dépendent du type de service recherché. Le coût des lignes peut également varier en fonction des métriques choisies.

Si le protocole RIP est adapté à la gestion du routage dans de petits réseaux, OSPF s'applique à des réseaux beaucoup plus complexes.

IS-IS

L'algorithme IS-IS a été principalement développé par l'ISO (ISO 10589). Il décrit un routage hiérarchique fondé sur la décomposition des réseaux de communication en domaines. Dans un domaine, les différents nœuds indiquent leur état aux routeurs IS-IS afférents. Les communications interdomaines sont effectuées par un routage vers un point d'accès au domaine déterminé par les routeurs chargés des communications externes au domaine.

IGRP (Interior Gateway Routing Protocol)

Version améliorée de RIP, IGRP a été conçu par Cisco Systems pour ses propres routeurs. Il intègre le routage multichemin, la gestion des routes par défaut, la diffusion de l'information toutes les 90 secondes au lieu de toutes les 30 secondes, la détection des bouclages, c'est-à-dire des retours à un point par lequel le paquet est déjà passé, etc. Ce protocole a lui-même été étendu pour une meilleure protection contre les boucles par le protocole EIGRP (Extended IGRP).

EGP (Exterior Gateway Protocol)

EGP est le premier algorithme de routage à avoir été mis au point, au début des années 1980, pour router un paquet d'un système autonome vers un autre.

Il comporte trois procédures essentielles, qui permettent l'échange d'informations. La première procédure concerne la définition d'une passerelle voisine. Cette dernière étant connue, une deuxième procédure détermine le lien qui permet aux deux voisins de communiquer. La troisième procédure concerne l'échange de paquets entre deux voisins connectés par un lien. Les faiblesses d'EGP sont apparues avec le développement exponentiel d'Internet et le besoin d'éviter certaines zones politiquement sensibles.

BGP (Border Gateway Protocol)

Pour répondre aux faiblesses d'EGP, un nouvel algorithme a été mis en chantier par l'IETF sous le nom de BGP. Une première version, BGP-1, a été implémentée en 1990, suivie de près par BGP-2 puis BGP-3. Au bout de quelques années a été déployé BGP-4, qui permet de gérer beaucoup plus efficacement les tables de routage de grande dimension en rassemblant en une seule ligne plusieurs sous-réseaux.

BGP apporte de nouvelles propriétés par rapport à EGP, en particulier celle de gérer les boucles, qui devenaient courantes dans EGP puisque ce protocole ne s'occupe que des couples de voisins, sans prendre en compte les rebouclages possibles par un troisième réseau autonome.

Les messages échangés par le biais de BGP-4 sont les suivants :

- open : pour ouvrir une relation avec un nœud voisin.
- update : pour transmettre des informations au sujet d'une seule route ou demander la destruction de routes qui ne sont plus disponibles.
- keepalive : pour acquitter les messages open et confirmer que la relation de voisinage est toujours vivante.
- notification : pour envoyer un message d'erreur.

Les trois grandes procédures fonctionnelles suivantes sont définies dans BGP :

- acquisition des nœuds voisins ;
- possibilité d'atteindre le voisin ;
- possibilité d'atteindre des réseaux.

Deux routeurs sont considérés comme voisins s'ils sont dans le même réseau. Si les deux routeurs sont dans des domaines autonomes distincts, ils peuvent avoir besoin d'échanger des informations de routage. Pour cela, il faut d'abord réaliser une acquisition des voisins, c'est-à-dire permettre à deux nœuds qui ne sont pas dans le même système autonome d'échanger des informations de routage. L'acquisition doit être faite par une procédure formelle puisqu'un des deux nœuds peut ne pas avoir envie d'échanger de l'information de routage. Pour réaliser l'acquisition, un nœud émet le message OPEN. Si le routeur distant accepte la relation, il renvoie un KEEPALIVE. Une fois la relation établie, pour maintenir la relation active les nœuds s'échangent des KEEPALIVE. Chaque nœud maintient une base de données des réseaux qu'il peut atteindre et de la route permettant d'arriver à ces différents réseaux. Quand un changement intervient, le routeur diffuse un message UPDATE vers les autres routeurs, ce qui permet à ceux-ci de se mettre à jour.

La figure 16.13 illustre le format du paquet de mise à jour BGP.

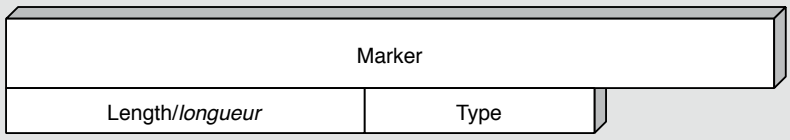


Figure 16.13

Format du paquet de mise à jour BGP

Le champ Marker est réservé à l'authentification. L'émetteur peut mettre un texte chiffré qui ne peut être déchiffré que par le récepteur possédant la clé de chiffrement. Length donne la longueur du message en octet. Les types de message sont OPEN, UPDATE, KEEPALIVE et NOTIFICATION.

Pour mettre en place une relation de voisinage, le routeur de départ initie une connexion TCP puis envoie un message OPEN. Ce message indique le système autonome dans lequel l'émetteur se trouve ainsi que l'adresse IP du routeur. Il inclut également un paramètre HOLD TIME PARAMETER, qui indique le nombre de secondes proposées pour le temporisateur Hold Timer afin de déterminer le temps maximal entre deux messages provenant de l'émetteur (KEEPALIVE, UPDATE). Si le distant accepte la relation, il calcule le minimum de son propre temporisateur Hold Timer et de celui de l'émetteur et l'envoie à l'émetteur.

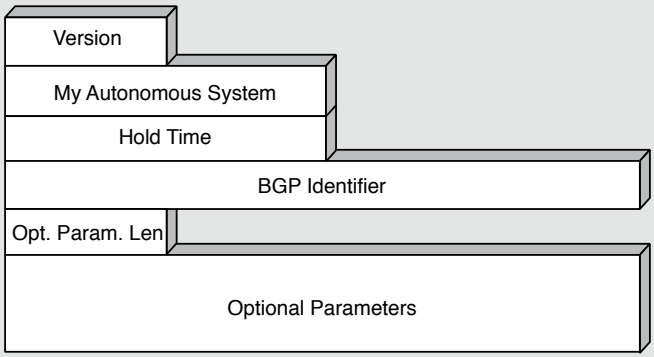


Figure 16.14

Champs du paquet OPEN de BGP

Les champs du paquet OPEN sont indiqués à la figure 16.14. Ces champs sont les suivants :

- Version : valeur sur un octet indiquant la version du protocole BGP utilisé (4 pour BGP-4).
- My Autonomous System (mon système autonome) : valeur sur 2 octets indiquant le numéro de système autonome de l'émetteur.
- Hold Time (temps de retenue) : champ de 2 octets indiquant le nombre de secondes que l'émetteur propose pour le compteur de retenue. Ce dernier permet d'éviter les bouclages infinis dans les systèmes autonomes. Une fois qu'un périphérique BGP reçoit un message open, il doit calculer la valeur du compteur de retenue qui va être utilisé. Pour cela, il choisit la plus petite valeur entre le compteur de retenue qu'il vient de recevoir dans son message open et la valeur qui a été configurée pour lui-même. La valeur choisie est en fait le nombre de secondes entre la réception de messages keepalive et update envoyés par l'émetteur.
- BGP Identifier (identifiant BGP) : champ de 4 octets indiquant l'identifiant BGP. Cet identifiant est fondé sur l'adresse IP assignée au périphérique BGP.
- Optional Parameters Length : champ d'un octet indiquant la taille totale du champ Optional Parameters en octet. Si la valeur est 0, c'est qu'il n'y a pas de paramètres optionnels.
- Optional Parameters : champ contenant la liste des paramètres optionnels qui sont représentés par des triplets Parameter Type, Parameter Length et Parameter Value. Le champ Parameter Type identifie de manière unique chaque paramètre optionnel. Le champ Parameter Length indique la taille en octet du champ Parameter Value. Le champ Parameter Value est un champ de taille variable (c'est pourquoi sa taille est indiquée dans le champ Parameter Length) contenant le paramètre optionnel lui-même.
- Le message keepalive ne prend en compte que l'en-tête des messages BGP. Il doit être émis suffisamment souvent pour que le temporisateur Hold Timer ne se déclenche pas.

- Les messages update permettent d'acheminer deux types de messages :
- Les informations au sujet d'une seule route, qui sont enregistrées dans les bases de données d'information des routeurs.
- Les informations au sujet d'une liste de routes qui vont être détruites.

Les messages NOTIFICATION sont envoyés quand une erreur a été détectée. Les erreurs suivantes peuvent être émises :

- message header error : une erreur dans l'en-tête du message a été détectée comme un défaut d'authentification ou une erreur de syntaxe.
- open message error : une erreur dans la syntaxe du message open ou un refus de la valeur du Hold Timer a été détecté.
- update message error : une erreur dans le message update a été détectée comme une erreur de syntaxe.
- hold timer expired : le temporisateur Hold Timer a expiré, et la session de voisinage est fermée.
- finite state machine error : une erreur procédurale s'est produite.
- cease : pour fermer une connexion avec un autre routeur dans une circonstance non prise en charge par les messages précédents.

IDRP (Interdomain Routing Protocol)

Les estimations de départ prévoyaient qu'Internet serait constitué de dizaines de réseaux et de centaines de machines. Ces chiffres ont été multipliés par 10, 100 puis 1 000 pour les réseaux et par 1 000, 10 000 et 100 000 pour les machines. Ces démultiplications ne sont pas les seuls révélateurs du succès d'Internet. Les mesures montrent que le débit qui passe sur le réseau dépasse très largement celui représenté par l'ensemble des paroles téléphoniques échangées dans le monde entier.

Une telle explosion pose la question de la capacité des mécanismes de routage mis en place à en supporter la charge. Pour réduire les risques de saturation et prolonger les mécanismes actuels, la solution immédiate consiste à généraliser le subnetting. Le subnetting consiste à donner une adresse commune particulière, le masque, à l'ensemble des stations participant au même réseau logique, même si les adresses IP des stations de ce réseau logique proviennent de sous-réseaux distincts. Cela permet aux tables de routage de croître plus lentement.

Dans l'environnement IPv6, un nouveau protocole, IDRP, fruit d'études consacrées au routage entre les domaines de routage (*routing domain*) par l'ISO, a été adapté au monde Internet pour réaliser le routage entre systèmes autonomes. Le rôle d'IDRP est légèrement différent de celui des protocoles fonctionnant à l'intérieur d'un domaine, puisqu'il définit une politique de routage entre systèmes autonomes et non seulement un algorithme de routage. La politique définie dans cette proposition conduit les routeurs d'un système autonome à se mettre d'accord pour, par exemple, ne pas passer par un domaine déterminé ou ne pas autoriser d'autres systèmes autonomes à envoyer des paquets IP vers un système autonome déterminé. En d'autres termes, il doit y avoir une concertation entre routeurs pour ne fournir que les indications correspondant à la politique définie.

Les algorithmes de routage de type OSPF ou RIP sont appliqués par des routeurs qui ont tous le même objectif : trouver la meilleure route possible, en minimisant soit le nombre de saut, soit le temps de traversée du réseau, ou en optimisant la capacité de transport. Ces algorithmes s'appuient sur des notions de poids : si les liens ont des poids n_i, le chemin emprunté est celui dont la somme des poids des liens traversés est la plus faible. Le routage IDRP a aussi comme objectif de trouver les bons chemins, mais avec des restrictions pour chaque système autonome. L'algorithme repose sur des vecteurs de distance (Path Vector Routing), qui tiennent compte du chemin de bout en bout en plus des poids pour aller vers les nœuds voisins.

Comme le nombre de systèmes autonomes peut croître rapidement avec l'augmentation des capacités de traitement des routeurs, il a été décidé de regrouper les systèmes autonomes en confédérations. Le protocole IDRP travaille sur le routage entre ces confédérations. Pour véhiculer l'information de routage, IDRP utilise des paquets spécifiques, portés dans des paquets IP. Dans la zone IP, le champ En-tête suivant comporte le numéro 45 et indique le protocole IDRP.

NAT (Network Address Translation)

Le protocole IP version 4, que nous utilisons massivement actuellement, offre un champ d'adressage limité et insuffisant pour permettre à tout terminal informatique de disposer d'une adresse IP. Une adresse IP est en effet codée sur un champ de 32 bits, ce qui offre un maximum de 2^{32} adresses possibles, soit en théorie 4 294 967 296 terminaux raccordables au même réseau.

Pour faire face à cette pénurie d'adresses, et en attendant la version 6 du protocole IP, qui offrira un nombre d'adresses beaucoup plus important sur 128 bits, il faut recourir à un partage de connexion en utilisant la translation d'adresse, ou NAT (Network Address Translation).

Ce mécanisme se rencontre fréquemment à la fois en entreprise et chez les particuliers. Il distingue deux catégories d'adresses : les adresses dites publiques, c'est-à-dire visibles et accessibles de n'importe où (on dit aussi routables sur Internet), et les adresses dites privées, c'est-à-dire non routables sur Internet et adressables uniquement dans un réseau local, à l'exclusion du réseau Internet.

Le NAT consiste à établir des relations entre l'adressage privé dans un réseau et l'adressage public pour se connecter à Internet.

Adresses privées et adresses publiques

Dans le cas d'un réseau purement privé, et jamais amené à se connecter au réseau Internet, n'importe quelle adresse IP peut être utilisée. Dès qu'un réseau privé peut être amené à se connecter sur le réseau Internet, il faut distinguer les adresses privées des adresses publiques. Pour cela, chaque classe d'adresses IP dispose d'une plage d'adresses réservées, définies comme des adresses IP privées et donc non routables sur Internet. La RFC 1918 récapitule ces plages d'adresses IP, comme l'indique le tableau 16.2.

Classe d'adresses	Plages d'adresses privées	Masque réseau	Espace adressable
A	10.0.0.0 à 10.255.255.255	255.0.0.0	Sur 24 bits, soit 16 777 216 terminaux
B	172.16.0.0 à 172.31.255.255	255.240.0.0	Sur 20 bits, soit 1 048 576 terminaux
C	192.168.0.0. à 192.168.255.255	255.255.0.0	Sur 16 bits, soit 65 536 terminaux

TABLEAU 16.2 • Plages d'adresses privées

Dans ce cadre, et avant d'introduire la notion de NAT, les utilisateurs qui possèdent une adresse IP privée ne peuvent communiquer que sur leur réseau local, et non sur Internet,

tandis qu'avec une adresse IP publique, ils peuvent communiquer sur n'importe quel réseau IP.

L'adressage privé peut être utilisé librement par n'importe quel administrateur ou utilisateur au sein de son réseau local. Au contraire, l'adressage public est soumis à des restrictions de déclaration et d'enregistrement de l'adresse IP auprès d'un organisme spécialisé, l'IANA (Internet Assigned Numbers Authority), ce que les FAI effectuent globalement en acquérant une plage d'adresses IP pour leurs abonnés.

La figure 16.15 illustre un exemple d'adressage mixte, dans lequel on distingue les différentes communications possibles, selon un adressage de type privé ou public.

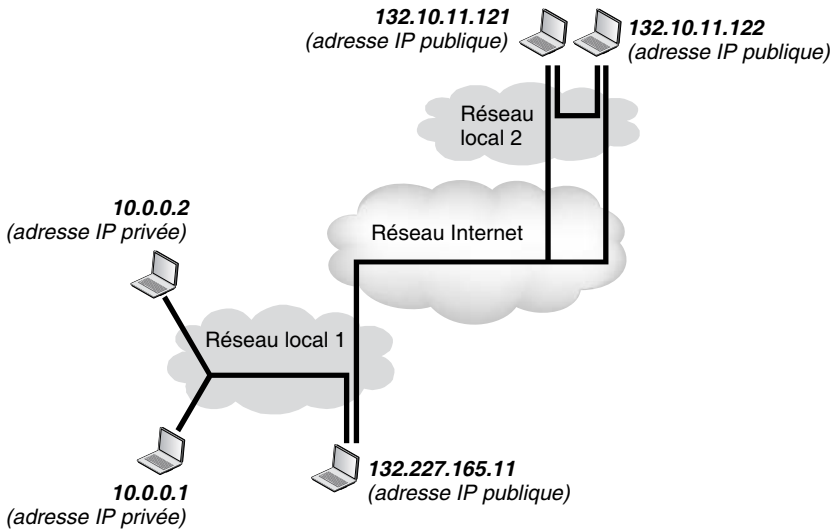


Figure 16.15

Adresses privées et publiques

Partager une adresse IP privée

Moyennant la souscription d'un accès Internet auprès d'un FAI, ce dernier fournit à ses utilisateurs une adresse IP privée. Dans un même foyer ou une même entreprise, deux utilisateurs ne peuvent communiquer en même temps sur Internet avec cette seule adresse IP fournie. Les adresses IP privées conviennent généralement pour couvrir un réseau privé, de particulier ou d'entreprise, mais pas pour communiquer directement avec les réseaux publics.

Pour résoudre ce problème et permettre à un terminal disposant d'une adresse IP privée de communiquer avec le réseau public, le processus de NAT fait intervenir une entité tierce entre un terminal, ayant une adresse IP privée, et tout autre terminal ayant une adresse IP publique. Ce mécanisme consiste à insérer un boîtier entre le réseau Internet et le réseau local afin d'effectuer la translation de l'adresse IP privée en une adresse IP publique. Aujourd'hui, la plupart des boîtiers, ou Home Gateway, des FAI proposent à

leurs abonnés cette fonctionnalité. Toutes les machines qui s'y connectent reçoivent par le biais du service DHCP (Dynamic Host Configuration Protocol) une adresse IP privée, que le boîtier se charge de translater en une adresse IP publique.

La figure 16.16 illustre un exemple dans lequel une passerelle NAT réalise une translation d'adresses pour quatre terminaux. Cette passerelle possède deux interfaces réseau. La première est caractérisée par une adresse IP publique (132.227.165.221). Connectée au réseau Internet, elle est reconnue et adressable normalement dans le réseau. La seconde interface est caractérisée par une adresse IP non publique (10.0.0.254). Connectée au réseau local, elle ne peut communiquer qu'avec les terminaux qui possèdent une adresse IP non publique de la même classe.

Lorsqu'un terminal ayant une adresse IP privée tente de se connecter au réseau Internet, il envoie ses paquets vers la passerelle NAT. Celle-ci remplace l'adresse IP privée d'origine par sa propre adresse IP publique (132.227.165.221). On appelle cette opération une translation d'adresse. De cette manière, les terminaux avec une adresse IP privée sont reconnus et adressables dans le réseau Internet par une adresse IP publique.

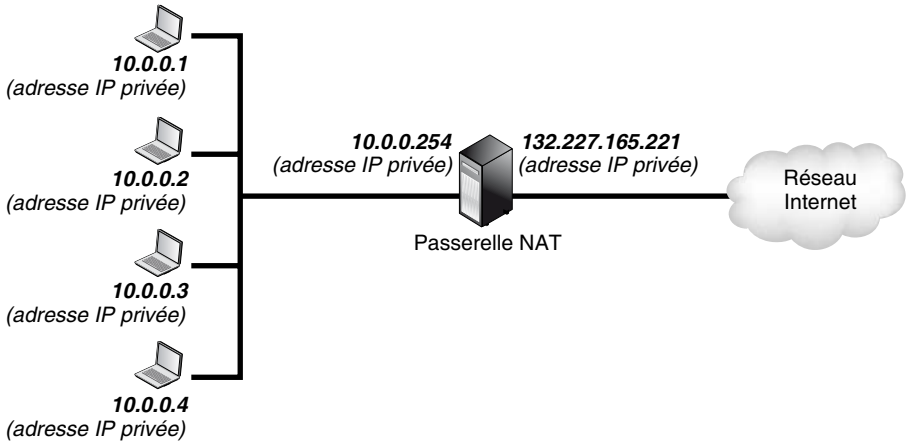


Figure 16.16
Translation d'adresses

La translation d'adresse est bien sûr réalisée dans les deux sens d'une communication, afin de permettre l'émission de requêtes aussi bien que la réception des réponses correspondantes. Pour cela, le boîtier NAT maintient une table de correspondance des paquets de manière à savoir à qui distribuer les paquets reçus.

Par exemple, si un émetteur dont l'adresse IP est 10.0.0.3 envoie vers la passerelle NAT un paquet à partir de son port 12345, la passerelle NAT modifie le paquet en remplaçant l'adresse IP source par la sienne et le port source par un port quelconque qu'elle n'utilise pas, disons le port 23456. Elle note cette correspondance dans sa table de NAT. De cette manière, lorsqu'elle recevra un paquet à destination du port 23456, elle cherchera cette affectation de port dans sa table et retrouvera la source initiale.

Ce cas est illustré à la figure 16.17.

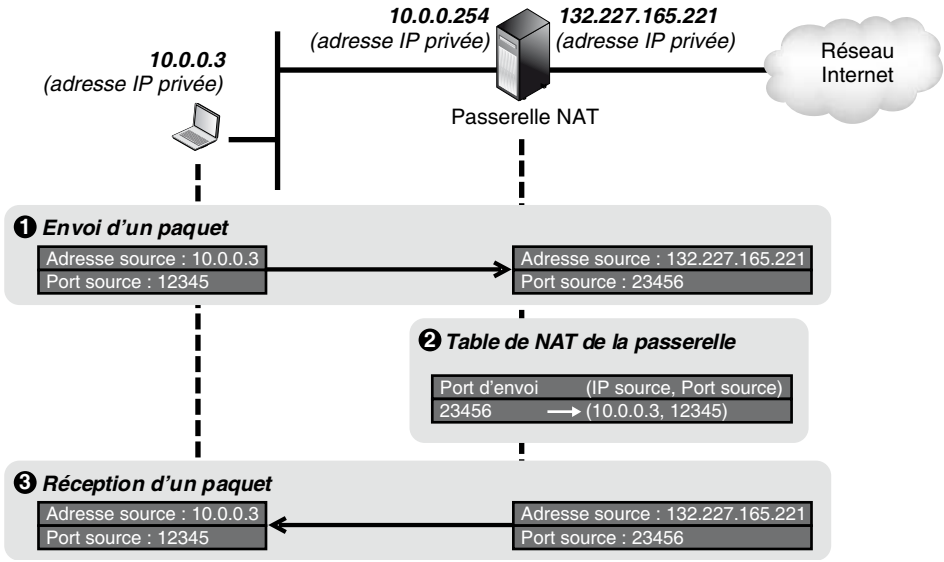


Figure 16.17

Modification de paquets lors du NAT

Avantages du NAT

Le premier atout du NAT est de simplifier la gestion du réseau en laissant l'administrateur libre d'adopter le plan d'adressage interne qu'il souhaite. Étant privé, le plan d'adressage interne ne dépend pas de contraintes externes, que les administrateurs ne maîtrisent pas toujours. Par exemple, si une entreprise utilise un plan d'adressage public et qu'elle change de FAI, elle doit modifier l'adresse de tous les terminaux qui composent son réseau. Au contraire, avec le NAT et un plan d'adressage privé, le choix d'un nouveau fournisseur d'accès Internet n'a pas d'impact sur les terminaux. Dans ce cas, l'administrateur n'a pas besoin de reconfigurer les adresses IP de tous les terminaux de son réseau. Il lui suffit de modifier, au niveau de la passerelle NAT, le pool d'adresses IP publiques, qui est affecté dynamiquement aux adresses IP privées des terminaux du réseau local.

Le deuxième atout du NAT est d'économiser le nombre d'adresses IP publiques. Le protocole réseau IP, qui est utilisé dans l'Internet actuel dans sa version 4, présente une limitation importante, car le nombre d'adresses IP disponible est faible comparé au nombre de terminaux susceptibles d'être raccordés au réseau Internet. Comme cette ressource est rare, sa mise à disposition à un coût pour les administrateurs qui souhaitent en bénéficier.

Le NAT comble cette pénurie d'adresses propre à la version 4 d'IP en offrant la possibilité d'économiser les adresses IP à deux niveaux distincts. Tous les terminaux d'un réseau

local n'ont pas forcément besoin d'être joignables de l'extérieur, mais peuvent se limiter à une connexion interne au réseau. Par exemple, des serveurs d'intranet, des annuaires d'entreprise, des serveurs dédiés aux ressources humaines avec des informations confidentielles de suivi du personnel ou bien encore des serveurs de tests n'ont pas à être joignables à partir du réseau Internet, mais seulement en interne au sein de l'entreprise. En conséquence, ces serveurs peuvent se suffire d'une adresse IP privée, qui ne sera jamais « nattée » par le boîtier NAT puisque ces serveurs reçoivent des requêtes mais n'en émettent jamais.

Un deuxième niveau d'économie d'adresses IP publique est opéré avec le mécanisme que nous avons mentionné à la section précédente, qui permet de masquer plusieurs terminaux disposant chacun d'une adresse IP privée avec une seule adresse IP publique, en jouant sur les ports utilisés. Cette méthode est très couramment employée, car elle n'impose aucune condition quant au nombre de terminaux susceptibles d'accéder à Internet dans le réseau local.

Un autre avantage important du NAT concerne la sécurité. Les terminaux disposent en effet d'une protection supplémentaire, puisqu'ils ne sont pas directement adressables de l'extérieur. En outre, le boîtier NAT offre la garantie que tous les flux transitant entre le réseau interne et l'extérieur passent toujours par lui. Si un terminal est mal protégé et ne dispose pas d'un pare-feu efficace, le réseau dans lequel il se connecte peut ajouter des mécanismes de protection supplémentaires au sein de la passerelle NAT, puisqu'elle représente un passage obligé pour tous les flux. Globalement, l'administrateur concentrer les mécanismes de sécurisation à un point de contrôle unique et centralisé. Cela explique que, bien souvent, les boîtiers NAT sont couplés avec des pare-feu filtrant les flux.

Conclusion

Nous avons introduit dans ce chapitre l'architecture des réseaux IP. Il y a quinze ans, on aurait pu dénombrer une vingtaine d'architectures de niveau paquet, chaque grande société d'informatique déployant sa propre architecture.

Aujourd'hui, on peut dire qu'il n'existe pratiquement plus qu'une seule architecture de niveau paquet dans le monde, celle provenant de l'Internet. Si elle est encore concurrencée, c'est non plus par d'autres solutions de niveau 3 mais par les architectures de niveau trame, qui consistent à placer le paquet IP dans une trame dans la machine terminale et à la transporter à l'intérieur de la trame tout le long du chemin. Arrivée dans la machine terminale du destinataire, la trame est décapsulée pour restituer son paquet IP. L'architecture de cette solution est bien de niveau trame (couche 2, ou liaison).

Les réseaux du futur seront sans aucun doute les témoins d'une confrontation des architectures de niveau paquet IP et des architectures de niveau trame, symbolisées par MPLS.

17

Les réseaux IP : gestion et contrôle

Nous avons parcouru au chapitre précédent l'architecture et les principaux protocoles du monde IP. Un réseau ne peut être complet sans une gestion du réseau et un contrôle de ses ressources. En particulier, une des ambitions du monde IP est de parvenir à proposer une qualité de service à ses utilisateurs.

Ce chapitre examine les principaux protocoles de gestion et de contrôle des ressources, depuis les protocoles de signalisation jusqu'aux protocoles de gestion de la sécurité et de la mobilité des utilisateurs en passant par les protocoles de contrôle de la qualité de service IntServ et DiffServ.

Les protocoles de contrôle

Plusieurs protocoles ont été normalisés pour transporter des paquets de contrôle. Nous détaillons dans les sections qui suivent ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Protocol), dont les rôles sont de transporter des informations sur les anomalies de fonctionnement et de superviser le fonctionnement de groupes d'utilisateurs sur Internet.

ICMP (Internet Control Message Protocol)

Dans un transfert en mode sans connexion, que nous avons décrit au début du chapitre 4, chaque passerelle et chaque machine fonctionnent de façon autonome. De même, le routage et l'envoi des datagrammes se font sans coordination avec l'émetteur. Ce système

fonctionne bien tant que toutes les machines n'ont pas de problème et que le routage est correct, mais cela n'est pas toujours le cas.

Outre les pannes du réseau et des machines, des problèmes surviennent lorsqu'une machine est déconnectée du réseau de façon temporaire ou permanente, lorsque la durée de vie du datagramme expire ou lorsque la congestion d'une passerelle est trop importante. Pour permettre aux machines de rendre compte de ces anomalies de fonctionnement, on a ajouté à Internet le protocole d'envoi de messages de contrôle ICMP.

Le destinataire d'un message ICMP n'est pas un processus application mais le logiciel Internet de la machine. Quand un message est reçu, IP traite le problème. Les messages ICMP ne sont pas uniquement envoyés par les passerelles. N'importe quelle machine du réseau peut envoyer des messages à n'importe quelle autre machine. De la sorte, on a un protocole unique pour tous les messages de contrôle et d'information. Le tableau 17.1 récapitule les principaux messages de contrôle ICMP.

Code message	Type de message ICMP	Code message	Type de message ICMP
0	Echo Reply	12	Parameter Problem on a Datagram
3	Destination Unreachable	13	Timestamp Request
4	Source Quench	14	Timestamp Reply
5	Redirect	17	Address Mask Request
8	Echo Request	18	Address Mask Reply
11	Time Exceeded for a Datagram		

TABLEAU 17.1 • Messages de contrôle ICMP

Chaque message est doté de son propre format, c'est-à-dire de la composition des champs des informations de supervision. Ce format permet de transporter les informations adéquates pour rendre compte de l'erreur. Les messages ICMP sont transportés dans le champ Données des datagrammes IP. Or ces derniers peuvent être perdus. En cas d'erreur d'un datagramme contenant un message de contrôle, aucun message de rapport de l'erreur n'est transmis, afin d'éviter une explosion du nombre de paquets transportés dans le réseau, que l'on nomme avalanche.

ICMP prend beaucoup plus d'importance avec IPv6, la dernière version du protocole IP, où ARP (Address Resolution Protocol) est remplacé par la fonction ND (Neighbor Discovery) d'ICMP. Cette fonction permet à une station de découvrir le routeur dont elle dépend et les hôtes qu'elle peut atteindre localement. La station construit pour cela une base de connaissances en examinant les paquets qui transitent par son intermédiaire et prend ensuite des décisions de routage et de contrôle. La correspondance de l'adresse IP d'une station avec les adresses locales est appelée résolution d'adresse. Elle est effectuée par ND (Neighbor Discovery).

La station qui utilise ND émet une requête NEIGHBOR SOLICITATION sur sa ligne. L'adresse du destinataire est une adresse multicast prédéterminée de type FF02::1:pruv:wxyz. Cette adresse multicast correspond à une connexion qui part d'un point donné et se dirige vers plusieurs points de destination. Elle est complétée par la valeur pruv:wxyz des 32 derniers bits de l'adresse de la station. Dans IPv6, la valeur du Next-Header est 58 pour indiquer un message ICMP. Le code du message ICMP est 135 pour indiquer une requête NEIGHBOR SOLICITATION. Si la station n'a pas de réponse, elle effectue une nouvelle demande. Les stations qui se reconnaissent sur la même ligne émettent vers la station émettrice un NEIGHBOR ADVERTISEMENT. Pour discuter avec un utilisateur sur un autre réseau, la station a besoin de s'adresser à un routeur. La requête ROUTER SOLICITATION est utilisée à cet effet. La fonction ND permet au routeur gérant la station de se faire connaître. Le message de réponse contient de nombreuses options, comme le temps de vie du routeur — si le routeur ne donne pas de ses nouvelles dans ce temps, il est considéré comme indisponible.

Les messages ROUTER SOLICITATION et ROUTER ADVERTISEMENT ne garantissent pas que le routeur qui s'est fait connaître est le meilleur. Un routeur peut s'en apercevoir et envoyer les paquets de la station vers un autre routeur grâce à une redirection, en en avertissant le poste de travail émetteur.

Une dernière fonction importante d'ICMP permet d'avertir de la perte de communication avec un voisin. Cette fonction est assurée par une requête NEIGHBOR UNREACHABILITY DETECTION.

IGMP (Internet Group Management Protocol)

Internet définit des groupes de diffusion, formés d'ensembles de machines participant à un même travail, de telle sorte qu'un message émis par un participant puisse parvenir à l'ensemble des autres participants. Ces groupes de diffusion doivent être contrôlés pour, par exemple, accueillir de nouveaux clients ou en laisser partir. Le rôle du protocole IGMP est d'effectuer ce contrôle sur les communications entre les membres du groupe.

Les groupes de diffusion sont dynamiques. Une machine peut se rattacher à un groupe ou le quitter à tout moment, l'hôte devant seulement être capable d'émettre et de recevoir des datagrammes en multicast. Cette fonction IP de diffusion vers les membres d'un groupe n'est pas limitée à un groupe se trouvant dans un même sous-réseau physique. Les passerelles propagent également les informations d'appartenance à un groupe et gèrent le routage de façon que chaque machine reçoive une copie de chaque datagramme envoyé au groupe.

Les machines communiquent aux passerelles leur appartenance à un groupe en utilisant le protocole IGMP. Ce dernier est conçu pour optimiser l'utilisation des ressources du réseau. Dans la plupart des cas, le trafic IGMP consiste en un message périodique envoyé par la passerelle gérant le multipoint et en une seule réponse pour chaque groupe de machines d'un sous-réseau.

Pour réaliser la communication à l'intérieur du groupe, le protocole IP Multicast est utilisé. Celui-ci gère les émissions multipoint vers l'ensemble des participants à un groupe et

permet l'envoi de datagrammes à plusieurs destinations à la fois de façon performante. IP utilise les adresses de classe D pour indiquer qu'il s'agit d'un envoi multipoint.

Les protocoles de signalisation

La signalisation est un aspect particulièrement débattu dans l'environnement IP, puisqu'elle est *a priori* contradictoire avec la philosophie du monde IP, qui place une adresse complète dans le paquet de façon à pouvoir router à tout moment ce paquet vers son destinataire. L'avantage d'une signalisation normalisée et adoptée par toute la communauté IP est de mettre en place l'équivalent de circuits virtuels. Sur de tels circuits, le flot de paquets peut disposer d'une qualité de service lui permettant d'accueillir des applications exigeantes, comme la parole téléphonique.

Les sections qui suivent présentent les protocoles de signalisation du monde IP, au premier rang desquels RSVP (Resource reSerVation Protocol). Un groupe spécifique de l'IETF, NSIS (Next Step In Signaling), a été créé en 2002 pour décider de la signalisation à suivre dans le futur monde IP. Ce groupe est arrivé à de premières conclusions, que nous détaillons au chapitre 36, dévolu à la signalisation.

RSVP

RSVP semble le plus intéressant des protocoles de signalisation de nouvelle génération. Son rôle est d'avertir les nœuds intermédiaires de l'arrivée d'un flot correspondant à des qualités de service déterminées. Par lui-même, RSVP ne permet pas de lancer explicitement la réservation de ressources à la demande d'une application puis de relâcher ces ressources à la fin.

La signalisation s'effectue sur un flot (*flow*), qui est envoyé vers un ou plusieurs récepteurs. Ce flot est identifié par une adresse IP ou un port de destination, ou encore une référence de flot, ou flow-label, dans IPv6.

Du point de vue de l'opérateur de réseau, le protocole RSVP est lié à une réservation, laquelle doit être effectuée dans les nœuds du réseau sur une route particulière ou sur les routes déterminées par un multipoint. Les difficultés rencontrées pour mettre en œuvre ce mécanisme sont de deux ordres : déterminer la quantité de ressources à réserver à tout instant et réserver les ressources sur une route unique, étant donné que le routage des paquets IP fait varier le chemin à suivre.

RSVP effectue la réservation à partir du récepteur, ou des récepteurs dans le cas d'un multipoint. Cela peut paraître surprenant à première vue, mais cette solution s'adapte à beaucoup de cas de figure, en particulier au multipoint. Lorsqu'un nouveau point s'ajoute au multipoint, ce dernier peut réaliser l'adjonction de réservation d'une façon plus simple que ne pourrait le faire l'émetteur.

Les paquets RSVP sont transportés dans la zone de données des paquets IP. La partie supérieure des figures 17.1 à 17.3 illustre les en-têtes d'IPv6. La valeur 46 dans le champ En-tête suivantindique qu'un paquet RSVP est transporté dans la zone de données.

Outre deux champs réservés, le paquet RSVP contient les huit champs suivants :

- Version. Indique le numéro de la version de RSVP.
- Flags. Quatre bits réservés pour une utilisation ultérieure.
- RSVP Type. Le type caractérise le message RSVP. Actuellement, deux types sont plus spécifiquement utilisés : le message de chemin et le message de réservation. Les valeurs qui ont été retenues pour ce champ sont les suivantes :
  1 path message
  2 reservation message
  3 error indication in response to path message
  4 error indication in response to reservation message
  5 path teardown message
  6 reservation teardown message
- Cheksum. Permet de détecter des erreurs sur le paquet RSVP.
- Longueur du message. Indiquée sur 2 octets.
- Réservé. Premier champ réservé aux extensions ultérieures.
- Identificateur du message. Contient une valeur commune à l'ensemble des fragments d'un même message.
- Réservé. Autre champ réservé à des extensions ultérieures.
- Plus de fragment. Bit indiquant que le fragment n'est pas le dernier. Un zéro est mis dans ce champ pour le dernier fragment.
- Position du fragment. Indique l'emplacement du fragment dans le message.

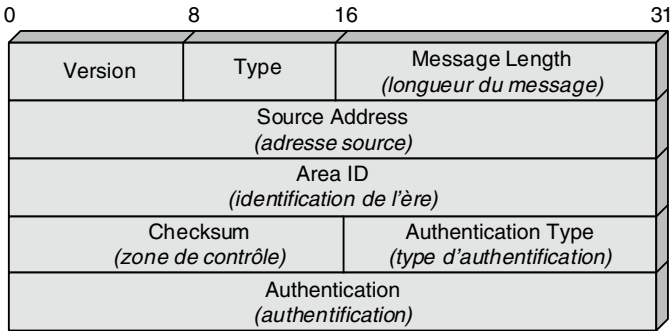


Figure 17.1

Format du message RSVP

La partie Message RSVP regroupe une série d'objets. Chaque objet se présente de la même façon, avec un champ Longueur de l'objet sur 2 octets puis le numéro de l'objet sur un octet, qui détermine l'objet, et enfin un octet pour indiquer le type d'objet.

Le tableau 17.2 récapitule les quinze objets définis.

Numéro objet	Type	Description
0	NULL	Ignoré par le récepteur
1 SESSION	1	Session IPv4 (destination du flot)
	2	Session IPv6
3 RSVP_HOP	1	Adresse du prochain nœud (IPv4)
	2	Adresse du prochain nœud (IPv6)
4 INTEGRITY		Données d'authentification
5 TIME_VALUES	1	Fréquence de rafraîchissement
6 ERROR_SPEC	1	Information d'erreur pour IPv4
	2	Information d'erreur pour IPv6
7 SCOPE	1	Liste des hôtes IPv4 sur lesquels la réservation s'exerce
	2	Liste des hôtes IPv6 sur lesquels la réservation s'exerce
8 STYLE	1	Style de réservation
9 FLOWSPEC	1	Spécification d'un flot demandant un contrôle du délai
	2	Spécification d'un flot demandant une qualité de service
	3	Spécification d'un flot demandant une qualité de service garantie
	254	Spécification d'un flot contenant plusieurs sous-flots
10 FILTER_SPEC	1	Filtre pour IPv4 à appliquer au flot
	2	Filtre pour IPv6 utilisant des valeurs du port source
	3	Filtre pour IPv6 utilisant des valeurs des étiquettes de flots
11SENDER_TEMPLATE	1	Description du flot IPv4 que l'émetteur génère
	2	Description du flot IPv6 que l'émetteur génère
12 SENDER_TSPEC	1	Borne supérieure sur le trafic généré par l'émetteur
13 ADSPEC		Information d'avertissement d'un flot émis par l'émetteur
14 POLICY_DATA	1	Information sur la politique suivie par un flot
	254	Information sur les politiques suivies par plusieurs flots
20 TAG	1	Collection d'objets associés à un nom donné

TABLEAU 17.2 • Objets de RSVP

Les spécifications de RSVP contiennent les descriptions précises des chemins suivis par les messages, y compris les objets nécessaires et l'ordre dans lequel ces objets apparaissent dans le message.

Les figures 17.2 et 17.3 donnent des exemples de messages RSVP. La figure 17.4 décrit en complément le format d'indication des erreurs dans RSVP.

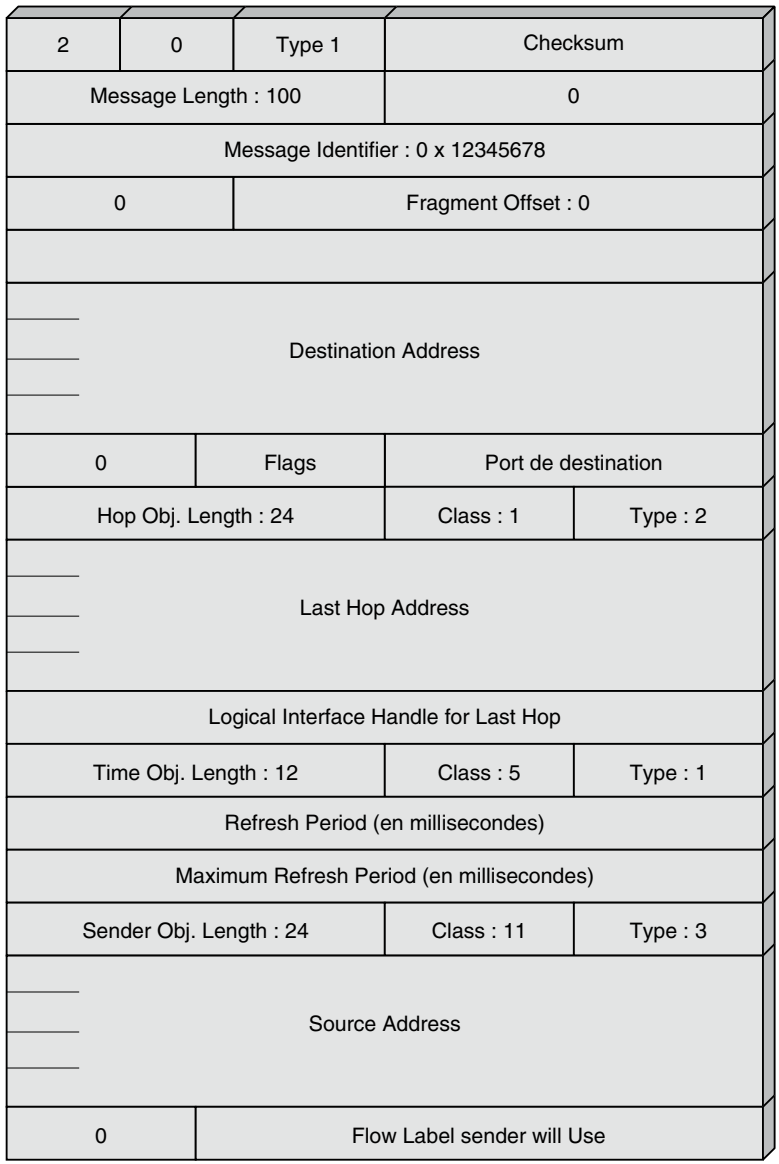


Figure 17.2

Message pour déterminer le chemin RSVP

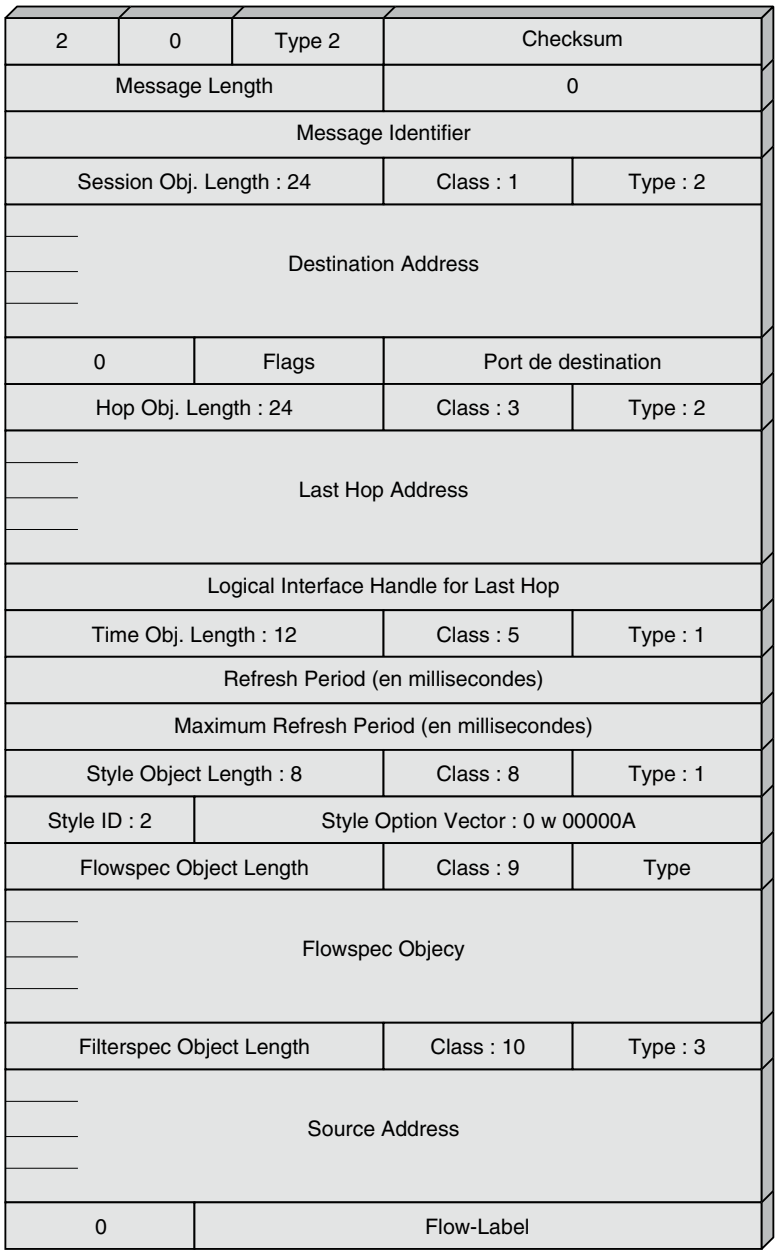


Figure 17.3

Paquet de réservation RSVP

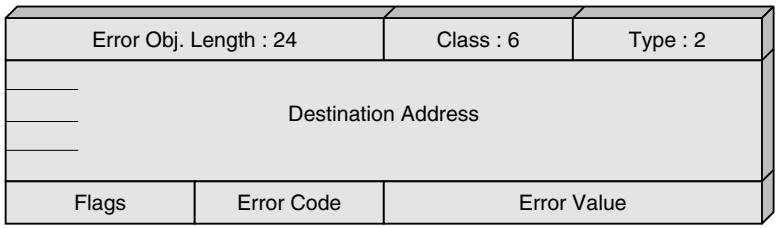


Figure 17.4

Format d'indication des erreurs dans RSVP

Comme expliqué précédemment, RSVP n'est pas un protocole de réservation mais une signalisation, qui permet aux nœuds de faire de leur mieux par rapport à la connaissance qu'ils ont des principaux flots qui vont les traverser. Il faut ensuite appliquer une politique d'ordonnancement des paquets, de type fair-queuing, pour optimiser les différentes qualités de service requises sur les flots.

RTP (Real-time Transport Protocol)

La prise en charge d'applications temps réel, comme la parole téléphonique ou la visioconférence, est le défi lancé à Internet. Ces applications demandent des qualités de service que les protocoles classiques d'Internet ne peuvent offrir. RTP a été conçu pour tenter de résoudre ce problème, qui plus est directement dans un environnement multipoint, en prenant à sa charge aussi bien la gestion du temps réel que l'administration de la session multipoint.

Pour réaliser cela, deux intermédiaires sont nécessaires, des translateurs et des mixeurs. Un translateur a pour fonction de traduire une application codée dans un certain format en un autre format, mieux adapté au passage par un sous-réseau. Par exemple, une application de visioconférence codée en MPEG pourrait être décodée et recodée en H.261 pour réduire la quantité d'informations transmises. Un mixeur a pour rôle de regrouper plusieurs applications correspondant à plusieurs flots distincts en un seul flot conservant le même format. Cette approche est particulièrement intéressante pour les flux de paroles numériques.

Pour réaliser le transport en temps réel, un second protocole, RTCP (Real-Time Control Protocol), a été ajouté à RTP puisque les paquets RTP ne transportent que les données des utilisateurs et non les informations de supervision.

Le protocole RTCP accepte les cinq types de paquets suivants :

- 200 : sender report (rapport de l'émetteur) ;
- 201 : receiver report (rapport du récepteur) ;
- 202 : description source (description de la source) ;
- 203 : bye (au revoir) ;
- 204 : application specific (application spécifique).

Ces différents paquets donnent aux nœuds du réseau les instructions nécessaires à un meilleur contrôle des applications temps réel.

Le chapitre 29 présente en détail l'utilisation de ce protocole pour la téléphonie IP.

Les protocoles de sécurité

TCP/IP ne permet pas une interopérabilité universelle. Dans certains environnements, les administrateurs ont besoin de limiter cette interopérabilité pour protéger les données privées. Ces restrictions, qui renvoient au problème général de la sécurité, prennent un relief particulier dans le cas d'Internet, dont la fiabilité est plus difficile à assurer que pour un simple ordinateur. Le problème est de savoir comment un utilisateur s'appuyant sur TCP/IP peut s'assurer de la protection de ses machines et de ses données contre les accès non autorisés.

Un groupe de travail a exploré la question de la sécurisation de la messagerie en expérimentant un service de messagerie privée amélioré. L'idée consiste à mettre en œuvre un mécanisme permettant à l'émetteur de chiffrer son message et de l'envoyer sur un Internet ouvert sans permettre à une personne autre que le destinataire de le décrypter.

Des travaux sur le filtrage des paquets dans les passerelles ont produit une variété de mécanismes qui permettent aux administrateurs de fournir des listes explicites de contrôle d'accès. Une liste d'accès spécifie un ensemble de machines et de réseaux au travers desquels la passerelle peut router les datagrammes. Si l'adresse n'est pas autorisée, le datagramme est détruit. Dans la plupart des implémentations, la passerelle enregistre la tentative de violation dans un journal. Ainsi, il est possible d'utiliser des filtres d'adresses pour surveiller les communications entre les machines.

La qualité de service

La qualité de service est une condition nécessaire au passage du multimédia dans les réseaux IP. Les réflexions menées sur l'architecture TCP/IP pour aller dans ce sens sont nombreuses.

L'IETF a d'abord proposé l'architecture ISA (Integrated System Architecture), qui regroupe des protocoles tels que IPv6 et RSVP. Pour que cette architecture soit efficace, il faut se placer dans un réseau intranet, où une affectation des coûts par rapport au service demandé est possible. Dans le cas contraire, l'ensemble des utilisateurs acquiert rapidement la priorité la plus haute.

Cette architecture se fonde essentiellement sur la connaissance de ce qui est transporté dans le paquet IP. Dans IPv4, les informations se trouvent dans le champ ToS (Type of Service). Dans IPv6, on utilise la zone de priorité et éventuellement le flow-label. Les routeurs peuvent prendre en compte cette information et traiter les paquets suivant un ordonnancement prédéterminé. Plusieurs solutions d'ordonnancement peuvent être choisies, dont l'une des plus classiques est le fair-queuing.

Le fair-queuing consiste à placer les clients entrants dans plusieurs files d'attente en fonction de leur priorité et à les traiter dans un ordre qui les satisfasse tous au mieux. Si

l'on prend les clients strictement dans leur ordre de priorité, les derniers servis risquent d'avoir une qualité de service désastreuse, alors même qu'un paquet prioritaire pourrait parfois attendre sans que cela le défavorise.

L'IETF a fait de nombreuses autres propositions ces dernières années pour introduire la qualité de service dans les réseaux IP. Nous ne décrivons ici que les deux plus importantes, IntServ et DiffServ.

L'IETF propose l'utilisation de deux grandes catégories de services, qui se déclinent en sous-services dotés de différentes qualités de service : les services intégrés IntServ (Integrated Services) et les services différenciés DiffServ (Differentiated Services). Les services intégrés sont gérés indépendamment les uns des autres, tandis que les services différenciés rassemblent plusieurs applications simultanément. La première solution est souvent choisie pour le réseau d'accès et la seconde pour l'intérieur du réseau lorsqu'il y a beaucoup de flots à gérer.

Les services intégrés IntServ disposent des trois classes suivantes :

- Le service garanti (Guaranteed Service), qui est l'équivalent des CBR et VBR-rt de l'ATM.
- Le service contrôlé (Controlled Load), qui est l'équivalent du service ABR avec un minimum garanti (guaranteed minimum cell rate).
- Le best-effort, qui est l'équivalent de l'UBR ou du GFR.

Les services différenciés, ou DiffServ, disposent des trois classes suivantes :

- Le service garanti (Expedited Forwarding), ou service Premium, qui est l'équivalent des CBR et VBR-rt de l'ATM.
- Le service contrôlé (Assured Forwarding), qui est l'équivalent du service ABR avec minimum garanti (Guaranteed Minimum Cell Rate).
- Le best-effort, équivalant à l'UBR ou au GFR.

IntServ (Integrated Services)

Le service IntServ intègre deux niveaux de service différents avec des garanties de performance. C'est un service orienté flot, c'est-à-dire que chaque flot peut faire sa demande spécifique de qualité de service. Pour obtenir une garantie précise, le groupe de travail IntServ a considéré que seule une réservation de ressources était capable d'apporter à coup sûr les moyens de garantir la demande.

Comme expliqué précédemment, trois sous-types de services sont définis dans IntServ : un service avec une garantie totale, un service avec une garantie partielle et le service best-effort. Le premier correspond aux services rigides avec contraintes fortes à respecter, et les deuxième et troisième aux services dits élastiques, qui n'ont pas de contraintes fortes.

Lorsqu'ils reçoivent une demande *via* le protocole RSVP, les routeurs peuvent l'accepter ou la refuser. Cette demande s'effectue comme pour le protocole RSVP du récepteur vers l'émetteur après une phase aller. Une fois la demande acceptée, les routeurs placent les paquets correspondants dans une file d'attente de la classe de service demandée.

Le service IntServ doit posséder les composantes suivantes :

- Une procédure de signalisation pour avertir les nœuds traversés. Le protocole RSVP est supposé remplir cette tâche.
- Une méthode permettant d'indiquer la demande de qualité de service de l'utilisateur dans le paquet IP afin que les nœuds puissent en tenir compte.
- Un contrôle de trafic pour maintenir la qualité de service.
- Un mécanisme pour faire passer le niveau de qualité au réseau sous-jacent, s'il existe.

Le service garanti GS affecte une borne supérieure au délai d'acheminement. Pour cela, un protocole de réservation comme RSVP est nécessaire. La demande de réservation comporte deux parties : une spécification de la qualité de service déterminée par un FlowSpec et une spécification des paquets qui doivent être pris en compte par un filtre, le FilterSpec. En d'autres termes, certains paquets du flot peuvent avoir une qualité de service mais pas forcément les autres. Chaque flot possède sa qualité de service et son filtre, qui peut être fixe (*fixed filter*), partagé avec d'autres sources (*shared-explicit*) ou encore spécifique (*wildcard filter*).

Le service partiellement garanti CL (Controlled Load) doit garantir une qualité de service à peu près égale à celle offerte par un réseau peu chargé. Cette classe est essentiellement utilisée pour le transport des services élastiques. Les temps de transit dans le réseau des flots CL doivent être similaires à ceux de clients d'une classe best-effort dans un réseau très peu chargé. Pour arriver à cette fluidité du réseau, il faut intégrer une technique de contrôle.

Les deux services doivent pouvoir être réclamés par l'application *via* l'interface. Deux possibilités sont évoquées dans la proposition IntServ : l'utilisation de la spécification GQoS Winsock2, qui permet le transport d'applications point-à-point et multipoint, et RAPI (RSVP API), qui est une interface applicative sous UNIX.

L'ordonnancement des paquets dans les routeurs est un deuxième mécanisme nécessaire. Un de ceux les plus classiquement proposés est le WFQ (Weighted Fair Queuing). Cet algorithme placé dans chaque routeur demande une mise en file d'attente des paquets suivant leur priorité. Les files d'attente sont servies dans un ordre déterminé par un ordonnancement dépendant de l'opérateur. Généralement, le nombre de paquets servis à chaque passage du serveur dépend du paramètre de poids de la file d'attente.

Il existe de nombreuses solutions pour gérer la façon dont le service est affecté aux files d'attente, généralement fondées sur des niveaux de priorité. Citons notamment l'algorithme Virtual Clock, qui utilise une horloge virtuelle pour déterminer les temps d'émission, et SCFQ (Self-Clocked Fair Queuing), qui travaille sur des intervalles de temps minimaux entre deux émissions de paquets d'une même classe, intervalle dépendant de la priorité.

Le service IntServ pose le problème du passage à l'échelle, ou scalabilité, qui désigne la possibilité de continuer à bien se comporter lorsque le nombre de flots à gérer devient très grand, comme c'est le cas sur Internet. Le contrôle IntServ se faisant sur la base de flots individuels, les routeurs du réseau IntServ doivent en effet garder en mémoire les

caractéristiques de chaque flot. Une autre difficulté concerne le traitement des différents flots dans les nœuds IntServ : quel flot traiter avant tel autre lorsque des milliers de flots arrivent simultanément avec des classes et des paramètres associés distincts ?

En l'absence de solution reconnue à tous ces problèmes, la seconde grande technique de contrôle, DiffServ, essaie de trier les flots dans un petit nombre bien défini de classes, en multiplexant les flots de même nature dans des flots plus importants mais toujours en nombre limité. IntServ peut cependant s'appliquer à de petits réseaux comme les réseaux d'accès. D'autres recherches vers des processeurs de gestion spécialisés dans la qualité de service ont débouché récemment sur des équipements capables de traiter plusieurs dizaines, voire centaines de milliers de flots.

Le groupe de travail ISSLL (Integrated Services over Specific Link Layers) de l'IETF cherche à définir un modèle IntServ agissant sur un niveau trame de type ATM, Ethernet, relais de trames, PPP, etc. En d'autres termes, l'objectif est de proposer des mécanismes permettant de faire passer le niveau de priorité de la classe vers des classes parfois non équivalentes et de choisir dans le réseau sous-jacent des algorithmes susceptibles de donner un résultat équivalent à celui qui serait obtenu dans le monde IP.

DiffServ (Differentiated Services)

Le principal objectif de DiffServ est de proposer un schéma général permettant de déployer de la qualité de service sur un grand réseau IP et de réaliser ce déploiement assez rapidement.

DiffServ sépare l'architecture en deux composantes majeures : la technique de transfert et la configuration des paramètres utilisés lors du transfert. Cela concerne aussi bien le traitement reçu par les paquets lors de leur transfert dans un nœud que la gestion des files d'attente et la discipline de service. La configuration de tous les nœuds du chemin s'effectue selon une manière appelée PHB (Per-Hop Behavior). Ces PHB déterminent les différents traitements correspondant aux flots qui ont été différenciés dans le réseau.

DiffServ définit la sémantique générale des PHB et non les mécanismes spécifiques qui permettent de les implémenter. Les PHB sont définis une fois pour toutes, tandis que les mécanismes peuvent être modifiés et améliorés voire être différents suivant le type de réseau sous-jacent.

Les PHB et les mécanismes associés doivent facilement pouvoir être déployés dans les réseaux IP, ce qui demande que chaque nœud puisse gérer les flots grâce à un certain nombre de mécanismes, comme l'ordonnancement, la mise en forme ou la perte des paquets traversant un nœud.

DiffServ agrège les flots en classes, appelées agrégats, qui offrent des qualités de service spécifiques. La qualité de service est assurée par des traitements effectués dans les routeurs spécifiés par un indicateur situé dans le paquet IP. Les points d'agrégation des trafics entrants sont généralement placés à l'entrée du réseau. Les routeurs sont configurés grâce au champ DSCP (DiffServ Code Points) du paquet IP, qui forme la première partie d'un champ plus général appelé DS (Differentiated Service) et contenant aussi un

champ CU (Currently Unused). Dans IPv4, ce champ DS est pris sur la zone ToS (Type of Service), qui est de ce fait redéfinie par rapport à sa première utilisation. Dans IPv6, ce champ se situe dans la zone TC (Traffic Class) de la classe de service.

La figure 17.5 illustre le champ DS dans les paquets IPv4 et IPv6. Le champ DSCP prend place dans le champ TOS (Type of Service) d'IPv4 et dans le champ Traffic Class d'IPv6. Le champ DSCP tient sur 6 des 8 bits et est complété par deux bits CU. Le DSCP détermine la classe de service PHB.

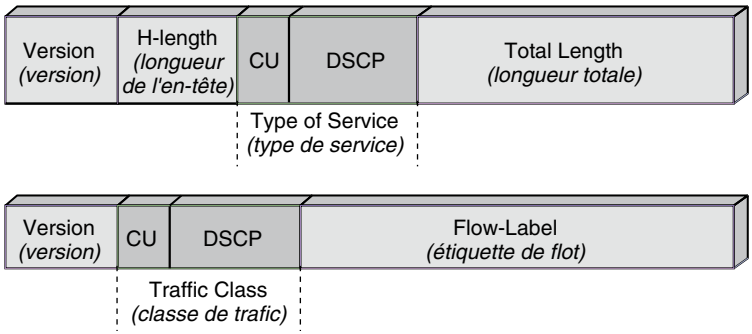


Figure 17.5

Champ DSCP des paquets IPv4 et IPv6

Le champ de 6 bits du DSCP doit être interprété par le nœud pour attribuer au paquet le traitement correspondant à la classe PHB indiquée. Les deux bits CU doivent être ignorés lors du traitement dans un nœud DiffServ normalisé. Par l'intermédiaire d'une table, les valeurs du DSCP déterminent les PHB acceptables par le nœud. Une valeur par défaut doit toujours être indiquée lorsque le champ DSCP ne correspond à aucun PHB.

Les opérateurs de télécommunications peuvent définir leurs propres valeurs de DSCP pour un PHB donné, à la place de la valeur recommandée par la standardisation de l'IETF. Ces opérateurs doivent toutefois fournir dans les passerelles de sortie la valeur standard du DSCP de façon que ce champ soit interprété convenablement par l'opérateur suivant. En particulier, un DSCP non reconnu doit toujours être interprété par une valeur par défaut.

La définition de la structure du champ DS est incompatible avec celle du champ ToS de la RFC 791 qui définit IPv4. Ce champ TOS avait été conçu pour indiquer les critères à privilégier dans le routage. Parmi les critères prévus se trouvent le délai, la fiabilité, le coût et la sécurité.

Outre le service BE (best-effort), deux PHB assez semblables à ceux de IntServ sont définis dans DiffServ :

- EF (Expedited Forwarding), ou service garanti, que l'on appelle aussi service Premium ou Premier.
- AF (Assured Forwarding), ou service assuré, que l'on appelle aussi parfois Assured Service ou encore service Olympic ou Olympique.

Il existe quatre sous-classes de services en AF déterminant des taux de perte acceptables pour les flots de paquets considérés. On peut les classer en Platinium (platine), Gold (or), Silver (argent) et Bronze (bronze). Comme cette terminologie n'est pas normalisée, il est possible d'en rencontrer d'autres. À l'intérieur de chacune de ces classes, trois sous-classes triées selon leur degré de précédence, c'est-à-dire leur niveau de priorité les uns par rapport aux autres, sont définies. La classe AF1*x* est la plus prioritaire, puis vient la classe AF2*x,* etc. Il existe donc au total douze classes standardisées, mais peu d'opérateurs les mettent en œuvre. En règle générale, les opérateurs se satisfont des trois classes de base du service AF, et donc de cinq classes au total en ajoutant les services EF et BE.

Les valeurs portées par le champ DSCP associées à ces différentes classes sont illustrées à la figure 17.6. Par exemple, la valeur 101110 du champ DSCP indique que le paquet est de type EF (Expedited Forwarding). La classe Best Effort porte la valeur 000000.

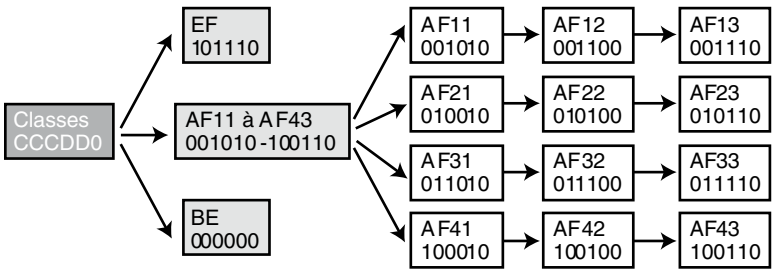


Figure 17.6

Classes de service de DiffServ et valeurs des champs DSCP associés

Le DSCP 11x000 est réservé à des classes de clients encore plus prioritaires que la classe EF. Il peut, par exemple, être utilisé pour des paquets de signalisation.

EF (Expedited Forwarding)

Le PHB EF (Expedited Forwarding) est défini comme un transfert de paquets pour une agrégation de flots provenant de nœuds DiffServ telle que le taux de service des paquets de cet agrégat soit supérieur à un taux déterminé par l'opérateur. Le trafic EF doit pouvoir recevoir un taux de service indépendamment des autres trafics circulant dans le réseau. En terme encore plus précis, le taux du trafic EF doit être supérieur ou égal au taux déterminé par l'opérateur mesuré sur n'importe quel intervalle de temps au moins égal à la taille d'une MTU (Maximum Transmission Unit). Si le PHB EF est implémenté grâce à un mécanisme de priorité sur les autres trafics, il faut que le taux de trafic de l'agrégat EF ne dépasse pas une limite qui deviendrait inacceptable pour les PHB des autres classes de trafic.

Plusieurs types de mécanismes d'ordonnancement peuvent être utilisés pour répondre à ces contraintes. Une file prioritaire est le mécanisme le plus simple pour réaliser le

service (le PHB) EF tant qu'il n'y a pas d'autres files d'attente plus prioritaires pour préempter les paquets EF de plus d'un paquet pour une proportion de temps déterminée par le taux de service des paquets de l'agrégat EF. Il est possible d'utiliser une file d'attente normale dans un groupe de files d'attente gérées par un mécanisme de tour de rôle avec poids (Weighted Round Robin) ou d'utiliser un partage de la bande passante de la file de sortie du nœud, permettant à la file EF d'atteindre le taux de service garanti par l'opérateur. Un autre mécanisme potentiel, appelé partage CBQ (Class Based Queuing), donne à la file EF une priorité suffisante pour obtenir au moins le taux de service garanti par l'opérateur.

Le trafic Expedited Forwarding correspond au trafic sensible au délai et à la gigue. Il est doté d'une priorité forte dans les nœuds mais doit être contrôlé pour que la somme des trafics provenant des différentes sources et passant sur une même liaison ne dépasse pas la capacité nominale déterminée par l'opérateur.

Plusieurs solutions permettent de réserver la bande passante proposée aux flots de paquets EF. Un protocole de type RSVP, par exemple, peut effectuer les réservations de bande passante nécessaires. Une autre solution consiste à utiliser un serveur spécialisé dans la distribution de la bande passante, ou Bandwidth Broker. Ce serveur de bande passante réalise le contrôle d'admission en proposant une réservation centralisée.

AF (Assured Forwarding)

Les PHB AF (Assured Forwarding) assurent le transfert de paquets IP pour lesquels une certaine qualité de service peut être garantie. Les trafics AF sont subdivisés en *n* classes AF distinctes. Dans chaque classe un paquet IP se voit assigner un taux de perte maximal et une priorité à la perte, correspondant à des classes de précédence. Un paquet IP qui appartient à la classe AFi et qui possède un taux de perte correspondant à la précédence j est marqué par un DSCP AFij (*voir figure 17.7*). Comme expliqué précédemment, douze classes sont définies pour DiffServ, correspondant à quatre classes AF avec des garanties sur la perte de paquets. Les quatre classes correspondant aux taux de perte garantie sont appelées Platinium, Or, Argent et Bronze, chaque classe ayant trois niveaux de précédence différents.

Les paquets d'une classe AF sont transférés indépendamment de ceux des autres classes AF. En d'autres termes, un nœud ne peut pas agréger de flots ayant des DSCP différents dans une classe commune.

Un nœud DiffServ doit allouer un ensemble de ressources minimales à chaque PHB AF pour que ceux-ci puissent remplir le service pour lequel ils ont été mis en place. Une classe AF doit posséder des ressources minimales en mémoire et en bande passante pour qu'un taux de service minimal, déterminé par l'opérateur, puisse être réalisé sur une échelle de temps potentiellement assez longue. En d'autres termes, sur un intervalle de temps relativement long, pouvant se compter en seconde, une garantie de débit doit être procurée aux services AF.

Un nœud AF doit pouvoir être configuré pour permettre à une classe AF de recevoir plus de ressources de transfert que le minimum quand des ressources supplémentaires

sont disponibles dans le réseau. Cette allocation supplémentaire n'est pas forcément proportionnelle au niveau de la classe, mais l'opérateur doit être capable de réallouer les ressources libérées par la classe EF sur les PHB AF. Les précédences doivent toutefois être respectées, une classe de meilleure précédence ne devant pas perdre plus de paquets qu'une classe avec une précédence inférieure, même si la perte reste en dessous du niveau admissible.

Un domaine implémentant des services AF doit, par l'intermédiaire des routeurs frontière, être capable de contrôler les entrées de trafics AF pour que les qualités de service déterminées pour chaque classe AF soient satisfaites. Les routeurs frontière doivent pour cela mettre en place des mécanismes de mise en forme du trafic (*shaper*), de destruction de paquets (*dropper*), d'augmentation ou de diminution des pertes de paquets par classe AF et de réassignation de trafics AF dans d'autres classes AF. Les actions d'ordonnancement ne doivent pas causer de remise en ordre des paquets d'un même microflot, un microflot étant un flot particulier à l'intérieur d'un agrégat d'une classe de PHB.

L'implémentation d'une stratégie AF doit minimiser le taux de congestion à l'intérieur de chaque classe, même si des congestions de courte durée sont admissibles suites à des superpositions de flots continus de paquets (*bursts*). Cela demande un algorithme de gestion dynamique dans chaque nœud AF. Un exemple d'un tel algorithme est RED (Random Early Discard). La congestion à long terme doit aussi être évitée grâce à des pertes de paquets correspondant aux niveaux de précédence, et celle à court terme grâce à des files d'attente permettant de mettre en attente certains paquets. Les algorithmes de mise en forme du trafic doivent par ailleurs être capables de détecter les paquets susceptibles d'engendrer des congestions à long terme.

L'algorithme de base permettant d'effectuer le contrôle des trafics AF est WRED, ou Weighted RED. Il consiste à essayer de maintenir le réseau dans un état fluide. Les pertes de paquets doivent être proportionnelles à la longueur des files d'attente. En d'autres termes, les paquets en surplus puis les paquets normaux sont éliminés dès que le trafic n'est plus fluide. Le temps écoulé depuis la dernière perte sur un même agrégat est pris en compte dans l'algorithme. La procédure essaie de distribuer le contrôle à l'ensemble des nœuds et non plus au seul nœud congestionné. Les algorithmes de destruction de paquets doivent être indépendants du court terme et des microflots, ainsi que des microflots à l'intérieur des agrégats.

L'interconnexion de services AF peut être assez difficile à réaliser du fait de la relative imprécision des niveaux de service des différents opérateurs s'interconnectant.

Une solution pour permettre la traversée d'un agrégat dans un réseau IP non conforme à DiffServ consiste à réaliser un tunnel avec une qualité de service supérieure à celle du PHB. Lorsqu'un agrégat de paquets AF utilise le tunnel, la qualité de service assurée par ce dernier doit permettre au PHB de base d'être respecté à la sortie du tunnel.

Un client qui demande un trafic Assured Forwarding doit négocier un agrément de service, ou SLA, correspondant à un profil déterminé par un ensemble de paramètres de qualité de service, ou SLS. Le SLS indique un taux de perte et, pour les services EF, un temps de réponse moyen et une gigue du temps de réponse. Le trafic n'entrant pas dans

le profil est détruit en priorité si un risque de congestion existe qui ne permettrait pas au trafic conforme d'atteindre sa qualité de service.

Architecture d'un nœud DiffServ

L'architecture d'un nœud DiffServ est illustrée à la figure 17.7. Elle comprend une entrée contenant un classificateur (*classifier*), dont le rôle est de déterminer le bon chemin à l'intérieur du nœud. L'embranchement choisi dépend de la classe détectée par le classificateur.

Viennent ensuite des organes appelés Meter, ou métreurs. Un métreur détermine si le paquet a les performances requises par sa classe et décide de la suite du traitement. Le métreur connaît l'ensemble des files d'attente du nœud ainsi que les paramètres de qualité de service demandés par l'agrégat auquel appartient le paquet. Il peut décider de la destruction éventuelle d'un paquet, si sa classe le permet, ou de son envoi vers une file d'attente de sortie. Le nœud DiffServ peut aussi décider de changer ce paquet de classe ou bien de le multiplexer avec d'autres flots, comme nous le verrons. L'organe Dropper, ou suppresseur, peut décider de perdre ou non, c'est-à-dire de détruire ou non le paquet, tandis que le suppresseur absolu (Absolute Dropper) élimine automatiquement le paquet.

En d'autres termes le métreur (Meter) peut prendre une décision de destruction et envoyer le paquet dans un suppresseur absolu (Absolute Dropper), alors que le métreur (Meter) ne fait que déterminer les paramètres de performance et laisse au suppresseur (Dropper) le soin de détruire ou non le paquet suivant d'autres critères que la mesure brute de la performance.

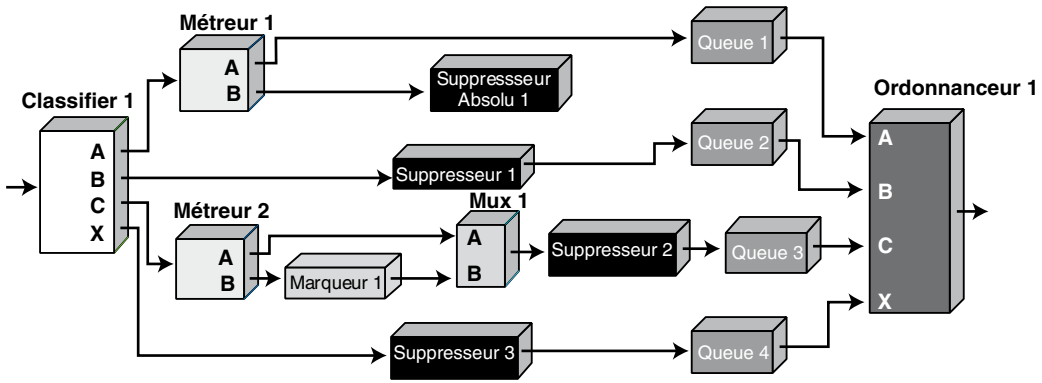


Figure 17.7

Architecture d'un nœud DiffServ

Pour certains paquets, comme les paquets BE (Best Effort), il n'est pas nécessaire de se poser la question de la performance puisqu'il n'y a aucune garantie sur l'agrégat. Il suffit de savoir si le paquet doit être perdu ou non. Cela correspond à la branche D sur la figure 17.7. Sur cette même figure, la première branche (A) correspond aux clients EF ou Premium, les deux suivantes (B et C) à des clients AF, avec des clients Gold dans le

chemin haut et Silver ou Bronze dans l'autre chemin, et la dernière branche (D) à des clients BE.

L'architecture d'un nœud DiffServ se termine par des files d'attente destinées à mettre en attente les paquets avant leur émission sur la ligne de sortie déterminée par le routage. Un algorithme de précédence est utilisé pour traiter l'ordre d'émission des paquets. L'ordonnanceur (Scheduler) s'occupe de cette fonction. L'algorithme le plus simple revient à traiter les files suivant leur ordre de priorité et à ne pas laisser passer les clients d'une autre file tant qu'il y a encore des clients dans une file prioritaire.

De nombreux autres algorithmes permettent de donner un poids spécifique aux files d'attente de telle façon qu'un client non prioritaire puisse être servi avant un client prioritaire. Parmi ces algorithmes, citons WFQ (Weighted Fair Queuing), dans lequel chaque file d'attente comporte un poids, par exemple 70 pour la file EF, 20 pour la file AF Gold et 10 pour l'autre file AF. L'ordonnanceur (Scheduler) laisse passer pendant 70 % du temps les clients EF. Si ces clients dépassent l'utilisation de 70 %, l'ordonnanceur accepte de laisser passer des clients AF Gold pendant les 20 % du temps restant et pendant 10 % des clients AF Silver ou Bronze.

L'ensemble des actions subies par un paquet dans un nœud DiffServ est réalisé par un organe général appelé conditionneur (Conditioner). Un conditionneur de trafic peut contenir les éléments suivants : métreur, marqueur (Marker), metteur en forme et suppresseur de paquets. Un flot est sélectionné par le classificateur. Un métreur est utilisé pour mesurer le trafic en comparaison du profil. La mesure effectuée par le métreur pour un paquet déterminé peut être utilisée pour déterminer s'il faut envoyer le paquet vers un marqueur ou un suppresseur de paquet.

Lorsque le paquet sort du conditionneur, il doit posséder la valeur appropriée du DSCP. Le métreur obtient les propriétés temporelles du flot de paquets sélectionnés par le classificateur en fonction d'un profil déterminé par un TCA (Traffic Conditioning Agreement). Le métreur envoie ces informations aux autres organes du conditionneur, lesquels mettent en œuvre des fonctions spécifiques adaptées aux paquets pour que ceux-ci reçoivent les traitements appropriés, qu'ils se trouvent dans le profil ou hors profil.

Les marqueurs de paquets positionnent le champ DSCP à une valeur particulière et ajoutent le paquet au flux agrégé correspondant. Le marqueur peut être configuré pour marquer tous les paquets à la bonne valeur du DSCP ou pour choisir un DSCP particulier pour un ensemble de PHB prédéterminé.

Les metteurs en forme ont pour objectif de retarder des paquets d'un même flot pour les mettre en conformité avec un profil déterminé. Un metteur en forme possède généralement une mémoire de taille finie permettant de retarder les paquets en les mettant en attente. Ceux-ci peuvent être détruits s'il n'y a pas de place disponible en mémoire pour les mettre en conformité.

Les suppresseurs détruisent les paquets d'un même flot qui ne sont pas conformes au profil de trafic. Ce processus est parfois appelé « policing » de trafic. Un suppresseur est parfois implémenté dans le metteur en forme lorsqu'un paquet doit être rejeté, s'il est impossible de le remettre dans le profil.

Les conditionneurs de trafic sont le plus souvent placés dans les nœuds d'entrée et de sortie des domaines DS. Puisque le marquage des paquets est effectué par les nœuds d'entrée du domaine, un agrégat provenant d'un autre opérateur est supposé être conforme au TCA approprié.

Les PHB (Per Hop Behavior)

Un PHB est une description de la façon de transférer des paquets d'un même agrégat à l'intérieur d'un nœud DiffServ. La façon de transférer des paquets est un concept très général dans ce contexte. Par exemple, s'il n'y a qu'un seul PHB dans un nœud, la façon de transférer les paquets est simple et permet facilement de déduire le temps de réponse, les pertes et la gigue, qui ne dépendent que de la charge du nœud. Des distinctions sur la façon de transférer des paquets peuvent s'observer lorsque plusieurs agrégats ayant des PHB différents entrent en compétition dans un nœud pour acquérir de la mémoire ou de la bande passante. Les PHB doivent donc définir les moyens par lesquels les ressources sont attribuées aux différents agrégats.

Le PHB le plus simple est celui qui garantit une bande passante d'au moins x % d'une liaison physique sur un intervalle de temps significatif par rapport à la vie de l'agrégat. Ce PHB est facile à mesurer, même en présence de nombreux autres agrégats ayant des PHB différents. Un PHB un peu plus complexe pourrait garantir au moins x % d'une liaison physique avec un partage équitable de la bande passante non distribuée entre les agrégats traversant un nœud. En règle générale, l'observation d'un PHB dépend des contraintes posées par les différents agrégats qui se partagent les nœuds de transfert.

Des PHB peuvent être spécifiés pour la priorité d'allocation des ressources (mémoire, bande passante, etc.) des nœuds de transfert en fonction des garanties accordées aux différents paquets des agrégats (délai, perte, etc.). Ces PHB peuvent être utilisés comme des briques de base qui permettent de construire des groupes de PHB cohérents. Les groupes de PHB se partagent des contraintes communes s'appliquant à chaque PHB à l'intérieur d'un groupe. Les relations entre les PHB à l'intérieur d'un groupe peuvent s'exprimer en terme de priorité de perte de paquets relative ou absolue, autrement dit avec des seuils déterministes ou stochastiques, ou de partage équilibré des ressources.

Les PHB sont implémentés dans les nœuds au moyen de gestionnaires de mémoires et de mécanismes d'ordonnancement de paquets. Ils sont définis par la façon dont les transferts s'effectuent et dépendent fortement des politiques d'allocation de ressources, plutôt que de l'implémentation de mécanismes particuliers. Une grande variété de mécanismes peuvent être utilisés pour implémenter un groupe de PHB particulier. Plusieurs groupes de PHB peuvent être implémentés dans un nœud et dans un domaine, par exemple. Les groupes de PHB doivent être définis de telle sorte que l'allocation des ressources entre les groupes puisse se déduire facilement et que les mécanismes puissent être partagés par les différents groupes de PHB. La définition d'un groupe de PHB indique les conflits possibles avec les groupes de PHB déjà définis de façon à éviter les opérations incohérentes.

Un PHB est sélectionné dans un nœud par la valeur du DSCP portée par un paquet. Les PHB standards on un DSCP associé. L'ensemble des DSCP étant plus grand que l'espace disponible pour les DSCP recommandés dans DiffServ, le champ DS laisse la possibilité

en local de faire correspondre un PHB à plusieurs DSCP. Tous les DSCP doivent toutefois avoir un PHB correspondant. Si ce n'est pas le cas, un PHB par défaut est affecté à un DSCP non connu.

Le modèle d'architecture de DiffServ

Dans le modèle d'architecture d'un réseau DiffServ le trafic entrant dans le réseau est classifié et éventuellement conditionné dans les routeurs frontière du réseau. Une fois la classification effectuée, les trafics sont agrégés par les PHB dans des agrégats. À l'intérieur du réseau, les paquets sont transférés suivant la valeur de leur DSCP.

Un domaine DiffServ, appelé communément domaine DS, correspond à un ensemble de nœuds DiffServ, ou nœuds DS, contigus qui opèrent selon une politique de contrôle commune et un ensemble de PHB communs. Ce domaine DS comporte une frontière composée de nœuds DS capables d'effectuer la classification dans les PHB du domaine et de conditionner les trafics. Les routeurs frontière peuvent soit utiliser les DSCP standards, soit transformer les DSCP par défaut dans des DSCP propriétaires. Les PHB déterminés par les classificateurs doivent permettre de réaliser les SLA négociés par les clients de ces agrégats.

Un domaine DS consiste en un ou plusieurs réseaux IP ayant le même système de gestion. Le gestionnaire du réseau détermine les caractéristiques des PHB qu'il peut proposer en fonction des SLA de ses clients et des ressources dont il dispose. Le domaine contient des routeurs frontière et des routeurs intérieurs. Les routeurs frontière sont capables d'effectuer la classification des flots entrant dans le réseau. Ils doivent éventuellement posséder des fonctions de conditionnement définies par un agrément de conditionnement de trafic, ou TCA (Traffic Conditioning Agreement). Les nœuds intérieurs sont capables de réaliser certaines fonctions élémentaires de conditionnement du trafic, comme la transformation du marquage du DSCP.

Un hôte attaché directement à un routeur interne doit posséder les fonctions de routeur frontière ou être connecté à un routeur interne possédant ces fonctions. Un routeur frontière possède à la fois les propriétés d'un nœud d'entrée et d'un nœud de sortie. Un nœud d'entrée est doté des fonctions de traitement des TCA, et un nœud de sortie de celles de conditionnement des flots afin que ceux-ci soient conformes à la normalisation.

Une région mettant en œuvre des services différenciés, ou région DiffServ ou encore DS, est un environnement comprenant un ou plusieurs domaines DS. Une région DS permet la mise en place de services différenciés sur l'ensemble de la région. Les domaines DS à l'intérieur d'une même région peuvent réaliser les conditionnements nécessaires à la mise en œuvre d'un service différencié de bout en bout dans la région.

L'accès d'un flot dans un domaine DS s'effectue grâce au traitement du SLA en provenance de l'extérieur du réseau et lié au flot examiné. Un SLA peut spécifier une classification ou un profil de trafic et les actions à effectuer sur les trafics entrant ou non dans le SLA. Le TCA entre les domaines est dérivé de ce SLA.

Le processus de classification identifie le ou les PHB dans lequel le trafic doit être inséré. Un conditionnement peut être effectué pour permettre cette adéquation. Le

conditionnement est réalisé par un metteur en forme, un contrôleur (*policing entity*) ou un remarquage, de sorte que les caractéristiques du flot correspondent bien à la définition du TCA du domaine.

Le classificateur de paquets sélectionne les flots grâce à une étude de leurs caractéristiques. Cette étude peut porter sur l'analyse de l'application par son numéro de port ou par le biais d'un filtre. Deux types de classificateurs sont proposés dans les réseaux Diff-Serv : les classificateurs BC (Behavior Classifier), qui ne travaillent que sur le DSCP du champ DS, et les classificateurs MF (Multi-Field), qui sélectionnent les paquets sur des combinaisons d'informations provenant de l'analyse des paquets ou des flots. Les classificateurs doivent être configurés par un système de gestion respectant le TCA. Le classificateur doit être capable d'authentifier le flot pour des raisons de sécurité.

Le profil de trafic précise les propriétés temporelles du trafic sélectionné par le classificateur. Le classificateur détermine les règles à suivre si un paquet particulier n'est pas conforme au profil déterminé par le TCA. Par exemple, un profil fondé sur un token-bucket implique que :

si DSCP = *x,* utiliser le token-bucket *r, b*

Ce profil indique que tous les paquets marqués avec le DSCP *x* doivent voir leur performance comparée à une métrique. L'état associé à un paquet est obtenu par le métreur et doit correspondre au token-bucket de taux *r* et d'une taille du burst égale à *b.* Dans cet exemple, les paquets hors profil sont ceux qui arrivent quand un nombre insuffisant de jetons (*tokens*) est disponible. Le concept « dans et hors profil » peut être étendu à plus de deux niveaux. Plusieurs niveaux de conformité pour un profil donné peuvent donc être définis.

Des actions de conditionnement peuvent être décidées pour les paquets entrants et sortants. De ce fait, différentes solutions de comptabilité peuvent être mises en œuvre pour déterminer le coût du service. Les paquets se trouvant dans le profil peuvent être admis à entrer dans le domaine DS sans conditionnement supplémentaire ou, à l'inverse, leur DSCP peut être modifié. Cela se produit lorsque le DSCP est positionné à une valeur qui n'est pas celle définie par défaut ou que le paquet entre dans un domaine DS en utilisant un PHB qui n'est pas conforme au standard. Un paquet hors profil peut être soit mis en attente jusqu'à ce que le paquet entre dans le profil, soit détruit ou marqué par un nouveau DSCP. Les paquets hors profil peuvent éventuellement être agrégés à une classe PHB inférieure et, par exemple, transportés dans une classe BE. Un profil de trafic est une composante optionnelle du TCA.

Allocation des ressources

L'implémentation, la configuration et l'administration des groupes de PHB acceptés pour les nœuds d'un domaine DS doivent permettre la partition des ressources entre les différents agrégats, en accord avec les politiques d'affectation des ressources. Les conditionneurs de trafic doivent contrôler que les ressources sont correctement affectées en fonction des TCA. Quoiqu'un ensemble de services puisse être déployé en l'absence de fonctions de conditionnement complexes (en utilisant des politiques de marquage

statiques), des fonctions comme le contrôle des flots (*policing*), la mise en forme, et le remarquage dynamique permettent le déploiement de services suivant des métriques de performance prédéterminées.

Une entité de contrôle doit pouvoir arbitrer entre des décisions d'allocation de ressources contradictoires. Il existe une grande variété de modèles pour réaliser ces contrôles. Cependant, le passage à l'échelle de la technique DiffServ nécessite que le contrôle des domaines ne requière pas une gestion microscopique des ressources du réseau. Le contrôle passant le plus facilement l'échelle s'effectue en boucle ouverte à l'échelle du temps de traitement des paquets.

La standardisation des PHB doit spécifier un DSCP recommandé parmi les valeurs de DSCP disponibles. Les fonctions correspondantes doivent inclure la gestion de la file d'attente, l'allocation des mémoires, la destruction des paquets et la sélection de la ligne de sortie. Enfin, une spécification des méthodes permettant de résoudre les incompatibilités entre les groupes de PHB doit être ajoutée à la standardisation.

La spécification d'un groupe de PHB doit indiquer le nombre de PHB individuels présents dans le groupe. Si plusieurs PHB travaillent en parallèle dans un même groupe, les interactions et les contraintes à respecter entre les PHB doivent être clairement indiquées. Par exemple, la spécification du groupe doit indiquer si la probabilité de réordonnancement des paquets dans un même microflot augmente lorsque différents paquets de ce microflot empruntent différents PHB à l'intérieur du groupe et sont donc marqués par des DSCP différents.

Quand le fonctionnement d'un groupe peut dépendre de contraintes entre PHB, la définition des PHB doit décrire le comportement des conditionneurs lorsque ces contraintes sont violées. De plus, si des actions telles qu'une perte de paquet ou un remarquage sont requises lorsque les contraintes sont violées, ces actions doivent être parfaitement stipulées.

Un groupe de PHB peut être spécifié pour un usage local à l'intérieur d'un domaine de façon à permettre de définir des fonctions spécifiques d'un domaine. Dans ce cas, les spécifications d'un PHB sont utiles pour permettre l'interfonctionnement de ces PHB à l'intérieur d'un groupe. Cependant, tous les groupes de PHB qui sont définis pour un usage local ne doivent pas être pris en compte dans la normalisation. Seuls les groupes de PHB standards doivent être absolument spécifiés pour permettre l'interfonctionnement des nœuds de transfert des équipementiers.

Il est possible qu'un paquet marqué pour un PHB à l'intérieur d'un groupe de PHB soit remarqué s'il est sélectionné pour être transféré par un autre PHB de ce groupe. Trois raisons peuvent nécessiter ce remarquage :

- Les DSCP associés à un groupe de PHB correspondent à des états du réseau.
- Des conditions impliquent une modification du niveau du PHB utilisé pour un flot.
- La frontière entre deux domaines n'est pas couverte par un SLA. Dans ce cas, les DSCP à sélectionner au passage de la frontière sont déterminés par des politiques locales.

La spécification d'un PHB doit clairement indiquer les circonstances dans lesquelles des paquets marqués pour un PHB donné à l'intérieur d'un groupe de PHB doivent être dirigés vers un autre PHB du groupe. S'il est interdit que le PHB d'un paquet soit modifié, la spécification doit indiquer clairement les risques encourus lorsque le PHB est modifié malgré tout. Le risque de changement d'un PHB à l'intérieur ou à l'extérieur d'un groupe de PHB augmente fortement la probabilité d'avoir à réordonnancer un microflot. Les PHB à l'intérieur d'un groupe peuvent transporter des sémantiques différentes qu'il peut être difficile de dupliquer si les paquets sont remarqués dans un autre PHB.

Pour certains groupes de PHB, il peut être approprié d'indiquer un changement d'état en remarquant les paquets vers un autre PHB à l'intérieur du groupe. Si un groupe de PHB est déterminé pour refléter l'état du réseau, la définition d'un PHB doit être capable de décrire la relation entre les PHB et les états du réseau qu'ils reflètent. De plus, si ces PHB limitent les possibilités de transfert qu'un nœud peut réaliser, ces contraintes peuvent être spécifiées dans les actions qu'un nœud peut prendre.

Le processus de spécification d'un groupe de PHB est par nature incrémental. Quand un nouveau groupe de PHB est proposé, les interactions avec les PHB déjà implémentés doivent être documentées. Quand un nouveau groupe de PHB est créé, il peut être totalement nouveau quant à son objet mais également être une extension plus ou moins complexe d'un groupe déjà défini. Dans les deux cas, les interactions à l'intérieur du nouveau groupe doivent être spécifiées en fonction des autres groupes de PHB. En particulier, le réordonnancement des paquets des microflots doit être discuté. Si des opérations concourantes doivent être effectuées par des PHB appartenant à des groupes différents, il faut en spécifier les interactions. Si le groupe de PHB est une extension d'un groupe de PHB déjà existant, il est nécessaire que les interactions soient spécifiées avec soin.

La conformité d'un PHB avec sa définition doit pouvoir être vérifiée par diverses règles, comme l'utilisation de tables de conformité, la prise en compte de tests ou de pseudo-codes, etc. De plus, les spécifications d'un PHB doivent inclure des éléments de sécurité. En particulier, les groupes de PHB doivent indiquer le processus à activer en réaction à des attaques par déni de service ou à des attaques visant à réduire ou violer le contrat de service.

Une spécification de PHB doit enfin inclure une section détaillant les moyens employés pour la configuration et la gestion des PHB.

Élément de normalisation des PHB

Comme expliqué précédemment, ce sont les caractéristiques d'un PHB qui doivent être standardisées et non les algorithmes particuliers ou les mécanismes implémentés pour le réaliser. Le comportement d'un nœud est défini par un ensemble de paramètres qui permettent de déterminer comment le contrôle des paquets doit s'exercer sur les interfaces (nombre de files d'attente, priorités rattachées, longueur des files d'attente, disciplines de service, algorithmes de perte de paquets, poids associés aux préférences, seuils, etc.).

Pour illustrer la distinction entre un PHB et un mécanisme, indiquons qu'un conditionneur de trafic adapté au PHB est un système de files d'attente disposant d'algorithmes

de type WFQ (Weighted Fair Queuing), WRR (Weighted Round Robin) ou de leurs variantes, ou encore CBQ (Class Based Queuing), séparément ou en combinaison. Les PHB peuvent être définis individuellement ou en groupe. La spécification du groupe de PHB doit décrire les conditions selon lesquelles un paquet doit être remarqué pour sélectionner un autre PHB à l'intérieur du groupe.

Chaque PHB standardisé doit avoir un DSCP associé, alloué parmi les 32 DSCP potentiels. Cette spécification laisse de la place pour faire évoluer les DSCP en utilisant l'ensemble des possibilités offertes par le champ DS. Les équipementiers sont libres d'offrir des paramètres spécifiques pour leur PHB. Quand un PHB standardisé est accepté dans un nœud, un équipementier doit pouvoir utiliser tout algorithme qui satisfasse à la définition du PHB pour réaliser son implémentation. Les possibilités offertes par les ressources implémentées dans le nœud et les moyens de configuration du nœud déterminent la façon dont les paquets sont traités pour réaliser le PHB.

Les opérateurs ne sont pas requis d'utiliser les mêmes mécanismes de configuration pour réaliser les services différenciés à l'intérieur de leur réseau et sont libres de configurer à leur façon les paramètres de leurs nœuds de transfert de sorte à satisfaire les PHB pris en compte.

DiffServ, ATM et Ethernet

DiffServ permet de déterminer de grandes classes de clients pour lesquelles une garantie peut être apportée lors du transfert des paquets. Cependant, de nombreux réseaux n'utilisent pas la technologie IP pour réaliser le transport proprement dit et lui préfèrent, par exemple, ATM ou Ethernet.

Si la valeur du DSCP peut être facilement trouvée dans un routeur en examinant le paquet IP, il n'en va pas de même lorsque le paquet IP est encapsulé dans une trame ATM ou Ethernet. Il faut donc que le routeur soit capable de répercuter la valeur du DSCP dans une garantie de qualité de service équivalente à celle du PHB. De surcroît, IntServ peut également être utilisé dans de petits réseaux dans lesquels le passage à l'échelle ne se pose pas.

Il est possible de faire coexister IntServ et DiffServ, puisque les classes sont relativement équivalentes. On peut donc très bien utiliser IntServ dans des réseaux d'accès et DiffServ dans le réseau cœur. Le service Guaranteed Service est de même type que le service EF (Expedited Forwarding) ou Premium, et les services Controlled Load équivalent aux services AF.

Dans le cas de l'ATM, les services sont de type différent. Le service EF a les mêmes garanties que les services CBR (Constant Bit Rate) et VBRrt (Variable Bit Rate real-time), mais l'ATM a séparé en deux les services avec une forte garantie sur le temps de réponse : un service pour les flots à débit constant émulant des circuits et un service pour les flots à débit variable avec de fortes contraintes temporelles.

Pour les services correspondant à AF, la correspondance est plus complexe. Les services ABR (Available Bit Rate), GFR (Guaranteed Frame Rate) et VBRnrt (Variable Bit Rate no real-time) de l'ATM sont des services de type AF dans lesquels il n'y a de garantie que sur

les taux de perte, et non sur les délais de transfert. Le service ABR peut être rapproché d'un service AF de type Gold dans lequel aucune perte de paquet n'est acceptée. Cependant, un service ABR peut accepter des taux de perte, pouvant rapprocher ce service d'un service AF de type argent ou bronze. Les algorithmes permettant de garantir que tous les paquets arrivent au destinataire sont totalement différents de ceux du monde IP. Ici, c'est un algorithme de contrôle des accès fondé sur les taux (*rate based*) qui permet de garantir qu'il y a toujours une place disponible en mémoire pour recevoir une cellule ATM. Cet algorithme augmente ou diminue le débit à l'entrée d'un circuit virtuel ATM.

Le service GFR est fondamentalement différent. Il se propose de garantir un taux de perte de paquet et non plus un taux d'erreur. De nouveau, on peut retrouver les différentes classes de services AF mais avec une garantie différente. Le service VBRnrt est également différent de ce que peuvent offrir les services AF. Le meilleur rapprochement serait un service AF de type bronze dans lequel une contrainte temporelle assez large pourrait être garantie. L'objectif de ce service VBRnrt est le transport de vidéo sans voie de retour.

Enfin, le service BE (Best Effort) de DiffServ est équivalent au service UBR (Unspecified Bit Rate) de l'ATM.

La correspondance entre les PHB et les possibilités offertes par les réseaux Ethernet est beaucoup plus complexe puisque la qualité de service proposée par Ethernet est définie de façon ouverte. On utilise les trois éléments binaires du champ IEEE 802.1p, situés dans la zone VLAN de la trame Ethernet, pour déterminer les niveaux de priorité. Il est donc possible de déterminer huit niveaux de priorité. Si on laisse au moins le premier niveau pour les informations de contrôle et plus généralement pour la signalisation, il reste sept niveaux. Il n'est donc pas possible de mettre en parallèle les quatorze niveaux proposés par DiffServ et les qualités de service acceptables dans Ethernet.

Pour trouver une équivalence, il faudrait définir dans Ethernet l'équivalent des PHB les plus classiques et implémenter dans les commutateurs Ethernet les mêmes fonctions de traitement que celles réalisées dans les routeurs DiffServ. Cette solution n'étant pas envisageable dans l'état actuel des commutateurs Ethernet, il faudra trouver le moyen, grâce aux contrôles disponibles et aux traitements des priorités dans les réseaux Ethernet, de garantir des services équivalents à ceux de DiffServ.

IP Mobile

Le protocole IP est de plus en plus souvent présenté comme une solution possible pour résoudre les problèmes posés par les utilisateurs mobiles. Le protocole IP Mobile peut être utilisé sous IPv4, mais le manque d'adresses potentiel complique la gestion de la communication avec le mobile. IPv6 est préférable, du fait de son grand nombre d'adresses disponibles, qui permet d'attribuer des adresses temporaires aux stations en cours de déplacement.

Le fonctionnement d'IP Mobile est le suivant :

1. Une station possède une adresse de base, avec un agent qui lui est attaché et qui a pour rôle de suivre la correspondance entre l'adresse de base et l'adresse temporaire.

2. Lors d'un appel vers la station mobile, la demande est acheminée vers la base de données détenant l'adresse de base.
3. Grâce à l'agent, il est possible d'effectuer la correspondance entre l'adresse de base et l'adresse provisoire et d'acheminer la demande de connexion vers le mobile.

Cette solution est semblable à celle utilisée dans les réseaux de mobiles, qu'il s'agisse de la version européenne GSM ou américaine IS-95.

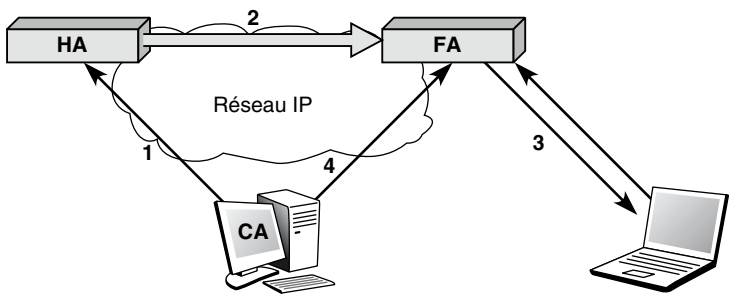
La terminologie employée dans IP Mobile est la suivante :

- Mobile Node, ou nœud mobile : terminal ou routeur qui change son point d'attachement d'un sous-réseau à un autre sous-réseau.
- Home Agent, ou agent Home : routeur du sous-réseau sur lequel est enregistré le nœud mobile.
- Foreign Agent, ou agent Foreign : routeur du sous-réseau visité par le nœud mobile.

L'environnement IP Mobile est formé de trois fonctions relativement disjointes :

- La découverte de l'agent (Agent Discovery) : lorsque le mobile arrive dans un sous-réseau, il recherche un agent susceptible de le prendre en charge.
- L'enregistrement : lorsqu'un mobile est hors de son domaine de base, il enregistre sa nouvelle adresse (Care-of-Address) auprès de son agent Home. Suivant la technique utilisée, l'enregistrement peut s'effectuer soit directement auprès de l'agent Home, soit par l'intermédiaire de l'agent Foreign.
- Le tunneling : lorsqu'un mobile se trouve en dehors de son sous-réseau, les paquets doivent lui être délivrés par une technique de tunneling, qui permet de relier l'agent Home à l'adresse Care-of-Address.

Les figures 17.8 et 17.9 illustrent les schémas de communication d'IP Mobile pour IPv4 et IPv6.



HA (Home Agent) FA (Foreign Agent) CA (Care-of-Address)

Figure 17.8

IP Mobile pour IPv4

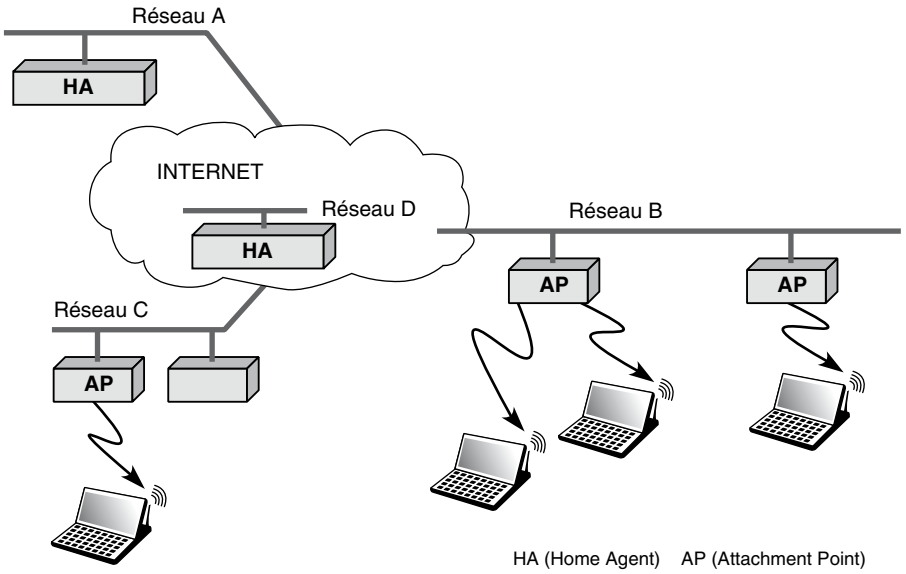


Figure 17.9
IP Mobile pour IPv6

Configuration automatique des réseaux IP

L'installation et l'exploitation des logiciels TCP/IP requièrent une certaine expertise. Une première fonctionnalité que l'on peut ajouter au démarrage d'un réseau IP consiste à automatiser l'installation et la maintenance de l'environnement IP et des protocoles associés, de façon à permettre à un utilisateur de relier sa machine au réseau sans avoir à déterminer manuellement la valeur des paramètres. De ce fait, un utilisateur peut connecter son ordinateur à Internet sans faire appel à un spécialiste pour installer les logiciels et mettre à jour les paramètres de configuration et de routage. En particulier, il est possible d'obtenir une configuration automatique d'un calculateur par de nouveaux protocoles permettant à une machine d'obtenir et d'enregistrer automatiquement toutes les informations sur les noms et les adresses dont elle a besoin.

Des groupes de travail examinent les améliorations qui peuvent encore être apportées à l'environnement Internet. Le groupe Apprentissage des routeurs travaille sur des protocoles qui permettent à une machine de découvrir les routeurs qu'elle peut utiliser. Actuellement, il est nécessaire de configurer l'adresse d'un routeur par défaut. Le protocole permettra de découvrir les adresses des passerelles locales et de tester en permanence ces adresses pour savoir lesquelles peuvent être utilisées à tout instant.

Le protocole DHCP (Dynamic Host Configuration Protocol) est utilisé pour initialiser et configurer dynamiquement une nouvelle machine connectée. Le protocole NDP (Neighbor Discovery Protocol) permet, avec l'aide des protocoles ARP et ICMP, d'auto-

configurer les adresses et la configuration de la MTU (Maximum Transmission Unit), ou taille maximale des données pouvant être contenues dans une trame physique.

La MTU désigne la plus grande taille possible d'un datagramme lui permettant d'être transporté par les différentes trames utilisées dans les sous-réseaux traversés, sans qu'il soit nécessaire de la fragmenter. Par exemple, si un paquet IP doit transiter par un premier sous-réseau, dans lequel les trames les plus longues sont de 1 500 octets, puis un deuxième réseau, dans lequel la trame maximale est de 1 000 octets, et enfin un troisième sous-réseau acceptant la taille maximale de 450 octets, la MTU est de 450 octets. Le calcul de la MTU s'effectue en recherchant la plus petite MTU sur un chemin particulier.

La taille optimale d'un segment TCP dépend de la MTU, car les datagrammes plus grands que la MTU sont fragmentés, tandis que les datagrammes plus petits sont remplis d'une proportion plus importante de données de supervision. La partie concernant les données de supervision s'appelle l'overhead. Dans l'exemple précédent, si la partie des données de supervision fait 50 octets, on voit que le fait de prendre une MTU de 450 octets oblige de transporter 50 octets chaque fois qu'il y a 450 octets à transporter, c'est-à-dire que 10 % de la charge correspond à de l'overhead. Si la MTU avait été choisie à 1 500 octets, seulement 3,2 % d'overhead aurait été porté par le réseau.

Si la MTU est connue, TCP optimise le débit en construisant des segments assez longs pour tenir dans un datagramme, lui-même transporté dans une seule trame physique, la plus grande possible. De la même façon, UDP peut améliorer le débit en tenant compte de la MTU pour choisir la taille des datagrammes.

Conclusion

Le monde des réseaux IP est très vivant et se développe à vive allure. Son organisme de normalisation, l'IETF, se réunit trois fois par an, et le nombre de groupes de travail mobilisés dépasse la centaine. Ce chapitre ne pouvait refléter qu'un certain nombre de ces travaux.

Les grandes tendances des années 2000 se focalisent sur la qualité de service, la sécurité et la mobilité, que nous rencontrerons tout au long de cet ouvrage dans des chapitres dédiés.

Partie V

Les réseaux de mobiles

Les réseaux hertziens concernent l'ensemble des systèmes de communication qui utilisent les voies hertziennes. Ces réseaux se présentent quasiment toujours sous la forme de réseaux cellulaires, c'est-à-dire d'un ensemble de zones géographiques, appelées cellules, arrosées par des antennes situées au centre. Les réseaux de mobiles utilisent ces réseaux hertziens cellulaires en permettant le passage d'une cellule à une autre sans couper la communication. Les réseaux sans fil, au contraire, ne permettent que le nomadisme, c'est-à-dire le déplacement de l'utilisateur entre les connexions, l'utilisateur restant immobile lors de la connexion. Les réseaux satellite forment un troisième exemple de réseau hertzien, avec des cellules fixes ou mobiles suivant la position et la vitesse du satellite. L'objectif de cette partie est d'examiner les réseaux de mobiles. Les réseaux sans fil sont étudiés à la partie VI.

La mobilité est devenue en quelques années une fonction primordiale réclamée par les utilisateurs, d'abord pour la téléphonie puis pour la transmission de données. La mobilité lors d'une communication téléphonique est totalement banalisée depuis le GSM. En revanche, les connexions à haut débit ne le sont que depuis l'arrivée de l'UMTS haut débit, avec le HSDPA. Encore que le débit augmente si le client est immobile ou se déplace très lentement. Les réseaux de mobiles et les réseaux sans fil se sont développés de façon non concertée, ce qui a donné naissance à deux catégories de produits totalement distinctes.

Le chapitre 18 présente les réseaux de mobiles que nous connaissons bien de nom : le GSM et l'UMTS, c'est-à-dire la 2G et le début de la 3G. Le chapitre 19 s'intéresse à la 3G+ et à la 4G. La 3G+ démarre réellement le passage vers la transmission de données et donc l'intégration des réseaux de mobiles aux réseaux Internet. Cette intégration permet de faire converger les réseaux de terminaux fixes et les réseaux de mobiles vers un réseau unique, le NGN (Next Generation Network), qui est examiné au chapitre 20.

18

Les réseaux de mobiles 2G et 3G

Les réseaux de mobiles font partie de la famille des réseaux cellulaires. Une cellule est une zone géographique dont tous les points peuvent être atteints à partir d'une même antenne. Lorsqu'un utilisateur d'un réseau cellulaire se déplace et change de cellule, le cheminement de l'information doit être modifié pour tenir compte de ce déplacement. Cette modification s'appelle un changement intercellulaire, ou handover, ou encore hand-off. La gestion des handovers est souvent délicate puisqu'il faut trouver une nouvelle route sans interrompre la communication. La gestion de la mobilité est un autre problème complexe, qui demande généralement deux bases de données, un HLR (Home Location Register), qui tient à jour les données de l'abonné, et un VLR (Visitor Location Register), qui gère le client dans la cellule où il se trouve.

Les quatre générations de réseaux de mobiles

Les communications entre utilisateurs mobiles se développent rapidement et représentent un énorme marché pour cette première décennie du XXIe siècle. Quatre générations de réseaux de mobiles se sont succédé, qui se distinguent par la nature de la communication transportée :

- 1G : communication analogique ;
- 2G : communication numérique sous forme circuit ;
- 3G : communication sous forme paquet, sauf pour la parole téléphonique ;
- 4G : communication multimédia sous forme paquet à très haut débit.

Nous présentons en détail dans ce chapitre les générations 2G et 3G et reportons au chapitre suivant les générations 3G+ et 4G, qui permettent de réaliser des réseaux à haut débit.

Les services fournis par la première génération de réseaux de mobiles sont quasi inexistants en dehors de la téléphonie analogique. Son succès est resté très faible en raison du coût des équipements, qui n'ont pas connu de miniaturisation. La deuxième génération est passée au circuit numérique. La normalisation d'un faible nombre d'interfaces air a permis le développement de composants en grande série et l'arrivée de la téléphone mobile dans le grand public. La troisième génération repose sur une technologie paquet mais garde le circuit pour la parole. Enfin la quatrième génération est totalement paquet et ressemble à un réseau Internet hertzien.

Le tableau 18.1 récapitule les différentes générations de réseaux de mobiles.

Génération	Réseau sans fil	Réseau cellulaire
1re génération	CTO, CT1	NMT, R2000, AMPS, TACS
2e génération	CT2, DECT, PHS	GSM, D-AMPS, DCP, PCS1800/1900, IS95A/IS41 et IS136/IS41
2e génération et demie		GPRS, IS95B
3e génération		UMTS, W-CDMA, cdma2000, EDGE, DECT
3e génération et demie	Wi-Fi, WiMAX	HSDPA, HSUPA, HSOPA, LTE
4e génération	Multitechnologie Wi-xx	LTE-Advanced (LTE-A), WiMAX IEEE 802.16m

TABLEAU 18.1 • Générations de réseaux de mobiles

La 2G

La 2G représente réellement le démarrage des réseaux de mobiles. Nous allons commencer par décrire l'architecture de ce système, qui a été repris par les générations suivantes mais en utilisant un vocabulaire en grande partie différent.

Chaque cellule dispose d'une station de base, ou BTS (Base Transceiver Station), qui assure la couverture radio. Une station de base comporte plusieurs porteuses, qui desservent les canaux de trafic des utilisateurs, un canal de diffusion, un canal de contrôle commun et des canaux de signalisation. L'interface intermédiaire est l'interface air. Chaque station de base est reliée à un contrôleur de station de base, ou BSC (Base Station Controller). Le BSC et l'ensemble des BTS qui lui sont raccordés constituent un sous-système radio, ou BSS (Base Station Subsystem). Les BSC sont tous raccordés à des commutateurs du service mobile, appelés MSC (Mobile services Switching Center). L'interface entre le sous-système radio et le commutateur de service mobile est appelée interface A.

L'architecture d'un réseau de mobiles 2G est illustrée à la figure 18.1.

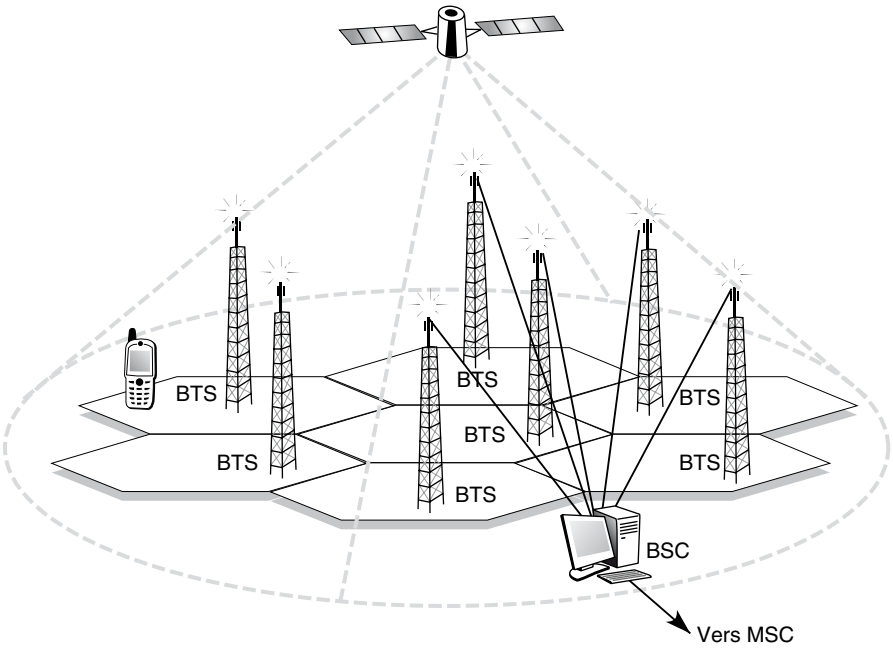


Figure 18.1

Architecture d'un réseau de mobiles

La mobilité dans les réseaux 2G

La mobilité, caractéristique essentielle des réseaux que nous étudions dans ce chapitre, donne la possibilité de se déplacer dans la zone de couverture sans que la communication soit coupée, et donc de changer de cellule, voire de réseau.

La gestion de la mobilité revêt deux aspects :

- La gestion de la localisation, qui permet au réseau de connaître à tout instant l'emplacement du terminal, des utilisateurs et du point d'accès au réseau avec suffisamment de précision pour acheminer les appels aux utilisateurs appelés là où ils se trouvent.
- Le transfert intercellulaire, ou handover, qui permet d'assurer une continuité des appels lors d'un changement de cellule.

Les réseaux de deuxième génération sont caractérisés par une mobilité spécifique en fonction de leur type. Les réseaux sans fil téléphoniques correspondent à une application particulière des réseaux fixes, dans laquelle l'utilisateur peut disposer des services offerts par le réseau fixe au prix d'une mobilité restreinte de son terminal. Ils proposent à l'utilisateur ce que l'on appelle une mobilité personnelle, en s'appuyant sur les concepts UPT (Universal Personal Telecommunications) de télécommunications personnelles universelles.

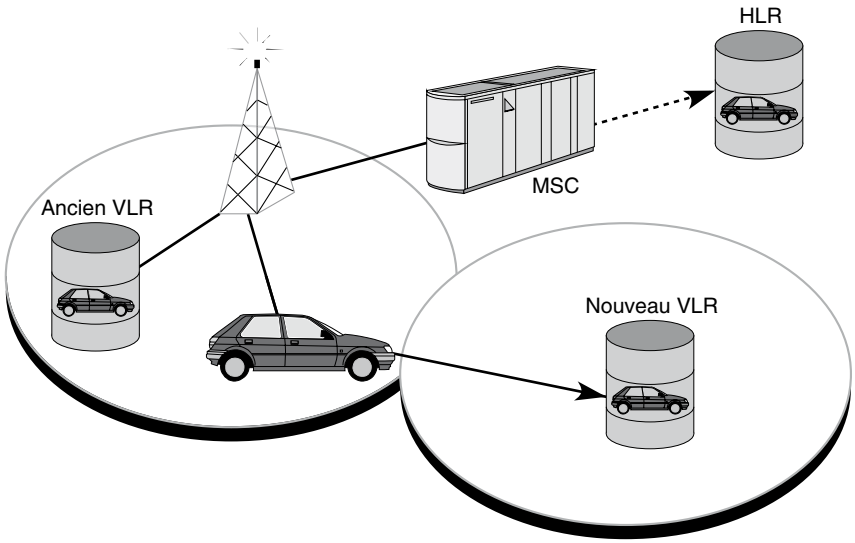


Figure 18.2
Handover et création d'un enregistrement dans un nouveau VLR

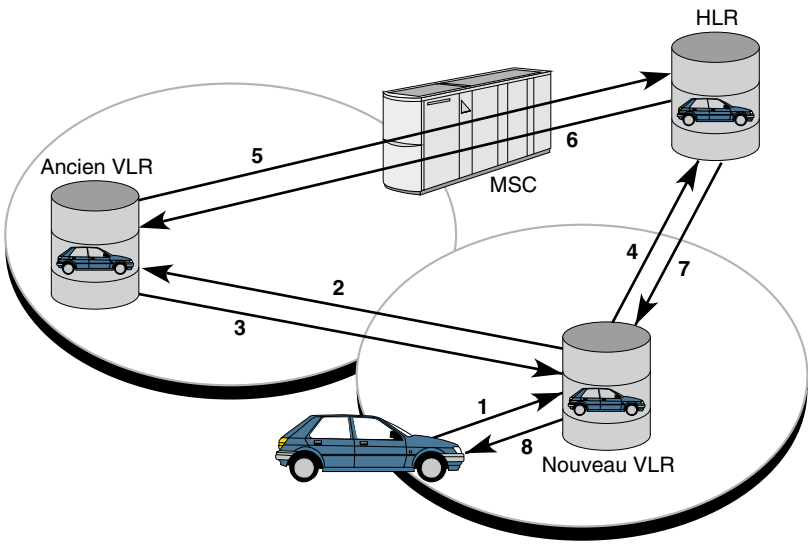


Figure 18.3
Étapes de mise à jour du HLR

Les réseaux cellulaires offrent une plus grande mobilité du terminal. En revanche, ils n'autorisent généralement qu'une faible mobilité personnelle. Pour des systèmes comme le GSM, les fonctions UPT se limitent à la possibilité d'utiliser la carte d'identification

qui se trouve à l'intérieur du terminal, la carte SIM (Subscriber Identity Module), dans n'importe quel autre équipement terminal.

La mobilité requiert une gestion, qui s'effectue généralement à l'aide de deux bases de données : le HLR, qui tient à jour les données de l'abonné, et le VLR, qui gère le client dans la cellule où il se trouve. Dans la réalisation de la mise à jour, deux types de localisation sont prévus : lorsque l'IMSI (International Mobile Subscriber Identity) peut être fourni par l'ancien VLR, et lorsque l'IMSI ne peut pas être fourni par l'ancien VLR.

Les figures 18.2 et 18.3 illustrent le handover et la création d'un nouvel enregistrement dans la nouvelle base de données VLR ainsi que les étapes de mise à jour du HLR. Les flèches indiquent l'ordre dans lequel les commandes sont envoyées lors de la procédure de changement de cellule.

La transition vers la 3G

La mise en place de la troisième génération de réseaux de mobiles a demandé un laps de temps assez long, de l'ordre d'une dizaine d'années. Les raisons à cela sont, d'une part, le besoin de repartir de zéro du point de vue des infrastructures et, d'autre part, un manque de capitaux de la part des opérateurs de mobiles à la suite de l'achat de licences à des prix très élevés dans certains pays comme la Grande-Bretagne ou l'Allemagne. Ce laps de temps a été mis à profit pour améliorer la deuxième génération et lui permettre d'approcher les performances de la troisième. Le GPRS (General Packet Radio Service) est le nom donné en Europe à l'amélioration de la technique GSM pour obtenir cette deuxième génération et demie.

Les réseaux de la génération 2,5G se caractérisent souvent, comme c'est le cas dans le GPRS, par un double réseau cœur, un réseau cœur pour le transport du téléphone et un réseau cœur pour le transport des données sous forme de paquets. À ce double réseau cœur, s'ajoutent des terminaux spécifiques, capables de gérer à la fois les voies téléphoniques, comme dans le GSM, et les voies de données, beaucoup plus sporadiques.

Les données sont mises dans de tout petits paquets dans le terminal lui-même, où elles attendent que le canal radio soit vide avant d'être émises. En d'autres termes, la téléphonie s'effectue de la même façon que dans la deuxième génération, en utilisant des slots de temps réservés lors de la mise en place du circuit téléphonique. Les circuits de l'interface radio sont prolongés sur les circuits du réseau cœur. On retrouve ici le caractère circuit de la transmission de la deuxième génération. En revanche, les paquets de données attendent des slots libres pour être émis vers le réseau à transfert de paquets.

Pour ces transferts de données, la difficulté consiste à déterminer de façon probabiliste le nombre de clients qui peuvent être acceptés sur une même fréquence, sachant que les clients paquet émettent à des instants aléatoires. Il est donc très difficile de prévoir le moment de passage des paquets sur l'interface radio. Le service est évidemment fortement asynchrone. Le coût est lié au nombre de paquets transmis et non à la durée de la communication, comme lors d'une conversation téléphonique.

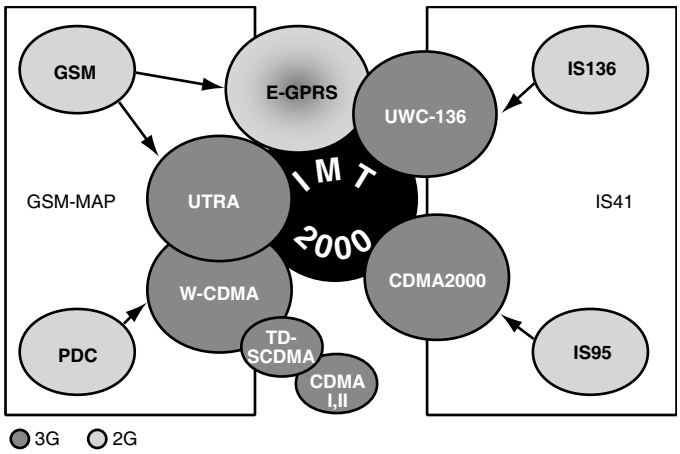
Les infrastructures d'un tel réseau sont quasiment identiques à celles du réseau GSM. Il suffit d'ajouter le réseau à transfert de paquets et la gestion des slots vides qui doivent être mis à profit pour émettre des paquets de données. La deuxième génération et demie utilise des réseaux à commutation de trames. Si cette génération se prolonge longtemps, le réseau cœur pour les données se transformera en un réseau ATM ou en un réseau MPLS.

La technologie EDGE, qui fait également partie de la transition vers la troisième génération, est examinée à l'annexe N.

La 3G

La figure 18.4 illustre les évolutions des systèmes de deuxième génération vers des systèmes de troisième génération. L'ETSI propose l'UTRA, la partie radio de l'UMTS, et l'E-GPRS comme évolutions du GSM. De son côté, l'ARIB (Association of radio Industries and Businesses) propose le WCDMA (Wideband Code Division Multiple Access) comme évolution du PDC (Personal Data Communications system). Ces systèmes sont fondés sur le réseau fixe du GSM.

Les interfaces radio de l'UMTS et du WCDMA étant semblables, la recherche de compromis a consisté à modifier quelques paramètres de la couche physique, tels que la vitesse de modulation ou le nombre de slots par trame. De même, des propositions très semblables, tels le TD-SCDMA chinois et les CDMA I et II coréens, ont-elles été fondues dans l'UMTS.



CDMA2000	(Code Division Multiple Access)
CDMA I, II	(Code Division Multiple Access)
E-GPRS	(Enhanced General Packet Radio Service)
GSM	(Global System for Mobile communications)
GSM MAP	(GSM Mobile Application Part)
IMT	(International Mobile Telecommunications System)
IS	(Interim Standard)
TD-SCDMA	(Time Division-Synchronous CDMA)
UTRA	(UMTS Terrestrial Radio Access)
UWC136	(Universal Wireless Communications 136)
W-CDMA	(Wideband-Code Division Multiple Access)

Figure 18.4

Évolution des technologies mobiles 2G-3G

Soutenant des solutions techniques fondées sur le réseau fixe du GSM, les organismes de normalisation régionaux se sont regroupés autour de l'UMTS pour lui donner du poids en tant que solution candidate à l'IMT 2000. Fin 1998, le 3GPP (Third Generation Partnership Project) a été créé dans ce but. Quelques semaines plus tard, un deuxième groupe mondial, le 3GPP2, était créé autour du cdma2000.

Le 3GPP

Lors de sa création, le 3GPP regroupait des organismes de standardisation régionaux, parmi lesquels l'ETSI pour l'Europe, ARIB et TTC (Telecommunications Technology Committee) pour le Japon, TTA (Telecommunications Technology Association) pour la Corée et T1P1 pour les États-Unis. Peu après, le CWTS (China Wireless Telecommunication Standard) rejoignait le projet.

La structure du 3GPP est semblable à celle de l'ETSI. Le 3GPP est organisé en groupes de travail, les TSG (Technical Specification Group), spécialisés dans un domaine et produisant des spécifications techniques. Ces groupes techniques sont encadrés par une équipe de coordination de projet, qui s'assure que la standardisation progresse au rythme prévu. La figure 18.5 illustre la structure générale du 3GPP.

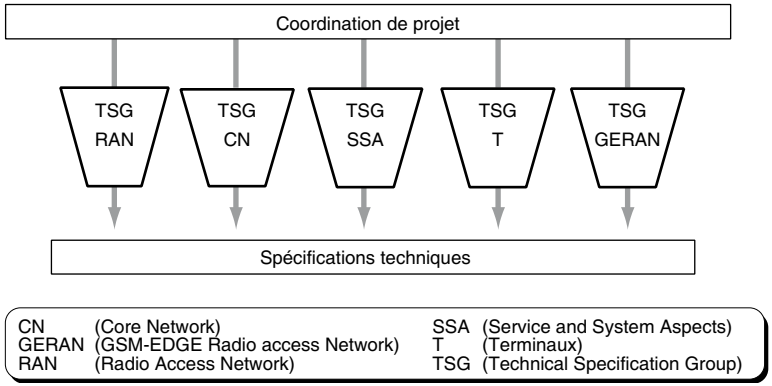


Figure 18.5
Structure du 3GPP

Les cinq domaines techniques suivants sont représentés au 3GPP :

- **RAN (Radio Access Network).** Ce groupe étudie l'UTRAN en général, c'est-à-dire les couches basses de l'accès radio, ainsi que les protocoles mis en œuvre sur les interfaces Iu, Iub et Iur. Un dernier sous-groupe spécifie les gabarits d'émission et de réception des stations de base.
- **CN (Core Network).** Traite du réseau fixe et des protocoles associés (signalisation, gestion de la mobilité, établissement d'appel), de l'architecture de service et de l'interconnexion avec les réseaux extérieurs.
- **SSA (Service and System Aspects).** Ce groupe se focalise sur les services, et notamment sur les services de téléphonie, avec la spécification des codecs. Il aborde également les aspects de sécurité et de confidentialité des communications.
- **T (Terminals).** Examine principalement les aspects relatifs à la carte SIM et spécifie les tests de conformité des mobiles.
- **GERAN (GSM Enhanced Radio Access Network).** Ce groupe réunit les travaux sur les évolutions du GSM (GPRS, EDGE).

Le 3GPP fournit un accès gratuit à toutes les spécifications, qu'elles soient définitives ou en cours d'élaboration. Ces dernières sont disponibles par FTP ou par une interface de type Web sur le site du 3GPP. Chaque sous-groupe de travail dispose de surcroît d'une liste de diffusion qui permet de prolonger ou d'initier les débats des réunions plénières. Ces listes sont, elles aussi, d'accès libre.

Les cinq concepts d'accès radio

L'ETSI a étudié cinq solutions techniques pour l'UTRA (UMTS Terrestrial Radio Access). Communément appelés α, β, γ, δ et ε, ces solutions proposent des schémas d'accès radio différents.

- α, ou le WCDMA. Il s'agit d'un CDMA large bande (Wideband CDMA). Le qualificatif « large bande » provient du fait que, comparativement au seul système CDMA existant à l'époque, l'IS95, le WCDMA requiert des canaux beaucoup plus larges, de 5 MHz. L'une des caractéristiques principales du système est sa flexibilité, qui lui permet d'accepter tout type de débit, allant de quelques kilobits par seconde à plusieurs centaines de kilobits par seconde. Cette solution est à l'origine du mode FDD de l'UMTS.
- β, ou l'OFDMA. Fondée sur des modulations OFDM (Orthogonal Frequency Division Multiplexing), cette solution mélange en fait TDMA et OFDMA. L'OFDMA consiste à partager les porteuses OFDM entre différents utilisateurs. L'allocation de plus ou moins de porteuses à un utilisateur offre une grande flexibilité dans les débits, mais les variations d'enveloppe du signal OFDM rendent complexe le design des amplificateurs de puissance des terminaux. Cette solution a donc été éliminée au moment des travaux mais est réapparue pour les réseaux de quatrième et cinquième générations.
- δ, ou le TD-CDMA. Ce système hybride TDMA-CDMA consiste à prendre une trame TDMA et à multiplexer plusieurs utilisateurs dans un même slot par du CDMA. Pour ce faire, on applique de l'étalement de spectre dans chaque slot, ce qui rend la bande utilisée plus large. Ce concept a été développé dans un premier temps pour des canaux larges de 1,6 MHz puis a donné lieu au mode TDD (Time Division Duplex) de l'UMTS dans des canaux de 5 MHz.
- γ, ou le W-TDMA. Le Wideband TDMA, ou TDMA large bande, consiste à prendre un système TDMA de type GSM, mais avec des canaux beaucoup plus larges (1,6 MHz) que les 200 kHz du GSM, sans utiliser d'étalement de spectre. Cette solution assez peu pratique pour accepter des bas débits et offrir les mêmes services de voix que les systèmes 2G a été rejetée.
- ε, ou l'ODMA. L'ODMA (Opportunity Driven Multiple Access) est une technique de relais applicable en principe à toutes les autres solutions. Un utilisateur qui ne bénéficie pas de conditions radio favorables communique avec la station de base par l'intermédiaire d'autres mobiles, situés entre l'utilisateur et la station de base, plutôt que d'émettre à pleine puissance et engendrer beaucoup d'interférences. Par de multiples petits bonds, la communication s'effectue dans des conditions correctes. Malheureusement, la possibilité de voir sa batterie se décharger pour d'autres communications que la sienne est assez mal vue par la majorité des utilisateurs. C'est pourquoi cette solution est restée optionnelle, même si elle est devenue très à la mode du fait de l'engouement pour les réseaux ad-hoc (*voir le chapitre 23*).

Après une première procédure de sélection fondée sur des comparaisons techniques, un vote a lieu en janvier 1998 pour statuer sur le concept retenu. Aucune majorité absolue ne se dégageant, l'UMTS serait composite, α pour les bandes appairées (mode FDD) et δ pour les bandes non appairées (mode TDD). Bien que ces deux solutions diffèrent dans

l'accès physique, les couches supérieures sont fortement semblables et peuvent apparaître comme deux modes d'une même solution.

En décembre 1998, l'UMTS est transféré au sein du 3GPP, avec pour première conséquence une harmonisation avec la solution WCDMA d'ARIB. Puis une activité plus importante du mode FDD s'est dessinée par rapport au mode TDD, avec cependant un poids important du TDD qui a été choisi par la Chine et son milliard d'utilisateurs potentiels.

L'UMTS

Cette section présente en détail la première version stabilisée de l'UMTS, dite *release* 99, publiée en mars 2000.

Les évolutions de l'UMTS sont abordées au chapitre suivant. Pour éviter de relier ces versions à une date, l'UMTS a choisi de les nommer R5 (*release* 5), R6, etc.

Architecture générale

L'architecture de l'UMTS s'appuie sur la modularité. Ses éléments constituants doivent être indépendants, de façon à autoriser en théorie des mises à jour de telle ou telle partie du système sans avoir à en redéfinir la totalité.

L'UMTS définit trois domaines : le domaine utilisateur, le domaine d'accès radio, ou UTRAN, et le réseau cœur (Core Network). Ces domaines sont séparés par des interfaces, respectivement l'interface Uu et l'interface Iu.

Des strates fonctionnelles sont appliquées à cette architecture de façon à séparer les fonctions en groupes indépendants :

- La strate d'accès radio (transport/access stratum) contient les protocoles et fonctions relatifs à l'accès radio.
- La strate de service (serving stratum) contient tout ce qui permet l'établissement d'un service de télécommunications.
- La strate « personnelle » (home stratum) est dédiée aux fonctions qui permettent de mémoriser et de récupérer les informations relatives à un utilisateur pour personnaliser ses services et environnements.
- La strate applicative (application stratum) représente les applications qui sont mises en œuvre de bout en bout.

Le domaine utilisateur est similaire à ce qui a été défini en GSM. Il se compose d'un terminal capable de gérer l'interface radio et d'une carte à puce, la carte U-SIM, qui contient les caractéristiques de l'utilisateur et de son abonnement. De même, le domaine du réseau fixe est semblable à celui du GPRS. En revanche, l'accès radio de l'UMTS, l'UTRAN, est complètement différent et est décrit en détail ci-dessous.

L'architecture générale de l'UMTS est illustrée à la figure 18.6.

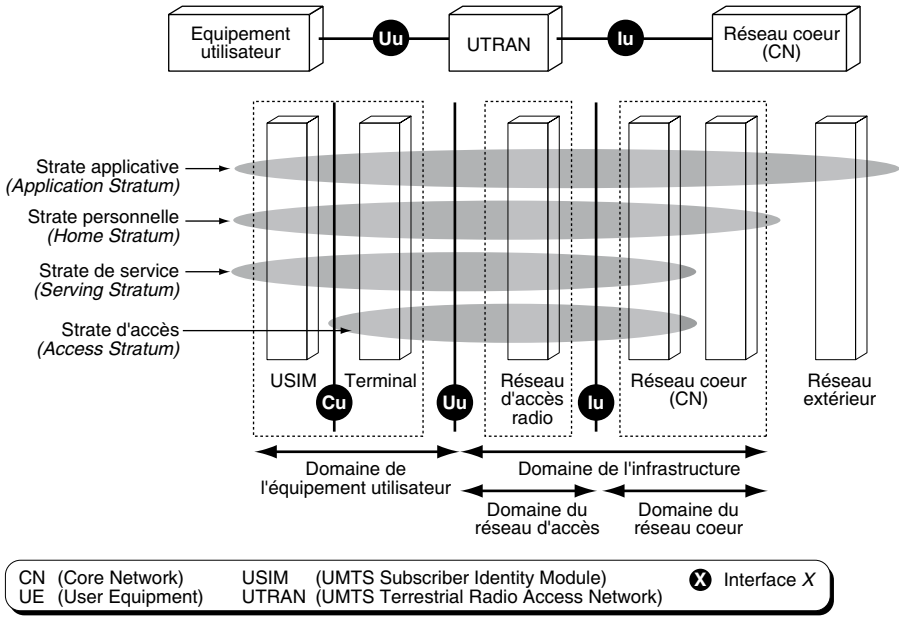


Figure 18.6

Architecture générale de l'UMTS

L'UTRAN regroupe les stations de base, appelées NodeB dans le vocabulaire de l'UMTS, et les contrôleurs de stations de base, ou RNC (Radio Network Controller).

Scindé en deux parties, le réseau cœur est constitué d'un réseau cœur de type circuit et d'un réseau cœur de type paquet. Le réseau cœur circuit est composé, à l'image de celui du GSM, de commutateurs circuits, les MSC (Mobile service Switching Center), de passerelles vers les réseaux téléphoniques publics, les G-MSC (Gateway MSC), et de serveurs dédiés aux SMS, les SMS-GMSC (SMS Gateway MSC).

Le réseau cœur orienté paquet est semblable à celui du GPRS. Il est composé de commutateurs paquet, les SGSN (Serving GPRS Support Node) et les GGSN (Gateway GPRS Support Node), qui relient le réseau de l'opérateur au monde extérieur, lequel peut être représenté par un réseau paquet public ou un réseau paquet d'un autre opérateur. Le réseau situé entre les GGSN et les SGSN est un réseau paquet quelconque, le plus souvent un réseau IP.

Pour gérer les données relatives aux utilisateurs, telles que leur position dans le réseau, leur abonnement, etc., les bases de données introduites dans le GSM sont toujours présentes dans l'UMTS. Il s'agit, entre autres, des HLR (Home Location Register), VLR (Visitor Location Register) et EIR (Equipment Identity Register).

La signalisation échangée entre ces éléments du réseau réutilise le système de signalisation CCITT n° 7, ou SS7.

L'UTRAN

Avant de rejoindre le 3GPP, UTRAN signifiait UMTS Terrestrial Radio Access. Lors de la création du 3GPP, le sigle a perdu son origine européenne pour signifier Universal Terrestrial Radio Access. On y retrouve l'approche modulaire qui domine dans l'UMTS, la signalisation étant séparée du transport des informations. Il existe par conséquent deux catégories de protocoles, les protocoles du plan utilisateur (*user plane protocols*) et les protocoles du plan de contrôle (*control plane protocols*).

La strate d'accès de l'UTRAN est reliée aux autres strates par des points d'accès de services (*service access point*) de trois types : service de contrôle commun, pour la diffusion d'informations générales, service de contrôle dédié, pour un utilisateur spécifique, et service de notification, pour diffuser des informations non pas à toute la cellule mais à des utilisateurs spécifiques.

Les éléments constituant l'UTRAN sont les stations de base, ou NodeB, dans le vocabulaire de l'UMTS, et les contrôleurs de stations de base, les RNC (Radio Network Controller). Un RNC et plusieurs NodeB forment un sous-système radio, ou RNS (Radio Network Subsystem).

Terminologie UMTS-GSM

Plutôt que de reprendre les sigles du GSM, l'UMTS a redéfini la majorité d'entre eux, même s'ils renvoient à des entités similaires dans le réseau d'accès radio.

Le tableau 18.2 compare la terminologie du GSM et celle de l'UMTS relative au réseau d'accès radio.

UMTS	GSM	Commentaire
UE (User Equipment)	MS (Mobile Station)	
NodeB	BTS (Base Transceiver Station)	Un NodeB est moins autonome qu'une BTS.
RNC (Radio Network Controller)	BSC (Base Station Controller)	Un RNC est plus complexe qu'un BSC puisqu'il contrôle complètement les NodeB.
UMSC (UMTS MSC)	MSC (Mobile-services Switching Center)	
RNS (Radio Network Subsytem)	BSS (Base Station Subsystem)	
Interface Iub	Interface Abis	Entre BTS et BSC (NodeB-RNC)
Interface Iu	Interface A	Entre BSC (RNC) et réseau cœur
Interface Iur	Inexistante	Entre 2 RNC.

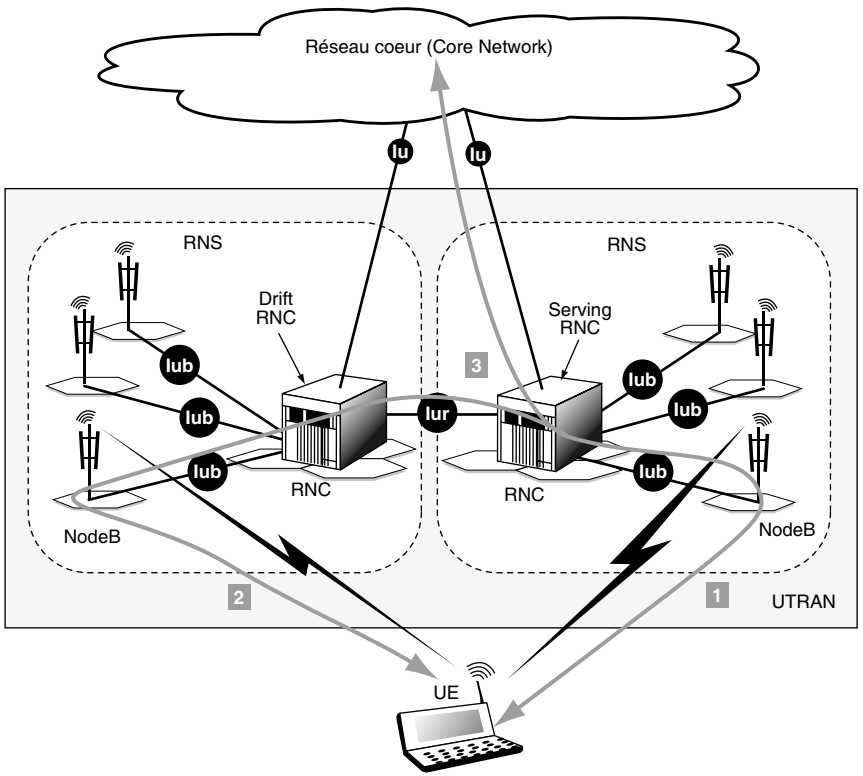
TABLEAU 18.2 • Comparaison de la terminologie du réseau d'accès radio

Un NodeB est connecté à un RNC par le biais de l'interface Iub, et un RNC l'est au réseau cœur par le biais de l'interface Iu. Contrairement au GSM, l'UTRAN définit une interface supplémentaire entre deux RNC, l'interface Iur. Cette interface a été introduite du fait de la spécificité de l'accès radio, qui est fondé sur du CDMA. Le CDMA permet le *soft-handover,* c'est-à-dire l'établissement de deux chemins ou davantage entre le réseau et un mobile *via* deux stations de base potentiellement différentes. La séparation-combinaison

des deux chemins se fait dans l'UTRAN, et il n'y a donc, au-delà du RNC, qu'un chemin possible vers le réseau cœur.

Le RNC qui se trouve à l'extrémité de ce chemin unique entre l'UTRAN et le réseau cœur est appelé RNC serveur (Serving RNC ou SRNC), car c'est lui qui permet à l'utilisateur d'être connecté avec le réseau cœur. Dans le cas d'un mobile en *soft-handover,* le RNC par lequel transite un chemin supplémentaire entre le mobile et le SRNC est appelé DRNC (Drift RNC).

Ces notions de Serving et Drift RNC (*voir figure 18.7*) sont relatives à un utilisateur : un même RNC peut donc être Serving pour un utilisateur et Drift pour un autre. Un RNC est, au départ, un contrôleur de station de base, c'est-à-dire qu'il gère les stations de base à distance. Par conséquent, pour les NodeB, on parle de CRNC (Controlling RNC).



1 **Le mobile est connecté** au réseau coeur *via* son Serving RNC.
2 **Il établit une nouvelle connexion** avec une autre station de base en soft-handover.
3 **Les deux chemins sont recombinés** dans le Serving RNC. Le RNC par lequel transite le nouveau chemin est appelé Drift RNC. Serving et Drift RNC communiquent à travers l'interface Iur.

RNC	(Radio Network Controller)	UE	(User Equipment)
RNS	(Radio Network Subsystem)	UTRAN	(UMTS Terrestrial Radio Access Network)

Figure 18.7

Les notions de Serving et de Drift RNC

La figure 18.8 illustre la découpe en couches de l'UTRAN, qui regroupe une couche physique PHY, une couche de partage des ressources MAC (Medium Access Control), une couche de fiabilisation du lien radio RLC (Radio Link Control), une couche d'adaptation des données PDCP (Packet Data Convergence Protocol) et une entité transverse, le RRC (Radio Resource Controller), qui contrôle le tout. La couche BMC (Broadcast Multicast Control), non finalisée dans la *release* 99 du standard, traite de service de diffusion dans une cellule ou un ensemble de cellules. Ces couches recouvrent les couches 1 et 2 du modèle de référence de l'OSI à 7 couches, même si certaines fonctions du RRC peuvent être rattachées à la couche 3.

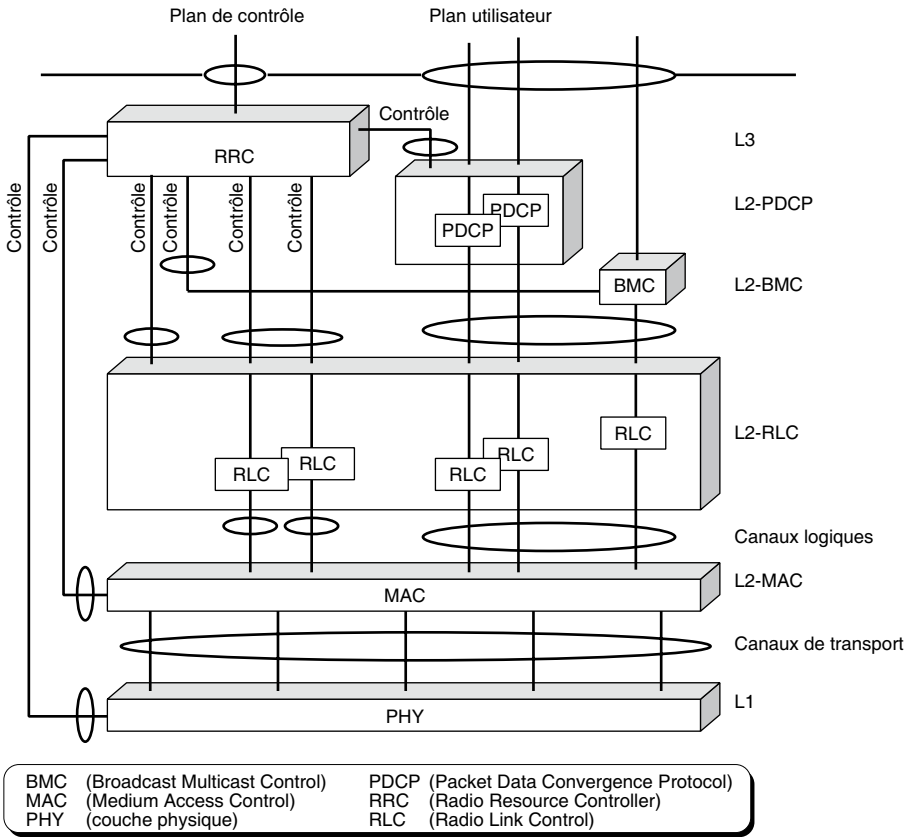


Figure 18.8

Architecture en couches de l'UTRAN

On retrouve dans cette architecture les deux plans de protocole, le plan utilisateur, dont les données traversent les couches PDCP, RLC, MAC et PHY, et le plan de contrôle, auquel appartient le RRC.

Toujours dans l'approche modulaire de l'UMTS, sous la couche physique se trouvent des canaux physiques, entre la couche physique et la couche MAC des canaux de transport et entre le MAC et le RLC des canaux logiques. Ces canaux représentent des points d'accès de services rendus par la couche inférieure à la couche supérieure.

La couche physique

C'est dans cette couche que les modes FDD et TDD de l'UMTS diffèrent le plus. La section suivante présente le mode FDD, qui est considéré comme le mode majeur de l'UMTS puisqu'on lui a alloué plus de fréquences dans le spectre.

Le mode FDD

Comme son nom l'indique, le mode FDD (Frequency Division Duplex) utilise un duplex en fréquences, dans lequel la voie montante et la voie descendante sont séparées en fréquences. Mobile et station de base communiquent en continu et simultanément dans les deux directions. La communication entre la station de base et le mobile s'établit par une technique d'étalement de spectre, qui est à la base du CDMA. Le débit chip est constant : 3,84 Mchip/s.

On appelle canal physique l'association d'une fréquence porteuse, d'une paire de codes, l'un pour l'embrouillage et l'autre pour l'étalement (*scrambling* ou *channelization code*), et d'une durée temporelle exprimée en multiple de chip. Des multiples particuliers sont prédéfinis dans l'UMTS : un slot représente 2 560 chips, une trame 38 400 chips (15 slots), soit respectivement 0,667 ms et 10 ms.

Il existe des canaux physiques dédiés, alloués à un utilisateur en particulier, et des canaux physiques communs, partagés entre tous les utilisateurs. Certains canaux physiques sont visibles des couches supérieures et servent à transmettre les informations des couches supérieures, tandis que d'autres ne sont utiles qu'au bon fonctionnement de la couche physique.

Le tableau 18.3 synthétise les canaux physiques du mode FDD de l'UMTS.

La structure du canal d'accès aléatoire PRACH est adaptée à l'aloha discrétisé, qui est, comme en GSM et dans les autres systèmes radiomobiles, la technique d'accès utilisée. Néanmoins, si, en GSM, deux stations lançant une requête en même temps entrent en collision, ici, le CDMA permet de jouer sur la dimension code : le paquet d'accès initial est étalé par un code parmi 16 choisis aléatoirement par le mobile. Ce code, aussi appelé signature, permet de distinguer plusieurs mobiles entrant dans le réseau quasi simultanément. Cela a bien sûr un coût en termes de complexité, puisque la station de base doit surveiller en permanence les 16 codes possibles.

Le rôle majeur de la couche physique est d'étaler et contracter (« désétaler ») le signal respectivement en émission et en réception, opération à la base de la séparation des utilisateurs en CDMA. L'UMTS définit deux étapes d'étalement. La première consiste à multiplier le signal à transmettre par une séquence de chips au débit beaucoup plus rapide. C'est l'étalement à proprement parler, nommé *scrambling* ou *channelization*. La deuxième étape est la modulation du signal en QPSK.

	Nom	Rôle
Dédiés	DPDCH (Dedicated Physical Data CHannel)	Pour le transport des données dédiées à un utilisateur ; bidirectionnel
	DPCCH (Dedicated Physical Control CHannel)	Pour le contrôle du DPDCH ; bidirectionnel
Communs (visibles des couches supérieures)	PRACH (Physical Random Access CHannel)	Pour l'accès initial des mobiles dans le réseau ; UL uniquement
	PCPCH (Physical Common Packet CHannel)	Canal partagé montant ; UL uniquement
	PDSCH (Physical Downlink Shared CHannel)	Canal partagé pour des transmissions descendantes sporadiques ; DL uniquement
	PCCPCH (Primary Common Control Physical CHannel) SCCPCH (Secondary Common Control Physical CHannel)	Diffusion d'information système (primary) ; Paging et réponse des couches hautes aux accès initiaux (secondary) ; DL uniquement
Communs (uniquement couche physique)	AICH (Acquisition Indicator CHannel)	Pour une réponse de la couche physique aux accès initiaux ; DL uniquement
	SCH (Synchronization CHannel)	Permet au mobile de se synchroniser au réseau ; DL uniquement
	CPICH (Common Pilot CHannel)	Canal pilote commun ; permet au mobile de se synchroniser sur la cellule et d'estimer la puissance reçue (mesure à l'origine des handovers) ; DL uniquement.

TABLEAU 18.3 • Canaux physiques de l'UMTS FDD

Le mode TDD

Le mode TDD est fondé sur une méthode d'accès hybride entre le TDMA et le FDMA. La séparation entre le sens montant et le sens descendant se fait dans le temps. Certains slots de la trame — la même que celle définie dans le mode FDD — sont dédiés à la voie montante, et d'autres à la voie descendante. La répartition des slots dans la trame est flexible, quoiqu'il faille avoir au moins un slot montant et descendant, mais un opérateur peut configurer son système avec 14 slots descendants et 1 slot montant.

Le TDD peut donc supporter très facilement du trafic asymétrique, alors que, par construction, le mode FDD est symétrique, autant de spectre étant alloué au sens montant qu'au sens descendant. Le TDD est mis en œuvre dans les bandes non appairées, contrairement au FDD, qui est utilisé dans les bandes appairées.

Alors qu'en FDD une communication peut s'effectuer en continu dans la trame, les slots n'étant qu'une base de temps pour le contrôle de puissance en boucle fermée, en TDD, le slot retrouve toute l'essence du TDMA : une communication est centrée sur un ou quelques slots.

Le fait que le CDMA consiste à partager un slot entre plusieurs utilisateurs a de multiples conséquences. Du fait qu'un utilisateur ne dispose que d'un ou quelques slots pour sa communication, il doit, pour obtenir des débits semblables au mode FDD, transmettre sur un slot à un débit beaucoup plus élevé. Or, le rythme chip est le même en TDD qu'en FDD : 3,84 Mchip/s. Par conséquent, en TDD les facteurs d'étalement sont beaucoup plus faibles qu'en FDD. Du coup, des techniques de réception plus élaborées, trop complexes

en FDD, telles que la détection conjointe, sont en pratique réalisables en TDD. De plus, la structure des canaux physiques du TDD est différente. Par exemple, le burst normal du TDD possède une séquence connue du récepteur au milieu du slot, permettant l'estimation de canal slot par slot, exactement comme dans le GSM.

Les communications montantes doivent arriver dans le bon slot de la station de base, car une mauvaise synchronisation pourrait créer des interférences d'un slot à l'autre. Cette contrainte n'existe pas en FDD. Pour y faire face, le mode TDD a défini, à l'instar du GSM, des temps de garde autour du slot pour absorber les différences de temps de propagation des utilisateurs d'une cellule. La taille de ce temps de garde limite l'usage du TDD aux microcellules et aux picocellules. Les stations de base doivent être également synchronisées entre elles, sinon, il pourrait y avoir des interférences entre les slots montants d'une cellule et les slots descendants des cellules voisines, puisque toutes les transmissions sont à la même fréquence – en UMTS, il n'y a pas de planification cellulaire comme dans un système GSM.

Malgré ces différences, le TDD et le FDD présentent sensiblement les mêmes caractéristiques physiques. Ces dernières sont recensées au tableau 18.4.

	FDD	TDD
Accès multiple	W-CDMA	TD-CDMA
Séparation DL-UL	FDD	TDD
Facteur d'étalement	256-4 (UL) 512-4 (DL)	16-1
Handover	Soft	Hard
Fréquence chip	3,84 Mchip/s	Idem
Structure de trame	15 slots par trame de 10 ms	Idem
Filtre de mise en forme	Cosinus surélevé roll-off 0,22	Idem
Espacement des porteuses	5 MHz	Idem
Trame	10 ms, 15 slots, 2 560 chip/slot	Idem
Modulation	QPSK	Idem
Codage	Non codé, convolutif, turbo	Idem
Entrelacement	10, 20, 40 ou 80 ms	Idem

TABLEAU 18.4 • Caractéristiques physiques du FDD et du TDD

Les couches MAC et RLC

La couche MAC effectue l'association des canaux logiques, visibles par la couche supérieure, la couche RLC, et des canaux de transport que lui offre la couche physique. De plus, elle sélectionne le format de transport, du moins dans sa partie dynamique, le plus approprié, compte tenu des conditions radio du moment. Elle gère en outre les priorités entre les flux d'un même utilisateur et entre différents utilisateurs. La couche MAC se contente d'appliquer les règles de priorité érigées par le RRC (Radio Resource Controller), qui a une meilleure connaissance à la fois des différentes QoS requises par les utilisateurs et de la charge de la cellule. La couche MAC est également responsable de la collecte des mesures sur le volume du trafic et les conditions de propagation de la cellule pour les transmettre au RRC.

On retrouve dans la couche MAC le principe de modularité de l'UMTS : comme cette couche doit gérer différents types de canaux, plusieurs entités MAC sont définies : le MAC-b pour les canaux de diffusion, le MAC-c/sh pour les canaux partagés et le MAC-d pour les canaux dédiés. Ces entités ne se situent pas forcément dans le même élément de l'UTRAN. En effet, la gestion des canaux de diffusion est locale à une cellule. Le MAC-b peut donc être localisé dans la station de base. En revanche, à cause du *soft-handover,* la gestion des canaux dédiés doit remonter jusqu'au SRNC. Ainsi, le MAC-d se trouve dans les RNC. Les décisions prises par le MAC-d sont transmises à la cellule *via* le CRNC, en utilisant l'interface Iur, entre SRNC et CRNC, puis l'interface Iub, entre CRNC et NodeB.

Les canaux logiques entre MAC et RLC sont décrits au tableau 18.5. Ils sont séparés en deux groupes, les canaux de contrôle et les canaux de trafic. Les principes d'association entre canaux logiques et canaux de transport que doit respecter la couche MAC sont standardisés.

	Nom	Rôle
Trafic	DTCH (Dedicated Traffic CHannel)	Pour le transfert des données dédies à un utilisateur ; bidirectionnel
	CTCH (Common Traffic CHannel)	Canal point à multipoint pour le transfert de données à un groupe d'utilisateurs ; DL uniquement
Contrôle	BCCH (Broadcast Control CHannel)	Pour la diffusion d'informations système ; DL uniquement
	PCCH (Paging Control CHannel)	Pour le paging ; DL uniquement
	DCCH (Dedicated Control CHannel)	Pour le transfert d'information de contrôle (établissement d'appel, handover, etc.) dédiée à un utilisateur ; bidirectionnel
	CCCH (Common Control CHannel)	Pour le transfert d'information de contrôle partagée par les utilisateurs (accès initial, réponse à l'accès initial) ; bidirectionnel

TABLEAU 18.5 • Canaux logiques

La couche RLC (Radio Link Control) permet de fiabiliser les transmissions sur l'interface radio, tout en réalisant un contrôle de flux. Les fonctions de la couche RLC sont les suivantes : segmentation et réassemblage, concaténation ou bourrage des blocs d'information issus des couches supérieures, pour en faire des paquets de taille acceptée par la couche MAC, détection des duplications, retransmission, remise en ordre des paquets reçus et chiffrement.

Trois modes d'opération sont en fait disponibles :

- Le mode transparent, qui se contente d'effectuer les opérations de segmentation-réassemblage.
- Le mode non acquitté, qui numérote les paquets et détecte les erreurs. Il n'effectue pas de retransmission pour les corriger, l'entité RLC réceptrice ne transmettant pas les paquets erronés à la couche supérieure.
- Le mode acquitté, qui est le plus robuste offert par la couche RLC. Lorsqu'un paquet est erroné, des retransmissions sont effectuées suivant la stratégie d'ARQ sélectif.

Le RRC

Le RRC (Radio Resource Controller) est l'« éminence grise » de l'UTRAN. La majorité des échanges de la signalisation entre le mobile et l'UTRAN se fait avec le RRC. De plus, il pilote toutes les autres couches, en fonction des QoS requises sur les communications et de la charge du réseau. Pour cela, il existe des connexions de contrôle entre le RRC et les autres couches de l'UTRAN, comme illustré à la figure 18.9.

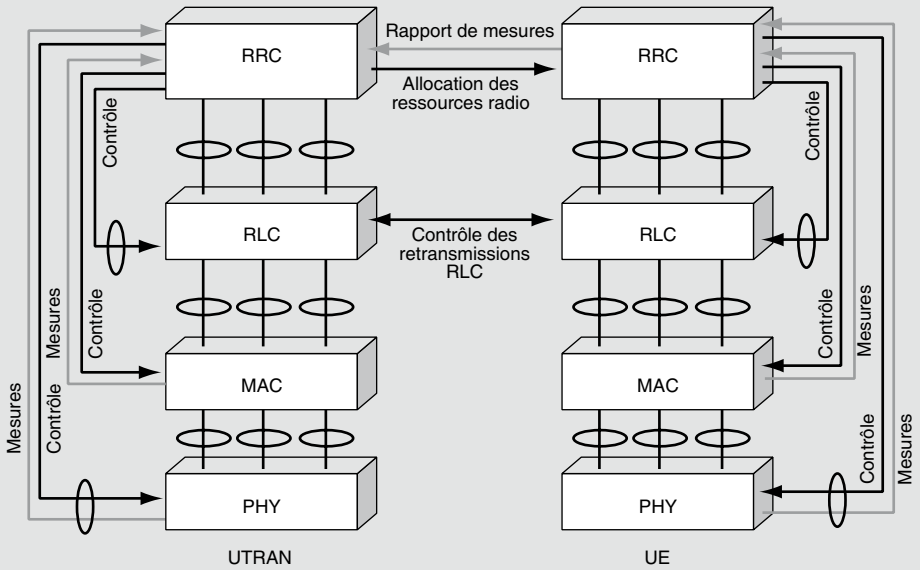


Figure 18.9

Schéma de fonctionnement du RRC

Le RRC est aussi le point de contact des échanges de signalisation avec le réseau cœur. Ainsi, en réponse à une demande de connexion du mobile (dans le cas d'un appel sortant ou du réseau cœur pour les appels entrants), l'entité RRC du mobile va négocier avec l'entité RRC du réseau l'ouverture d'un « tuyau » radio, ou RAB (Radio Access Bearer). Ce RAB est doté de paramètres permettant d'en caractériser la qualité de service. Les débits maximal et moyen, la taille des paquets transmis, le délai, le taux d'erreur résiduel et la priorité peuvent être négociés dans l'établissement du RAB. Le RRC, en tenant compte de la charge courante de la cellule, configure alors les couches inférieures pour que la QoS négociée soit respectée. La configuration s'applique aux ressources dans tout l'UTRAN, c'est-à-dire non seulement sur l'interface radio mais également sur l'interface Iub entre NodeB et RNC.

Les interfaces

Comme pour l'ensemble de l'UMTS, un effort de modélisation a porté sur la standardisation des interfaces pour les rendre modulaires. Le modèle générique des interfaces est illustré à la figure 18.10.

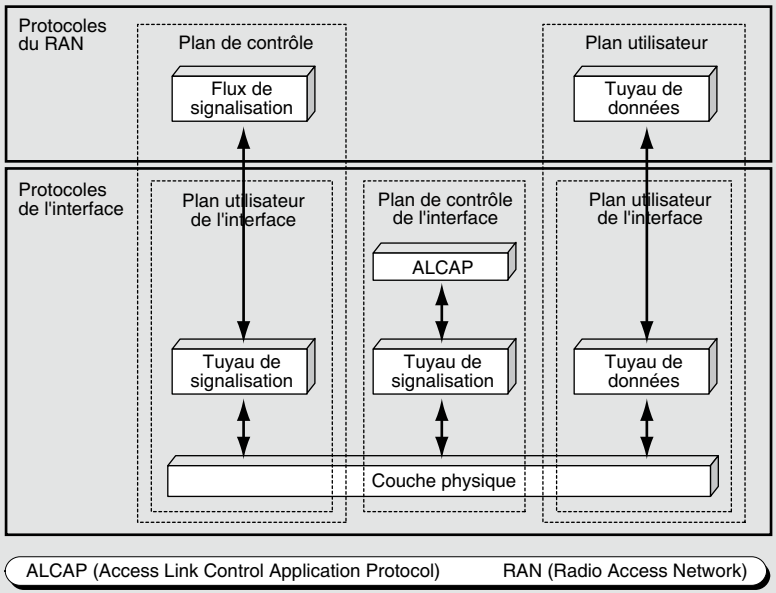


Figure 18.10

Le modèle générique des interfaces de l'UTRAN

La découpe horizontale permet de séparer ce qui est transporté sur l'interface (Radio Network Layer) d'avec le moyen de transport utilisé sur l'interface (Transport Network Layer). La découpe verticale permet de séparer le plan de contrôle du plan utilisateur. Le plan de contrôle contient tous les messages de contrôle échangés entre les entités de l'UTRAN. Le plan utilisateur contient les protocoles utilisés pour encapsuler les données utilisateur sur les interfaces. Il y a de plus la signalisation locale à l'interface (le Transport Network Control Plane) nécessaire à l'établissement des chemins sur cette interface.

Dans la version 99 des spécifications, les interfaces sont bâties sur de l'ATM. Par conséquent, on retrouve entre l'ATM et la signalisation, dans le plan de contrôle, ou dans les données utilisateur encapsulées, dans le plan utilisateur, toutes les couches d'adaptation classiques d'ATM, telles que l'AAL-2, pour l'établissement de circuits, ou l'AAL-5, pour le transport des paquets. Du fait de la découpe horizontale, rien n'empêche le remplacement d'ATM par une autre technologie : seule la brique Transport Network Layer serait à changer.

Ce modèle générique ce décline en fonction des interfaces de l'UTRAN. Sur l'interface Iub, entre NodeB et RNC, la signalisation entre RNC et NodeB est contenue dans le NBAP (NodeB Application Part). On y trouve, par exemple, les messages permettant de gérer les ressources radio, tels que création-suppression d'un lien radio, contrôle de puissance, etc. Le plan utilisateur est quant à lui constitué de protocoles d'encapsulation adaptés à tous les types de trafic.

L'interface Iur se situe entre deux RNC. Elle n'existait pas dans le GSM et est due au *soft-handover*. L'ensemble de la signalisation se nomme le RNSAP (Radio Network Subsystem Application Part). Le plan utilisateur comporte les mêmes protocoles que sur l'interface Iub. L'interface Iu permet de connecter l'UTRAN au réseau cœur. Le réseau cœur de l'UMTS est similaire au réseau cœur du GSM-GPRS. L'interface Iu est donc double et est composée d'une interface vers le domaine circuit du réseau cœur (entre UTRAN et U-MSC (UMTS MSC), appelée Iu-CS, et d'une interface vers le domaine paquet (entre UTRAN et 3G-SGSN), appelée Iu-PS.

Les services et la QoS

La philosophie de définition des services de l'UMTS est différente de celle du GSM et de ses évolutions. Plutôt que de standardiser des services, l'UMTS a préféré définir des boîtes à outils permettant de construire des services.

Le GSM n'offre pas la possibilité aux opérateurs de se différencier les uns des autres pour les services de télécommunications, la distinction ne pouvant se faire que sur la couverture d'un territoire — mais désormais tous les opérateurs possèdent une couverture nationale en GSM — ou l'approche commerciale. De plus, l'introduction de nouveaux services en GSM est difficile, compte tenu de la rigidité du système et de la nécessité de standardiser ces services. Cette limitation, particulièrement ressentie par des opérateurs bridés dans la proposition de nouveaux services, disparaît dans l'UMTS.

En effet, l'UMTS, fidèle à son esprit de modularité, spécifie plusieurs outils permettant la création de services variés, spécifiques d'un opérateur. Ces outils permettent de surcroît la création d'un environnement personnalisé, ou VHE (Virtual Home Environment), que l'utilisateur peut retrouver dans son intégrité, quel que soit l'endroit où il se trouve : à son domicile, sur son lieu de travail ou en déplacement.

Parmi ces outils standards, on trouve les systèmes d'exploitation des terminaux mobiles et des cartes SIM, nommés respectivement MExE (Mobile station application Execution Environment) et USAT (USIM Application Toolkit), une architecture de service ouverte, OSA (Open Service Architecture), les services téléphoniques intelligents, ou CAMEL (Customized Applications for Mobile Network Enhanced Logic), et enfin tout ce qui peut venir du monde IP, regroupé dans IP Toolkits.

Le réseau UMTS offre aux opérateurs qui créent ces services destinés aux utilisateurs la possibilité de les caractériser en classes de qualité de service. Pour cela, deux critères ont été retenus. Le premier est la tolérance au délai ; le second la tolérance aux erreurs. La figure 18.11 illustre les différentes classes de QoS et quelques exemples de services associés.

L'UMTS a spécifié les moyens de définir plus finement les exigences de qualité de service, en particulier dans les RAB, comme expliqué précédemment. Pour respecter ces exigences, une signalisation spécifique a été définie. Son principe consiste à s'assurer de proche en proche, en impliquant toutes les entités du réseau sur le trajet de la communication, que la QoS demandée peut être assurée.

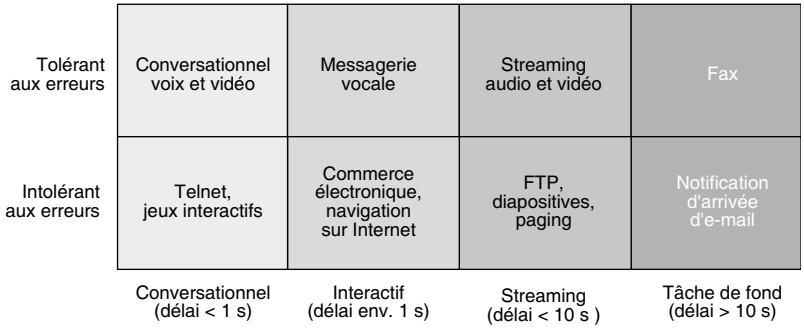


Figure 18.11

Les classes de qualité de service dans l'UMTS

Les débits offerts par l'UMTS sont conformes aux exigences de l'IMT 2000 : 2 Mbit/s pour une mobilité faible et des conditions radio favorables, le mobile ne devant pas trop s'éloigner de la station de base, 384 Kbit/s pour une mobilité moyenne, dans une ville, par exemple, et 144 Kbit/s dans un environnement rural. Bien que ces débits soient techniquement réalisables, ils ne sont que rarement atteints en pratique. L'une des raisons à cela est que, comme dans tout système radio mobile, il existe une différence entre les débits théoriques, vantés dans les approches commerciales, et les débits réels, que constatent les utilisateurs.

Conclusion

Ce chapitre a présenté les réseaux de mobiles de deuxième génération et du début de la troisième génération, ainsi que les principaux protocoles utilisés dans ces architectures. Un débat a surgi concernant le manque de débit de la troisième génération en raison de la largeur assez faible de la partie du spectre accordée à cette génération. Une solution à ce problème consiste à densifier fortement le réseau en créant des cellules de plus en plus petites. Cette solution permet, par une meilleure réutilisation des fréquences, d'atteindre les capacités annoncées. Cependant, cette densification est très onéreuse et se heurte de front aux associations de consommateurs, qui voient d'un mauvais œil la multiplication des antennes.

Les générations décrites dans ce chapitre concernent essentiellement la parole téléphonique avec peu de possibilité de transmission de données. Le chapitre suivant entre de plein fouet dans les générations de mobiles Internet pour atteindre avec la 4G les mêmes caractéristiques qu'un réseau IP fixe.

19

Les réseaux de mobiles 3G+ et 4G

Nous avons examiné au chapitre précédent les premières générations de réseaux de mobiles, celles qui se préoccupaient en priorité de la téléphonie. Avec la 3G+ et la 4G, l'important devient la transmission de données et l'intégration des réseaux de mobiles dans l'environnement IP. La 4G marquera la convergence totale avec le réseau Internet fixe. Les clients ne verront plus aucune différence entre une connexion mobile et une connexion fixe.

La 3G+ commence avec la release 5 de l'UMTS. Les différentes releases sont les suivantes :

- Release 5 (2002) – UMTS R5 : définition de l'IMS que nous détaillerons au chapitre suivant ; introduction du HSDPA (High-Speed Downlink Packet Access) permettant un débit descendant des données jusqu'à 10 Mbit/s ; amélioration du GSM-Edge, en particulier pour la téléphonie.
- Release 6 (2004) – UMTS R6 : introduction de l'IMS phase 2, du HSUPA (High-Speed Uplink Packet Access) permettant d'augmenter le débit descendant à 6 Mbit/s ; interconnexion simple avec les réseaux Wi-Fi ; introduction du MBMS (Multimedia Broadcast/Multicast Service).
- Release 7 (2007) – UMTS R7 : introduction de la technologie MIMO utilisée dans Wi-Fi (*voir le chapitre 22*) ; amélioration des performances et de la QoS ; introduction de HSPA+ (High Speed Packet Access Evolution) ; introduction du « sans contact » en vue de nouvelles applications, comme les paiements.

- Release 8 (2008) – UMTS R8 : introduction de LTE (Long Term Evolution), de l'OFDMA à la place du CDMA (non compatibilité avec les releases précédentes sur ce point) et d'un réseau tout IP (sauf pour la partie téléphonique).
- Release 9 (2009) – UMTS R9 : introduction d'un calendrier « green », c'est-à-dire de solutions permettant d'économiser l'énergie électrique dépensée par les stations de base du fait de l'importante consommation des antennes et équipements associés. Cette release propose également une normalisation des femtocells (*voir ci-après*), des services d'alerte et de WiMAX comme technologie 4G ; amélioration de la compatibilité IP.
- Release 10 (2011) – UMTS R10 : première release correspondant à la 4G LTE Advanced. Cette version sera compatible avec la release 8 sur le LTE.
- Release 11 (2012) – UMTS R11 : cette release s'occupera des services et de l'interopérabilité des services entre environnements fixe et mobile.
- Release 12 (2013) – UMTS R12 : bien qu'en cours de discussion au moment de l'écriture de cette section, elle pourrait commencer à concerner la 5G qui verrait l'arrivée d'antennes mobiles (avion, ballon, station orbitale, lune, etc.).

La génération 3G+

On considère souvent que la 3G+ correspond aux hauts débits de données, c'est-à-dire de plus de 1 Mbit/s. Cette valeur est obtenue par la technologie HSDPA dans le sens descendant et par son successeur HSUPA (High-Speed Uplink Packet Access) dans le sens montant. Nous détaillons ces deux technologies dans cette section.

La 3G+ contient également le standard LTE, qui introduit une véritable rupture dans l'interface radio puisque le CDMA est abandonné pour être remplacé par l'OFDMA. Cette rupture a été considérée pendant un certain temps comme le véritable démarrage de la 4G. En réalité, les normalisateurs ont préféré attendre la parfaite compatibilité avec Internet, en particulier sur la parole téléphonique, pour démarrer la 4G. LTE Advanced sera donc le premier produit 4G en suivant la release 10.

Le HSDPA

Le HSDPA offre des performances approximativement dix fois supérieures à la 3G (UMTS R5). C'est essentiellement une évolution logicielle qui permet cette augmentation des débits.

Le HSDPA possède un lien descendant — du réseau vers le terminal — en mode paquet en augmentation forte par rapport à l'UMTS. Le HSDPA fait partie de la famille HSPA (High-Speed Protocol Access). Nous détaillons plus loin ses versions plus évoluées HSUPA et HSOPA. Le déploiement existant en 2007 offre des débits de 1,8 Mbit/s, 3,6 Mbit/s, 7,2 Mbit/s et 14,4 Mbit/s sur le lien descendant, voire nettement plus avec la version évoluée, qui atteint 42 Mbit/s. Un autre aspect encore plus important concerne la bande passante globale, qui permet à de nombreux clients de se connecter simultanément.

Le HSDPA est une évolution relativement simple de l'UMTS, et c'est la raison pour laquelle on la classe dans la 3,5G, ou 3G+.

Les principales différences avec l'UMTS viennent des fonctions suivantes :

- Retransmissions beaucoup plus rapides à partir du NodeB grâce à l'algorithme HARQ (Hybrid Automatic Repeat reQuest).
- Nouvel ordonnancement dans le NodeB bien plus rapide que celui de l'UMTS grâce à l'algorithme FPS (Fast Packet Scheduling).
- Modulation et codage de type AMC (Adaptive Modulation and Coding).

Dans ce dernier protocole, une redondance incrémentale améliore nettement le débit : même lorsqu'un paquet arrive avec une erreur, le paquet erroné est conservé. Il est possible que, même si la retransmission du paquet débouche encore sur un paquet erroné, la combinaison des deux paquets erronés permette de corriger l'erreur.

Le canal descendant est partagé entre les utilisateurs en utilisant l'algorithme d'ordonnancement, puisque celui-ci tient compte de l'état du canal et des facteurs qui peuvent avantager la transmission vers tel utilisateur plutôt que vers tel autre. Pour cela, chaque utilisateur envoie périodiquement une indication de la qualité du signal, et ce jusqu'à 500 fois par seconde. Le NodeB utilise cette information pour ordonnancer les différents émetteurs pour les deux secondes suivantes. Les terminaux qui ont une bonne qualité de réception sur le canal descendant peuvent se voir affecter un débit nettement supérieur à celui des clients qui n'ont pas un bon canal descendant.

Lorsque le NodeB a choisi l'ordonnancement des clients, il optimise aussi le code à utiliser sur le canal. Cela implique que, sur la trame de 2 ms, les clients peuvent utiliser des codes différents. En résumé, chaque client a un débit réel spécifique, qui permet d'utiliser au mieux le canal en fonction de l'état du système.

La fonction de l'algorithme AMC (Adaptive Modulation and Coding) consiste à déterminer la modulation et le code utilisés en fonction de la qualité du canal. Le codage QPSK forme le schéma de base. Cependant, si le canal est de bonne qualité, la modulation 16QAM est adoptée, ce qui double le débit. Le codage QPSK permet d'atteindre 1,8 Mbit/s, et le codage 16QAM 3,6 Mbit/s. Des codages encore plus performants peuvent être utilisés dans certains cas de figure, pouvant permettre de monter jusqu'à des débits de 10,8 Mbit/s.

Parmi les autres améliorations du HSDPA, le débit montant peut atteindre 384 Kbit/s au lieu des 128 Kbit/s de l'UMTS. Le temps de latence de l'accès est bien meilleur, ce qui améliore la qualité de la voix téléphonique.

La release R7 de l'UMTS concerne une nouvelle augmentation des débits sur le lien descendant, avec des vitesses pouvant atteindre 42 Mbit/s. Les technologies permettant cet accroissement de la vitesse proviennent du MIMO (Multiple In Multiple Out) et de l'apparition d'antennes intelligentes.

La version suivante 3GPP R8 est encore plus ambitieuse et donne naissance au HSOPA. Cette technologie d'origine européenne atteint respectivement 100 et 200 Mbit/s respectivement dans les sens montant et descendant.

Le HSUPA

Le HSUPA s'intéresse à la voie montante, qui devrait atteindre à terme 5,76 Mbit/s. Sa spécification se trouve dans le document 3GPP R6 (release 6).

Le HSUPA utilise un canal montant amélioré nommé E-DCP (Enhanced Dedicated Channel), qui utilise les mêmes ingrédients que le HSDPA sur le canal descendant : adaptation des communications entre les terminaux et le NodeB pour optimiser l'utilisation globale du canal.

Parmi les algorithmes proposés dans cette norme, citons notamment les suivants :

- TTI (Transmission Time Interval) de longueur réduite.
- Protocole HARQ (Hybrid Automatic Repeat reQuest), qui effectue de la redondance incrémentale.
- Ordonnanceur de paquets, qui décide quand et comment sont transmis les paquets en utilisant la qualité des communications et l'état des files d'attente du récepteur.
- Possibilité de faire passer des paquets prioritaires, comme ceux de la ToIP hors du champ de l'ordonnancement. Ces paquets sont dits « non-scheduled ». L'objectif est de faire transiter des paquets avec des contraintes fortes non satisfaites par l'ordonnanceur, celui-ci ne tenant pas compte du synchronisme dont certains flots ont besoin.
- Couche MAC tenant compte des priorités des paquets ordonnancés et non ordonnancés. Le débit est déterminé à l'ouverture de la connexion.

Après la technologie HSUPA, le 3GPP a travaillé à une nouvelle amélioration avec le HSOPA, qui marque l'entrée dans la quatrième génération de réseaux de mobiles et l'entrée vers le très haut débit.

Le HSOPA

Le HSOPA (High Speed OFDM Packet Access) est une proposition du 3GPP LTE (Long Term Evolution). On appelle parfois cette norme le *super 3G*.

La différence fondamentale entre le HSOPA et les deux techniques précédentes provient de l'interface radio, qui est totalement modifiée pour passer à l'OFDMA. Cette interface étant incompatible avec les versions précédentes, HSDPA et HSUPA, il y a, à bien des égards, un changement de génération ; cependant, les normalisateurs ont préféré repousser l'introduction véritable de la 4G à la compatibilité totale avec Internet. Les débits sont de 50 Mbit/s dans le sens montant et 100 Mbit/s dans le sens descendant. Il est prévu que, sur une fréquence de 5 MHz de large, deux cents clients puissent être connectés simultanément à haut débit.

Le HSOPA travaillera de concert avec le HSDPA et le HSUPA, de sorte qu'un client devrait pouvoir se connecter sur la meilleure cellule possible par rapport à l'application en cours. Les passages d'une technologie à l'autre se feront de façon transparente.

Un autre objectif de cette norme est de permettre les handovers verticaux avec d'autres catégories de réseaux sans fil, dont WiMAX. Pour cela, le HSOPA utilisera le protocole TCP/IP, et les interconnexions pourront s'effectuer au travers du protocole IP.

L'interface E-UTRA (Evolved UTRA) a pour objectif de fonctionner avec toutes les interfaces radio de type IP, notamment avec la gamme Wi-*xx*. Cette interface utilise

l'OFDMA pour le lien descendant et le SC-FDMA (Single Carrier FDMA) sur le lien montant. La technologie MIMO, que nous détaillons au chapitre 22, est aussi adoptée sur l'E-UTRA, avec un maximum de quatre antennes.

L'OFDMA offre une flexibilité beaucoup plus grande que le CDMA de troisième génération. L'efficacité spectrale notamment, c'est-à-dire le nombre de bits émis par hertz, est bien meilleure.

Sur la bande descendante, les sous-bandes de l'OFDM seront de 15 kHz, avec un maximum de 2 048 sous-bandes. Les mobiles devront pouvoir recevoir les signaux de l'ensemble de ces 2 048 sous-bandes, mais une station de base n'aura besoin que de 72 sous-bandes. La trame radio est de 10 ms. La modulation est de type 16QAM et 64QAM.

Le LTE

Le LTE, ou Long Term Evolution, est l'abréviation promue par le 3GPP pour désigner la technologie commerciale correspondant au HSOPA, c'est-à-dire l'arrivée des technologies de radio mobile utilisant l'OFDMA. L'UMB (Ultra Mobile Broadband) promue par le 3GPP2 a pour sa part pour but de succéder au cdma2000, mais cette solution est en forte perte de vitesse par rapport au LTE.

Les interfaces sont associées à des antennes intelligentes et directives, qui permettent d'atteindre 50 Mbit/s dans le sens montant et 100 Mbit/s dans le sens descendant.

LTE Advanced

LTE Advanced et WiMAX phase 2 marquent le véritable démarrage de la 4G. LTE Advanced est naturellement la suite de LTE, avec une compatibilité IP. WiMAX phase 2 appartient également à la famille 4G et est par nature compatible IP. De nombreuses fonctions ont été révisées par rapport à WiMAX phase 1. La caractéristique essentielle reste cependant la totale compatibilité avec le monde IP.

De nombreux éléments nouveaux sont pris en compte dans la 4G représentée par le LTE Advanced. Les points marquants sont les suivants :

- Les nœuds relais qui permettent d'atteindre une antenne E-NodeB (Enhanced NodeB) ou encore eNB par l'intermédiaire d'un point relais. Cette solution a été essentiellement proposée dans le cadre de WiMAX phase 2 mais est reprise par le LTE Advanced. Nous l'introduisons un peu plus loin dans ce chapitre. La version 1 de WiMAX ne fait pas partie de la 3G ni de la 4G.
- Les solutions MIMO sont utilisées, que ce soit dans le sens antenne vers terminal ou dans le sens inverse. Le MIMO est décrit au chapitre 22.
- Les bandes passantes utilisées vont de 20 MHz à 100 MHz, ce qui permet de multiplier les débits jusqu'à un facteur 5 lorsque nécessaire.
- L'interface air est optimisée en fonction de l'emplacement du terminal et des interférences. En d'autres termes, on retrouve, comme dans la 3G+, un ensemble d'outils qui permettent d'accélérer les débits dès que le terminal se situe dans une zone où le signal est reçu avec une bonne qualité et au contraire dégradent le débit dès que le client se trouve dans un environnement difficile ou qu'il est fortement mobile.

- La 4G joue la carte de la compatibilité avec les environnements Wi-Fi qui se développent à grande vitesse afin de profiter de ces réseaux pour l'écoulement de trafics importants. Nous retrouverons un peu plus loin, avec le concept de femtocell, les problèmes de choix qui se posent pour éviter les conflits et cohabiter harmonieusement avec la génération Wi-Fi.
- La radio cognitive, que nous avons introduite au chapitre 10, est de plus en plus utilisée. Cela permet d'avoir à la fois une bande passante plus importante et une meilleure utilisation du spectre.
- La gestion et le contrôle du réseau sont beaucoup plus automatisés et deviennent autonomiques (*voir le chapitre 30*). En d'autres termes, un effort important est effectué pour obtenir un autopilotage de l'ensemble du système en matière de configuration, de sécurité, de disponibilité et de monitoring.
- Le codage de l'information est amélioré pour obtenir des taux de compression encore plus élevés que dans la 3G+. On pense notamment à des technologies comme MPEG-21. Les corrections d'erreurs seront améliorées, mais *a priori* à partir des techniques déjà utilisées dans la 3G+.
- La gestion des interférences est fortement améliorée, au point qu'elles sont quasiment supprimées. Ces technologies utilisent des antennes virtuelles (*beamforming*), qui, par leur directivité, permettent de déterminer un emplacement de la cellule à la demande.
- Les techniques utilisées sur l'interface air peuvent être asymétriques, par exemple une technique OFDMA sur la partie descendante et SC-FDMA sur la partie montante.

WiMAX phase 2

La phase 1 de WiMAX n'a eu que peu de succès pour différentes raisons non techniques. Pour rebondir, le groupe IEEE responsable de sa normalisation a demandé au 3GPP de devenir membre de la famille 4G. Cette demande a été accordée puisque WiMAX est complètement compatible avec le monde IP et offre une qualité de service et un système de gestion correspondant aux demandes des opérateurs de télécommunications. Cependant, comme nous l'avons vu, de nombreuses contraintes liées à la 4G devaient encore être prises en compte. C'est ce nouvel environnement qui a pris le nom de WiMAX phase 2.

Pour cela, le comité IEEE 802.16 a introduit les nouveaux groupes de travail suivants :

- IEEE 802.16g : Network Management Task Group (Management Plane Procedures & Services) ;
- IEEE 802.16h : License-Exempt Coexistence Task Group ;
- IEEE 802.16j : Mobile Multihop Relay Task Group ;
- IEEE 802.16m : Advanced Air Interface Task Group.

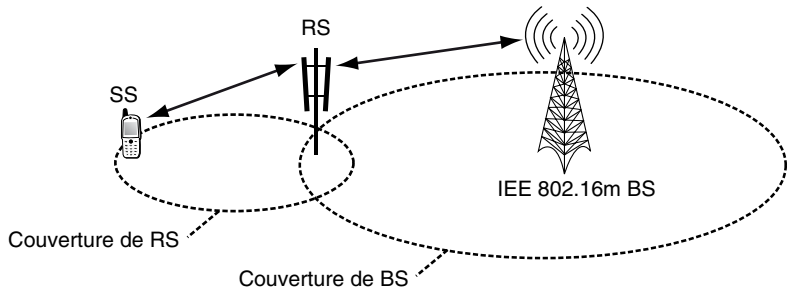
Le groupe le plus important est le dernier. Il a défini une interface radio améliorée permettant de doubler au minimum les débits pour obtenir 46 Mbit/s dans le sens descendant et toujours 4 Mbit/s dans le sens montant. WiMAX phase 2 augmente encore ces débits

pour être du même ordre de grandeur que ceux de LTE Advanced. Cette phase sera suivie de WiMAX phase 3, avec l'objectif de démultiplier de nouveau les vitesses pour atteindre plusieurs centaines de mégabits par seconde, voire le gigabit par seconde.

WiMAX phase 2 atteint déjà 100 Mbit/s en mobilité et jusqu'à 1 Gbit/s lorsque le terminal est immobile. Ces valeurs sont des débits crête et dépendent évidemment du nombre de clients connectés et actifs au moment de la mesure.

Pour ne pas reprendre des éléments communs au LTE Advanced, nous allons essentiellement décrire la proposition de *relais* qui est faite dans le standard IEEE 802.16m. Un tel relais est illustré à la figure 19.1. Les relais sont des antennes intermédiaires situées entre l'antenne principale et le terminal de l'utilisateur. Les antennes principales sont raccordées par une fibre optique au réseau cœur de l'opérateur. Lorsque l'on démultiplie les antennes, il faut réaliser du génie civil pour poser de nouveaux câbles terrestres. L'objectif des relais est d'éviter ce problème et de baisser les coûts de connexion. Le terminal est branché sur le relais, qui est lui-même connecté sur l'antenne principale par un faisceau hertzien. Ce dernier peut être situé dans les fréquences hautes, et être donc très directif, avec une large bande passante permettant de faire transiter des gigabits par seconde. Comme le faisceau est directif, il ne pollue pas l'environnement hertzien.

Cette solution permet de diminuer le coût de connexion tout en augmentant le débit global grâce à de petites antennes relais que l'on peut densifier à volonté.



Extension de couverture par déploiement d'équipements relais, ou RS (Relay Station)

BS (Base Station) : Station de base
RS (Relay Station) : Équipement relais
SS (Subscriber Station) : Équipement utilisateur

Figure 19.1

Un relais dans WiMAX phase 2

Les femtocells

La solution poussée à partir de la release 9 pour prendre en charge les énormes débits de la 4G provient de l'utilisation de femtocells. Les idées de base sont assez semblables à la technique du relais : pour ne pas avoir à construire un nouveau réseau très dense de connexion des antennes, on se sert de l'infrastructure fibre optique qui s'est mis en

place à partir de 2009 pour le très haut débit. Dans les faits, ce réseau optique n'est pas seulement dirigé pour le haut débit des utilisateurs mais bien pour prendre en charge les fantastiques débits que propose la 4G, les utilisateurs ne pouvant pas vraiment voir une différence entre un modem ADSL de haut de gamme et un modem optique à cause des contrôles du monde IP et en particulier du slow start.

Une femtocell est une antenne qui est montée sur la Home Gateway de l'utilisateur. Elle dessert tous les clients potentiels qui se trouvent dans la zone de couverture de l'antenne, laquelle peut avoisiner la dizaine de mètres, voire nettement plus en fonction des obstacles et des interférences. La femtocell est donc utilisée à la fois par le détenteur de la Home Gateway et par les visiteurs de la cellule.

Les avantages évidents de cette technologie sont la démultiplication des cellules et la densification colossale du réseau : en France plus de vingt millions d'antennes sont potentiellement disponibles. Un autre avantage très appréciable est la baisse de puissance des équipements qu'elle autorise. Une puissance maximale de 100 mW semble être le standard qui s'impose, cette puissance correspondant à celle de Wi-Fi dans une émission omnidirectionnelle.

La figure 19.2 illustre le principe de la femtocell.

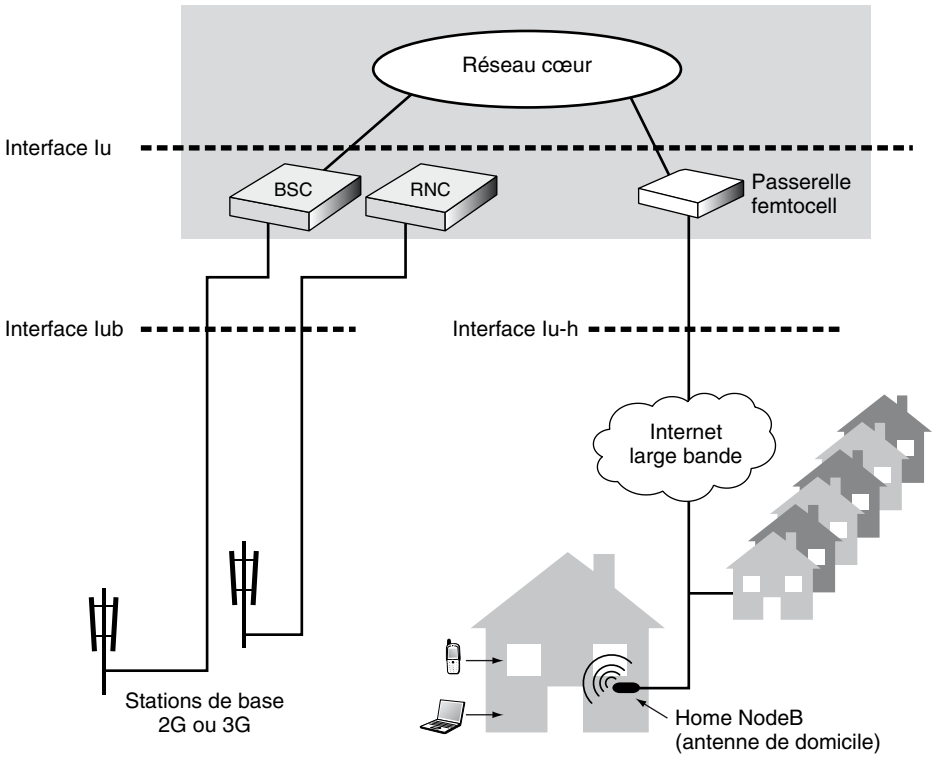
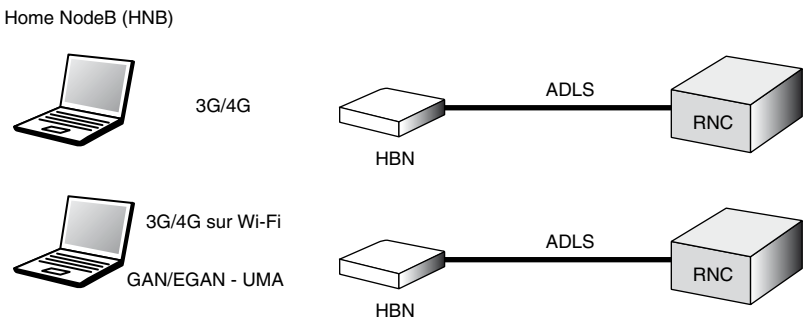


Figure 19.2
Une femtocell

Les antennes classiques sont reliées au réseau cœur par des commutateurs BSC ou RNC correspondant respectivement à la 2G et à la 3G. L'antenne femtocell est connectée sur une Femto Gateway, qui donne accès au réseau cœur. La connexion entre la Home Gateway et la Femto Gateway s'effectue par la connexion fibre optique et encore souvent par la connexion ADSL. Dans un premier temps, les terminaux connectés sont de type 3G+, et les débits sont encore assez limités par les contraintes radio.

Des questions se posent quant à l'utilité de l'antenne Wi-Fi, la possibilité d'une guerre entre Wi-Fi et 4G ou la suprématie de Wi-Fi au centre de la femtocell. Cependant, il y a peu de chances que l'antenne 4G remplace complètement l'antenne Wi-Fi. Pour cela, il faudrait que tous les équipements informatiques, imprimantes, PC, équipements multimédias, etc., soient munis d'une carte 4G. Il y a donc une forte probabilité que les deux systèmes vont coexister et que chacun prendra en charge les équipements qui lui seront le plus conformes.

Les nombreux produits femtocell qui arrivent sur le marché proposent des choix ; nous les avons illustrés à la figure 19.3. La Home Gateway prend en général le nom de HNB (Home NodeB) dès que ce boitier est disponible avec une antenne 3G ou 4G. Aujourd'hui, ces boîtiers servent essentiellement à connecter des mobiles 3G/4G permettant à l'opérateur d'offrir au client la possibilité d'utiliser son mobile 3G/4G en un endroit où il n'y a pas de signal.



UMA (Unlicensed Mobile Access), accès mobile sans licence
Nom commercial du 3GPP : Generic Access Network ou GAN standard.

Home NodeB (HNB) : Home NodeB (antenne de domicile)
RNC : RNC (Radio Network Controller), contrôleur du réseau radio
HBN : HG (Home Gateway), passerelle de domicile

Figure 19.3

Les différentes solutions de connexion sur une HNB

La HNB comporte en général deux interfaces radio : Wi-Fi et 3G/4G. Les équipements de télécommunications se branchent sur l'antenne 3G/4G et les équipements informatiques sur Wi-Fi. Le modem optique ou ADSL transporte simultanément les flots provenant des deux environnements. La deuxième solution représentée à la figure 19.3 correspond

à l'utilisation de Wi-Fi pour connecter à la fois les équipements de télécommunications et informatiques. Dans ce cas, la trame 3G/4G est encapsulée dans une trame Wi-Fi et décapsulée dans la Home Gateway. La trame 3G/4G est ensuite acheminée vers le RNC pour aller vers le réseau cœur. Cette solution s'appelle UMA (Unlicensed Mobile Access) dans le cas général, GAN (Generic Access Network) pour la 3G et EGAN (Enhanced GAN) pour la 4G.

Radio logicielle et radio cognitive

La radio cognitive a été introduite au chapitre 10. Elle représente sûrement l'une des plus importantes révolutions de ce début de siècle. Elle permet d'utiliser beaucoup mieux le spectre, qui est généralement très mal exploité. Cependant, une utilisation optimale ne pourra s'effectuer sans un certain nombre de progrès parallèles que nous allons expliciter.

La radio logicielle, ou *software radio*, ou encore SDR (Software Defined Radio), détermine un émetteur ou un récepteur radio qui est réalisé en logiciel. On voit tout de suite les implications d'une telle technologie puisque les caractéristiques de l'interface radio peuvent être modifiées à l'infini sans aucun problème technique, l'utilisateur pouvant disposer de l'interface dont il a besoin à un instant t et d'une interface complètement différente à l'instant $t + 1$. Bien évidemment, il faut un peu de matériel pour réaliser les calculs de codage, de modulation et de filtrage et pour l'émission proprement dite.

À la figure 19.4, nous avons représenté ce que l'on peut attendre de ces technologies dans les années qui viennent. Les objectifs sont réalisés en fonction de la flexibilité que peut atteindre la radio logicielle et l'intelligence provenant de la radio cognitive.

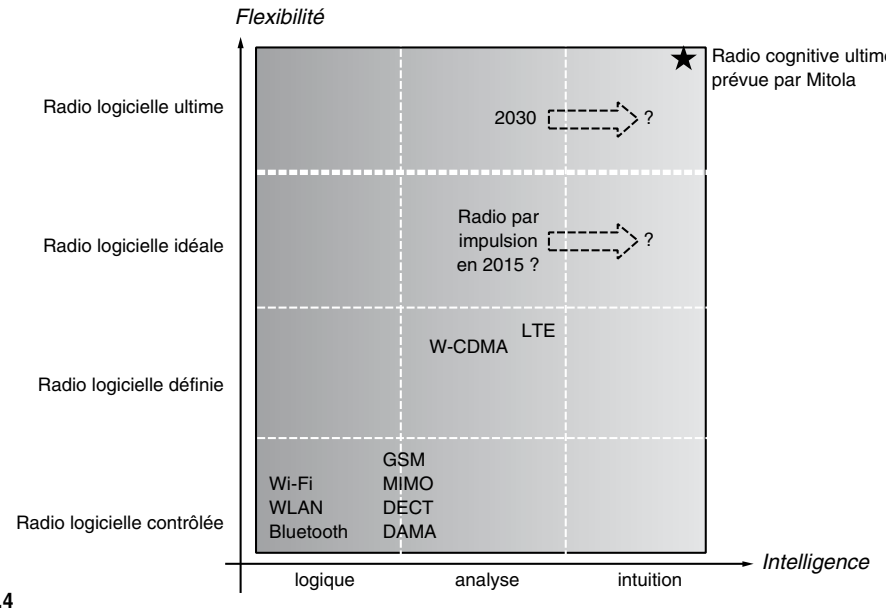


Figure 19.4

Radio logicielle et radio cognitive

Grâce à ces technologies, on devrait augmenter les débits par un facteur mille d'ici dix ans.

Les cellules sur mesure

Parmi les très nombreux axes de recherche et développement qui existent dans le domaine de la 4G, nous allons nous arrêter sur l'un d'entre eux parce qu'il paraît particulièrement prometteur. Il s'agit de construire des cellules sur mesure pour atteindre un terminal tout en diminuant les puissances au maximum. Cette solution permet une excellente réutilisation du spectre. L'idée est que la cellule dans laquelle se trouve l'utilisateur ne soit située qu'autour de lui et n'interfère pas avec un autre terminal à proximité. Cette solution est illustrée à la figure 19.5.

Au moment de l'émission du terminal, l'antenne est capable d'émettre de façon directionnelle à partir d'un grand nombre d'antennes dites virtuelles. En 2011, on peut disposer d'une antenne générale formée d'une centaine d'antennes virtuelles directives. Cette antenne récupère, comme le montre la figure 19.5, les cinq flots les plus puissants : le flot direct, deux flots avec un seul rebond et deux flots supplémentaires avec deux rebonds. Une fois cet apprentissage effectué, l'antenne principale est capable d'émettre vers le terminal en sens inverse, en reprenant exactement les flots reçus et en utilisant les antennes directives qui ont servi à recevoir le signal. La cellule est focalisée sur le client, ce qui permet une forte réutilisation des fréquences et une très faible puissance d'émission des antennes directives.

Cette solution se complique un peu lorsque le terminal utilisateur est en mouvement. Il faut dans ce cas que la détermination des antennes d'émission s'effectue en temps réel, ce qui peut conduire à des collisions.

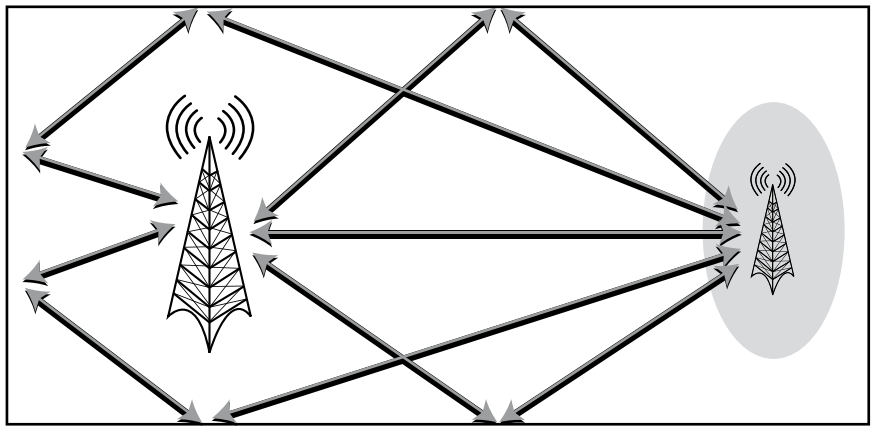


Figure 19.5
Une cellule à la demande

Conclusion

L'objectif des évolutions vers le LTE Advanced et WiMAX phase 2 est d'atteindre les très hauts débits fixés par l'UIT pour la 4G NGMN (Next Generation Mobile Network). Nous avons vu un certain nombre des éléments qui seront nécessaires pour atteindre le gigabit par seconde en crête par utilisateur.

Il faut également gérer et contrôler les handovers d'une façon précise pour atteindre ces très hauts débits. Des efforts sont également réalisés pour diminuer la consommation énergétique des antennes, qui comptent parmi les dispositifs les plus énergivores dans le monde de l'informatique et des télécommunications.

Des outils assez sophistiqués sont aujourd'hui disponibles ; nous pouvons noter ceux provenant de l'autonomique, que nous examinerons au chapitre 31, et ceux provenant de la virtualisation, que nous introduisons au chapitre 32.

20

Convergence fixe/mobile

La convergence fixe/mobile permet à toute application installée sur un serveur d'être utilisée à partir d'un équipement fixe ou mobile. La première condition pour arriver à cette convergence est qu'un mobile puisse rester connecté sur le réseau en mobilité sans que cela interrompe le déroulement de l'application. Les changements intercellulaires (handovers) doivent se dérouler de façon transparente et sans couture, c'est-à-dire en gardant la même qualité de service si l'application le nécessite.

Nous commencerons par introduire le concept de handover vertical, puis détaillerons le cas particulier de la technologie UMA (Unlicensed Mobile Access), qui permet d'utiliser un réseau X pour transporter les trames d'un réseau Y. Comme exemple classique, déjà rencontré au chapitre précédent, nous pouvons citer le transport des trames d'un terminal 3G/4G utilisant un réseau Wi-Fi. Nous introduirons ensuite la plate-forme générique proposée par le groupe IEEE 802.21, qui devient un des standards de prises en charge des handovers.

Dans la suite du chapitre, nous présenterons la plate-forme IMS (IP Multimedia Subsystem) à la base de la convergence fixe mobile. Elle a pour objectif de mettre en place une solution permettant de construire un système dans lequel toutes les machines connectées au réseau, qu'elles soient fixes ou mobiles, puissent communiquer entre elles.

Nous terminerons par le NGN (Next Generation Network), qui symbolise le réseau cœur unique de la convergence fixe mobile.

Handovers verticaux

Les handovers désignent les changements intercellulaires dans les réseaux de mobiles. Trois catégories de handovers peuvent être répertoriées : les handovers horizontaux, qui

permettent à un mobile de passer d'une cellule à une autre cellule de même type ; les handovers diagonaux, qui permettent à un mobile de passer d'une cellule à une autre cellule ayant des caractéristiques similaires, comme le passage d'un réseau Wi-*xx* à un réseau Wi-*yy*, Wi-Fi et WiMAX, par exemple ; les handovers verticaux, qui correspondent à une transition d'une cellule vers une cellule d'architecture complètement différente, comme Wi-Fi vers GSM ou UMTS.

La figure 20.1 illustre des handovers dans un réseau multitechnologie.

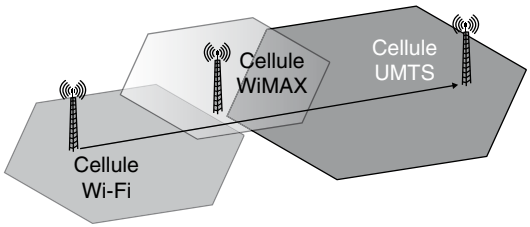


Figure 20.1

Handovers dans un réseau multitechnologie

On ne fait généralement pas de différence entre les handovers diagonaux et les handovers verticaux, qui sont tous intégrés dans les handovers verticaux.

Le changement d'antenne peut se faire de deux façons différentes : en soft-handover, c'est-à-dire en établissant des connexions simultanées avec les deux antennes, et en hard-handover, en demandant le passage instantané d'une antenne à une autre, comme dans le cas du GSM. Lors d'un handover vertical de type soft, il faut que le terminal soit capable de se connecter simultanément sur l'un et l'autre réseau, par exemple Wi-Fi et WiMAX.

La norme IEEE 802.21, Media Independent Handover, décrit une plate-forme capable de gérer les handovers dans le cadre des réseaux Wi-*xx,* par exemple le passage de WiMAX à Wi-Fi et réciproquement.

Deux solutions d'interfonctionnement sont possibles : le couplage fort (*tight coupling*) et le couplage lâche (*loose coupling*). Dans le couplage fort, promu par le 3GPP, deux éléments sont ajoutés : le WAG (Wireless Access Gateway) et le PDG (Package Data Gateway). Le couplage lâche est plutôt utilisé quand le réseau Wi-Fi n'est pas géré par un opérateur mais par un utilisateur privé.

Pour les hard-handovers, le moment choisi pour basculer d'une cellule à une autre est déterminé par un algorithme fondé sur le RSS (Relative Signal Strength) : le terminal bascule d'une cellule à l'autre lorsque la réception est plus forte dans la nouvelle cellule. Il peut aussi se fonder sur d'autres caractéristiques, comme le taux d'erreurs en ligne, le nombre de clients dans chaque cellule, le débit des clients connectés dans les deux cellules, etc. Si l'un des deux points d'accès est à la charge d'un opérateur, il faut aussi tenir compte du coût de connexion, du SLA de chaque client, etc.

UMA (Unlicensed Mobile Access)

UMA est un standard de fait qui provient en partie de la solution IEEE 802.21, que nous décrivons à la section suivante.

UMA a été développé pour les handovers entre GSM, UMTS, Bluetooth et Wi-Fi. Depuis 2005, l'UMA fait partie de la standardisation de l'ETSI 3GPP effectuée par le groupe de travail GAN (Generic Access Network). L'objectif est de permettre à un terminal voix-données-images connecté sur une antenne Wi-Fi de passer à une antenne GSM sans couture, c'est-à-dire sans interruption de la communication et *vice versa*. Les réseaux Bluetooth et UMTS sont également concernés.

Lorsqu'un terminal se trouve dans une cellule de type GSM ou UMTS, il communique avec une station de base, et la communication s'écoule vers le réseau cœur (Core Mobile Network) en transitant par un contrôleur de station de base. Quand le terminal détecte un réseau Wi-Fi, il établit une connexion IP sécurisée avec une passerelle appelée GAN Controller (GANC) se trouvant dans le réseau de l'opérateur. Le GANC translate le signal provenant du terminal en une communication dont le format est identique à celui qui proviendrait d'un contrôleur de station de base. Lorsque le terminal passe d'une connexion GSM à une connexion Wi-Fi, il est toujours vu comme étant connecté sur un contrôleur de station de base.

L'architecture UMA est illustrée à la figure 20.2.

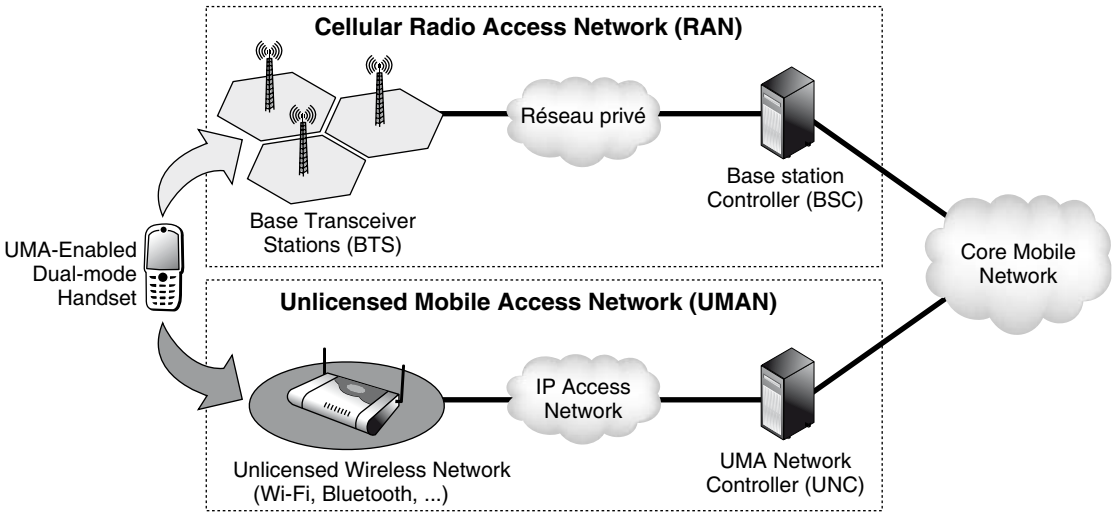


Figure 20.2

L'architecture UMA

Le terminal UMA possède quatre modes opératoires :

- GERAN-only, qui ne permet que le fonctionnement du réseau de mobiles.
- GERAN-preferred, qui utilise de préférence le réseau de mobiles et à défaut le réseau Wi-Fi.
- GAN-preferred, qui utilise de préférence le mode Wi-Fi au mode GSM.
- GAN-only, qui utilise uniquement la connexion Wi-Fi.

L'interface GSM est toujours utilisée pour au moins déterminer la localisation géographique de l'utilisateur et déterminer le serveur GANC à utiliser pour les points d'accès à raccorder.

L'avantage de cette solution pour les opérateurs est de pouvoir déployer des réseaux Wi-Fi bon marché, surtout dans les hotspots. De plus, les communications Internet des utilisateurs s'écoulent beaucoup mieux par Wi-Fi que par les techniques des réseaux de mobiles. De nombreux produits, en France surtout, utilisent cette technologie UMA pour compléter les Home Gateway.

Pour le client, l'UMA présente également de grands atouts économiques puisque l'accès par le biais de Wi-Fi est beaucoup moins onéreux que par les techniques de mobilité. Un seul numéro de téléphone peut être associé à l'équipement qui peut-être atteint aussi bien par GSM que par Wi-Fi.

Les désavantages de cette solution proviennent de la relative complexité de mise en place du système global et du poids des téléphones, qui sont légèrement plus lourds afin de pouvoir accueillir les deux systèmes simultanément.

Ce système fonctionne en fait comme une émulation de Wi-Fi en technique GSM. De ce fait, les applications gratuites deviennent payantes, à l'image de la téléphonie Skype, qui doit passer par un circuit.

IEEE 802.21

La normalisation effectuée au sein du groupe de travail IEEE 802.21 est une des plus importantes du groupe 802. Ce standard permet d'interconnecter entre eux les différents réseaux de la gamme Wi-*xx* afin de mettre en œuvre un réseau Internet sans fil de bout en bout.

La figure 20.3 illustre la réalisation de handovers verticaux à partir de trois réseaux de la famille Wi-*xx*. Les points d'accès sont connectés sur des contrôleurs multitechnologie, c'est-à-dire capables de gérer des points d'accès hétérogènes. Lorsqu'un client passe d'un réseau à un autre, il effectue un handover vertical. S'il part de la gauche de la figure pour aller vers la droite, il commence par faire un handover intracontrôleur géré par un seul et même contrôleur. Lors du second changement de cellule, le handover est intercontrôleur, les points d'accès des cellules ne se connectant pas sur le même contrôleur.

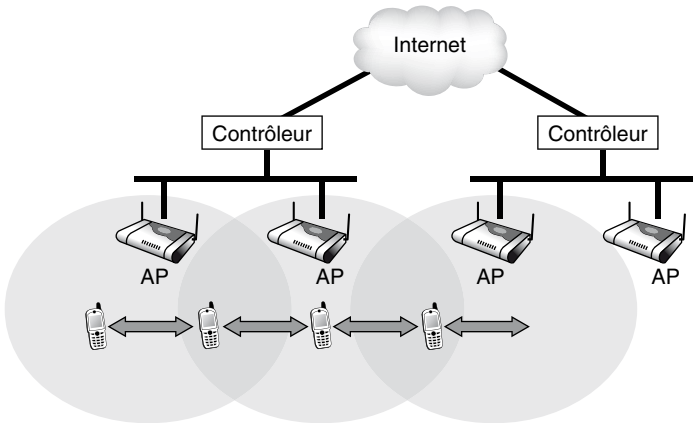


Figure 20.3

Handovers verticaux avec IEEE 802.21

Pour réaliser ces handovers verticaux, il faut que les stations mobiles aient au moins deux interfaces radio différentes susceptibles de marcher en parallèle. Ce cas est illustré à la figure 20.4.

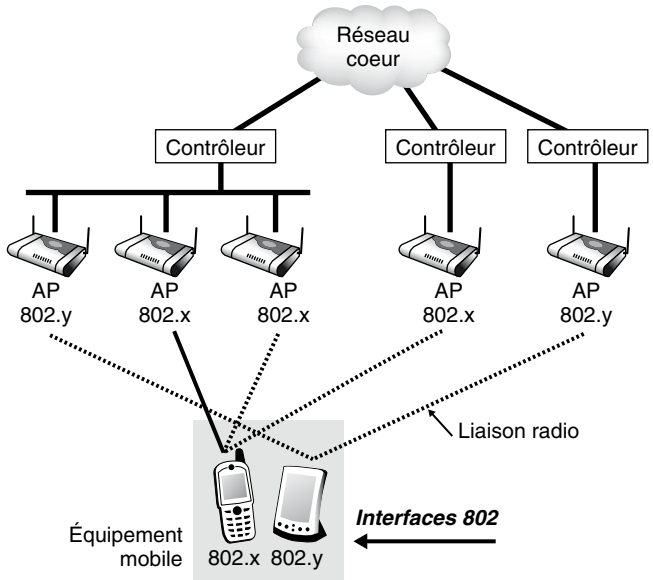


Figure 20.4

Interfaces parallèles dans un équipement mobile

L'objectif de la norme IEEE 802.21 (Media Independent Handover) est de développer des spécifications permettant de récupérer des informations de la couche trame et de la couche réseau pour les transmettre à une couche supérieure afin d'optimiser les handovers entre réseaux multitechnologie. Cette norme reprend à son compte des propositions effectuées dans différents organismes de normalisation, comme le 3GPP et le 3GPP2. Elle vise à permettre le passage intercellulaire entre les différents membres de la famille des réseaux IEEE 802, qu'ils soient sans fil ou filaires.

La norme prend donc en compte les handovers pour les utilisateurs aussi bien mobiles que fixes. Pour les utilisateurs mobiles, les handovers se produisent lors du passage d'une cellule de réseau sans fil à une autre.

Les handovers peuvent aussi se produire en raison d'un espacement de la couverture radio du fait du mouvement du terminal. Pour l'utilisateur stationnaire, les handovers peuvent devenir intéressants lorsque l'environnement alentour se modifie et qu'un nouveau réseau devient plus attractif. Par exemple, un utilisateur peut effectuer un handover pour se connecter sur un réseau à plus haut débit afin de réaliser un transfert de fichiers dans de meilleures conditions.

Les handovers doivent permettre la continuité de service, c'est-à-dire donner les moyens à l'application de rester cohérente par rapport à ses besoins. Par exemple, pour une conversation téléphonique, les utilisateurs ne doivent pas s'apercevoir d'un changement intercellulaire. Pour un transfert de fichiers, l'interruption est possible, mais le transfert doit reprendre là où il a été interrompu lors du changement de cellule.

Le standard IEEE 802.21 permet la coopération entre le mobile et l'infrastructure fixe du réseau pour réaliser les handovers. Le mobile prend en charge la détection des réseaux disponibles, tandis que l'infrastructure physique s'occupe de stocker les informations en provenance du réseau, comme la liste des cellules de voisinage et l'emplacement des mobiles.

Les terminaux et les points d'accès utilisent le mode multitechnologie afin de se connecter à plusieurs technologies radio et de transmettre sur plusieurs interfaces simultanément. Par exemple, le réseau multitechnologie peut avoir des cellules de petite dimension, de type personnel comme Wi-Fi, ou des réseaux personnels de type Bluetooth et de grandes cellules que l'on rencontre dans les techniques issues du 3GPP, du 3GPP2 ou d'IEEE 802.16.

Le processus de handover est typiquement déclenché par des mesures visant la meilleure attractivité d'un réseau. Ces mesures testent la qualité du signal, le taux d'erreurs de transmission, etc. Ils sont intégrés à la métrique utilisée dans les algorithmes de handover.

L'architecture IEEE 802.21

La norme couvre les trois grands domaines suivants :

- Une architecture permettant la continuité transparente du service pendant qu'un mobile change de cellule. Cette architecture s'appuie sur une pile protocolaire permettant de gérer la mobilité au cours du handover. La description architecturale n'adresse pas les détails d'exécution et ne fournit aucune indication sur la réalisation de l'algorithmique nécessaire. Elle décrit uniquement un modèle de référence du MIH (Media Independent Handover) pour différentes catégories de réseaux sans fil et mobiles.

- L'ajout d'un ensemble de fonctionnalités adaptées aux handovers dans les piles de protocoles de gestion de la mobilité et la création d'une nouvelle entité, appelée fonction MIH. Sont définis un ensemble de points d'accès indépendants du service et des primitives associées qui permettent d'accéder aux services de la fonction MIH. La fonction MIH fournit les services suivants :
  - Service MIS (Media Independent Service), qui fournit les informations des interfaces locales ou distances.
  - Service MIC (Media Independent Command), qui fournit l'ensemble des commandes permettant aux utilisateurs MIH d'initialiser des commandes sur les éléments logiciels et matériels concernant les handovers.
  - Service MII (Media Independent Information), qui fournit le modèle d'information et de gestion de cette information pour que la prise de décision de déclenchement des handovers soit la meilleure possible. Le terminal mobile peut accéder à ces informations par le biais de son point d'accès de rattachement.
- La définition de primitives additionnelles dans la couche MAC correspondant aux différentes technologies de réseaux sans fil. Ces primitives permettent de récupérer et d'utiliser les informations de niveau MAC pendant le handover. Le groupe 802.21 encourage les différentes associations de normalisation à reprendre ces éléments dans leurs normes.

La figure 20.5 illustre l'emplacement de la fonction MIH dans la pile protocolaire associée aux handovers et à la gestion de la mobilité.

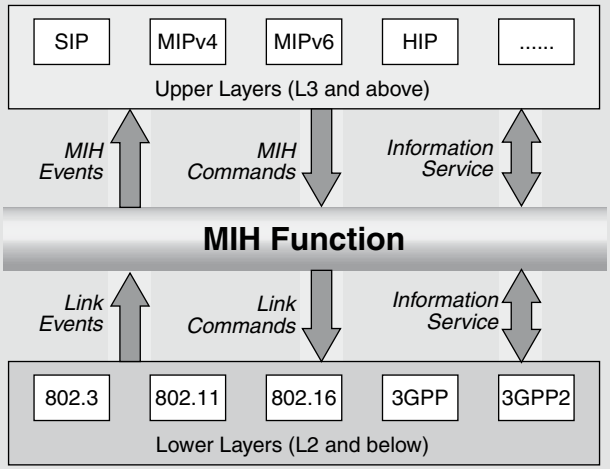


Figure 20.5

Emplacement de la fonction MIH dans la pile protocolaire IEEE 802.21

La fonction MIH fournit des services aux couches supérieures grâce à une interface simple (SAP), indépendante de la technologie sous-jacente, et obtient des services des couches inférieures par tout un ensemble d'interfaces dépendantes des réseaux sous-jacents.

Les hypothèses suivantes ont été faites pour le développement de cette norme :

- Le nœud mobile est capable de gérer des interfaces multiples, qui peuvent être avec ou sans fil.
- La fonction MIH est une entité logique, dont la définition n'a aucune implication sur la façon de la mettre en œuvre dans le nœud mobile ou dans l'infrastructure du réseau.
- La fonction MIH sur le terminal mobile reçoit sans interruption des informations sur les caractéristiques des réseaux d'accès. Ces informations proviennent des couches basses de la pile protocolaire, effectuant la gestion de la mobilité, du terminal mobile ainsi que des éléments de réseau.

L'intention des normalisateurs est de fournir des spécifications génériques des couches trame et réseau afin qu'elles ne soient pas dépendantes des caractéristiques des terminaux, des points d'accès ou des réseaux radio. En tant que telles, les spécifications IEEE 802.21 doivent s'appliquer aux familles de réseaux radio provenant du 3GPP, du 3GPP2 et de la famille IEEE 802.

L'interopérabilité et la conformité sont définies de la façon suivante :

- L'implémentation doit permettre aux services d'accéder aux primitives provenant des utilisateurs et de les recevoir. La spécification ne décrit toutefois pas cette implémentation, laissant une certaine liberté de mise en œuvre aux fabricants. Seuls les formats et la sémantique des paramètres de service doivent suivre les recommandations décrites dans le standard.
- Les protocoles indiqués dans le standard 802.21, ainsi que les échanges de messages et la machine d'état doivent être conformes au texte de la norme. Plusieurs classes d'interopérabilité et de conformité dans l'implémentation sont également définies pour un ensemble de caractéristiques obligatoires ou facultatives.

En conclusion, le standard IEEE 802.21 est d'une grande importance dans la construction du futur Internet hertzien puisqu'il permettra le passage sans couture d'un réseau Wi-*xx* à un réseau Wi-*yy*.

IMS (IP Multimedia Subsystem)

L'IMS (IP Multimedia Subsystem) est conçu pour fournir aux utilisateurs la possibilité d'établir des sessions multimédias dans un environnement de convergence fixe/mobile. En particulier, la session doit pouvoir être ouverte entre n'importe quel serveur et n'importe quel terminal, qu'ils soient connectés en mobile ou en fixe. À cet effet, le protocole SIP (Session Initiation Protocol), qui a été introduit dans les réseaux IP pour mettre en place les sessions téléphoniques, a été choisi pour sa grande généralité d'ouverture et de fermeture de session.

Le réseau cœur est un réseau à transfert de paquets IP. Les accès sont aussi de type IP ou IP-CAN (IP-Connectivity Access Network). Le rôle de l'IP-CAN est d'interconnecter les terminaux mobiles au réseau cœur.

L'IMS est parfois appelé IP Multimedia Core Network Subsystem. Les entités composant son architecture peuvent être classées en trois catégories : éléments de contrôle de sessions, ou CSCF (Call Session Control Function), éléments assurant l'interfonctionnement avec le domaine circuit (BGCF, MGCF, IM-MGW, SGW), serveurs d'application et ressources média (AS, MRFC, MRFP).

Les entités fonctionnelles de l'architecture de l'IMS sont illustrées à la figure 20.6.

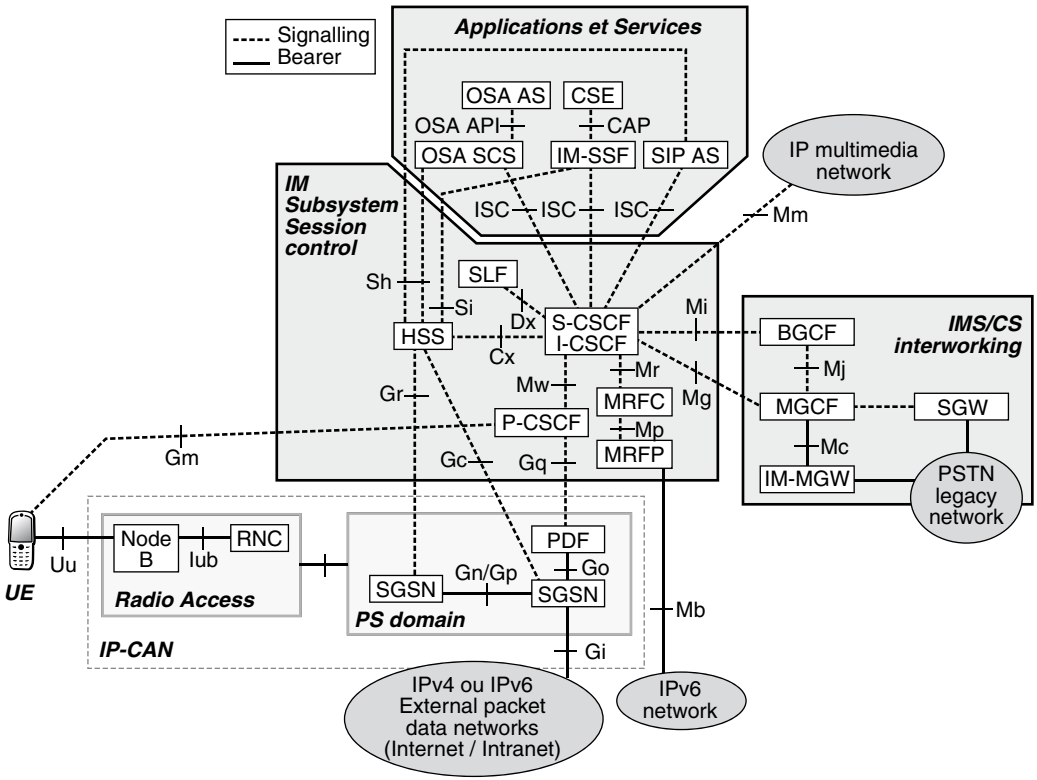


Figure 20.6

Entités fonctionnelles de l'architecture générale de l'IMS

Les entités fonctionnelles de contrôle de sessions sont des évolutions des SIP-Proxy appelés CSCF (Call Session Control Function).

On distingue trois types de CSCF constituant la couche de contrôle de session :

- Proxy-CSCF (P-CSCF). C'est le premier point de contact de l'IMS pour les utilisateurs. Le P-CSCF achemine les messages SIP (messages d'enregistrement register vers l'I-CSCF et autres messages, par exemple invite pour l'établissement de session, vers l'UE et l'I/S-CSCF). Le P-CSCF assure l'intégrité de la signalisation SIP en maintenant une association de sécurité avec l'utilisateur et contrôle l'exécution des politiques de médias en examinant le contenu SDP des messages SIP. Le P-CSCF est en charge de la compression et de la décompression des messages SIP afin de réduire la signalisation sur la voie radio (interface Uu). Enfin, il génère les CDR (Call Data Records), nécessaires à la taxation. Ces CDR sont collectés par le GCF (Gateway Charging Function).
- Interrogating-CSCF (I-CSCF). C'est le point de contact pour toutes les connexions destinées à un utilisateur dans le réseau, en particulier les connexions externes. Pendant

la phase d'enregistrement, l'I-CSCF interroge le HSS afin de déterminer le S-CSCF associé à l'utilisateur. C'est le point d'entrée dans le réseau pour toute la signalisation SIP. Il peut également assurer la fonction de THIG (Topology Hiding Inter-network Gateway) en cachant la configuration et la topologie du réseau par rapport aux réseaux externes ; il intercepte dans ce cas tous les messages SIP entre le P-CSCF et le S-CSCF. Enfin, il génère des CDR.

- Serving-CSCF (S-CSCF). C'est l'entité fonctionnelle responsable de l'enregistrement des utilisateurs (rôle de Registrar au sens de l'IETF) et du contrôle des sessions pour assurer le support des services. Le S-CSCF assure l'authentification et l'autorisation des utilisateurs. Il exécute également les politiques de médias en examinant le contenu SDP des messages SIP et assure l'acheminement des messages SIP entre les différentes entités I-CSCF, S-CSCF, P-CSCF et BGCF. Il assure enfin le déclenchement des services en vérifiant si les critères de filtrage (iFC) reçus du HSS sont remplis ; dans ce cas, il achemine les messages SIP vers un serveur d'applications. Enfin, il génère des CDR.

L'interface ISC (IMS Service Control) se situe entre les S-CSCF et les plates-formes de service. Elle permet l'accès aux services situés dans les serveurs d'applications, ou AS (Application Server). Un AS peut être localisé dans le HPLMN ou dans un réseau tiers. L'interface de contrôle des services (interface ISC) est fondée sur SIP.

Dans l'architecture de service de l'IMS, trois types d'AS hébergent les logiques de service et constituent la couche d'exécution de service : les serveurs d'applications SIP et les serveurs CAMEL et Open Service Access.

Les serveurs d'applications SIP contiennent la logique de service pour les applications SIP. Il s'agit du principal type de serveur d'applications de l'IMS. Notons que les services peuvent, par exemple, être composés de Service Capabilities, comme Presence, Multimedia Messaging et Conferencing.

OSA (Open Service Access) permet l'utilisation de fonctionnalités du système UMTS par des applications tierces *via* une interface ouverte, OSA Application Programming Interface. L'OSA Gateway est l'entité connectée *via* l'interface ISC vers le S-CSCF et supportant l'OSA API vers les applications tierces.

Les applications CAMEL peuvent être accédées *via* l'IM-SSF (IP Multimedia Service Switching Function) spécifiée dans le standard. L'intérêt de cette entité est principalement de permettre la réutilisation par l'IMS des services de réseau intelligent déployés dans les réseaux GSM/UMTS, par exemple le prépaiement. L'IM-SSF est un convertisseur de protocoles SIP-CAP (CAMEL Application Part). Il est toutefois peu probable que cette entité soit largement déployée, la réutilisation des composants de services de réseau intelligent ou le développement d'interfaces SIP sur les serveurs CAMEL étant préférés à cette solution.

Les applications peuvent aussi résider dans les SIP-Proxy ; beaucoup de prototypes existants à ce jour sont limités à ce modèle.

Le MRF (Media Resource Fonction) est l'entité fonctionnelle en charge de la modification des flux médias. Cette entité est utilisée pour le mixage des flux RTP (pont de conférence), pour la génération d'annonces (voix/vidéo), et pour le transcodage. Le MRF est

constitué de deux entités fonctionnelles : le MRFC (Media Resource Function Controller), qui interprète les messages SIP issus des serveurs d'applications, et le MRFP (Media Resource Function Processor), qui est responsable du traitement des flux multimédias. Le MRFP est commandé par le MRFC par le biais du protocole H.248.

Le HSS (Home Subscriber Server) est la base de données maître UMTS ou sont stockées les données des utilisateurs. Le HSS inclut le HLR (Home Location Register) et l'AuC (Authentication Centre). Cette entité stocke les identités des utilisateurs, leurs informations d'enregistrement, leurs paramètres d'accès et leurs informations de déclenchement de services. Lorsqu'un même réseau dispose de plusieurs HSS, ce qui est presque toujours le cas, le SLF (Subscription Locator Function) est utilisé pour localiser le HSS associé à un utilisateur donné. Notons que le HSS et le SLF ne font pas partie de l'IMS.

Accès multiple à l'IMS

Dans l'évolution du monde circuit vers le monde paquet (*voir les chapitres 1 et 2*), un certain nombre de verrous restent à lever pour permettre un déploiement massif de l'architecture NGN (Next Generation Network), principalement l'intégration des nombreuses technologies de réseaux d'accès d'aujourd'hui et de demain et l'intégration dans les équipements terminaux des logiciels d'accès. De même, la transition des réseaux hétérogènes que l'on utilise aujourd'hui vers le NGN est un obstacle à franchir.

La première évolution nécessaire est l'ouverture de l'IMS à de nouveaux réseaux d'accès, ou l'accès multiple. En effet, la réduction des coûts d'investissement et d'exploitation passe par la mutualisation de certains équipements du cœur de réseau, notamment les Proxy SIP.

L'accès à l'IMS à partir de plusieurs types de réseaux d'accès permettra d'offrir des services convergents et des offres fixe/mobile. L'accès au service quel que soit le réseau d'accès est un principe fondateur du NGN. C'est aussi un des principes des architectures B3G (Beyond 3G) ou super-3G ou encore LTE (Long Term Evolution). Pour que l'IMS soit un des piliers de l'architecture B3G et LTE, cette évolution est essentielle.

Plusieurs types de réseaux d'accès alternatifs à l'interface UMTS, Wi-*xx*, *x*DSL et câble doivent être envisagés. Dans la Release 5 de l'UMTS, l'IMS a été défini uniquement pour un accès au travers de l'interface UMTS. Un des apports essentiels de la Release 6 est de fournir des services de façon indépendante de l'accès en prenant en compte un réseau d'accès de type Wi-Fi. Le projet initial était de disposer d'un seul standard IMS commun au 3GPP et au 3GPP2, qui n'utilisent pas le même réseau de connectivité IP. Ce projet initial a ensuite été étendu aux réseaux Wi-*xx*.

Une des idées fortes développée pour l'IMS est l'accès multiple. Il s'agit, d'une part, d'élargir les types de réseaux d'accès pouvant offrir des services SIP en prenant en compte des accès fixes (*x*DSL et câble), et, d'autre part, de proposer des solutions permettant un interfonctionnement des réseaux Wi-*xx* au-delà des mécanismes existants. Il a fallu pour cela étudier les aspects architecturaux et de services liés à un accès à un cœur IMS mutualisé à partir de différentes technologies d'accès et identifier les entités et les mécanismes IMS susceptibles d'être mutualisés. Une réduction des disparités architecturales en jeu est un point clé dans l'élaboration d'offres convergentes et de nomadisme. Elle permettra en outre de bâtir une offre constructeur plus uniforme.

La possibilité de réutiliser les mêmes entités fonctionnelles pouvant supporter des services 3GPP IMS et les services multimédias du NGN est un enjeu essentiel pour l'avenir des télécommunications. L'approche proposée, consistant en la définition d'un IMS indépendant de l'accès, est maintenant soutenue par un grand nombre d'acteurs, parmi lesquels les principaux constructeurs et opérateurs. Ainsi, un opérateur IMS pourra proposer des services convergents, quel que soit le type d'accès disponible, fixe ou mobile.

La figure 20.7 illustre le principe de fonctionnement de l'accès multiple à l'IMS.

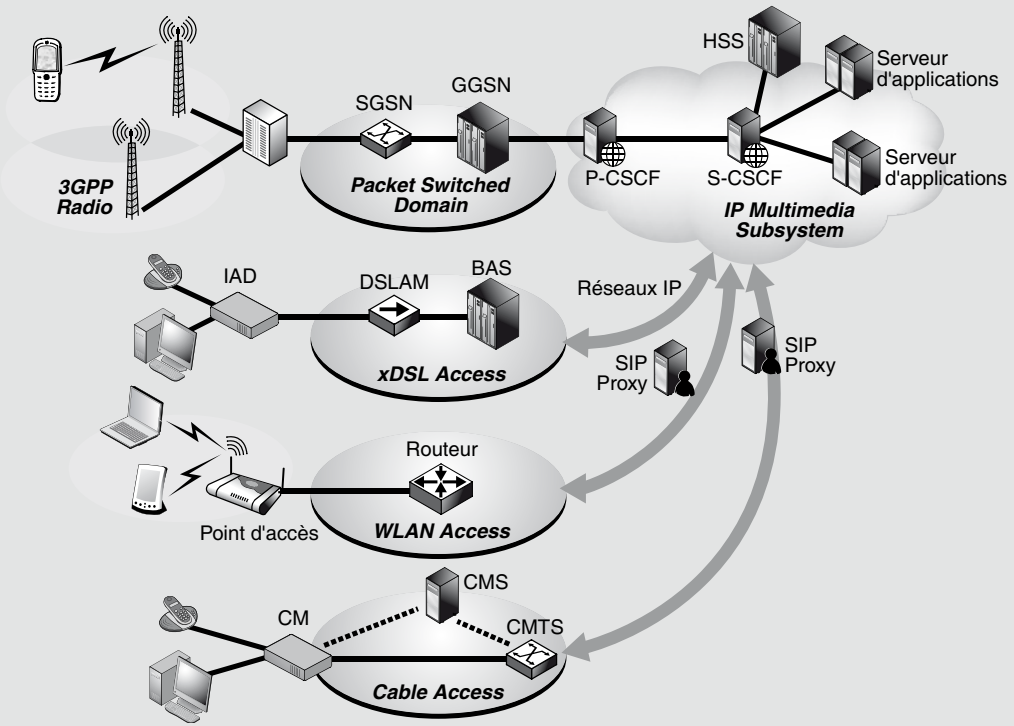


Figure 20.7
Accès multiple à l'IMS

Les bénéfices de l'accès multiple pour un opérateur sont les suivants :

- réduction des coûts d'investissement (CAPEX) et d'opération (OPEX) ;
- backbone IP unique pour plusieurs réseaux d'accès ;
- mutualisation des équipements de contrôle de session pour les réseaux fixes et mobiles ;
- gestion commune des utilisateurs fixes et mobiles et de leurs profils ;
- possibilité pour un opérateur de bénéficier de l'ensemble des revenus provenant du fixe, du mobile, de la voix et d'Internet.

Pour sa part, l'utilisateur tirera de ces évolutions les principaux bénéfices suivants :

- interactions de service résolues dans le cadre de l'accès multiple ;
- services convergents, par exemple offre du service de présence unifiée, de messaging ou de localisation ;
- facturation unique ;
- numéro de téléphone ou identifiant public SIP (SIP URI) unique ;
- à plus long terme, nomadisme et continuité de session interdomaine.

NGN (Next Generation Network)

Le NGN marque la convergence fixe/mobile pour un réseau cœur unique sur lequel se rattachent aussi bien les terminaux fixes que mobiles. Ces terminaux peuvent être raccordés par une technologie quelconque sur le cœur de réseau. Comme la définition même du NGN est assez imprécise, on utilise ce terme pour marquer la convergence vers un réseau unique en mode paquets capable de transporter tous les services. Des organes de normalisation ont des groupes de travail spécialisés sur ce domaine, en particulier l'UIT-T et l'ETSI (qui a également le groupe TISPAN sur des objectifs identiques, que nous verrons dans la section suivante).

On définit parfois le NGN comme le réseau apportant la propriété d'être toujours connecté sur le réseau (Always-on Network) et d'apporter la propriété du village global (Global Village) dans laquelle tous les êtres humain peuvent se considérer appartenir à un même village.

Les propriétés du NGN acceptées par les instances de normalisation contiennent l'utilisation d'un chemin et donc d'un mode commuté. Ce mode commuté est aujourd'hui MPLS Ethernet Forwarding, c'est-à-dire la commutation de trames Ethernet sur un réseau MPLS. Le NGN doit être capable de mettre en relations deux « choses » entre elles, une chose pouvant être n'importe quoi connectable sur le réseau : un RFID, un terminal mobile, un objet intelligent, un serveur, etc. On parle dans ce cas de réseau T2T (Thing to Thing).

Un problème lié aux applications T2T est l'adressage : le NGN doit être capable de gérer 100 milliards d'adresses. Pour y arriver simplement l'utilisation intensive d'adresses IP privées en IPv4 est une première solution. IPv6 est une seconde solution plus élégante mais qui demande le passage d'IPv4 vers IPv6, ce que l'occident refuse pour le moment. Une autre solution pointe son nez à l'horizon, le Post-IP, qui correspond à la génération postérieure à IP et dont l'un des buts est de passer facilement à l'échelle (scalabilité) et d'être beaucoup plus sécurisé.

Le projet TISPAN

TISPAN, fusions de TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) et de SPAN (Services and Protocols for Advanced Networks), est à un groupe de l'ETSI visant à définir une infrastructure mutualisable pour le contrôle des sessions voix, vidéo ou multimédia entre de multiples réseaux d'accès, *x*DSL en particulier.

L'architecture définie par TISPAN repose sur l'utilisation de l'IMS pour la partie contrôle de session et service. Le projet TISPAN est constitué de sept comités techniques (Services, Architecture, Protocoles, Numbering addressing and routing, Testing, Security et Network Management).

TISPAN souhaite standardiser les réseaux pour la fourniture de services NGN en prenant en charge les réseaux classiques à commutation de circuit et en mettant en œuvre la téléphonie sur IP. Plusieurs aspects sont abordés dans différents groupes de travail, tels que services, architecture, protocoles, numérotation, sécurité, qualité de service, administration, correspondant aux comités techniques précédents.

TISPAN définit une architecture dont les premiers déploiements ont été effectués en 2008. Cette architecture est illustrée à la figure 20.8.

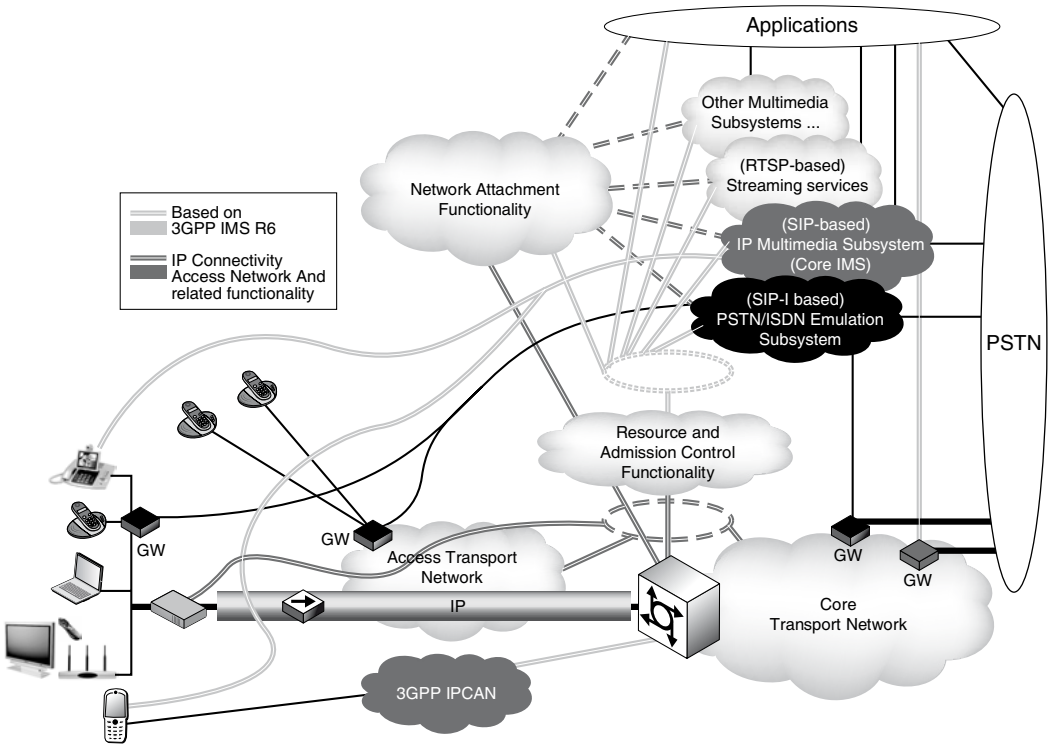


Figure 20.8
L'architecture TISPAN

Conclusion

Ce chapitre a introduit les éléments de converge des architectures réseau permettant d'interconnecter des réseaux radio hétérogènes, à commencer par ceux de la convergence fixe/mobile, afin de n'en former qu'un seul.

L'objectif de cette convergence est de pouvoir utiliser une application quelconque située sur un serveur connecté au réseau cœur depuis un équipement terminal, qu'il soit fixe ou mobile. Cette convergence devrait permettre aux opérateurs d'effectuer des économies importantes en ne dupliquant pas les applications orientées réseau fixe et réseau mobile.

Partie VI

Les réseaux sans fil

21

Les réseaux personnels

Les réseaux personnels connectent les équipements qui se trouvent dans les poches et les cartables pour les relier entre eux avec des débits suffisants afin d'y faire transiter voix, données et vidéo.

La portée de ces réseaux est faible, de l'ordre de quelques mètres. Bluetooth a longtemps été la seule implémentation de tels réseaux, mais elle est aujourd'hui concurrencée par de nombreuses propositions et produits provenant de normes édictées par le groupe de travail IEEE 802.15, par les industriels eux-mêmes avec la nouvelle génération Wi-Fi:pour réseaux personnels (WiGig) et par le groupe IEEE 802.11, qui normalise Wi-Fi et qui commence à s'intéresser aux réseaux personnels.

Les WPAN

Le groupe IEEE 802.15 a été mis en place en mars 1999 dans le but de réfléchir aux réseaux hertziens d'une portée d'une dizaine de mètres, ou WPAN (Wireless Personal Area Network), avec pour objectif de réaliser des connexions entre les différents portables d'un même utilisateur ou de plusieurs utilisateurs. Ce type de réseau peut interconnecter un PC portable, un téléphone portable, un PDA ou tout autre terminal de ce type. Trois groupes de services ont été définis, A, B et C.

Le groupe A utilise la bande du spectre sans licence d'utilisation (2,4 GHz) en visant un faible coût de mise en place et d'utilisation. La taille de la cellule autour du point d'émission est de l'ordre du mètre. La consommation électrique doit être particulièrement faible pour permettre au terminal de tenir plusieurs mois sans recharge électrique. Le mode de transmission choisi est sans connexion. Le réseau doit pouvoir travailler en parallèle d'un réseau IEEE 802.11. Sur un même emplacement physique, il peut donc y avoir en même

temps un réseau de chaque type, les deux pouvant fonctionner éventuellement de façon dégradée.

Le groupe B affiche des performances en augmentation, avec un niveau MAC pouvant atteindre un débit d'au moins 100 Mbit/s. Le réseau de base doit pouvoir interconnecter seize machines ou plus et proposer un algorithme de QoS, ou qualité de service, pour autoriser le fonctionnement de certaines applications, comme la parole téléphonique, qui demande une qualité de service très stricte. La portée entre l'émetteur et le récepteur atteint une dizaine de mètres, et le temps maximal pour se raccorder au réseau ne doit pas dépasser la seconde. Enfin, cette catégorie de réseau doit posséder des passerelles avec les autres catégories de réseaux 802.15.

Le groupe C introduit de nouvelles fonctionnalités importantes pour particuliers ou entreprises, comme la sécurité de la communication, la transmission de la vidéo et la possibilité de roaming, ou itinérance, entre réseaux hertziens.

Pour répondre à ces objectifs, des groupements industriels se sont mis en place, comme Bluetooth, la WiMedia Alliance ou WiGig. Bluetooth regroupe plus de huit cents sociétés qui ont réalisé une spécification ouverte de connexion sans fil entre équipements personnels. Bluetooth est fondé sur une liaison radio entre deux équipements, tandis que la WiMedia Alliance s'intéresse aux connexions à très haut débit sur une courte portée. En fait, le standard risque d'être tout autre avec l'arrivée des réseaux de type Wi-Fi dans le cadre des réseaux personnels.

IEEE 802.15

Le groupe de travail IEEE 802.15 a commencé par se scindé en quatre sous-groupes :

- IEEE 802.15.1, pour les réseaux de catégorie C ;
- IEEE 802.15.3 pour les réseaux de catégorie B ;
- IEEE 802.15.4 pour les réseaux de catégorie A ;
- IEEE 802.15.2 pour s'occuper des problèmes d'interférences avec les autres réseaux utilisant la bande des 2,4 GHz.

Il s'est ensuite fortement agrandi, avec l'arrivée de nombreux groupes ou sous-groupes de travail, notamment les suivants :

- TG3c (Task Group 3c), qui propose un réseau personnel dans les gammes de 57 à 64 GHz, ce qui permettrait d'atteindre des vitesses de transmission de plusieurs gigabits par seconde.
- TG5, qui définit les réseaux mesh, susceptibles de couvrir une surface géographique plus importante qu'un réseau personnel (*voir le chapitre 23*).
- TG6, qui s'occupe du BAN (Body Area Network), un réseau que les personnes pourront porter sur eux pour des raisons médicale, expérimentale, sportive, etc. Les directions prises par ce groupe technique pointent vers une consommation électrique faible et des fréquences basses, avec une portée de 2 à 3 m. Des propriétés de haute

sécurité sont bien sûr indispensables dans ces réseaux BAN. Plusieurs propositions sont actuellement à l'étude : UWB, Wi-Fi spécifique, Bluetooth, etc.

- TG7, qui œuvre pour les réseaux de domicile avec une technologie VLC (Visible Light Communications). Ce réseau utilise les équipements avec des LED et des photodiodes, qui peuvent se trouver dans tous les équipements lumineux, comme les néons, les feux rouges de la circulation, les panneaux lumineux, etc. La transmission s'effectue entre 400 et 800 THhz et peut apporter des débits de plusieurs centaines de mégabits par seconde étant donné la bande passante disponible. Il est possible d'avoir des extensions à plus longue portée, d'un kilomètre, par exemple, mais avec des débits beaucoup plus faibles (quelques centaines de kilobits par seconde).

Le choix du groupe IEEE 802.15.1 s'est tourné vers Bluetooth, présenté en détail à la section suivante. En fait, c'est l'IEEE qui avait repris la normalisation réalisée au Bluetooth Special Interest Group (Bluetooth SIG). Après plusieurs années d'effort, l'IEEE annonça en 2005 l'abandon de la technologie Bluetooth au profit de la technique UWB. Du coup, c'est le Bluetooth SIG qui reprit les travaux de normalisation que nous allons détailler à la section suivante.

Le groupe IEEE 802.15.3 est orienté vers le haut débit et l'UWB (Ultra Wide Band). Cette interface radio a été récupérée par la WiMedia Alliance et par le groupe SIG (Bluetooth Special Interest Group). Après moultes tractations, problèmes techniques et discussions sur les brevets, le Bluetooth SIG a abandonné la solution UWB, comme nous allons le voir.

Le groupe IEEE 802.15.4 définit un réseau à faible portée, de l'ordre de quelques mètres, pour interconnecter tous les capteurs et actionneurs que l'on peut trouver, dans les jouets, les équipements domestiques, les commandes radio, etc. Ce standard, appelé ZigBee, commence à avoir un franc succès et nous allons l'examiner en détail un peu plus loin.

Bluetooth

Le Bluetooth SIG (Special Interest Group), constitué au départ par Ericsson, IBM, Intel, Nokia et Toshiba et rejoint par plus de deux mille cinq cents sociétés, définit les spécifications de Bluetooth.

C'est une technologie peu onéreuse, grâce à sa forte intégration sur une puce unique de 9 mm sur 9 mm. Les fréquences utilisées sont comprises entre 2 400 et 2 483,5 MHz. On retrouve la même gamme de fréquences dans la plupart des réseaux sans fil utilisés dans un environnement privé, que ce dernier soit personnel ou d'entreprise. Cette bande ne demande pas de licence d'exploitation.

On a longtemps pensé que les techniques UWB pourraient succéder à Bluetooth ou être intégrées dans Bluetooth : c'était le point de vue de l'IEEE 802.15.1. Cependant, la consommation électrique de cette solution s'est révélée assez prohibitive. C'est la raison pour laquelle Wi-Fi semble avoir la capacité de prendre une place de choix dans les réseaux personnels à haut débit, que ce soit par des extensions de Bluetooth ou de réseaux purement Wi-Fi.

La succession des standards du Bluetooth SIG est la suivante.

- Bluetooth 1.0 : cette version de base de Bluetooth avait de nombreux défauts, notamment le fait que les produits commercialisés pouvaient être incompatibles.
- Bluetooth 1.1 : première vraie norme à avoir été ratifiée par l'IEEE 802.15.1 en 2002.
- Bluetooth 1.2 : apporte de nombreuses améliorations, comme une plus grande rapidité de découverte de l'environnement et une capacité de transmission de 721 Kbit/s. C'est ce standard, ratifié par le groupe IEEE 802.15.1 en 2005 que nous allons détailler dans la suite.
- Bluetooth 2.0 + EDR : augmente fortement le débit par une solution EDR (Enhanced Data Rate). La nouvelle valeur du débit est de 3 Mbit/s, mais, en vitesse réelle, on est largement en dessous de 2 Mbit/s. Cette augmentation est due à une modulation plus performante, utilisant à la fois du GFSK et du PSK (Phase Shift Keying) portant deux ou trois éléments binaires par baud.
- Bluetooth 2.1 + EDR : ce standard, approuvé en 2007 par le Bluetooth SIG, est une version intermédiaire apportant des améliorations sur la sécurité et le pairage des terminaux.
- Bluetooth 3.0 + HS : cette génération a eu pour objectif de faire décoller le débit de la technologie Bluetooth avec une version HS (High Speed). Ce standard a été adopté en 2009. Comme les technologies de partage du support physique et de transmission ne sont pas performantes dans Bluetooth, l'idée est d'ajouter une nouvelle technique d'émission à la place de Bluetooth au moment de la transmission proprement dite. La technologie basse consommation de Bluetooth est utilisée quand le réseau est inactif, et la technologie Wi-Fi au moment des transmissions.
- Bluetooth 4.0 : ce standard de 2010 a pour objectif premier de consommer le moins possible et de rassembler les différentes solutions Bluetooth. Nokia, qui avait fait des recherches sur la basse consommation de Bluetooth, avait proposé un nouveau produit, appelé WiBree. Plutôt que de standardiser ce nouveau produit, Nokia s'est allié en 2007 au Bluetooth SIG pour incorporer les avancées de WiBree dans Bluetooth. Le nom provisoire de cette nouvelle génération, Bluetooth ULP (Ultra Low Power), a été abandonné pour devenir en avril 2010 Bluetooth LE (Low Energy).

Bluetooth 4.0 rassemble, dans un même standard, à la fois le Bluetooth 2.1 de base, le Bluetooth 3.0 + HS, avec Wi-Fi pour la transmission, et le Bluetooth LE.

Schémas de connexion

Plusieurs schémas de connexion ont été définis par les normalisateurs. Le premier d'entre eux correspond à un réseau unique, appelé piconet, qui peut prendre en charge jusqu'à huit terminaux, avec un maître et huit esclaves. Le terminal maître gère les communications avec les différents esclaves. La communication entre deux terminaux esclaves transite obligatoirement par le terminal maître. Dans un même piconet, tous les terminaux utilisent la même séquence de saut de fréquence.

Un autre schéma de communication consiste à interconnecter des piconets pour former un scatternet, d'après le mot anglais *scatter,* dispersion. Comme les communications se font toujours sous la forme maître-esclave, le maître d'un piconet peut devenir l'esclave du maître d'un autre piconet. De son côté, un esclave peut être l'esclave de plusieurs maîtres. Un esclave peut se détacher provisoirement d'un maître pour se raccrocher à un autre piconet puis revenir vers le premier maître, une fois sa communication terminée avec le second.

La figure 21.1 illustre des connexions de terminaux Bluetooth dans lesquelles un maître d'un piconet est esclave du maître d'un autre piconet et un esclave est esclave de deux maîtres. Globalement, trois piconets sont interconnectés par un maître pour former un scatternet.

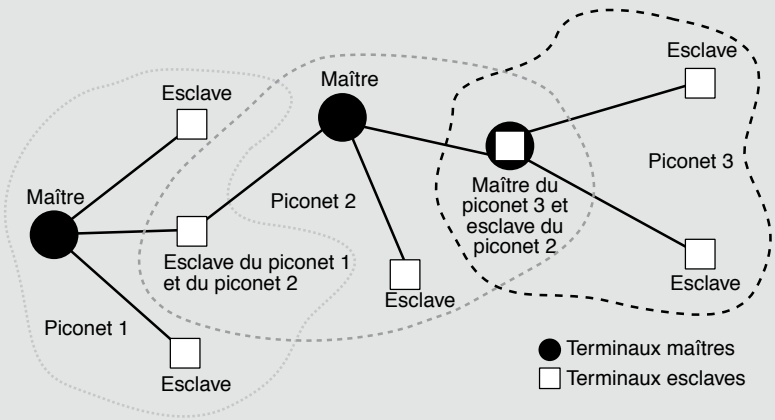


Figure 21.1

Schéma de connexion de terminaux Bluetooth

La communication à l'intérieur d'un piconet peut atteindre près de 1 Mbit/s. Comme il peut y avoir jusqu'à huit terminaux, la vitesse effective diminue rapidement en fonction du nombre de terminaux connectés dans une même picocellule. Un maître peut cependant accélérer sa communication en travaillant avec deux esclaves en utilisant des fréquences différentes.

Communications

La communication sur une liaison Bluetooth entre deux machines peut atteindre un débit de 433,9 Kbit/s dans une communication bidirectionnelle (full-duplex). Les débits sont égaux à 723,2 Kbit/s dans un sens et 57,6 Kbit/s dans l'autre en cas de communication déséquilibrée.

Les communications peuvent être de deux types : asynchrone ou synchrone. Une communication synchrone, ou SCO (Synchronous Connection-Oriented link), permet un débit synchrone de 64 Kbit/s. Ce type de connexion autorise le passage de la parole téléphonique avec une garantie de service. Une communication asynchrone, ou ACL

(Asynchronous Connection-less Link), permet des trafics asynchrones avec plus ou moins de protection. Le débit peut atteindre 723,2 Kbit/s.

Plusieurs catégories de communications peuvent être définies sur une connexion Bluetooth : une seule communication asynchrone, trois communications simultanées en SCO ou une SCO avec une ACL symétrique de 433,9 Kbit/s. Cela donne un débit total de la liaison de presque 1 Mbit/s dans le dernier cas. Un terminal esclave ne peut prendre en charge, au maximum, que deux canaux SCO provenant de deux terminaux distincts.

De façon plus précise, le temps est découpé en tranches, ou slots, à raison de 1 600 slots par seconde. Un slot fait donc 625 µs de long, comme illustré à la figure 21.2. Un terminal utilise une fréquence sur un slot puis, par un saut de fréquence (Frequency Hop), il change de fréquence sur la tranche de temps suivante, et ainsi de suite.

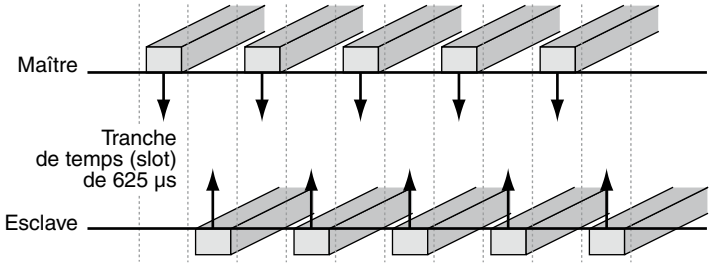


Figure 21.2
Découpage en slots

Un client Bluetooth utilise de façon cyclique toutes les bandes de fréquences. Les clients d'un même piconet possèdent la même suite de sauts de fréquence, et, lorsqu'un nouveau terminal veut se connecter, il doit commencer par reconnaître l'ensemble des sauts de fréquence pour pouvoir les respecter. Une communication s'exerce par paquet. En règle générale, un paquet tient sur un slot, mais il peut s'étendre sur trois ou cinq slots (*voir figure 21.3*). Le saut de fréquence à lieu à la fin de la communication d'un paquet.

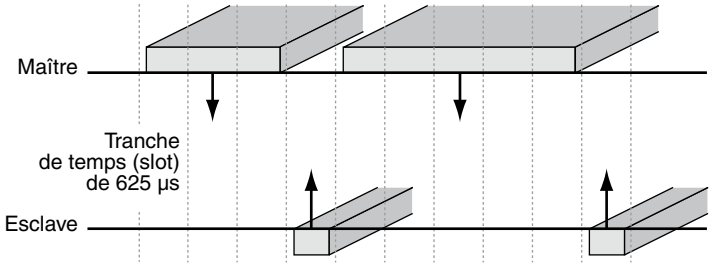


Figure 21.3
Transmission sur plusieurs slots

Fonctionnement de Bluetooth

Comme indiqué précédemment, Bluetooth permet la réalisation de petits réseaux personnels de quelques mètres carrés, les piconets. Les terminaux se connectent entre eux par l'intermédiaire d'un maître. La puissance de transmission peut atteindre 100 mW (milliwatt), ce qui permet une émission sur plusieurs dizaines de mètres. Il est possible de réduire cette puissance à 2,5 et 1 mW pour atteindre une portée de quelques mètres.

À une puissance de 100 mW, une batterie peut tenir assez longtemps, à condition d'utiliser des options d'économie d'énergie. Pour cette raison, des états de basse consommation ont été introduits dans la norme Bluetooth, qui autorisent une autonomie de plusieurs jours.

États des terminaux BluetoothLes terminaux Bluetooth autorisent des états spécifiques permettant au terminal de dépenser moins d'énergie et donc de prolonger la durée d'utilisation de la batterie. La figure 21.4 illustre les états possibles d'un terminal Bluetooth.

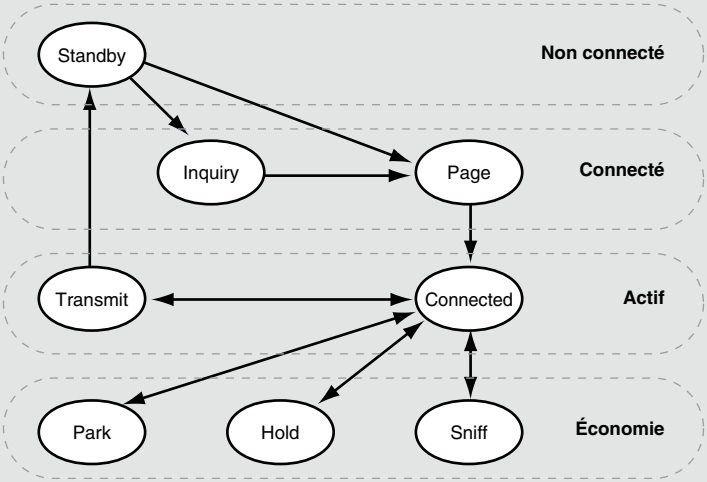


Figure 21.4

États d'un terminal Bluetooth

Dans l'état parqué (Park), le terminal ne peut ni recevoir ni émettre. Il peut seulement se réveiller de temps en temps pour consulter les messages émis par le maître. Utilisant le minimum d'énergie, il n'est pas comptabilisé dans une picocellule et peut donc être remplacé par un autre terminal dans les sept connexions que peut recevoir un maître.

L'état suspendu (Hold) indique que le terminal ne peut que recevoir des communications synchrones de type SCO. Le terminal se met en veille entre les instants synchrones de réception des paquets. L'état de repos actif (Sniff) permet au terminal de décider des slots pendant lesquels il travaille et de ceux pendant lesquels il se met à l'état de repos.

Dans un état de marche normal, le terminal maître doit être dans l'état Inquiry et l'esclave dans l'état Inquiry Scan. Le maître émet une signalisation pour initialiser la communication. Dans ce cas, si l'esclave reçoit les messages, il passe dans un état Inquiry Response, qui lui permet d'envoyer un message au maître lui précisant son adresse et l'état de son horloge. Il passe ensuite dans un nouvel état, Page Scan, dans lequel il attend de recevoir un paquet contenant son adresse sur l'une des neuf fréquences disponibles.

À réception du message, le maître passe à l'état Page, dans lequel il met à jour ses tables de connexion puis envoie un message vers l'esclave. Lorsque l'esclave détecte ce message, il se place dans l'état Slave Response puis répond au maître en indiquant son code d'accès. Le maître se met alors dans l'état Master Response et envoie un paquet Frequency Hopping Synchronization, qui permet à l'esclave de se synchroniser sur l'horloge du maître, puis passe à l'état connecté (Connected). De même, lorsque l'esclave reçoit ce message, il passe à l'état connecté (Connected). Le maître n'a plus qu'à effectuer une interrogation, ou polling, vers l'esclave pour vérifier qu'il y a bien eu connexion.

Techniques d'accès

Bluetooth met en œuvre une technique temporelle synchronisée dans laquelle le temps est divisé en tranches de longueur égale, appelées slots. Un slot correspond au temps élémentaire de transmission d'un paquet. Un paquet peut demander un temps de transmission plus ou moins long, qui ne peut pas accéder cinq slots.

Le format standard d'un paquet Bluetooth est illustré à la figure 21.5.

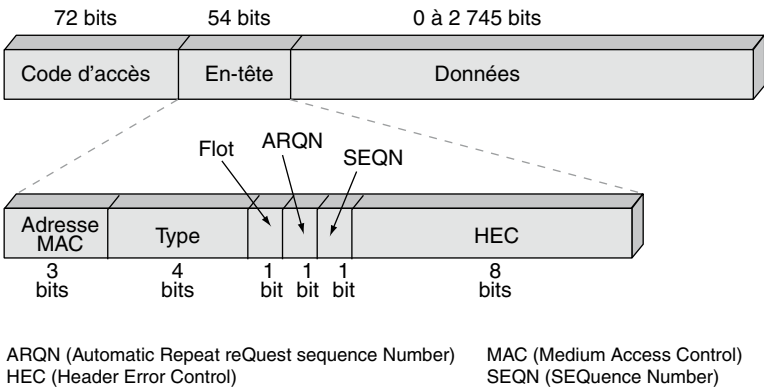


Figure 21.5

Format d'un paquet Bluetooth

Les 72 premiers bits du paquet permettent de transporter le code d'accès tout en effectuant une synchronisation entre les composants Bluetooth. Cette zone se compose de 4 bits, de préambule 0101 ou 1010, permettant de détecter le début de la trame, puis de 64 ou 68 bits pour le code et enfin de 4 bits de terminaison — lorsque le corps fait 64 bits — permettant de détecter la fin de la synchronisation en utilisant les séries 0101 ou 1010. Les 54 bits suivants consistent en trois fois une même séquence de six champs de longueur 3, 4, 1, 1, 1 et 8 bits. Ces champs servent à indiquer l'adresse d'un membre actif du piconet, ainsi qu'un numéro de code, un contrôle de flux piconet, une demande d'acquittement et un contrôle d'erreur des transmissions. Le champ de 18 bits est répété trois fois de suite pour s'assurer de sa réception correcte au récepteur. La zone de données qui s'étend ensuite de 0 à 2 745 bits contient une zone de détection d'erreur sur un ou deux octets.

Trois grands types de paquets sont définis dans Bluetooth, les paquets de contrôle, les paquets SCO et les paquets ACL. Les paquets de contrôle permettent de gérer les connexions des terminaux Bluetooth entre eux. Les paquets SCO correspondent aux communications synchrones de type SCO, et les paquets ACL aux transferts de données asynchrones.

Dans chacun de ces types de paquets, plusieurs sous-catégories peuvent être distinguées :

- Les paquets DV (Data-Voice), qui portent à la fois des données et de la parole.
- Les paquets DMx (Data-Medium) pour les paquets ACL en mode asynchrone avec un encodage permettant la correction des erreurs en ligne. La valeur x, qui vaut 1, 3 ou 5, indique la longueur du paquet en nombre de slots.
- Les paquets DHx (Data-High) pour les paquets ACL en mode asynchrone mais sans correction d'erreur, permettant ainsi un débit effectif plus élevé. De même que précédemment, x indique la longueur du paquet.
- Les paquets HVy (High-quality-Voice) pour les paquets SCO en mode synchrone sans correction d'erreur. La valeur y indique le type de contrôle d'erreur dans le paquet. Si y = 1, un FEC (Forward Error Correction) de 1/3 est utilisé. Dans ce cas, le corps du paquet contient une redondance par l'émission de trois fois la même information. Si y = 2, un FEC de 2/3 est utilisé. Dans ce cas, on transforme à l'aide d'un code la suite d'éléments binaires à transmettre de façon à détecter et corriger les erreurs. Si y = 3, aucune protection n'est utilisée.

Sécurité et fonctions de gestion

Trois niveaux de sécurité ont été définis dans Bluetooth. Le premier niveau n'a pas de gestion de sécurité. Le deuxième niveau instaure une sécurité à l'échelon applicatif en introduisant un processus d'identification lors de l'accès au service. Le troisième niveau introduit une sécurité plus importante en travaillant sur la liaison Bluetooth. Un processus d'authentification est mis en place, qui peut être suivi par un chiffrement à l'aide de clés privées pouvant atteindre 64 bits – la norme cite 128 bits comme future extension.

La sécurité est un élément important dans les systèmes de liaison radio puisque l'émission est diffusée et peut potentiellement être captée par les récepteurs environnants. Dans Bluetooth, deux équipements, par exemple deux PDA situés dans les poches de deux utilisateurs du métro, pourraient très bien entrer en communication par hasard. Pour éviter cela, Bluetooth offre des mécanismes d'authentification et de chiffrement au niveau MAC.

La principale technique d'authentification provient d'un programme automatique mis en place dans les terminaux Bluetooth, qui permet l'authentification et le chiffrement par une génération de clés par session. Chaque connexion peut utiliser ou non le mécanisme de chiffrement dans un sens seulement ou dans les deux sens simultanément. Seules des clés de 40 ou 64 bits peuvent être utilisées, ce qui confère une sécurité relativement faible, quoique suffisante pour le type de communication transitant entre deux terminaux Bluetooth. Si une sécurité supplémentaire doit être obtenue, il est nécessaire d'utiliser un chiffrement au niveau de l'application.

L'algorithme de sécurité utilise le numéro d'identité du terminal, ainsi qu'une clé privée et un générateur aléatoire interne à la puce Bluetooth. Pour chaque transaction, un nouveau numéro aléatoire est tiré pour chiffrer les données à transmettre. La gestion des clés est prise en charge par l'utilisateur sur les terminaux qui doivent s'interconnecter.

En utilisant le même procédé pour réaliser le chiffrement dans un scatternet, il est nécessaire de procéder, au début de la mise en relation, à un échange de clés privées entre les possesseurs de piconets indépendants.

Dans un piconet, un système de gestion est nécessaire pour réaliser les fonctions classiques de mise en œuvre des communications. Le processus de gestion des liaisons prend en charge les procédures classiques d'identification ainsi que la négociation des paramètres d'authentification. Il prend également à sa charge la configuration de la liaison, c'est-à-dire la définition des paramètres de fonctionnement. Ce processus de gestion s'effectue par un échange de requêtes-réponses entre les deux extrémités de la liaison.

L'architecture Bluetooth

L'objectif de l'architecture Bluetooth est de permettre l'interconnexion de tout type de terminal qui possède l'interface radio Bluetooth. Cette architecture est composée de deux grands types de couches : les couches matérielles et les couches logicielles, comme l'illustre la figure 21.6.

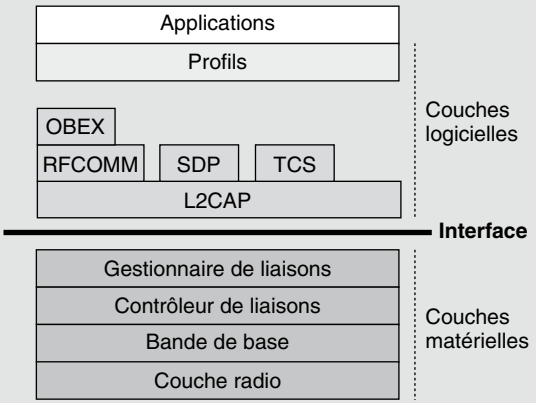


Figure 21.6

L'architecture Bluetooth

Les couches basses correspondent à la partie transmission sur l'interface radio, que nous avons examinée aux sections précédentes. La distance entre l'émetteur et le récepteur dépend de la puissance d'émission. Trois classes ont été définies : la classe 1 correspond à une puissance de 100 mW et à une portée d'une centaine de mètres, la classe 2, de 2,5 mW et d'une portée d'une quinzaine de mètres, et le classe 3, la plus classique, de 1 mW et d'une portée d'un mètre. Les adresses sont gérées au niveau de la bande de base et sont gérées par l'IEEE sur une longueur de 48 bits.

Le contrôleur de liaison a pour objectif de gérer la configuration de la liaison. Le gestionnaire de liaison vise la sécurité en gérant l'authentification et le chiffrement.

La couche L2CAP (Logical Link Control & Adaptation Protocol) permet de multiplexer les flots qui proviennent des différents protocoles de niveau supérieur. Les protocoles situés au-dessus correspondent à des services de transport sur l'interface série RS-232 (RFCOMM), à la découverte de service avec SDP (Service Discovery Protocol) et au protocole d'échange d'objet OBEX (Object Exchange). Au-dessus de cette couche, des profils d'équipements ont été choisis pour permettre de mettre en place une relation simple entre terminaux de même nature (une vingtaine de profils ont été définis).

UWB

Le groupe de normalisation MBOA (MultiBand OFDM Alliance) a défini les éléments de base pour la réalisation d'une vision complète d'un écosystème qui offrirait aux consommateurs un large éventail de produits pour la gestion et le contrôle des réseaux de domicile.

La couche radio UWB (Ultra Wide Band) et la plate-forme de convergence forment ensemble le mécanisme fondamental de transport pour différentes applications, y compris l'IEEE 1394 (FireWire), et le nouveau cadre provenant du consortium DLNA (Digital Living Network Alliance).

L'alliance OFDM multibande (MBOA), établie en 2003 et formalisée dans un groupe d'intérêt (SIG) en 2004, a été établie pour favoriser la production d'une norme globale pour les solutions sans fil de l'UWB. Ses deux cents membres comprenaient des industriels des semi-conducteurs, du calcul scientifique, de l'électronique grand public et des dispositifs mobiles.

Les caractéristiques de MBOA pour la couche physique (PHY) et le contrôleur d'accès de médias (IMPER) sont finalisées et disponibles pour les sociétés membres de l'alliance. Cette dernière s'est fondue dans une autre alliance plus importante, la WiMedia Alliance en mars 2005. Malheureusement, la technologie UWB pour des raisons de consommation d'énergie n'a pas du tout eu le succès espéré et plusieurs standards du réseau personne, comme Bluetooth, ont abandonné l'idée de reprendre cette technologie au niveau physique. Après bien des discussions la WiMedia Alliance s'est dissoute en 2009 en poussant le Wireless USB Promoter Group (que l'on appelle souvent Wireless USB et même WUSB) à promouvoir le produit de base de la WiMedia Alliance.

WiMedia Alliance

La WiMedia Alliance est un groupement d'industriels ayant fortement contribué au développement du concept UWB, notamment sous forme de couches protocolaires de niveau logiciel.

Cette alliance vise à favoriser la connectivité et l'interopérabilité des produits UWB. La plate-forme commune illustrée à la figure 21.7 permet à de multiples applications de fonctionner ensemble sur une interface radio commune.

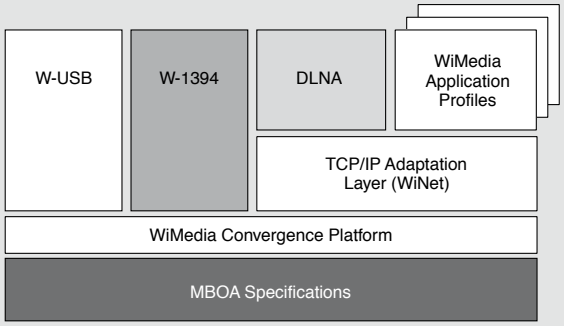


Figure 21.7
Plate-forme de la WiMedia Alliance

La combinaison de l'interface radio proposée utilisant l'OFDM multibande et de l'architecture de la plate-forme WiMedia permet de réaliser la convergence pour l'exécution des versions sans fil provenant de l'UWB : WUSB, IEEE 1394, WiNet et DLNA.

WiMedia a également défini plusieurs spécifications pour faciliter l'arrivée de nouveaux produits :

- WiNEP (WiMedia Network Encapsulation Protocol), qui permet de prendre en charge l'environnement TCP/IP.
- WiMCA (WiMedia Alliance's Convergence Architecture), qui définit l'architecture de la plate-forme de convergence de WiMedia. Cette architecture est interopérable entre plusieurs fournisseurs. La plate-forme établit des politiques équitables pour toutes les entités accédant par le canal radio UWB. Des processus ont en outre été mis en place pour assurer la sécurité et la qualité de service.
- SMP (Streaming Media Profil), qui définit les protocoles et les formats pour le streaming en utilisant des primitives provenant d'UPnP (*voir le chapitre 11*).
- DIP (Digital Imaging & Printing Profile), qui propose un protocole et des formats d'application pour UPnP permettant de réaliser des applications d'imagerie numérique et d'impression.

Wireless USB

Le groupe WUSB a été constitué en 2004 par sept leaders de l'industrie : Agere Systems, HP, Intel, Microsoft Corporation, NEC, Philips et Samsung.

Ce groupe a rapidement proposé une charte définissant les spécifications du WUSB, avec une largeur de bande de 480 Mbit/s. Le WUSB a pour objectif de remplacer les câbles USB2. Cette interface sera de plus en plus disponible en natif sur les cartes mères pour les équipements alimentés électriquement.

Interface radio

Les origines de la technologie UWB remontent au travail commencé en 1962 sous les noms d'impulsion radio, de bande de base ou de communications sur des porteuses libres.

Le sigle Ultra-Wide Band a été proposé pour la première fois par le Département de la Défense aux États-Unis en 1989. Aujourd'hui, l'UWB définit, selon la FCC, n'importe quelle technologie radio s'étalant sur une partie du spectre occupant plus de 20 % de la fréquence centrale ou au minimum 500 MHz.

Identifiant les avantages des nouveaux produits qui pourraient incorporer cette technologie pour bénéficier des applications publiques de sûreté, d'entreprise et de consommation d'énergie restreinte, la FCC lui a alloué en 2002 une partie du spectre radio utilisable sans licence allant de 3,1 à 10,6 GHz. Une partie additionnelle du spectre est disponible pour les applications médicales, scientifiques et de secours incendie.

Plutôt que d'exiger une interface UWB utilisant l'ensemble de la bande passante disponible, représentant 7.5 GHz, pour transmettre les signaux d'information, la FCC a défini une largeur de bande minimale de 500 MHz à 10dB. Cette largeur de bande minimale, ainsi que d'autres conditions imposées par la FCC, protège la transmission des autres signaux provenant d'utilisateurs de cette partie du spectre. En effet, si la solution

d'émettre en dessous du bruit permet de ne pas perturber les autres utilisateurs de cette bande, en revanche ces autres utilisateurs pourraient perturber l'UWB. Par exemple, une connexion UWB dans un aéroport serait perturbée par les radars et autres équipements utilisant la bande UWB.

Il a été montré par de nombreuses expériences qu'une bande de 500 MHz était toujours disponible, même dans les environnements les plus perturbés. Cependant, cette flexibilité permise par le standard de la FCC augmente considérablement les options disponibles pour la conception des systèmes de communication UWB. Les concepteurs sont libres d'employer une combinaison de sous-bandes du spectre pour optimiser le fonctionnement du système, de la puissance nécessaire et de la complexité de conception.

Il est à noter que la puissance permise est inférieure en Europe dans la réglementation édictée par l'ETSI.

Les systèmes UWB peuvent maintenir un même niveau de puissance, comme s'ils employaient toute la largeur de bande, en intercalant des symboles dans les différentes sous-bandes. Dans un système multibande, l'information peut être transmise par la méthode fondée sur les impulsions traditionnelles sur la porteuse de base ou par des techniques plus avancées de multiporteuse.

Les systèmes fondés sur les impulsions sur la porteuse de base transmettent les signaux en modulant la phase d'impulsion. Cette solution provient d'une technologie éprouvée, qui s'appuie sur une conception simple de l'émetteur. Cela ne va toutefois pas sans inconvénients. Il est difficile de rassembler suffisamment d'énergie pour émettre le signal dans un environnement typique d'utilisation, avec beaucoup de surfaces réfléchissantes, en n'employant qu'une chaîne RF simple. Les limitations des temps de commutation peuvent être très strictes, à l'émetteur comme au récepteur.

La technique MB-OFDM (Multi-bandes OFDM) transmet les porteuses multiples simultanément de façon espacée sur des fréquences précises. L'utilisation d'algorithmes rapides de transformée de Fourier garantit une grande efficacité énergétique dans les cas de trajets multiples, tout en n'augmentant que légèrement la complexité de l'émetteur. Les bénéfices de cette solution MB-OFDM incluent la flexibilité et la forte élasticité spectrales ainsi qu'une forte résistance aux interférences radio et aux effets provenant des trajets multiples.

Les techniques de modulation OFDM ont été appliquées avec succès à de nombreux systèmes de communication commercialisés aux performances élevées, notamment Wi-Fi 802.11a/g, WiMAX 802.16a, HomePlug et les normes ADSL.

Fondée sur la technologie CMOS, l'utilisation du spectre de 3,1 à 4,8 GHz est considérée comme optimale pour des déploiements initiaux. La limite supérieure permet d'éviter des interférences avec la bande U-NII, où est localisée l'interface radio 802.11a, et de simplifier la conception des circuits radio et analogiques.

La bande de fréquences des 3,1-4,8 GHz est suffisante pour trois sous-bandes de 500 MHz, comme l'illustre la figure 21.8.

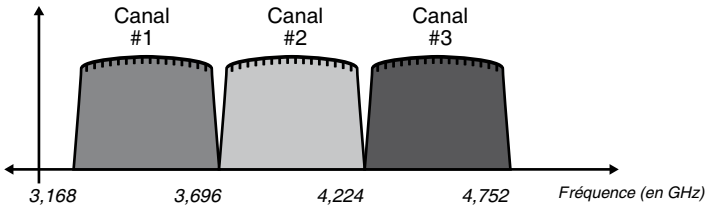


Figure 21.8

Allocation des fréquences pour un système MB-OFDM

Dans le groupe de travail IEEE 802.15.3, deux solutions ont été développées, une sur la bande classique des 2,4 GHz, qui atteindra une vitesse de 54 Mbit/s effective, et une qui utilise l'ensemble de la bande passante entre 3,1 et 10,7 GHz, mais à une puissance très faible, en dessous du bruit ambiant. De la sorte, cette solution ne gênera pas les applications civiles et militaires utilisant ces bandes.

Le spectre visé par cette technologie est illustré à la figure 21.9.

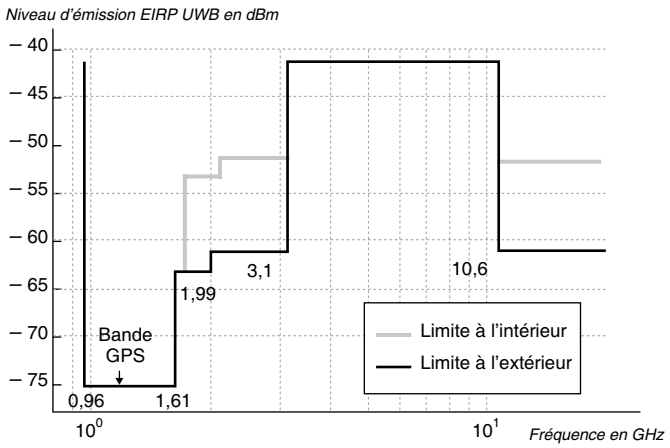


Figure 21.9

Partie du spectre pouvant être utilisée par l'UWB

En dépit de la très faible puissance utilisée, la bande passante de plus de 7 GHz permet d'obtenir une vitesse située entre 120 et 480 Mbit/s en fonction des perturbations externes.

Une des propriétés de l'UWB est de pouvoir prendre en charge des communications avec des équipements qui se déplacent à relativement faible vitesse. L'objectif est de connecter et déconnecter ces équipements en des temps extrêmement courts, de l'ordre de la seconde.

Complexité et énergie

Le système MB-OFDM a été spécifiquement conçu pour être le plus simple possible. Une seule chaîne de réception analogique rend l'architecture globale d'une grande simplicité

en limitant les symboles transmis à une modulation QPSK. L'espacement relativement grand entre les porteuses permet de réduire le bruit sur les circuits et d'améliorer la robustesse aux erreurs de synchronisation.

La durée de vie des batteries pour les mobiles est un facteur critique pour les utilisateurs. L'accès de type MB-OFDM est capable de tenir plusieurs heures dans des conditions typiques avant qu'une recharge ne soit exigée.

Le tableau 21.1 récapitule les puissances nécessaires, en fonction du débit, estimées pour un système MB-OFDM avec un cœur CMOS de 90 microns.

Débit	Puissance de transmission	Puissance en réception	Puissance en cours de sommeil
110 Mbps	93 mW	155 mW	15 µW
200 Mbps	93 mW	169 mW	15 µW

TABLEAU 21.1 • Énergie nécessaire pour l'UWB

Sécurité

La technologie UWB est conçue pour embarquer les éléments nécessaires pour que la sécurité soit assurée en permanence. Des mécanismes de confidentialité sont mis en application à plusieurs niveaux protocolaires afin d'assurer la robustesse nécessaire aux environnements sans fil tout en restant transparents pour les utilisateurs.

L'expérience acquise au fur et à mesure de la croissance des réseaux Wi-Fi et Bluetooth ont également guidé les choix effectués pour l'architecture de sécurité. La plupart des solutions mises en œuvre sont identiques à celles promues par la norme IEEE 802.11i, que nous détaillons au chapitre suivant.

La sécurité des communications est assurée par une authentification et un chiffrement de l'information. L'authentification utilisera sûrement le protocole EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). L'utilisation de l'algorithme AES (Advanced Encryption Standard) avec une clé de 128 bits doit garantir la sécurité du transport de l'information.

ZigBee

Les réseaux ZigBee sont l'inverse des réseaux UWB. Leur objectif est de consommer extrêmement peu d'énergie, de telle sorte qu'une petite batterie puisse tenir presque toute la durée de vie de l'interface, mais à un débit faible.

La première version de ZigBee date de 2004 et la seconde de 2007. Elles sont compatibles et la première version est aujourd'hui abandonnée. Les réseaux ZigBee sont employés dans de nombreuses applications comme les jeux électroniques utilisant la radio, les connexions de boitiers en domotique, des services depuis un terminal mobile, l'accès à des informations dans des centres commerciaux, etc. Une nouvelle alliance avec le RF4CE (Radio Frequency for Consumer Electronics) Consortium en 2009 a permis de développer le standard ZigBee RF4CE pour la connexions des équipements électroniques dans le domicile.

Deux types de transferts sont privilégiés dans ZigBee : la signalisation et la transmission de données basse vitesse.

La figure 21.10 illustre un environnement ZigBee pour le réseau de domicile.

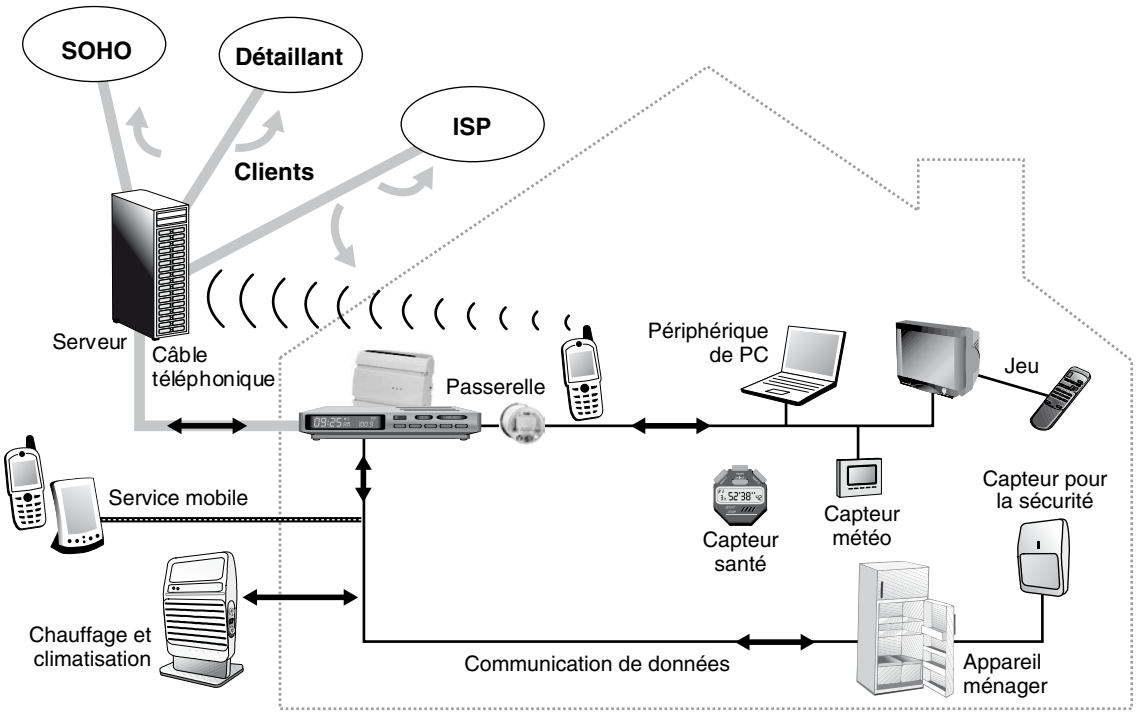


Figure 21.10

Réseau ZigBee pour la domotique

Dans la normalisation, ZigBee peut avoir trois vitesses possibles :

- 250 Kbit/s avec la bande classique des 2,4 GHz ;
- 20 Kbit/s avec la bande des 868 MHz disponible en Europe ;
- 40 Kbit/s avec la bande des 915 MHz disponible en Amérique du Nord.

Ces différentes possibilités sont récapitulées au tableau 21.2.

	Bande	Couverture	Débit données	Numéro de canal
2,4 GHz	ISM	Mondiale	250 Kbit/s	16
868 MHz		Europe	20 Kbit/s	1
915 MHz	ISM	Amerique	40 Kbit/s	10

TABLEAU 21.2 • Bandes de fréquence et débits de ZigBee

Les réseaux ZigBee devraient arriver en force sur le marché de la commande et des bas débits dans les domaines de la domotique, de la bureautique et de l'automatisme.

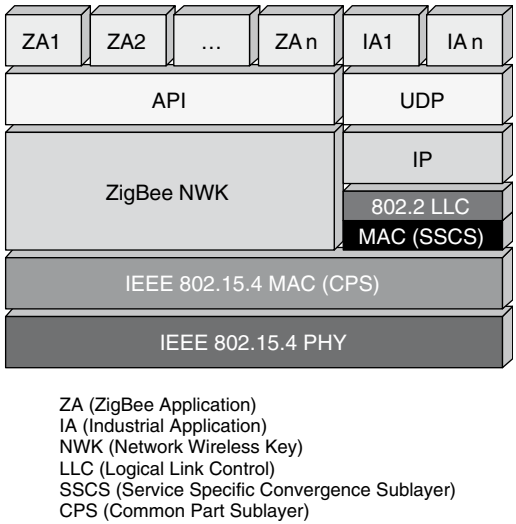


Figure 21.11

Architecture d'un réseau ZigBee

Comme illustré à la figure 21.11, l'architecture d'un réseau ZigBee contient cinq grandes couches. En partant du sommet, on trouve la couche applicative, qui utilise des profils applicatifs prédéterminés, la couche sous-jacente, qui correspond à l'interface applicative ou au protocole UDP si l'application est à distance, la couche ZigBee proprement dite, qui gère la topologie, le routage, la découverte de protocole et la sécurité, la couche MAC et la couche physique.

Le niveau applicatif

L'architecture protocolaire de ZigBee comporte des couches provenant de l'IEEE 802.15.4, comme la couche de contrôle d'accès (IMPER) et la couche physique (PHY) associées à la couche réseau de ZigBee (NWK). Les parties de la pile protocolaire qui nous intéressent dans cette section correspondent à la couche ZA et à l'API illustrée à la figure 21.14. La couche application de ZigBee comprend une sous-couche, le ZDO (ZigBee Device Object), déterminant les objets définis dans les équipements connectés. La sous-couche ZDO contient les tables de maintien des dispositifs d'association. Les responsabilités du ZDO incluent le rôle de l'équipement dans le réseau (coordonnateur ZigBee ou dispositif d'extrémité), la découverte des équipements dans le réseau et la détermination des services applicatifs.

Une API a été définie entre la couche réseau (NWK) et la couche applicative ZA. Cette interface contient un ensemble de services employés par le ZDO pour permettre aux objets applicatifs de communiquer avec la couche réseau.

L'adressage

L'exemple de connexion ZigBee illustré à la figure 21.12 comporte deux équipements communicants, l'un contenant deux commutateurs et l'autre quatre lampes.

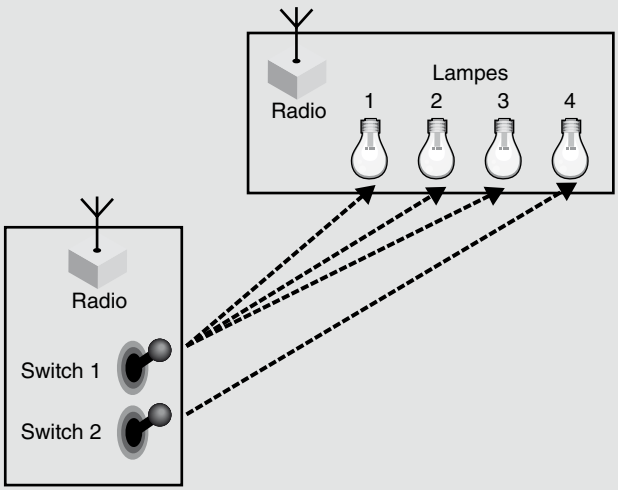


Figure 21.12

Exemple de connexion ZigBee

Une adresse est donnée à chaque équipement au moment de la connexion au réseau ZigBee. L'interrupteur 1 doit commander les lampes 1, 2 et 3 tandis que l'interrupteur 2 doit éclairer la lampe 4. ZigBee propose un sous-adressage de l'équipement élémentaire qui permet de réaliser ces communications.

La découverte des équipements ZigBee environnants s'effectue par des demandes en broadcast. Les adresses récupérées sont soit de type IEEE, soit de la couche réseau de ZigBee, c'est-à-dire NWK. Un échange s'ensuit permettant de découvrir le profil des équipements connectés. Les profils ZigBee sont la clé des communications entre composants ZigBee. Un exemple de profil serait celui d'un interrupteur électrique. Les équipements sont architecturés pour échanger des messages normalisés permettant de déterminer le profil.

La couche réseau fournit la fonctionnalité permettant d'utiliser la sous-couche IMPER d'IEEE 802.15.4 La couche NWK fournit deux services, consultés par deux points d'accès de service : le service de données et le service de gestion de NWK. Ces deux services fournissent l'interface avec la couche application et la couche IMPER.

La sécurité a été fortement introduite dans l'environnement ZigBee avec l'utilisation d'un chiffrement AES et une clé de 128 bits. Globalement, on retrouve la sécurisation introduite par WPA2 dans l'environnement Wi-Fi (*voir le chapitre 22*).

Wi-Fi personnel

Les réseaux personnels se sont démultipliés à cause d'un manque flagrant de normalisation entre les groupes de travail de l'IEEE et de toutes les initiatives des équipementiers. Cela peut expliquer l'arrivée du monde Wi-Fi dans l'univers des réseaux personnels. Cette arrivée s'effectue de trois façons différentes :

- Le réseau Bluetooth +HS, qui allie les couches hautes de Bluetooth avec une transmission Wi-Fi.
- Le WiGig, dont les débits sont de 6 Gbit/s en crête et les fréquences se situent dans la gamme des 60 GHz.
- Le groupe de travail IEEE 802.11ad, qui associe un Wi-Fi standard pour la détection des équipements et une technologie d'antenne directive à 60 GHz pour la transmission.

La Wireless Gigabit Alliance a été formée en 2009 pour réaliser un réseau sans fil, dans la bande des 60 GHz, capable de dépasser des débits d'un gigabit par seconde. Étant donné le choix de la bande de fréquence, ce réseau ne peut pratiquement qu'être un réseau personnel puisque la très haute fréquence utilisée ne permet pas au signal de traverser les obstacles.

La Wireless Gigabit Alliance pourrait à plus long terme proposer des spécifications dans les fréquences plus classiques du Wi-Fi. Le débit maximal est de 7 Gbit/s, mais le débit réel dépend de l'environnement, c'est-à-dire principalement de l'éloignement du point d'accès et des interférences. Ce groupe de travail se trouve confronté à un autre groupe d'industriels, le Wireless HD, qui défend une autre vision provenant des industriels de la vidéo. L'idée de ce groupe est de mettre la norme HDMI (High Definition Multimedia Interface) en environnement hertzien. Le produit attendu pourrait atteindre 25 Gbit/s.

Le groupe de travail IEEE 802.11ad a également l'objectif d'atteindre jusqu'à 6 Gbit/s dans la bande des 60 GHz, laquelle fournit des bandes libres suffisantes pour atteindre ces débits. Ce groupe de travail intègre dans un même module un Wi-Fi 802.11g ou n et un Wi-Fi de nouvelle génération sur la bande des 60 GHz. L'idée est de rechercher les terminaux qui ont besoin de communiquer avec le Wi-Fi standard et de passer la main à la partie haute fréquence pour avoir les débits annoncés.

Conclusion

Les réseaux personnels forment un vaste ensemble de solutions allant du très haut débit au très faible débit, avec des consommations énergétiques très diverses.

Deux grands axes semblent se mettre en place : le haut débit, avec les Bluetooth HD, l'UWB et différentes variantes de Wi-Fi personnels, et la très basse consommation, avec Bluetooth LE et ZigBee. La solution UWB est malmenée par sa forte consommation et pourrait laisser la place à une nouvelle génération de Wi-Fi. D'autres possibilités existent avec les réseaux de capteurs, comme 6LowPAN, de l'IETF, ou les RFID, que nous détaillons au chapitre 24.

22

Les réseaux Wi-Fi

La norme IEEE 802.11 a donné lieu à trois types de réseaux sans fil, ceux qui travaillent à la vitesse de 11 Mbit/s, ceux à 54 Mbit/s et ceux à 600 Mbit/s. Les premiers se fondent sur la norme IEEE 802.11b, les deuxièmes sur les normes IEEE 802.11a et g et les troisièmes sur la norme IEEE 802.11n. À ces trois générations vont succéder deux nouvelles générations : IEEE 802.11ac, à 2 Gbit/s, et IEEE 802.11af, qui pourrait atteindre 10 Gbit/s.

Pour le premier type, les fréquences choisies se situent dans la gamme des 2,4 GHz. Dans cette solution de réseau local par voie hertzienne, les communications peuvent se faire soit directement de station à station, mais sans qu'une station puisse relayer les paquets vers une autre station terminale, soit en passant par une borne de concentration, appelée point d'accès, ou AP (Access Point).

L'accès au support physique s'effectue par le biais du protocole MAC, interne au niveau MAC, pour tous les types de réseau Wi-Fi. De nombreuses options rendent toutefois sa mise en œuvre assez complexe. Le protocole MAC se fonde sur la technique d'accès CSMA/CD, déjà utilisée dans les réseaux Ethernet métalliques. La différence entre le protocole hertzien et le protocole terrestre provient de la façon de détecter les collisions. Dans la version terrestre, on détecte les collisions en écoutant la porteuse. Lorsque deux stations veulent émettre pendant qu'une troisième est en train de transmettre sa trame, cela mène automatiquement à une collision. Dans le cas hertzien, le protocole d'accès permet d'éviter la collision en obligeant les deux stations à attendre un temps différent avant de transmettre. Comme la différence entre les deux temps d'attente est supérieure au temps de propagation sur le support de transmission, la station qui a le temps d'attente le plus long trouve le support physique déjà occupé et évite ainsi la collision. Cette nouvelle technique s'appelle le CSMA/CA (Collision Avoidance).

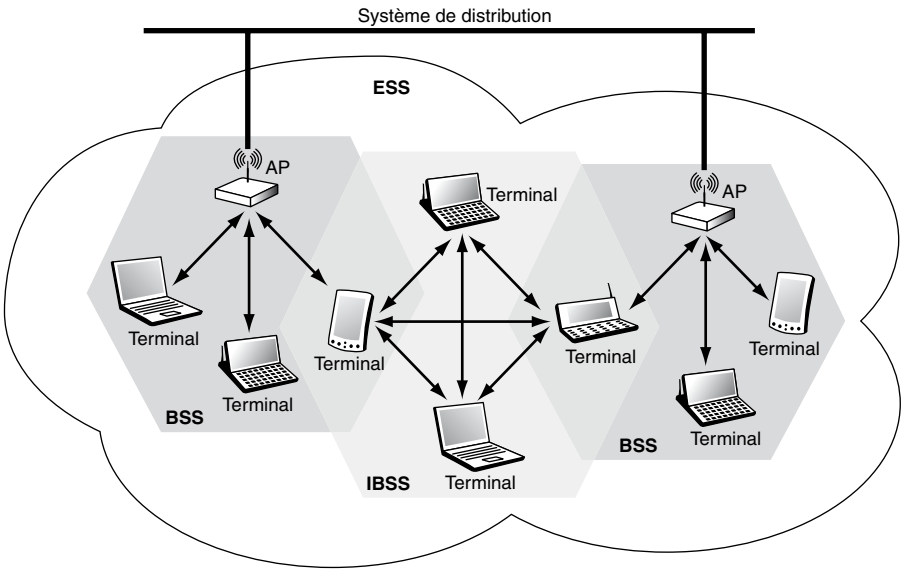
Comme nous venons de le voir, pour éviter les collisions, chaque station possède un temporisateur avec une valeur spécifique. Lorsqu'une station écoute la porteuse et que

le canal est vide, elle transmet. Le risque qu'une collision se produise est extrêmement faible, puisque la probabilité que deux stations démarrent leur émission dans une même microseconde est quasiment nulle. En revanche, lorsqu'une transmission a lieu et que d'autres stations se mettent à l'écoute et persistent à écouter, la collision devient inévitable. Pour empêcher la collision, il faut que les stations attendent avant de transmettre un temps permettant de séparer leurs instants d'émission respectifs. On ajoute pour cela un premier temporisateur très petit, qui permet au récepteur d'envoyer immédiatement un acquittement. Un deuxième temporisateur permet de donner une forte priorité à une application temps réel. Enfin, le temporisateur le plus long, dévolu aux paquets asynchrones, détermine l'instant d'émission pour les trames asynchrones.

IEEE 802.11

Les réseaux Wi-Fi proviennent de la norme IEEE 802.11, qui définit une architecture cellulaire. Un groupe de terminaux munis d'une carte d'interface réseau 802.11 s'associent pour établir des communications directes. Elles forment alors un BSS (Basic Service Set), à ne pas confondre avec le BSS (Base Station Subsystem) des réseaux GSM. La zone occupée par les terminaux d'un BSS peut être une BSA (Basic Set Area) ou une cellule.

Comme illustré à la figure 22.1, la norme 802.11 offre deux modes de fonctionnement, le mode infrastructure et le mode ad-hoc.



AP (Access Point) : point d'accès
BSS (Basic Set Service) : cellule de base
ESS (Extented Set Service) : ensemble des cellules de base
IBSS (Independent Basic Set Service) : cellule de base en mode ad-hoc

Figure 22.1

Architecture d'un réseau Wi-Fi

Le mode infrastructure est défini pour fournir aux différentes stations des services spécifiques, sur une zone de couverture déterminée par la taille du réseau. Les réseaux d'infrastructure sont établis en utilisant des points d'accès, qui jouent le rôle de station de base pour un BSS.

Lorsque le réseau est composé de plusieurs BSS, chacun d'eux est relié à un système de distribution, ou DS (Distribution System), par l'intermédiaire de leur point d'accès (AP) respectif. Un système de distribution correspond en règle générale à un réseau Ethernet filaire. Un groupe de BSS interconnectés par un système de distribution forme un ESS (Extented Service Set), qui n'est pas très différent d'un sous-système radio de réseau de mobiles.

Le système de distribution est responsable du transfert des paquets entre différents BSS d'un même ESS. Dans les spécifications du standard, il est implémenté de manière indépendante de la structure hertzienne de la partie sans fil. C'est la raison pour laquelle le système de distribution correspond presque toujours à un réseau Ethernet mais rien n'empêcherait d'utiliser un réseau Token-Ring ou FDDI (Fiber Distributed Data Interface). Une autre solution est d'utiliser le réseau Wi-Fi lui-même, ce qui donne les réseaux mesh.

L'ESS peut fournir aux différentes stations mobiles une passerelle d'accès vers un réseau fixe, tel qu'Internet. Cette passerelle permet de connecter le réseau 802.11 à un autre réseau. Si ce réseau est de type IEEE 802.x, la passerelle incorpore des fonctions similaires à celles d'un pont.

Un réseau en mode ad-hoc est un groupe de terminaux formant un IBSS (Independent Basic Service Set), dont le rôle consiste à permettre aux stations de communiquer sans l'aide d'une quelconque infrastructure, telle qu'un point d'accès ou une connexion au système de distribution. Chaque station peut établir une communication avec n'importe quelle autre station dans l'IBSS, sans être obligée de passer par un point d'accès. Comme il n'y a pas de point d'accès, les stations n'intègrent qu'un certain nombre de fonctionnalités, telles les trames utilisées pour la synchronisation.

Ce mode de fonctionnement se révèle très utile pour mettre en place facilement un réseau sans fil lorsqu'une infrastructure sans fil ou fixe fait défaut.

Architecture Wi-Fi

Comme tous les standards de l'IEEE, 802.11 couvre les deux premières couches du modèle de référence OSI. L'une de ses caractéristiques essentielles est qu'il définit une couche MAC commune à toutes les couches physiques. De la sorte, de futures couches physiques pourront être ajoutées sans qu'il soit nécessaire de modifier la couche MAC.

Couche physique

La couche physique a pour rôle de transporter correctement la suite de signaux 0 ou 1 que l'émetteur souhaite envoyer au récepteur. Elle est divisée en deux sous-couches, PLCP (Physical Layer Convergence Protocol) et PMD (Physical Medium Dependent).

La sous-couche PMD s'occupe de l'encodage des données, tandis que la sous-couche PLCP prend en charge l'écoute du support. Elle fournit pour cela un CCA (Clear Channel Assessment), qui est le signal utilisé par la couche MAC pour savoir si le support est occupé ou non.

IEEE 802.11 définit quatre couches physiques différentes :

- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)
- IR (Infrarouge)
- OFDM (Orthogonal Frequency Division Multiplexing)

Le FHSS et le DSSS utilisent la bande des 2,4 GHz de l'ISM (Industrial, Scientific, and Medical). Nous reviendrons sur cette bande sans licence. L'infrarouge n'est utilisé que dans les cas où les distances entre les différentes stations sont faibles.

La quatrième couche physique a été définie dans la bande des 5,2 GHz. Grâce au codage OFDM, des débits de 54 Mbit/s ont facilement été atteints. 802.11 est le premier standard à utiliser un codage OFDM pour une communication de type paquet. Cette technologie était jusqu'à présent utilisée pour des systèmes de transmission de données continue, tels que DVB (Digital Video Broadcasting) ou DAB (Digital Audio Broadcasting).

Pour qu'un signal soit reçu correctement, sa portée ne peut dépasser 50 m dans un environnement de bureau, 500 m sans obstacle et plusieurs kilomètres avec une antenne directive extérieure. Lorsqu'il y a traversée de murs porteurs, cette distance est souvent beaucoup plus restrictive.

Couche liaison de données

La couche liaison de données est composée essentiellement de deux sous-couches, LLC (Logical Link Control) et MAC. La couche LLC utilise les mêmes propriétés que la couche LLC 802.2 (*voir l'annexe E*). Il est de ce fait possible de relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE. La couche MAC, quant à elle, est spécifique de 802.11.

Le rôle de la couche MAC 802.11 est assez similaire à celui de la couche MAC 802.3 du réseau Ethernet terrestre, puisque les terminaux écoutent la porteuse avant d'émettre. Si la porteuse est libre, le terminal émet, sinon il se met en attente. Cependant, la couche MAC 802.11 intègre un grand nombre de fonctionnalités que l'on ne trouve pas dans la version terrestre.

Les fonctionnalités nécessaires pour réaliser un accès sur une interface radio sont les suivantes :

- procédures d'allocation du support ;
- adressage des paquets ;
- formatage des trames ;
- contrôle d'erreur CRC (Cyclic Redundancy Check) ;
- fragmentation-réassemblage.

L'une des particularités du standard est qu'il définit deux méthodes d'accès fondamentalement différentes au niveau de la couche MAC. La première est le DCF (Distributed Coordination Function), qui correspond à une méthode d'accès assez similaire à celle des réseaux traditionnels supportant le best-effort. Le DCF a été conçu pour prendre en charge le transport de données asynchrones, dans lequel tous les utilisateurs qui veulent transmettre des données ont une chance égale d'accéder au support.

La seconde méthode d'accès est le PCF (Point Coordination Function). Fondée sur l'interrogation à tour de rôle des terminaux, ou polling, sous le contrôle du point d'accès, la méthode PCF est conçue essentiellement pour la transmission de données sensibles, qui demandent une gestion du délai utilisé pour les applications temps réel, telles que la voix ou la vidéo.

Un réseau en mode ad-hoc utilise uniquement le DCF, tandis qu'un réseau en mode infrastructure avec point d'accès utilise à la fois le DCF et le PCF.

Techniques d'accès

Comme expliqué précédemment, le DCF est la technique d'accès générale utilisée pour permettre des transferts de données asynchrones en best-effort. D'après le standard, toutes les stations doivent la supporter. Le DCF s'appuie sur le CSMA/CA.

Dans Ethernet, le protocole qui implémente la technique d'accès CSMA/CD contrôle l'accès de chaque station au support et détecte et traite les collisions qui se produisent lorsque deux stations ou davantage transmettent simultanément. Dans les réseaux Wi-Fi, la détection des collisions n'est pas possible. Pour détecter une collision, une station doit être capable d'écouter et de transmettre en même temps. Dans les systèmes radio, la transmission couvre la réception de signaux sur la même fréquence et ne permet pas à la station d'entendre la collision : les liaisons radio ne sont jamais full-duplex. Comme une station ne peut écouter sa propre transmission, si une collision se produit, la station continue à transmettre la trame complète, ce qui entraîne une perte de performance du réseau. La technique d'accès de Wi-Fi doit tenir compte de ce phénomène.

Le protocole CSMA/CA

Le CSMA/CA évite les collisions en utilisant des trames d'acquittement, ou ACK (Acknowledgement). Un ACK est envoyé par la station destination pour confirmer que les données sont reçues de manière intacte.

L'accès au support est contrôlé par l'utilisation d'espaces intertrames, ou IFS (Inter-Frame Spacing), qui correspondent à l'intervalle de temps entre la transmission de deux trames. Les intervalles IFS sont des périodes d'inactivité sur le support de transmission. Les valeurs des différents IFS sont calculées par la couche physique.

Le standard définit trois types d'IFS :

- SIFS (Short Inter-Frame Spacing), le plus petit des IFS, est utilisé pour séparer les transmissions au sein d'un même dialogue (envoi de données, ACK, etc.). Il y a toujours une seule station pour transmettre à cet instant, ayant donc la priorité sur toutes les autres stations. La valeur du SIFS est de 28 µs.

- PIFS (PCF IFS), utilisé par le point d'accès pour accéder avec priorité au support. Le PIFS correspond à la valeur du SIFS, auquel on ajoute un temps, ou timeslot, défini dans l'algorithme de back-off, de 78 µs.
- DIFS (DCF IFS), utilisé lorsqu'une station veut commencer une nouvelle transmission. Le DIFS correspond à la valeur du PIFS, à laquelle on ajoute un temps de 128 µs.

Les terminaux d'un même BSS peuvent écouter l'activité de toutes les stations qui s'y trouvent. Lorsqu'une station envoie une trame, les autres stations l'entendent et, pour éviter une collision, mettent à jour un timer, appelé NAV (Network Allocation Vector), permettant de retarder toutes les transmissions prévues. Le NAV est calculé par rapport à l'information située dans le champ durée de vie, ou TTL, contenu dans les trames qui ont été envoyées. Les autres stations n'ont la capacité de transmettre qu'après la fin du NAV.

Lors d'un dialogue entre deux stations, le NAV est calculé par rapport au champ TTL des différentes trames qui sont envoyées (données, ACK, etc.). Le NAV est en fait un temporisateur, qui détermine l'instant auquel la trame peut être transmise avec succès. Une station source voulant transmettre des données écoute le support. Si aucune activité n'est détectée pendant une période de temps correspondant à un DIFS, elle transmet ses données immédiatement. Si le support est encore occupé, elle continue de l'écouter jusqu'à ce qu'il soit libre. Quand le support devient disponible, elle retarde encore sa transmission en utilisant l'algorithme de back-off avant de transmettre ses données.

Si les données envoyées sont reçues intactes, la station destination attend pendant un temps équivalent à un SIFS et émet un ACK pour confirmer leur bonne réception. Si l'ACK n'est pas détecté par la station source ou si les données ne sont pas reçues correctement ou encore si l'ACK n'est pas reçu correctement, on suppose qu'une collision s'est produite, et la trame est retransmise.

Lorsque la station source transmet ses données, les autres stations mettent à jour leur NAV, en incluant le temps de transmission de la trame de données, le SIFS et l'ACK.

La figure 22.2 illustre le processus de transmission des trames à partir d'un émetteur. Ce processus reprend les différentes attentes que nous venons de détailler.

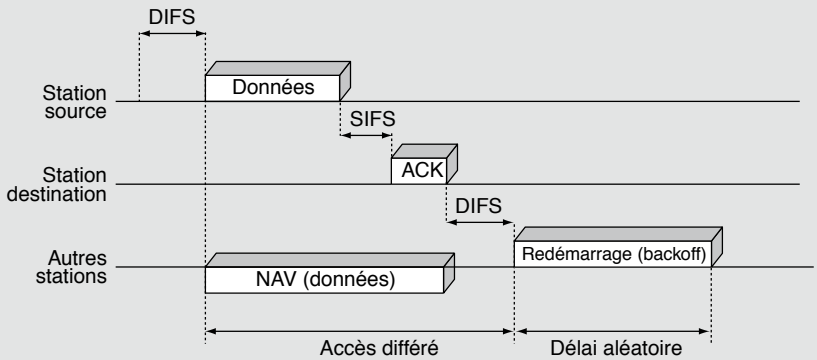


Figure 22.2

Processus de transmission des trames

L'algorithme de back-off permet de résoudre le problème de l'accès au support lorsque plusieurs stations veulent transmettre des données en même temps. Dans Wi-Fi, le temps est découpé en tranches, qui correspondent chacune à un timeslot. Contrairement au timeslot utilisé dans l'aloha, qui correspond à la durée minimale de transmission d'une trame, le timeslot utilisé dans Wi-Fi est un peu plus petit que la durée de transmission minimale d'une trame. Il est utilisé pour définir les intervalles IFS ainsi que les temporisateurs pour les différentes stations. Son implémentation est différente pour chaque couche physique.

Initialement, une station calcule la valeur d'un temporisateur, appelé timer de back-off, compris entre 0 et 7 et correspondant à un certain nombre de timeslots. Lorsque le support est libre, les stations décrémentent leur temporisateur jusqu'à ce que le support soit occupé ou que le temporisateur atteigne la valeur 0. Si le temporisateur n'a pas atteint la valeur 0 et que le support soit de nouveau occupé, la station bloque le temporisateur. Dès que le temporisateur atteint la valeur 0, la station transmet sa trame. Si deux ou plusieurs stations atteignent la valeur 0 au même instant, une collision se produit, et chaque station doit générer un nouveau temporisateur, compris cette fois entre 0 et 15.

Pour chaque tentative de retransmission, le temporisateur croît de la façon suivante :

$$[2^{2+i} \times \text{ranf}()] \times \text{timeslot}$$

i correspond au nombre de tentatives consécutives d'une station pour l'envoi d'une trame, et ranf() à une variable aléatoire uniforme comprise entre 0 et 1.

Grâce à cet algorithme, les stations ont la même probabilité d'accéder au support. Son seul inconvénient est de ne pas garantir un délai minimal et donc de compliquer la prise en charge d'applications temps réel telles que la voix ou la vidéo.

Fonctionnalités

Le passage d'une cellule à une autre sans interruption de la communication n'a pas été prévu dans les premières versions, si bien que le handover a dû être introduit dans les nouvelles.

De même, la sécurité a été renforcée pour éviter qu'un client ne prenne la place d'un autre ou qu'il n'écoute les communications d'autres utilisateurs.

Handovers

Dans les réseaux sans fil, les handovers interviennent lorsqu'un terminal souhaite se déplacer d'une cellule à une autre sans interrompre sa communication. Ils se font à peu près de la même manière que dans la téléphonie mobile, à quelques nuances près. Dans les réseaux sans fil, le handover s'effectue entre deux transmissions de données et non pas au milieu d'un dialogue.

Le standard ne fournit pas de mécanisme de handover à part entière mais définit certaines règles, telles que la synchronisation, l'écoute passive et active ou encore l'association et la réassociation, qui permettent aux stations de choisir le point d'accès auquel elles veulent s'associer.

Lorsque les terminaux se déplacent, c'est-à-dire lorsqu'ils changent de cellule ou qu'ils sont en mode d'économie d'énergie, ils doivent rester synchronisés pour pouvoir communiquer. Au niveau d'un BSS, les stations synchronisent leur horloge avec l'horloge du point d'accès. Pour conserver la synchronisation, le point d'accès envoie périodiquement

des trames balises, ou Beacon Frames, qui contiennent la valeur d'horloge du point d'accès. Lors de la réception de ces trames, les stations mettent à jour leur horloge pour rester synchronisés avec le point d'accès.

Quand un terminal veut accéder — après allumage ou retour d'un mode veille ou d'un handover — à un BSS ou à un ESS contrôlé par un ou plusieurs point d'accès, il choisit un point d'accès, auquel il s'associe, selon un certain nombre de critères, tels que la puissance du signal, le taux d'erreur des paquets ou la charge du réseau. Si la puissance du signal du point d'accès est trop faible, la station cherche un autre point d'accès plus approprié.

Cette recherche du meilleur point d'accès passe par l'écoute du support. Cette dernière peut se faire de deux manières différentes, passive ou active, selon des critères tels que les performances ou la consommation d'énergie :

- Écoute passive. La station attend de recevoir une trame balise venant du point d'accès.
- Écoute active. Lorsque la station a trouvé le point d'accès le plus approprié, elle lui envoie une requête d'association par l'intermédiaire d'une trame appelée Probe Request Frame et attend que le point d'accès lui réponde pour s'associer.

Dès que le terminal est accepté par le point d'accès, il se règle sur le canal radio le plus approprié. Périodiquement, le terminal surveille tous les canaux du réseau pour évaluer si un point d'accès possède de meilleures performances. Si tel est le cas, il s'associe à ce nouveau point d'accès et règle son canal radio en conséquence.

Les réassociations s'effectuent lorsqu'une station se déplace physiquement par rapport à son point d'accès d'origine, entraînant une diminution de la puissance du signal. Dans d'autres cas, les réassociations sont dues à des changements de caractéristiques de l'environnement radio ou à cause d'un trafic réseau trop élevé sur le point d'accès d'origine. Dans ce cas, le standard fournit une fonction d'équilibrage de charge, ou Load Balancing, qui permet de répartir la charge de manière efficace au sein du BSS ou de l'ESS et ainsi d'éviter les réassociations.

Sécurité

Dans les réseaux sans fil, le support est partagé. Tout ce qui est transmis et envoyé peut donc être intercepté. Pour permettre aux réseaux sans fil d'avoir un trafic aussi sécurisé que dans les réseaux fixes, le groupe de travail 802.11 a mis au point le protocole WEP (Wired Equivalent Privacy), dont les mécanismes s'appuient sur le chiffrage des données et l'authentification des stations.

D'après le standard, WEP est optionnel, et les terminaux ainsi que les points d'accès ne sont pas obligés de l'implémenter. Comme nous allons le voir, la sécurité n'est pas garantie avec le WEP, et un attaquant peut casser les clés de chiffrement sans trop de difficulté. La Wi-Fi Alliance, l'organisme en charge de la promotion de Wi-Fi, a développé un deuxième mode de protection, le WPA (Wi-Fi Protected Access), qui résout ces problèmes, au moins pour quelques années. Enfin, le groupe de travail 802 .11 a créé un sous-groupe spécifique, IEEE 802.11i, qui propose une solution pérenne, normalisée en juin 2004 : le WPA2.

Avant de présenter ces trois protocoles de sécurité, rappelons deux règles de protection élémentaires :

- Cacher le nom du réseau, ou SSID, de telle sorte qu'un utilisateur ne voie pas le réseau et ne puisse donc pas s'y connecter. Cette mesure de sécurité n'est hélas que provisoire. Si un attaquant écoute le réseau suffisamment longtemps, il finira bien par voir passer le nom du réseau puisqu'un utilisateur qui souhaite se connecter doit donner ce SSID.
- N'autoriser que les communications contrôlées par une liste d'adresses MAC, ou ACL (Access Control List). Cela permet de ne fournir l'accès qu'aux stations dont l'adresse MAC est spécifiée dans la liste.

WEP

Comme expliqué précédemment, la solution de gestion de la confidentialité et de l'authentification commercialisée avec les équipements Wi-Fi est le WEP.

Les trames transmises sur les réseaux sans fil sont protégées par un chiffrement. Seul un déchiffrement avec la bonne clé WEP statique, partagée entre le terminal et le réseau, est autorisé. Cette clé est obtenue par la concaténation d'une clé secrète de 40 ou 104 bits et d'un vecteur d'initialisation IV (Initialization Vector) de 24 bits. Celui-ci est changé dynamiquement pour chaque trame. La taille de la clé finale est de 64 ou 128 bits.

À partir de la clé obtenue, l'algorithme RC4 (Ron's Code 4) réalise le chiffrement des données en mode flux (*stream cipher*). Une clé RC4 a une longueur comprise entre 8 et 2 048 bits. La clé est placée dans un générateur de nombres pseudo-aléatoires, ou PRNG (Pseudo-Random Number Generator), issu des laboratoires RSA (Rivest, Shamir, Adleman). Ce générateur détermine une séquence d'octets pseudo-aléatoire, ou keystream. Cette série d'octets, appelée Ksi, est utilisée pour chiffrer un message en clair (Mi) à l'aide d'un classique protocole de Vernam, réalisant un ou exclusif XOR entre Ksi et Mi :

$$Ci = Ksi \oplus Mi.$$

Le message Mi est composé des données qui sont concaténées à leur ICV (Integrity Check Value). La trame chiffrée est ensuite envoyée avec son IV en clair. L'IV est un index qui sert à retrouver le keystream et donc de déchiffrer les données.

Le processus de chiffrement WEP est illustré à la figure 22.3.

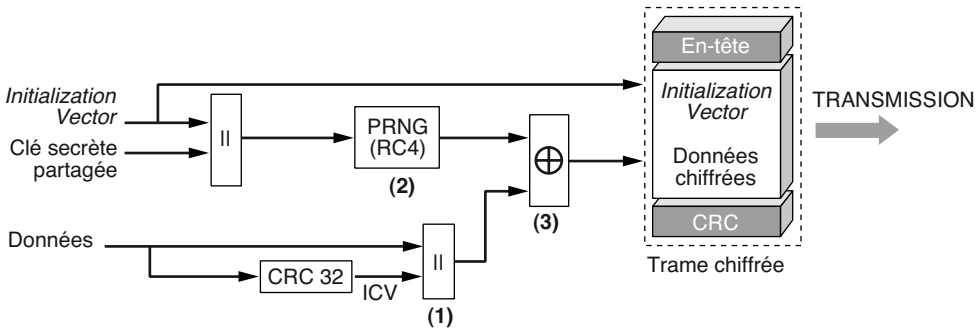


Figure 22.3

Chiffrement d'un paquet WEP

Cette méthode, qui utilise, dans Wi-Fi, des clés de 64 bits ou de 128 bits est facilement cassable en raison du vecteur d'initialisation de 24 bits, aisé à identifier, et de la clé d'une longueur de 40 ou 104 bits. Pour casser une clé de 104 bits, il suffit de récupérer au grand maximum un million de trames chiffrées. Le cassage de la clé ne demande que quelques minutes sur un serveur classique. Des techniques consistant à forcer le point d'accès à répondre permettent de récupérer le million de paquets nécessaires, souvent beaucoup moins, en quelques minutes. Il est donc fortement déconseillé d'utiliser cette solution de protection.

Deux techniques d'authentification sont associées au WEP :

- Open System Authentication
- Shared Key Authentication

Dans la première, qui est le système d'authentification par défaut, l'authentification est explicite. Un terminal peut donc s'associer avec n'importe quel point d'accès et écouter toutes les données qui transitent au sein du BSS. La seconde est nettement meilleure car elle utilise un mécanisme de clé secrète partagée.

Le mécanisme Shared Key Authentication se déroule en quatre étapes :

1. Une station voulant s'associer avec un point d'accès lui envoie une trame d'authentification.

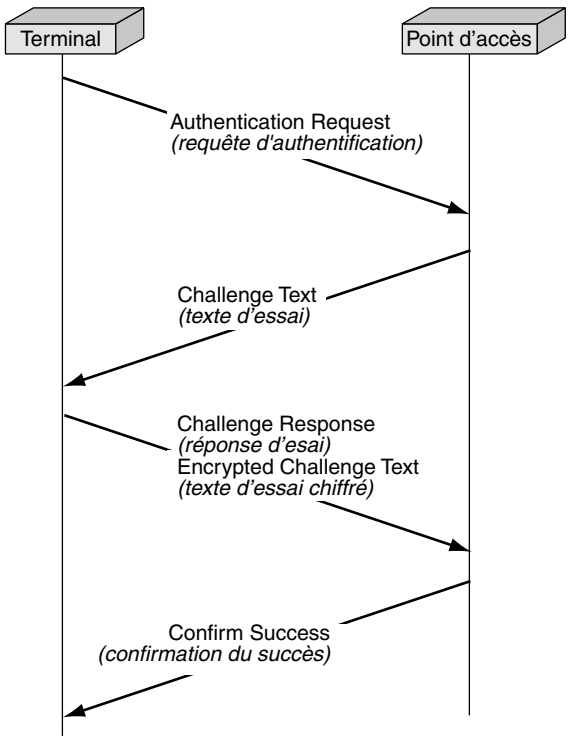


Figure 22.4

Fonctionnement du mécanisme Shared Key Authentication

2. Lorsque le point d'accès reçoit cette trame, il envoie à la station une trame contenant 128 bits d'un texte aléatoire généré par l'algorithme WEP.
3. Après avoir reçu la trame contenant le texte, la station la copie dans une trame d'authentification et la chiffre avec la clé secrète partagée avant d'envoyer le tout au point d'accès.
4. Le point d'accès déchiffre le texte chiffré à l'aide de la même clé secrète partagée et le compare avec celui qui a été envoyé plus tôt. Si le texte est identique, le point d'accès lui confirme son authentification, sinon il envoie une trame d'authentification négative.

La figure 22.4 illustre ces étapes.

Comme la clé utilisée pour cette authentification est la même que pour le chiffrement, à partir du moment où la clé a été cassée, l'authentification est également cassée.

Une amélioration importante de ces mécanismes a été apportée par l'introduction d'une authentification forte avec le protocole IEEE 802.1x. Nous décrivons ce dernier en détail un peu plus loin dans ce chapitre.

WPA et IEEE 802.11i

Nous avons souligné les faiblesses du protocole WEP. Le groupe de travail IEEE 802.11i a finalisé en juin 2004 une architecture destinée à combler ces lacunes. Ce standard est arrivé sur le marché en 2005 sous le nom de WPA2. Entre le moment où le WEP a été déconseillé et l'arrivée de WPA2, la Wi-Fi Alliance a soutenu la recommandation intermédiaire WPA. Fondé sur un sous-ensemble de 802.11i, WPA utilise le matériel existant (AP, carte réseau sans fil). Pour sa part, le WPA2 n'est pas compatible avec la première génération des équipements Wi-Fi. La différence essentielle entre WPA et WPA2 tient au protocole de chiffrement utilisé : RC4 pour WPA et AES pour WPA2.

Les apports de la norme IEEE 802.11i peuvent être classés en trois catégories :

- définition de multiples protocoles de sécurité radio ;
- éléments d'information permettant de choisir l'un d'entre eux ;
- nouvelle méthode de distribution des clés.

Le standard utilise 802.1x pour l'authentification et le calcul d'une clé maître, nommée PMK (Pairwise Master Key). En mode ad-hoc, cette clé est appelée PSK (Pre-Shared Key) et est distribuée manuellement.

Un RSN (Robust Security Network) 802.11i, ou réseau sécurisé, utilise donc 802.1x pour les services d'authentification et de gestion des clés. Le contrôle d'accès s'appuie sur une authentification forte des couches supérieures. Le RSN doit garantir sécurité et mobilité, intégrité et confidentialité, ainsi que passage à l'échelle et la flexibilité.

Sécurité et authentification

L'architecture sécuritaire doit fournir une authentification du client, indépendamment du fait qu'il se trouve dans son réseau de domiciliation ou dans un réseau étranger.

Une architecture avec serveur d'authentification centralisé de type RADIUS (Remote Authentication Dial-In User Server) peut satisfaire à cette exigence. Le client n'a plus à se préoccuper du point d'accès auquel il est associé.

Dans l'architecture 802.1x, un réseau comporte trois éléments en communication : un « supplicant », qui est la station 802.1x demandant à être authentifiée, un « authenticator », le point d'accès, et un serveur d'authentification, ou AS (Authentication Server), le plus souvent RADIUS.

Chaque authenticator partage un secret avec le serveur RADIUS avec lequel il communique. Ce secret est utilisé pour calculer un résumé HMAC-MD5 sur les paquets RADIUS échangés. Chaque paquet RADIUS contient un champ Request Authenticator, qui est un résumé HMAC-MD5 du paquet, calculé avec ce secret. Ce champ est inséré par le serveur RADIUS et vérifié par le point d'accès. Dans l'autre sens de communication, le serveur RADIUS vérifie l'attribut EAP Authenticator présent avec l'attribut EAP Message**.** Ces deux attributs offrent la possibilité d'une authentification mutuelle par paquet et préservent l'intégrité de la communication entre le serveur RADIUS et le point d'accès.

Puisqu'il est assez facile pour un attaquant équipé d'un outil de réception convenable d'écouter le trafic entre les stations sur le lien sans fil, l'architecture de sécurité proposée vise à fournir des garanties de confidentialité forte. Elle définit en outre un mécanisme de distribution dynamique de clés.

Passage à l'échelle et flexibilité

L'architecture 802.11i est extensible quant au nombre d'utilisateurs pris en charge et à la mobilité. Un utilisateur se déplaçant d'un point d'accès à un autre pourra être réauthentifié rapidement et de façon sécurisée.

De plus, pour répondre aux besoins de déploiement des réseaux sans fil dans les entreprises et les lieux publics, cette architecture de sécurité se veut flexible, afin d'en faciliter l'administration et de prendre en compte l'environnement de déploiement existant.

En séparant l'authenticator du processus d'authentification lui-même, le RSN permet le passage à l'échelle du nombre de points d'accès. La flexibilité est apportée par le fait que le message optionnel EAPoL-Key peut être désactivé pour un déploiement particulier, où la confidentialité des données n'est pas nécessaire.

Le modèle 802.11i précise comment le RSN interagit avec 802.1x. Deux types de protocoles assurent la sécurité au niveau MAC :

- TKIP (Temporal Key Integrity Protocol)
- CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol)

Un TSN (Transition Security Network) supporte les architectures pré-RSN, en particulier les mécanismes suivants hérités de la norme 802.11 :

- Open Authentication
- Shared Key Authentication
- WEP

Un réseau RSN doit supporter le protocole CCMP. Un TSN peut cependant assurer la transition avec les réseaux antérieurs en implémentant le protocole TKIP.

La figure 22.5 illustre les différents niveaux de sécurité qui doivent être pris en charge pour avoir une architecture sécurisée globale.

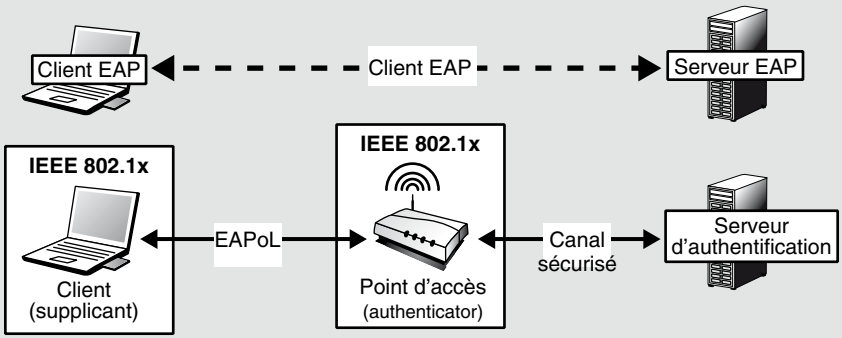


Figure 22.5

Niveaux de sécurité dans l'architecture 802.1x

L'authenticator (le point d'accès) et le serveur d'authentification (AS) réalisent une authentification mutuelle et établissent un canal sécurisé. Le modèle 802.11i ne décrivant pas les méthodes utilisées pour mener à bien cette opération, des protocoles tels que RADIUS, IPsec ou TLS/SSL peuvent être mis en œuvre.

Le client 802.1x, ou supplicant, et le serveur d'authentification s'authentifient mutuellement à l'aide du protocole EAP (Extensible Authentication Protocol) et gênèrent une clé maître PMK. Les éléments de cette procédure sont transportés par le canal sécurisé, dont les paramètres cryptographiques doivent être différents pour chaque client 802.1x. La clé PMK est partagée entre le client 802.1x et le point d'accès. Ceux-ci utilisent un protocole à quatre passes, ou 4-ways handshake, et des messages EAPoL-Key pour réaliser les opérations suivantes :

1. Confirmation de l'existence de la PMK.
2. Confirmation de la mise en service de la PMK.
3. Calcul de la clé PTK (Pairwise Transient Key) à partir de la PMK.
4. Mise en place des clés de chiffrement et d'intégrité des trames 802.11.
5. Confirmation de la mise en fonction des clés 802.11.

Ce processus est illustré à la figure 22.6.

Une clé GTK (Group Transient Key), transmise *via* des paquets EAPoL-Key depuis le point d'accès vers le client 802.1x, permet à ce dernier d'échanger des messages en mode broadcast et optionnellement en mode unicast. Dans le cas du mode dit Pre-Shared Key, la clé PMK est préinstallée entre le client 802.1x et le point d'accès.

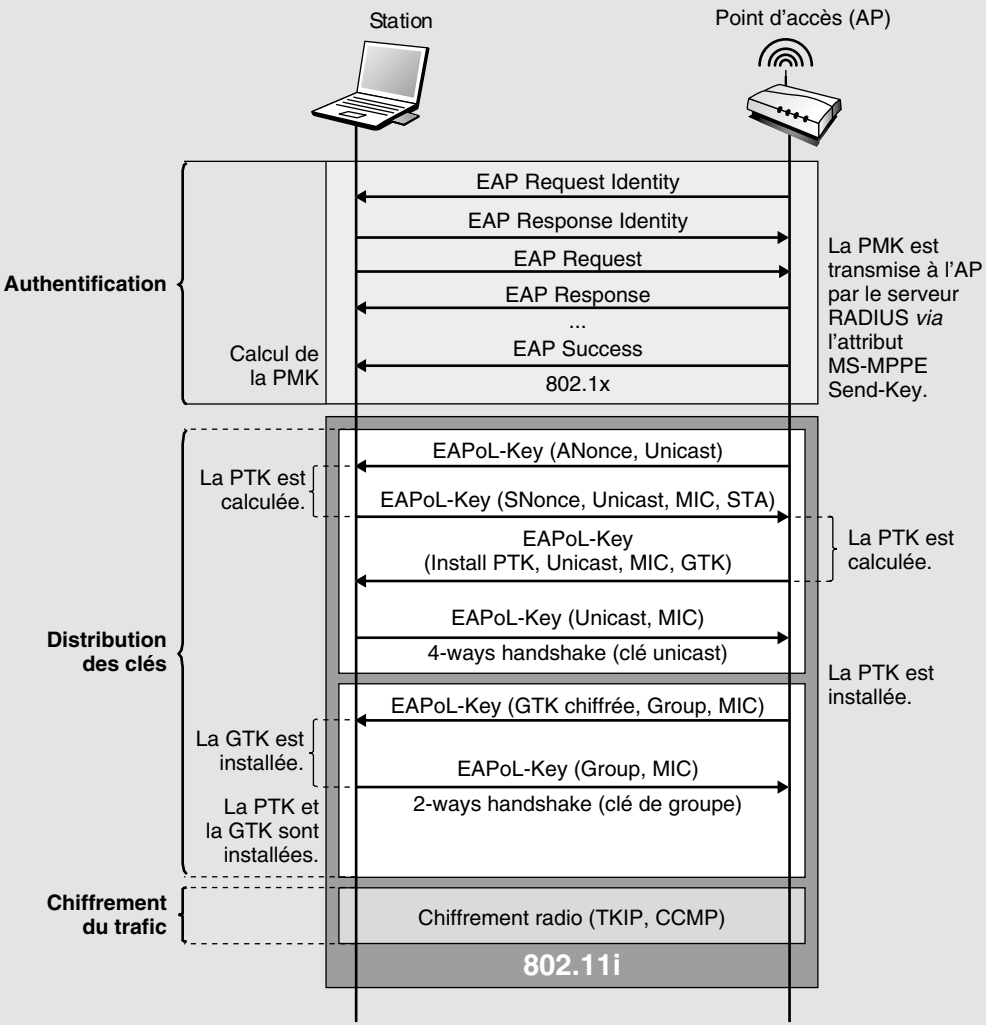


Figure 22.6

Fonctionnement du protocole à quatre passes 802.11i

Négociation de la politique de sécurité

Un point d'accès diffuse dans ses trames beacon ou probe des éléments d'information, ou IE (Information Element), afin de notifier au client 802.1x les indications suivantes :

- liste des infrastructures d'authentification supportées (typiquement 802.1x) ;
- liste des protocoles de sécurité disponibles (TKIP, CCMP, etc.) ;
- méthode de chiffrement pour la distribution d'une clé de groupe (GTK).

Une station 802.11 notifie son choix par un élément d'information inséré dans sa demande d'association. Cette démarche est illustrée à la figure 22.7.

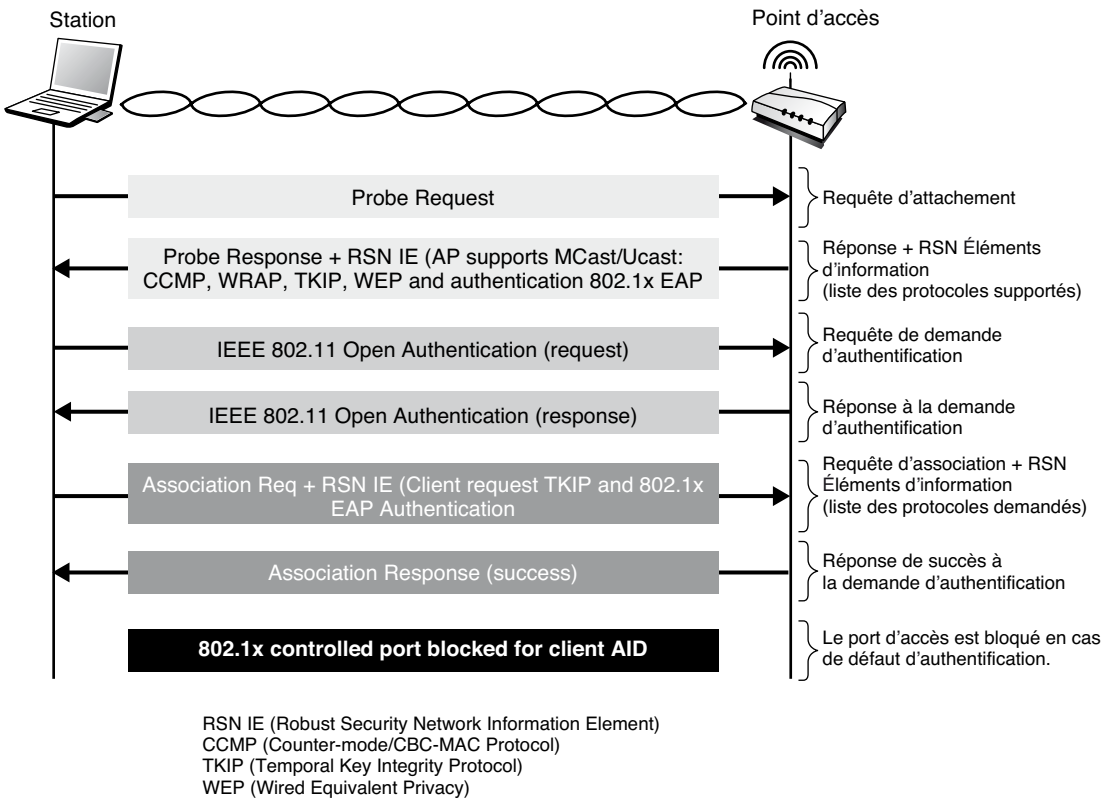


Figure 22.7

Négociation de la politique de sécurité

La sécurité des réseaux Wi-Fi a démarré sous de mauvais auspices. Aujourd'hui, les problèmes de départ sont résolus, et même en dehors de WPA et WPA2 (IEEE 802.11i) il existe de nombreuses solutions très fiables, comme l'utilisation de réseaux privés virtuels ou de technologies fondées sur la carte à puce.

Économie d'énergie

Les terminaux sans fil peuvent être fixes ou mobiles. Le problème principal des terminaux mobiles concerne leur batterie, qui n'a généralement que peu d'autonomie. Pour augmenter le temps d'activité des terminaux, le standard IEEE 802.11 prévoit un mode d'économie d'énergie. Plus précisément, il existe deux modes de fonctionnement d'un terminal :

- Continuous Aware Mode
- Power Save Polling Mode

Le premier correspond au fonctionnement par défaut, dans lequel la station est tout le temps allumée et écoute constamment le support. Le second permet une économie d'énergie. Dans ce cas, le point d'accès tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie et stocke les données qui leur sont adressées. Les stations qui sont en veille s'activent à des périodes de temps régulières pour recevoir une trame particulière, la trame TIM (Traffic Information Map), envoyée par le point d'accès.

Entre les trames TIM, les terminaux retournent en mode veille. Toutes les stations partagent le même intervalle de temps pour recevoir les trames TIM, de sorte à s'activer au même moment pour les recevoir. Les trames TIM font savoir aux terminaux mobiles si elles ont ou non des données stockées dans le point d'accès. Lorsqu'un terminal s'active pour recevoir une trame TIM et s'aperçoit que le point d'accès contient des données qui lui sont destinées, il envoie au point d'accès une requête, appelée Polling Request Frame, pour mettre en place le transfert des données. Une fois le transfert terminé, il retourne en mode veille jusqu'à réception de la prochaine trame TIM.

Pour des trafics de type broadcast ou multicast, le point d'accès envoie aux terminaux une trame DTIM (Delivery Traffic Information Map).

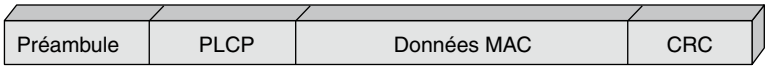
Trames Wi-Fi

Les paquets IP composés dans les terminaux du réseau sans fil doivent être transmis sur le support hertzien. Pour cela, ils doivent être placés dans une trame Ethernet. De plus, pour contrôler et gérer la liaison, il est nécessaire d'avoir des trames spécifiques.

Les trois types de trames disponibles dans Wi-Fi sont les suivantes :

- trame de données, pour la transmission des données utilisateur ;
- trame de contrôle, pour contrôler l'accès au support (RTS, CTS, ACK) ;
- trame de gestion, pour les associations ou les désassociations d'une station avec un point d'accès, ainsi que pour la synchronisation et l'authentification.

Toutes les trames Wi-Fi sont composées de la manière illustrée à la figure 22.8.



CRC (Cyclic Redundancy Check) PLCP (Physical Layer Convergence Protocol)
MAC (Medium Access Control)

Figure 22.8

Structure d'une trame Wi-Fi

Le préambule est dépendant de la couche physique et contient les deux séquences suivantes :

- Synch, de 80 bits alternant 0 et 1, qui est utilisée par le circuit physique pour sélectionner l'antenne à laquelle se raccorder.
- SFD (Start Frame Delimiter), une suite de 16 bits, 0000 1100 1011 1101, utilisée pour définir le début de la trame.

L'en-tête PLCP (Physical Layer Convergence Protocol) contient les informations logiques suivantes utilisées par la couche physique pour décoder la trame :

- Longueur de mot du PLCP_PDU : représente le nombre d'octets que contient le paquet, ce qui permet à la couche physique de détecter correctement la fin du paquet.
- Fanion de signalisation PLCP : contient l'information concernant la vitesse de transmission entre la carte coupleur et le point d'accès.
- Champ d'en-tête du contrôle d'erreur : champ de détection d'erreur CRC sur 16 bits.

La zone MAC transporte le protocole de niveau sous-jacent, comme illustré à la figure 22.9.

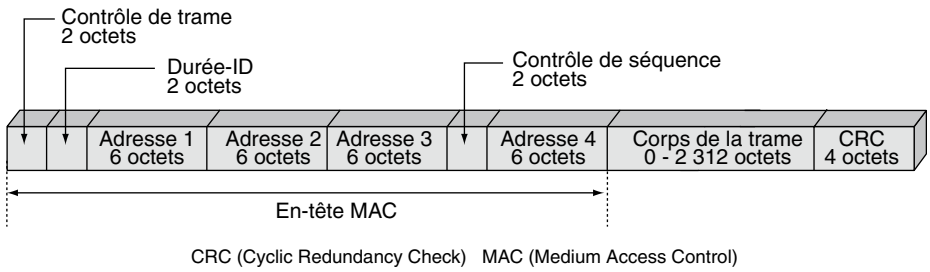


Figure 22.9
Zone MAC

IEEE 802.11a, b et g

Les réseaux Wi-Fi de base proviennent de la normalisation IEEE 802.11b sur la bande des 2,4 GHz. Comme expliqué précédemment, cette norme a pour origine des études effectuées dans le cadre général du groupe 802.11.

La proposition 802.11b s'est imposée comme standard, et plusieurs millions de cartes d'accès Wi-Fi ont été vendues. D'abord déployé dans les campus, les aéroports, les gares et les grandes administrations publiques ou privées, il s'est ensuite imposé dans les réseaux des entreprises pour permettre la connexion de PC portables et d'équipements de types PDA ou Smartphones. Les propositions 802.11a et g ont ensuite pris le relais suivi du 802.11n à partir de 2008 même si la norme officielle est sortie est 2009.

Les réseaux 802.11 travaillent avec des points d'accès dont la vitesse de transmission maximale brute est de 11, 54 et 600 Mbit/s et la portée de quelques dizaines de mètres.

Pour obtenir cette valeur maximale de la porteuse, il faut que le terminal soit assez près du point d'accès, à moins d'une vingtaine de mètres. Il faut donc, au moment de l'ingénierie du réseau, bien calculer le positionnement des différents points d'accès.

Treize fréquences sont disponibles aux États-Unis dans la bande des 2 400 à 2 483,5 MHz, donc d'une largeur de 83,5 MHz, et quatorze en Europe. Un point d'accès ne peut utiliser que trois porteuses au maximum, car l'émission demande une bande passante de 20 MHz qui s'étale en fait sur 25 MHz. Ces fréquences notées de 1 à 13 permettent d'utiliser comme porteuse les fréquences 1, 6 et 11 aux États-Unis (où seules les onze premières fréquences sont disponibles) et 1, 7, 13 en France.

Les réseaux 802.11b et 802.11g sont compatibles dans le sens ascendant. Une carte 802.11g peut donc se connecter à un réseau 802.11b à la vitesse de 11 Mbit/s, mais l'inverse est impossible. En revanche, les fréquences des réseaux 802.11b/g et 802.11a étant totalement différentes, il n'y a aucune compatibilité entre eux. Si l'équipement qui souhaite accéder aux deux réseaux comporte deux cartes d'accès, les fréquences peuvent toutefois se superposer.

Pour la partie physique, les propositions suivantes ont été retenues pour les réseaux 802.11a :

- Fréquence de 5 GHz dans la bande de fréquences sans licence U-NII (Unlicensed-National Information Infrastructure), qui ne nécessite pas de licence d'utilisation.
- Modulation OFDM (Orthogonal Frequency Division Multiplexing) avec 52 porteuses, autorisant d'excellentes performances en cas de chemins multiples.
- Huit débits, échelonnés de 6 à 54 Mbit/s. Le débit sélectionné par la carte d'accès dépend de la puissance de réception.

La distance maximale entre la carte et le point d'accès peut dépasser 100 m, mais la chute du débit de la communication est fortement liée à la distance. Pour le débit de 54 Mbit/s, la station mobile contenant la carte Wi-Fi ne peut s'éloigner que de quelques mètres du point d'accès. Au-delà, le débit chute très vite pour être approximativement équivalent à celui qui serait obtenu avec la norme 802.11b à 100 m de distance.

En réalisant de petites cellules, de façon que les fréquences soient fortement réutilisables, un réseau 802.11a permet à plusieurs dizaines de clients par 100 m2 de se partager entre 100 et 200 Mbit/s. Un tel réseau est dès lors capable de prendre en charge des flux vidéo de bonne qualité.

Les niveaux supérieurs au niveau MAC, c'est-à-dire à la couche gérant l'algorithme d'accès CSMA/CD, correspondent à ceux que l'on rencontre dans les réseaux Ethernet.

IEEE 802.11n

Avec les pré-produits IEEE 802.11n, le débit maximal a atteint fin 2007 les 108 Mbit/s, c'est-à-dire le double des standards IEEE 802.11a et 802.11g. Les réseaux 802.11n proposent un débit brut potentiel de 600 Mbit/s. En fait, le débit réel est très inférieur et est de l'ordre de 100 Mbit/s dans le meilleur des cas.

L'objectif du standard IEEE 802.11n est triple :

- Apporter des modifications aux niveaux MAC et PHY de telle sorte que le débit brut en crête dépasse les 100 Mbit/s pour atteindre 600 Mbit/s. Pour cela, la technologie MIMO est mise en œuvre.
- Améliorer très fortement le débit utile du système au niveau de l'application afin d'obtenir une centaine de mégabits par seconde.
- Rester compatible avec IEEE 802.11a et 802.11g.

On comprend bien les premier et dernier objectifs. Le second n'est pas moins clair si l'on se souvient des débits réels désastreux des premiers réseaux Wi-Fi : 5 à 6 Mbit/s au mieux dans le cas de 802.11b et quelque 20 Mbit/s pour 802.11a et 802.11g. L'objectif du nouveau standard est de proposer une vitesse de transfert effective de l'ordre de 100 Mbit/s.

IEEE 802.11n marque un tournant dans la compatibilité des produits puisqu'elle inclut le standard IEEE 802.11i pour la sécurité et la confidentialité du transport des données sur l'interface radio. Ce dernier standard n'étant pas compatible avec les deux premières générations, notamment avec l'utilisation d'AES, l'augmentation forte de la vitesse est l'occasion d'inciter les utilisateurs à changer complètement leur infrastructure de réseau sans fil.

Le standard IEEE 802.11e, que nous détaillons à l'annexe P, permettant de proposer une qualité de service autour d'une technologie de type DiffServ, est également inclus dans 802.11n. Cette intégration permet de donner des priorités aux différents flux qui traversent le réseau sans fil.

La norme IEEE 802.11n permet en natif de gérer la mobilité en intégrant le standard IEEE 802.11f. D'un réseau sans fil, on peut passer à un autre réseau sans fil, même si la gestion de la mobilité ne se fait qu'à des vitesses faibles, de type piéton.

MIMO

La technologie MIMO (Multiple Input Multiple Output) n'est pas nouvelle, mais elle n'arrive sur le marché qu'en cette fin de la première décennie des années 2000 du fait d'une implémentation très complexe. MIMO a pour objectif de transporter plusieurs flux en parallèle sur des antennes différentes mais en utilisant la même fréquence.

L'idée est de connecter plusieurs antennes sur l'émetteur, lesquelles émettent des flux différents sur la même fréquence. Grâce aux propriétés du multichemin que l'on trouve dans les environnements avec obstacles, les signaux arrivent à des instants différents au récepteur. Si le récepteur est assez puissant, il est capable de déchiffrer les suites binaires qui arrivent à des instants différents. Il faut noter que la technique MIMO n'est satisfaisante que dans les environnements avec obstacles et que l'utiliser en dehors des bâtiments réduit fortement son débit.

Le schéma de fonctionnement de MIMO est illustré à la figure 22.10, en supposant *n* émetteurs et *n* récepteurs. MIMO peut fonctionner avec une seule antenne de réception, mais avec le risque de ne pas récupérer tous les signaux. Dans cette figure, la même suite binaire est émise sur l'ensemble des antennes. L'objectif est d'augmenter la qualité de la transmission puisque le récepteur reçoit plusieurs fois le même bit et choisit la valeur la plus fortement reçue. Il faut dans ce cas avoir un nombre impair d'antennes pour être sûr de départager les éléments binaires reçus.

La diversité exprime qu'au lieu d'augmenter la qualité en augmentant le nombre de fois où le même bit est transmis, on peut augmenter le débit en transmettant des éléments binaires distincts. Cette deuxième solution est illustrée à la figure 22.11.

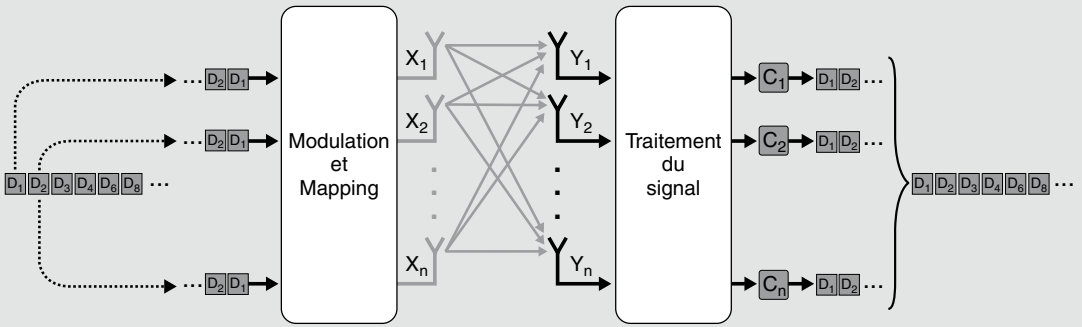


Figure 22.10

La technique MIMO avec augmentation de la qualité

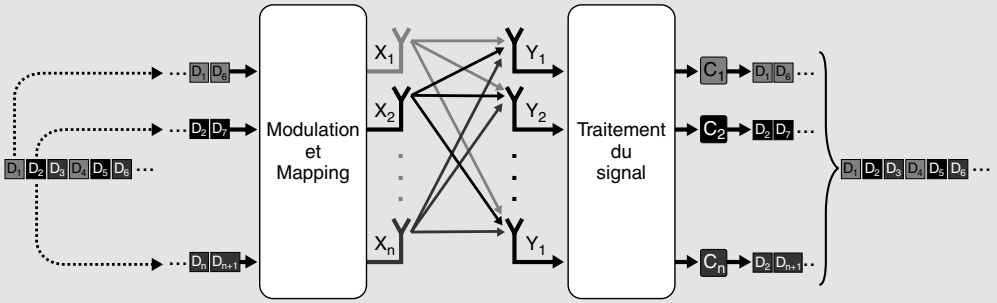


Figure 22.11

La technique MIMO

IEEE 802.11ac

IEEE 802.11ac est une version de Wi-Fi sur laquelle reposent beaucoup d'espoirs. C'est un Wi-Fi classique, mais avec des débits de plusieurs gigabits par seconde. Deux solutions sont en discussion et devraient se compléter. La première, assez simple, consiste à augmenter la largeur du canal de transmission en utilisant beaucoup plus la bande des 5 GHz. La seconde solution concerne la virtualisation des antennes. Cette technique consiste à permettre l'émission de plusieurs communications sur une même fréquence, mais dans des directions distinctes. Il y a un multiplexage dans l'espace d'où le nom de la technique SDMA (Space Division Multi ple Access). La figure 22.12 illustre cette technologie.

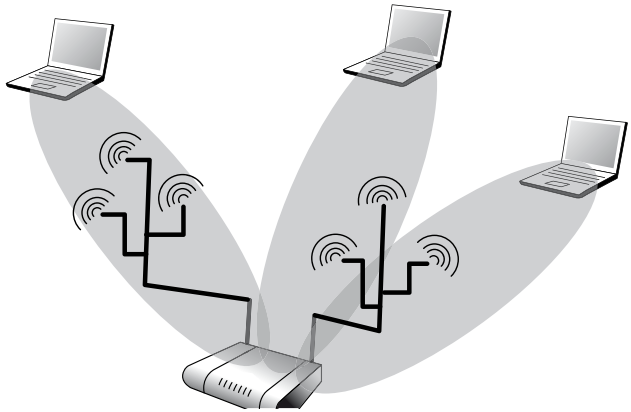


Figure 22.12
Le SDMA

La technologie SDMA, également connue sous le nom de MU-MIMO (Multiple MIMO), permet de connecter plusieurs utilisateurs simultanément sur la même fréquence sans interférences. Pour cela, on utilise des techniques de *beamforming*, qui permettent de diriger les signaux dans une direction déterminée, donnant ainsi naissance à des antennes directives. Les antennes virtuelles permettent de générer plusieurs antennes directives simultanément. La technique utilisée dans l'IEEE 802.11ac est encore appelée PU2RC (Per-User Unitary Rate Control).

Cette technologie permet de multiplier le débit par le nombre d'antennes virtuelles. Sur l'exemple de la figure 22.12, les deux antennes physiques donnent chacune naissance à trois antennes virtuelles, soit un total de six antennes virtuelles. Ces six antennes permettent de mettre en place six communications simultanées. Avec ces six antennes, on peut également réaliser trois communications MIMO 2x2 (deux antennes virtuelles communiquant avec deux antennes d'une machine distante). On aurait tout aussi bien pu avoir trois communications simultanées : une communication MIMO 3x3, une communication MIMO 2x2 et une communication simple.

Le débit crête atteint 250 Mbit/s par antenne virtuelle. Avec quatre antennes physiques portant chacune trois antennes virtuelles, nous obtenons douze antennes virtuelles. Le débit total est donc de 3 Gbit/s. Si, en plus, les bandes sont plus larges, disons 80 MHz à la place de 20 MHz, on peut dépasser les 12 Gbit/s.

Ces valeurs du nombre d'antennes virtuelles ne sont pour un avenir proche. Le groupe IEEE 802.11ac, avec 250 Mbit/s par antenne et un MIMO à deux antennes par client, revendique 500 Mbit/s par terminal. Avec quatre antennes physiques, on atteint 2 Gbit/s. Ces valeurs sont celles que l'on devrait pouvoir obtenir en 2013, sachant que la norme devrait être finalisée en décembre 2012. Pour obtenir des largueurs de bande allant jusqu'à 80 GHz, les bandes de fréquences devront se situer dans les bandes libres des 5 Ghz.

IEEE 802.11af

La technique IEEE 802.11af s'attaque à une solution totalement différente pour monter en débit : l'utilisation de la radio cognitive (*voir les chapitres 10 et 19*). Elle consiste à réutiliser les bandes de fréquences qui ne sont pas utilisées à un instant *t*. Les mesures qui ont été faites récemment montrent que les fréquences, en dépit de leur rareté et de leur prix, sont sous-utilisées, souvent en dessous de 10 % entre 0 et 20 GHz.

Les seules bandes fortement utilisées sont celles des opérateurs de télécommunications qui, grâce aux techniques TDMA et CDMA, présentent d'excellents taux. Les bandes réservées à la télévision, situées en-dessous du gigahertz, et pour cette raison particulièrement attractives pour les opérateurs, pourraient grâce à elles voir leurs points d'accès atteindre des portées de plusieurs centaines de mètres. De telles portées démontrent au passage que Wi-Fi pourrait s'attaquer aux clients WiMAX et 4G.

Le standard WiFi IEEE 802.11af, à ne pas confondre avec IEEE 802.3af, ou PoE (Power over Ethernet), est appelé TVWS (TV White Space). L'expression « espace blanc » (*white space*) renvoie précisément aux fréquences qui ne sont pas utilisées par les canaux de télévisions hertziennes. La largeur de bande utilisable en radio cognitive est de plusieurs dizaines de canaux de télévisions numériques. Les débits atteints peuvent être colossaux.

Une question importante concerne la façon dont sera utilisée cette radio cognitive. Sera-t-elle sauvage ou régulée ? En d'autres termes, les fréquences libres seront-elles utilisées en force (sans toutefois gêner le canal primaire si celui-ci émet), ou faudra-t-il une discipline commune entre le primaire et le secondaire ? Et pour cela, les opérateurs de télévision se mettront-ils d'accord avec les utilisateurs de 802.11af ? Des normalisations sont en cours dans différents groupes de travail, comme l'IEEE P1900, pour proposer des solutions acceptables par les deux parties.

Au niveau physique, la méthode utilisée dans l'IEEE 802.11af est de type FSS (Fixed Subcarrier Spacing) OFDM. Les canaux utilisés dans l'OFDM peuvent être contigus ou non, c'est-à-dire appartenir à des canaux de télévision qui se trouvent l'un à côté de l'autre ou au contraire séparés par des canaux de télévision actifs.

Un canal contient 64 porteuses. Jusqu'à 1 024 canaux peuvent être sélectionnés dans la technique continue et jusqu'à 256 en non continu. Le canal est en général de 20 MHz, mais il peut être plus petit, avec 5 ou 10 MHz, ou plus grand, avec 40 ou 80 MHz. Dans ces deux derniers cas, le nombre de porteuses peut être de 128 ou 256. Avec 256 porteuses, le débit devrait atteindre 500 Mbit/s, voire 1 Gbit/s. En utilisant des antennes virtuelles à huit directions en SDMA, le débit total pourrait atteindre en pointe, en additionnant les débits dans les différentes directions, de 4 à 8 Gbit/s.

La technique d'accès au support est la même que dans le Wi-Fi classique. Des classes de service utilisant une technique de type EDCA (Enhanced Distributed Channel Access) d'IEEE 802.11e (*voir l'annexe P*) sont disponibles et correspondent à Background, Best-Effort, Video et Voice. Une cinquième priorité, encore plus haute, est ajoutée pour l'écoute du spectre permettant de déterminer si les canaux sont libres ou utilisés par le primaire.

Qualité de service

La qualité de service est peut-être le problème le plus important des réseaux Wi-Fi, avant même la sécurité. La transmission reposant sur la qualité du lien radio, cette qualité peut se dégrader pour de multiples raisons, comme la présence d'un autre équipement, évoluant dans la même bande de fréquences, celle d'un autre réseau 802.11 ou une distance trop grande entre la station et le point d'accès.

Pour permettre à toutes les stations d'avoir un accès, même minimal, au réseau, IEEE 802.11 incorpore une fonction de variation du débit, appelée Variable Rate Shifting. Cette technique permet de faire varier le débit d'une station selon la qualité de son lien radio. Si, pour une station 802.11b donnée, l'environnement radio se dégrade pour cause d'interférences ou de distance, le débit chute de 11 à 5,5 puis 2 et enfin 1 Mbit/s. Lorsque les interférences disparaissent ou que la station se rapproche du point d'accès, le débit augmente automatiquement. Il en va de même pour les normes IEEE 802.11a, 802.11g et 802.11n.

De ce fait, le débit d'un point d'accès dépend des clients et non de l'antenne. Pour cette raison, il est particulièrement difficile d'assurer une qualité de service dans Wi-Fi.

Nous introduisons ci-après cette fonctionnalité de variation du débit. L'annexe P examine une seconde solution proposée par la norme IEEE 802.11e.

Variable Rate Shifting

Les stations 802.11b 1, 2 et 4 illustrées à la figure 22.13 étant proches du point d'accès, leur débit est de 11 Mbit/s. La station 3, qui est légèrement éloignée, n'a que 5,5 Mbit/s, et la station 5, soumise à des interférences, 1 Mbit/s. La station 4, qui se déplace en s'éloignant du point d'accès, voit son débit chuter.

La capacité de passer d'un débit à un autre augmente la zone de couverture du réseau. Comme le montrent les tableaux 22.1 et 22.2, plus la portée est faible et plus le débit est important. Cela vient du fait que les techniques de transmission, notamment le codage et la modulation, utilisées pour transmettre à faible débit autorisent une propagation du signal bien plus grande et donc une portée plus importante. Les valeurs de ces tableaux sont évidemment théoriques. Tout dépend de l'environnement réel dans lequel se situe le réseau. Le tableau 22.2 n'indique les distances que pour les débits correspondant aux réseaux Wi-Fi à 54 Mbit/s. Si une carte 802.11b se connecte sur un point d'accès 802.11g, les débits de 11, 5,5, 2 et 1 sont également possibles avec les distances indiquées dans le tableau 22.1.

Vitesse (en Mbit/s)	Portée à l'intérieur (en mètre)	Portée à l'extérieur (en mètre)
11	15	50
5,5	20	100
2	25	150
1	30	200

TABLEAU 22.1 • Portée d'un réseau Wi-Fi 802.11b

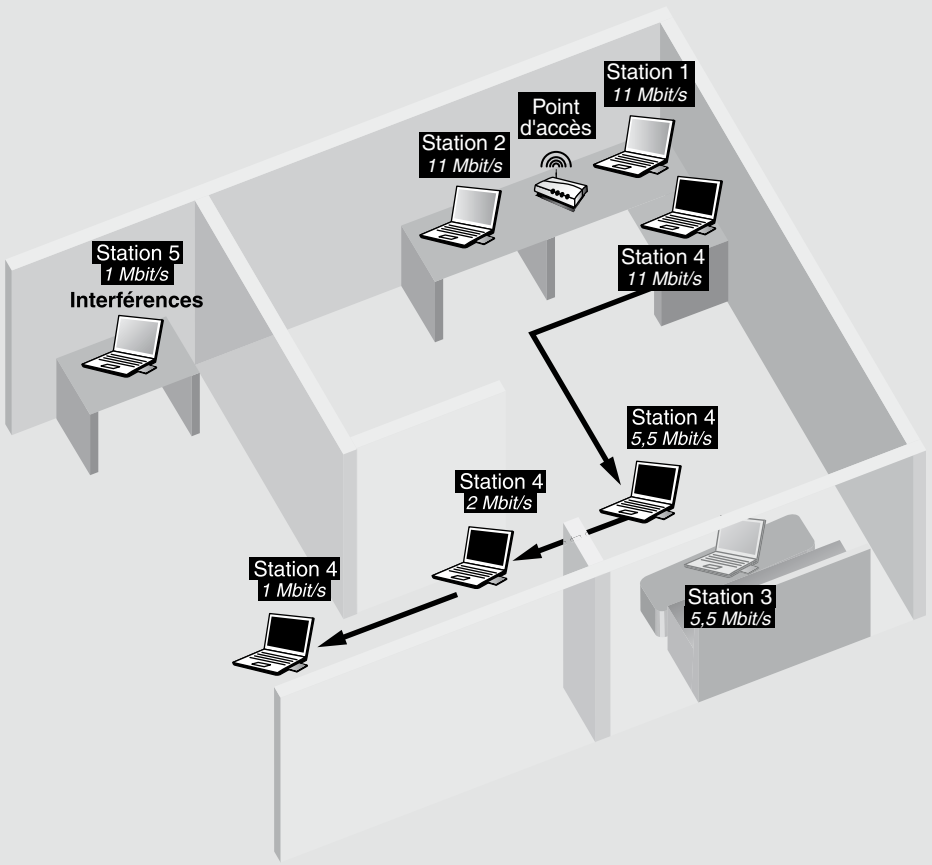


Figure 22.13

Effets sur le débit du Variable Rate Shifting

Débit (en Mbit/s)	Portée (en mètre)
54	3
48	6
36	9
24	12
18	14
12	16
9	18
6	20

TABLEAU 22.2 • Portée d'un réseau 802.11a/g en milieu intérieur

Sensibilité

Le passage d'une vitesse de transmission à une autre se fait en fonction de valeurs seuils, dites de sensibilité. Ces valeurs ne sont pas standardisées et sont laissées au soin des constructeurs. Deux produits différents situés en un même endroit peuvent donc offrir des débits différents. Lorsque la station s'éloigne du point d'accès, sa sensibilité accommode la qualité du lien avec le point d'accès, et le débit est modifié. Pour qu'une transmission s'effectue avec succès, la puissance du signal reçue par l'émetteur doit être supérieure ou égale à la sensibilité du récepteur. Ce mécanisme permet de fiabiliser la transmission en cas de mobilité relative de la station.

Vitesse (en Mbit/s)	CISCO SYSTEMS AIRONET	ORINOCO GOLD/SILVER
11	– 85 dBm	– 82 dBm
5,5	– 89 dBm	– 87 dBm
2	– 91 dBm	– 91 dBm
1	– 94 dBm	– 94 dBm

TABLEAU 22.3 • Sensibilité de deux cartes Wi-Fi 802.11b

Bien que ce mécanisme assure un service minimal, il peut devenir un inconvénient. Si la station qui émet se trouve en périphérie de la cellule ou est soumise à des interférences, son débit est de 1 Mbit/s. Les autres stations doivent donc attendre que l'émission des trames à 1 Mbit/s se termine pour avoir accès au support et transmettre à des vitesses plus importantes. Cette faible capacité de transmission influe fortement sur le débit utile du réseau. D'une valeur de 5 Mbit/s dans un réseau où tous les clients communiquent à un débit théorique de 11 Mbit/s, le débit utile total peut chuter à une valeur inférieure à 1 Mbit/s si des clients éloignés émettent à 1 Mbit/s. On constate qu'une seule station à bas débit fait chuter le débit global utile de toute la cellule.

Un autre facteur défavorable au débit est l'utilisation d'une application consommatrice de bande passante. Prenons l'exemple d'un utilisateur qui souhaite regarder une vidéo MPEG-2 en streaming sur son ordinateur portable. Le débit utile d'une telle application peut atteindre 5 Mbit/s, ce qui peut paraître suffisant pour un réseau tel que IEEE 802.11b si personne ne transmet au même instant. Si cet utilisateur se déplace, son débit chute, entraînant une détérioration de la qualité de l'application, voire son arrêt.

IEEE 802.11a et 802.11g utilisent aussi ce mécanisme de variation dynamique du débit, mais avec des effets qui peuvent être encore plus néfastes. Ainsi, le débit peut chuter de 54 Mbit/s à 6 Mbit/s en quelques mètres, soit une baisse de 48 Mbit/s. Si le point d'accès est compatible avec IEEE 802.11b, la chute peut aller jusqu'à 1 Mbit/s puisque ce standard autorise des débits de 11, 5,5, 2 et 1 Mbit/s.

En conclusion, si le mécanisme de variation dynamique du débit permet de conserver une certaine connectivité, c'est au prix d'une importante diminution des performances du réseau, qui peut se révéler catastrophique dans certains cas.

Équipements Wi-Fi

Un réseau Wi-Fi est réalisé avec de nombreux équipements, comme les points d'accès, les antennes, les ponts, les contrôleurs, etc. Dans cette section, nous allons faire un tour d'horizon de ces équipements afin d'en donner quelques caractéristiques.

Ces équipements étant généralement assez hétérogènes, un groupe de travail de l'IETF s'est penché sur la manière de réaliser des réseaux d'entreprise en utilisant plusieurs équipementiers. Ce groupe, appelé CAPWAP (Control And Provisionning of Wireless Access Point), propose de classifier les architectures Wi-Fi selon trois architectures :

- WLAN autonome (Autonomous WLAN Architecture)
- WLAN centralisée (Centralized WLAN Architecture)
- WLAN distribuée (Distributed WLAN Architecture)

Ces architectures sont illustrées à la figure 22.14. La première, à gauche sur la figure, correspond à des points d'accès « lourds », qui sont autonomes et se gèrent par eux-mêmes. La deuxième (en haut à droite), utilisée dans les réseaux d'entreprise, fait appel à un contrôleur. Le contrôleur permet de gérer de façon centralisée un grand nombre de points d'accès. La plupart des fonctions sont regroupées dans le contrôleur. Dans ce cas, les points d'accès sont allégés. On parle de points d'accès « légers ». La dernière architecture (en bas) est celle d'un réseau mesh. C'est l'architecture distribuée que nous examinerons au chapitre 23.

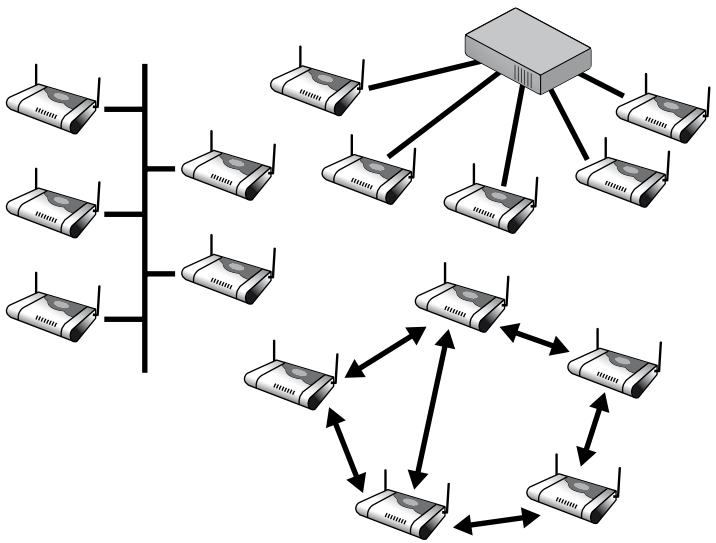


Figure 22.14
Les trois architectures de CAPWAP

Points d'accès

La fonction première du point d'accès est de permettre les communications dans la zone de couverture. Les fonctionnalités proposées sont assez limitées et dépendent du cadre d'utilisation du point d'accès : domestique, en entreprise ou dans un hotspot.

Certains constructeurs proposent des points d'accès dits logiciels. Ces derniers ne sont rien d'autre que des stations, généralement des ordinateurs fixes, équipées de cartes Wi-Fi dans lesquelles un logiciel est installé pour les transformer en points d'accès. Des logiciels libres, comme Host AP, permettent de configurer une station Wi-Fi en point d'accès.

Les points d'accès domestiques

Le rôle d'un point d'accès domestique est de permettre la connexion sans fil à Internet. Dans le cas où l'on souhaite connecter plusieurs stations, le point d'accès doit permettre le partage de connexion.

Ce type de point d'accès incorpore les mécanismes suivants :

- Modem ADSL/câble. L'intégration d'un modem ADSL/câble est de plus en plus courante. Elle évite l'achat de ce type de matériel auprès du FAI, dans le cas où ce dernier ne le fournit pas gratuitement.
- NAT (Network Address Translation). Ce mécanisme permet le partage de la connexion Internet.
- DHCP (Dynamic Host Configuration Protocol). Ce mécanisme s'appuie sur une architecture client-serveur pour permettre la configuration automatique des paramètres réseau des terminaux Wi-Fi. DHCP est totalement transparent pour l'utilisateur, mais il faut auparavant que les stations soient configurées pour permettre ce paramétrage automatique.
- Pare-feu. Du fait que la connexion Internet est partagée, il est nécessaire d'appliquer un pare-feu pour prévenir toute tentative d'attaque (virus, cheval de Troie ou vers) en bloquant l'utilisation de certaines applications susceptibles d'offrir une porte d'entrée à ces attaques.

La plupart des points d'accès intègrent un commutateur Ethernet 1 à 5 ports permettant le partage de la connexion Internet aussi bien pour le réseau Wi-Fi que pour Ethernet.

Dans le cas où la zone de couverture du point d'accès ne permet pas la connexion de toutes les stations au réseau, une modification d'antenne est nécessaire. Les points d'accès destinés aux particuliers disposent soit d'un connecteur d'antenne, dans le cas où l'antenne du point d'accès est interne, soit de la possibilité de modifier l'antenne ou les antennes externes d'origine. Avant tout changement d'antenne, il faut évidemment vérifier le type de connecteur proposé.

Même si la sécurité est un élément important à prendre en compte, on se contente généralement, dans le cadre d'un réseau Wi-Fi domestique, d'utiliser les mécanismes de base de Wi-Fi :

- Non-diffusion du SSID (Secure Set IDentifier).
- ACL (Access Control List), qui permet de définir les terminaux autorisés à se connecter.
- WEP (Wired Equivalent Privacy), de préférence sur 128 bits, qui permet d'authentifier et de chiffrer les communications au moyen d'une clé définie par l'utilisateur. Mais attention, comme nous l'avons vu, cette solution est déconseillée.
- WPA et WPA2 (Wireless Protected Access), qui offrent des mécanismes d'authentification et de chiffrement satisfaisants. Il est conseillé de prendre directement WPA2, la technologie WPA souffrant d'attaques depuis 2009 à cause de l'algorithme RC4.

L'ajout de systèmes de sécurité spécifiques entraînerait celui d'équipements réseau supplémentaires, ce qui compliquerait la configuration et engendrerait un coût non négligeable.

Les points d'accès d'entreprise

Contrairement aux points d'accès pour particuliers, les points d'accès d'entreprise possèdent généralement les fonctionnalités de partage de la connexion Internet par routeur, de NAT et de serveur DHCP, ce dernier étant en outre utilisé dans le cadre du réseau Ethernet.

Dans une entreprise, le point d'accès doit faciliter la configuration, l'évolutivité, l'installation et les connexions avec une sécurité accrue. Les fonctionnalités proposées sont les suivantes :

- Configuration du point d'accès. L'optimisation du réseau Wi-Fi est un critère essentiel pour l'administrateur réseau.

Cette optimisation passe essentiellement par la configuration de différents paramètres liés à la partie radio ou au standard 802.11. Par exemple, la limitation de la puissance d'émission du point d'accès ou les débits autorisés sont assez souvent des critères déterminants.

- Évolutivité. Pour éviter de changer tout le parc d'équipements installé, il est nécessaire que le point d'accès permette l'ajout de modules le transformant en point d'accès multistandard.
- PoE (Power over Ethernet). Lors de l'installation d'un point d'accès, ce dernier doit être connecté au réseau de l'entreprise par le biais d'un câble Ethernet et alimenté par une prise électrique. Le PoE réalise les deux fonctions en une, alimentant en électricité tout équipement par le biais du câble Ethernet.
- Log des événements réseau. Il est important pour l'administrateur réseau de savoir ce qui se passe sur son réseau pour se prémunir de tout type d'attaque. Le point d'accès doit donc permettre le stockage en mémoire de toutes les connexions, réussies comme échouées.
- Handover. Le handover, ou déplacement intercellulaire, permet de garder la transmission en cours lorsqu'on se déplace d'une cellule à une autre, autrement dit d'un point d'accès à un autre. Cette fonctionnalité n'étant pas présente dans le standard 802.11, elle est définie de manière propriétaire par les constructeurs. Si l'entreprise souhaite s'équiper d'un système de téléphonie Wi-Fi, ce mécanisme est nécessaire sous peine d'avoir une coupure de la conversation lors d'une phase de handover.
- Sécurité. Compte tenu des faiblesses de sécurité de Wi-Fi, il est nécessaire que le point d'accès incorpore tous les systèmes de sécurité disponibles, comme 802.1x (EAP-TLS, EAP-TTLS ou PEAP), 802.11i, HTTPS et surtout VPN (Virtual Private Network), ou réseau privé virtuel.
- VLAN (Virtual Local Area Network). Ce mécanisme permet de créer plusieurs réseaux virtuels au sein d'un même réseau physique et d'allouer des configurations spécifiques pour chaque réseau virtuel créé.

Lorsque la zone de couverture ne permet pas la connexion de toutes les stations en un endroit particulier de l'entreprise ou que le point d'accès doit être utilisé pour établir une liaison directive, ce dernier doit permettre l'ajout d'antennes supplémentaires, ce qui est généralement le cas aujourd'hui.

Si l'entreprise possède plus d'une dizaine de points d'accès, il est utile de disposer d'une solution logicielle ou matérielle permettant de configurer automatiquement tous les points d'accès.

Les points d'accès pour hotspot

Le rôle d'un hotspot est d'offrir des connexions transparentes pour les clients. Le réseau Wi-Fi doit donc accepter toutes les connexions venant de terminaux divers et variés. Les hotspots sont le plus souvent équipés en 802.11b ou 802.11g, très rarement en 802.11a.

Les caractéristiques de ces points d'accès sont similaires à celles des points d'accès d'entreprise, comme la configuration ou l'évolutivité, puisque les hotspots doivent supporter les différents standards.

La transparence des communications nécessite les deux mécanismes suivants :

- Dynamicité des paramètres réseau. La configuration des paramètres réseau d'une station peut être statique ou dynamique. Dans le cas où elle est dynamique, l'utilisation de DHCP permet d'allouer ces paramètres dynamiquement. Dans le cas où ces paramètres sont statiques, l'adresse IP de la station et celle du réseau ne correspondent pas, et il est impossible à la station de communiquer avec le réseau hotspot. Ce mécanisme permet d'allouer virtuellement à la station une adresse du réseau hotspot sans qu'elle change physiquement son adresse IP, permettant ainsi à la station de communiquer avec le réseau hotspot.

- Réacheminement SMTP. Contrairement aux paramètres réseau d'une station, les paramètres de messagerie POP et SMTP sont configurés manuellement par l'utilisateur ou l'administrateur de la machine. Or les serveurs SMTP étant propres à un FAI ou à une entreprise, lorsqu'on se déplace d'un domaine à un autre, il n'est pas possible d'envoyer de messages. Le réacheminement SMTP permet, de manière transparente, l'envoi d'e-mails sans que l'utilisateur ait à changer la configuration de son client de messagerie. C'est le point d'accès qui se charge de réacheminer l'e-mail en modifiant directement le serveur SMTP. Sachant que la messagerie est l'application la plus utilisée dans un hotspot, avec 80 % du trafic, il est essentiel pour un hotspot d'implémenter cette fonctionnalité.

Le nombre de points d'accès installés dans un hotspot tel qu'un aéroport ou une gare étant de l'ordre d'une centaine, il est indispensable d'avoir une solution logicielle ou matérielle permettant de configurer tous les points d'accès en même temps et non séquentiellement.

Contrôleurs

Les contrôleurs jouent un rôle important dans les réseaux d'entreprise. Ils peuvent être liés à un équipementier ou indépendants. Dans le premier cas, les fonctionnalités sont complémentaires entre celles situées dans le point d'accès et celles dans le contrôleur. L'inconvénient majeur est de devoir rester dans le giron de l'équipementier. Les contrôleurs ouverts permettent la connexion de la plupart des points d'accès légers et sont donc beaucoup plus universels.

Les principales fonctions d'un contrôleur sont les suivantes :

- Gérer la puissance d'émission des points d'accès pour permettre leur diminution ou augmentation en fonction du champ électromagnétique ou des pannes des autres points d'accès.
- Gérer le choix des fréquences pour adapter le plan de fréquences aux points d'accès.
- Gérer les problèmes de sécurité, par l'introduction d'un serveur d'authentification dans le contrôleur.
- Gérer les problèmes de passage intercellulaire (handover) entre les différentes cellules, même si elles ne sont pas issues de la même technologie.
- Implémenter un logiciel de gestion du nomadisme permettant d'affecter aux utilisateurs concernés les autorisations d'accès et les services auxquels ils ont droit.

Pour aller un peu plus loin dans cette nouvelle génération de gestion du nomadisme, prenons l'exemple du contrôleur Ucopia qui est illustré à la figure 22.15.

L'ensemble du trafic en provenance des utilisateurs Wi-Fi est redirigé vers le contrôleur Ucopia, qui est en coupure logique (ou physique) entre un parc de points d'accès et le réseau filaire. Le contrôleur filtre les flux Wi-Fi pour appliquer les politiques de sécurité et de nomadisme définies avec le Manager Ucopia. Le contrôleur respecte le standard 802.11i. Le protocole d'authentification entre les postes des utilisateurs Wi-Fi et le contrôleur Ucopia est fondé sur 802.1x/EAP ou HTTPS. Les flux sont chiffrés en AES. En complément, un VPN de type IPsec peut être établi entre les clients Wi-Fi et le contrôleur. Le serveur d'authentification RADIUS et le Manager Ucopia dialoguent avec le ou les annuaires LDAP à travers le protocole sécurisé LDAPS.

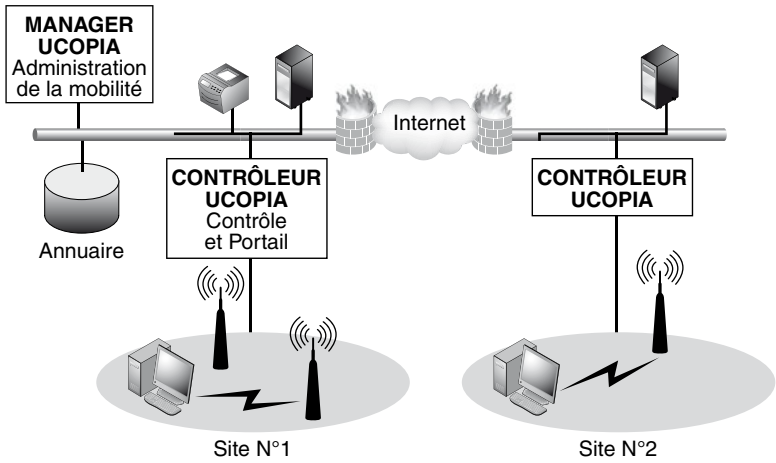


Figure 22.15

Architecture du contrôleur Ucopia

La solution Ucopia permet une gestion très fine du mécanisme d'adressage des utilisateurs du réseau sans fil, en fonction de leur profil et de la configuration du contrôleur. Il est notamment possible d'orienter leur trafic dans différents VLAN sur le réseau filaire en sortie du contrôleur. Les entreprises architecturant très souvent leur réseau en VLAN de manière à isoler les utilisateurs, il est important d'assurer une cohérence entre les infrastructures Wi-Fi et filaire et de continuer à bénéficier des mécanismes d'isolation réseau mis en place sur le réseau filaire. Du côté Wi-Fi, l'organisation du réseau peut également bénéficier d'une structuration en VLAN en encapsulant les SSID par des VLAN et en leur associant des plages d'adresses différenciées.

La solution Ucopia en environnement multisite peut être déployée avec un ou plusieurs contrôleurs Ucopia. Les contrôleurs peuvent être centralisés sur un site ou bien distribués sur différents sites. Indépendamment de l'architecture des contrôleurs, les annuaires peuvent également être centralisés ou répliqués sur chacun des sites. Pour les sites distants comprenant peu de points d'accès et/ou reliés au site principal par une connexion réseau de niveau 3, Ucopia propose un pont permettant d'établir un tunnel émulant un lien de niveau 2 entre le site distant et le site principal. Ainsi, les bornes distantes sont gérées de façon centralisée, sans contrôleur local.

La solution Ucopia inclut l'ensemble des modules nécessaires à son fonctionnement, ce qui lui permet d'être proposée dans un mode « clé en main » très simple à mettre en œuvre. Ce packaging convient parfaitement aux petites entreprises ou aux agences déportées d'une grande entreprise, ayant peu de besoins et de moyens d'intégration. À l'inverse, les grandes entreprises, aux infrastructures réseau complexes, souhaitent pouvoir réutiliser les solutions déjà déployées en termes de sécurité ou d'organisation réseau.

Ponts

Comme un pont Ethernet, un pont Wi-Fi a pour fonction d'étendre le réseau. Dans le cas de Wi-Fi, on étend le réseau Ethernet sur le réseau Wi-Fi et réciproquement.

L'un des principaux usages des ponts Wi-Fi est de relier les bâtiments entre eux grâce à une liaison Wi-Fi spécialisée. Pour cela, le pont doit permettre l'ajout d'une antenne spécifique et le réseau posséder tous les mécanismes de sécurité nécessaires.

La figure 22.16 illustre une liaison directive par l'utilisation de ponts Wi-Fi.

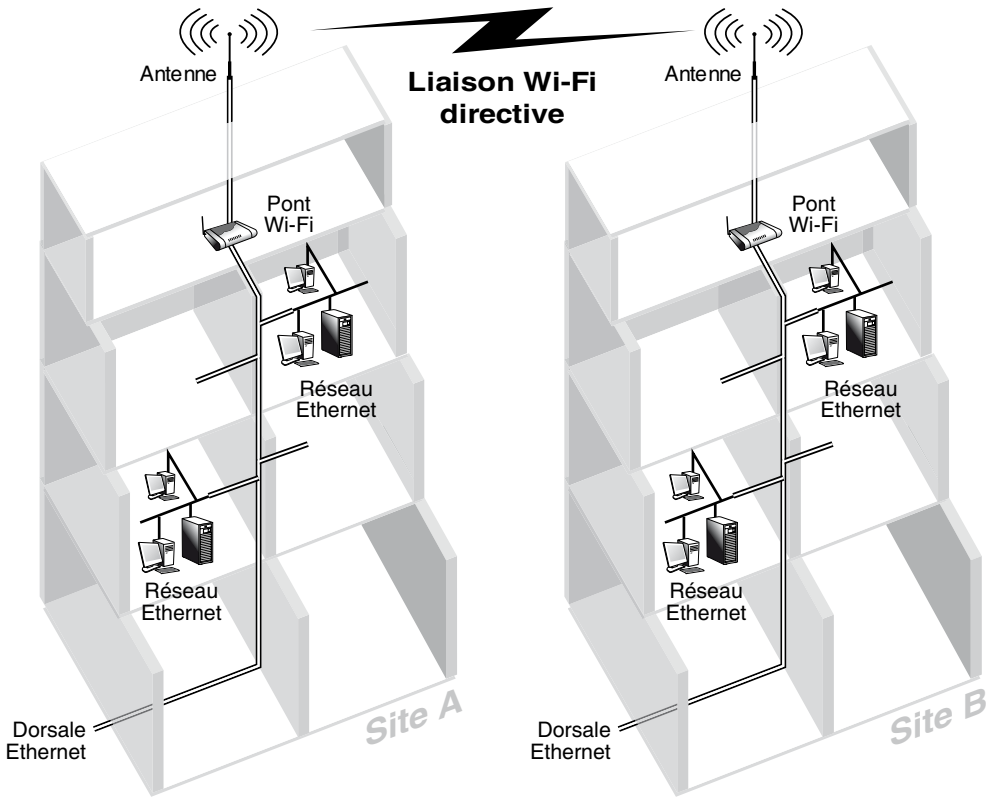


Figure 22.16

Liaison directive Wi-Fi à l'aide de ponts

Un autre usage des ponts est d'offrir, par le biais du point d'accès auquel il est connecté, l'accès à Internet à une console de jeux. À défaut d'une connexion Wi-Fi, les consoles de jeux de dernière génération possèdent au moins une connexion réseau Ethernet. Par le biais d'un module particulier, il suffit de relier le pont Wi-Fi à la console au moyen d'un câble Ethernet pour bénéficier de la connexion.

Ce fonctionnement est illustré à la figure 22.17.

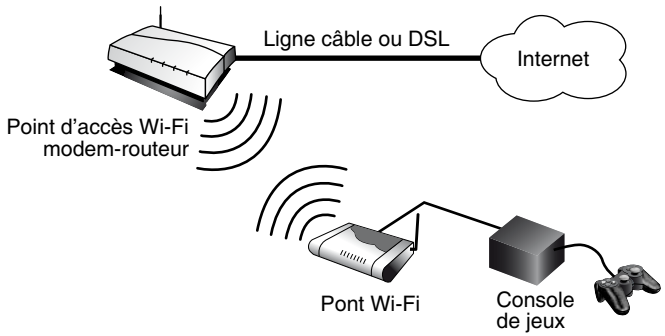


Figure 22.17

Partage de la connexion Internet avec une console de jeux

Antennes

Dans un réseau Wi-Fi, le signal transmis entre deux stations ou entre une station et un point d'accès peut être soumis à des interférences, dues à des obstacles à franchir ou à des équipements émettant dans la même bande de fréquences. La portée du signal radio est fonction à la fois de ces interférences, des obstacles présents dans l'environnement et de la puissance d'émission.

Si la portée du réseau Wi-Fi ne convient pas à l'utilisation souhaitée, des équipements tels que des amplificateurs permettent d'accroître la zone de couverture en augmentant la puissance du signal transmis, sachant que cette puissance ne doit pas excéder la valeur fixée par l'organisme de régulation local, l'Arcep (Autorité de régulation des communications électroniques et des postes) en France.

En pratique, chaque carte Wi-Fi est équipée d'une antenne omnidirectionnelle interne, qui ne peut être mobile que si la station elle-même est mobile. Si une station se trouve cachée par un obstacle tel que mur, meuble, personne, etc., ou qu'elle soit assez éloignée du point d'accès, il se peut qu'elle ne puisse accéder au réseau.

Dans certains cas, même si la station et la carte sont placées dans un endroit clos, derrière un bureau, par exemple, l'antenne peut fonctionner correctement. En effet, Wi-Fi permet de récupérer les transmissions issues des réflexions des ondes radio dans l'environnement. Suivant l'environnement, ces réflexions peuvent être plus ou moins fortes, mais cela permet à certaines stations de fonctionner malgré leurs contraintes spatiales. Dans les cas où la carte ne fonctionne pas très bien, voire pas du tout, l'ajout d'une antenne directionnelle est indispensable.

La figure 22.18 illustre un réseau Wi-Fi équipé d'antennes.

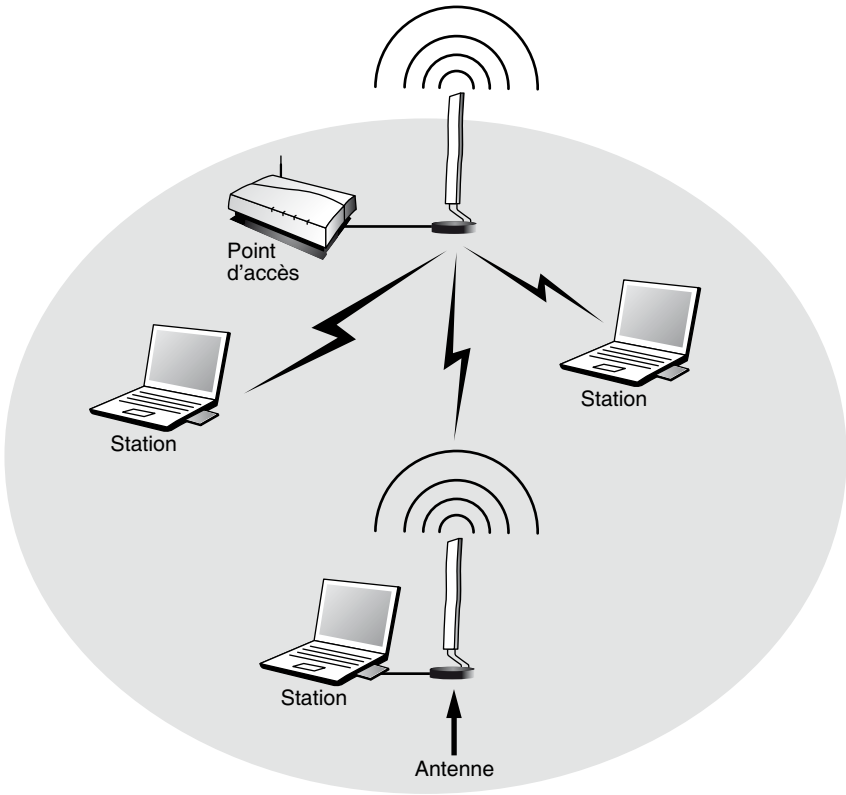


Figure 22.18
Réseau Wi-Fi équipé d'antennes

Une antenne peut être utilisée aussi bien par les stations qui se trouvent en périphérie du réseau, là ou le signal est le plus faible, que par le point d'accès ou les ponts pour étendre la zone de couverture du réseau. Le rôle de l'antenne n'est pas d'amplifier le signal, comme le ferait un amplificateur, mais d'améliorer la réception et l'émission des signaux. L'utilisation d'une antenne peut aussi permettre de créer des liaisons directives entre des bâtiments situés à des distances pouvant atteindre 30 kilomètres.

Pour améliorer la couverture d'un réseau Wi-Fi, une antenne omnidirectionnelle est recommandée. Une station peut se satisfaire d'une antenne directionnelle, voire sectorielle. Dans le cas de liaisons Wi-Fi entre bâtiments, le choix est limité aux antennes directives. Cette notion de directivité est liée au gain de l'antenne. Plus le gain est important, plus la directivité est forte et plus la zone de couverture est restreinte.

Cette directivité est exprimée par le gain de l'antenne, qui est calculé en fonction d'une antenne qui rayonnerait de manière homogène, c'est-à-dire à 360°, et aurait comme zone de couverture une sphère parfaite. Ce type d'antenne n'existe que théoriquement, du fait des contraintes physiques des ondes électromagnétiques.

Le gain d'une antenne est exprimé en décibel isotropique (dBi). Ce gain est équivalent à une puissance, d'où les formules suivantes :

$$P = 10^{G/10} \text{ et } G = 10 \log P$$

où *G* correspond au gain (en dBm ou dBi) et *P* à la puissance (en mW).

Le gain et la puissance dépendent de l'antenne et de sa directivité. Les lois françaises restreignent la puissance à une puissance PIRE (puissance isotropique rayonnée effective).

Types d'antennes

Différents types d'antennes sont utilisables en Wi-Fi, notamment omnidirectionnelles ou directionnelles. Les sections qui suivent détaillent les principales caractéristiques de ces antennes.

Omnidirectionnelles, ou omni

Ces antennes ressemblent à de longs cylindres verticaux, comme illustré à la figure 22.19. Elles constituent l'antenne de base fournie sur les cartes ou les points d'accès. Leur gain est compris entre 2,4 et 15 dBi.

Figure 22.19
Antenne omnidirectionnelle

Les antennes omni permettent d'arroser une large zone sur 360°. Leur inconvénient vient de la qualité souvent médiocre du signal transmis du fait qu'elles captent le bruit de l'environnement ambiant.

Directionnelles

On pourrait dire de ces antennes qu'il s'agit de moitiés d'omni, puisque leur zone de couverture est comprise entre 180° et 60°. Les principales antennes de ce type sont les Patch, Yagi et paraboles.

Sortes de longs cylindres, les antennes Yagi sont utilisées essentiellement à l'horizontale, comme l'illustre la figure 22.20. Fortement directives (entre 15° et 60°), leur gain est compris entre 10 et 20 dBi.

Les paraboles sont généralement fortement directives (18 à 24 dBi). La figure 22.21 illustre une antenne parabolique.

Figure 22.20
Antenne Yagi

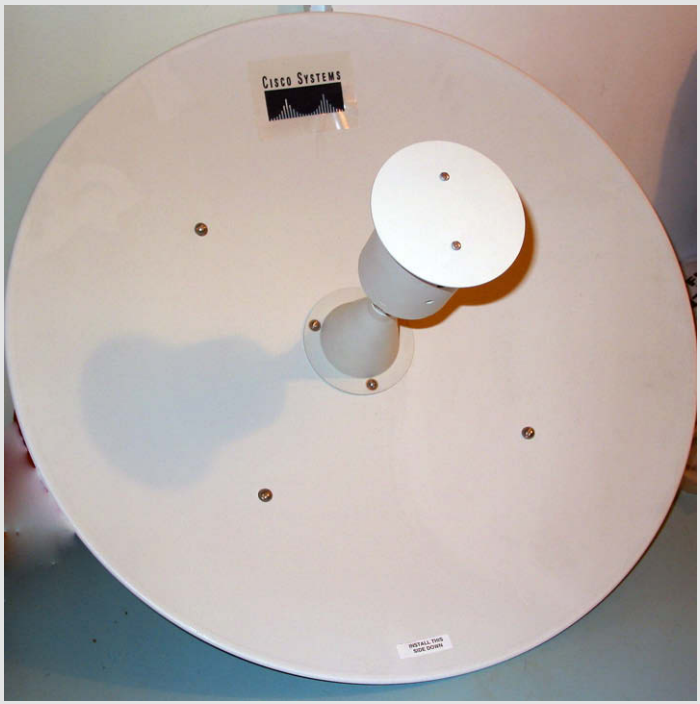


Figure 22.21
Antenne parabolique

Conclusion

Les réseaux Wi-Fi sont aujourd'hui bien implantés, et leur succès ne se dément pas. Plusieurs centaines de millions de points d'accès sont déployés, et les ventes mondiales dépassent largement les 100 000 points d'accès par jour ouvrable.

Après avoir envahi les domiciles, ils s'attaquent à l'entreprise. Les solutions de téléphonie IP et de télévision (IPTV) sur Wi-Fi se développent également très vite, malgré une qualité de service encore délicate à assurer.

Le futur de Wi-Fi est bien tracé par les nouveaux standards IEEE 802.11ac et af qui permettent d'augmenter les débits et la qualité de service.

23

Réseaux hertziens avec relais

Les réseaux hertziens avec relais font référence aux communications qui passent par des équipements intermédiaires dans la partie hertzienne. Il y a en général mémorisation et traitement du paquet avant retransmission vers un autre équipement, toujours par voie hertzienne. On parle aussi de réseaux multisaut. Lorsque les relais forment un réseau maillé, dans lequel chaque nœud est relié aux autres par plusieurs chemins, on parle de réseaux mesh. Les points d'accès formant le réseau mesh peuvent être fixes ou mobiles. Ces stations forment un réseau de base, en général un réseau d'opérateur ou l'équivalent. Les clients d'un réseau mesh forment un réseau ad-hoc . Lorsqu'il n'y a plus que des clients qui forment le réseau on obtient un réseau MANET (Mobile Ad-hoc NETwork). Le réseau ad-hoc se réfère à l'utilisation des clients comme routeurs.

Nous avons également regroupé dans ce chapitre les réseaux satellite qui utilisent des satellites comme relais. Ces satellites ont de plus en plus souvent des capacités de traitement voire de routage dans les constellations de satellites, ce qui nous permet de les inclure dans les réseaux hertziens avec relais.

Réseaux ad-hoc

Les réseaux de mobiles ad-hoc, ou réseaux MANET (Mobile Ad hoc NETwork) forment une catégorie importante des réseaux avec relais. L'infrastructure n'est composée que des stations elles-mêmes qui jouent le rôle d'émetteur, de récepteur et de routeur. Le routage permet le passage de l'information d'un terminal vers un autre, sans que ces terminaux soient reliés directement.

Un réseau ad-hoc est illustré à la figure 23.1.

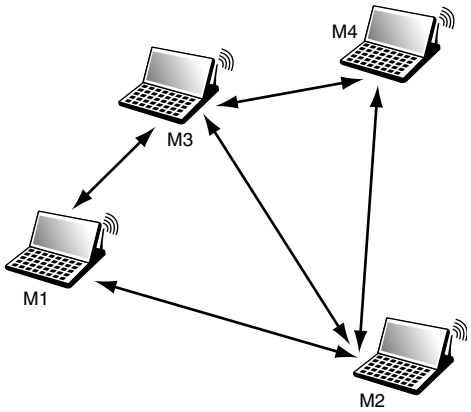


Figure 23.1
Réseau ad-hoc

Contrairement aux apparences, les réseaux ad-hoc datent de plusieurs dizaines d'années. Ils visent à réaliser un environnement de communication qui se déploie sans autre infrastructure que les mobiles eux-mêmes. En d'autres termes, les mobiles peuvent jouer le rôle de passerelle pour permettre une communication d'un mobile à un autre. Deux mobiles trop éloignés l'un de l'autre pour communiquer directement peuvent trouver un mobile intermédiaire capable de jouer le rôle de relais.

La difficulté majeure engendrée par ce type de réseau provient de la définition même de la topologie du réseau : comment déterminer quels sont les nœuds voisins et comment aller d'un nœud vers un autre nœud ? Deux solutions extrêmes peuvent être comparées. La première est celle d'un réseau ad-hoc dans lequel tous les nœuds peuvent communiquer avec tous les autres, impliquant une longue portée des émetteurs. Dans la seconde solution, au contraire, la portée hertzienne est la plus courte possible : pour effectuer une communication entre deux nœuds, il faut généralement passer par plusieurs machines intermédiaires. L'avantage de la première solution est la sécurité de la transmission, puisqu'on peut aller directement de l'émetteur au récepteur, sans dépendre d'un équipement intermédiaire. Le débit du réseau est minimal, les fréquences ne pouvant être réutilisées. Dans le second cas, si un terminal tombe en panne ou est éteint, le réseau peut se couper en deux sous-réseaux distincts, sans communication de l'un à l'autre. Bien évidemment, dans ce cas, le débit global est optimisé, puisqu'il peut y avoir une forte réutilisation des fréquences.

Les techniques d'accès sont du même type que dans les réseaux de mobiles. Cependant, du fait que tous les portables sont mobiles, de nouvelles propriétés doivent être apportées à la gestion des adresses des utilisateurs et au contrôle du routage.

La solution développée pour les réseaux ad-hoc prend pour fondement l'environnement IP. Les mobiles qui jouent le rôle de passerelles — le plus souvent l'ensemble des mobiles — implémentent un routeur dans leurs circuits, de telle sorte que les problèmes posés

reviennent essentiellement à des problèmes de routage dans Internet, la mobilité étant gérée par le protocole IP Mobile.

Les avantages des réseaux ad-hoc sont leurs extensions très simples, leur couverture physique et leur coût. Toutefois, pour en bénéficier pleinement, un certain nombre d'écueils sont à surmonter du fait de la mobilité des nœuds, notamment en ce qui concerne la qualité de service et la sécurité.

MANET est le groupe de travail de l'IETF qui se préoccupe de la normalisation des protocoles ad-hoc fonctionnant sous IP. Ce groupe s'est appuyé sur les protocoles classiques d'Internet et les a perfectionnés pour qu'ils puissent fonctionner avec des routeurs mobiles.

Deux grandes familles de protocoles ont été définies : les protocoles réactifs et les protocoles proactifs :

- Protocoles réactifs. Les terminaux ne maintiennent pas de table de routage mais s'en préoccupent lorsqu'une émission est à effectuer. Dans ce cas, on se sert essentiellement de techniques d'inondation pour répertorier les mobiles pouvant participer à la transmission.
- Protocoles proactifs. Les mobiles cherchent à maintenir une table de routage cohérente, même en l'absence de communication.

Les réseaux ad-hoc sont utiles dans de nombreux cas de figure. Ils permettent de mettre en place des réseaux dans un laps de temps restreint, en cas, par exemple, de tremblement de terre ou pour un meeting avec un très grand nombre de participants. Une autre possibilité est d'étendre l'accès à une cellule d'un réseau sans fil comme Wi-Fi. Comme illustré à la figure 23.2, un terminal situé hors d'une cellule peut se connecter à une machine d'un autre utilisateur se trouvant dans la zone de couverture de la cellule. Ce dernier sert de routeur intermédiaire pour accéder à l'antenne de la cellule.

Les réseaux ad-hoc posent de nombreux problèmes du fait de la mobilité de tous les équipements. Le principal d'entre eux est le routage nécessaire pour transférer les paquets d'un point à un autre point du réseau. L'un des objectifs du groupe MANET est de proposer une solution à ce problème. Quatre grandes propositions ont vu le jour, deux de type réactif et deux de type proactif. Parmi les autres problèmes, nous retrouvons la sécurité, la qualité de service et la gestion de la mobilité en cours de communication.

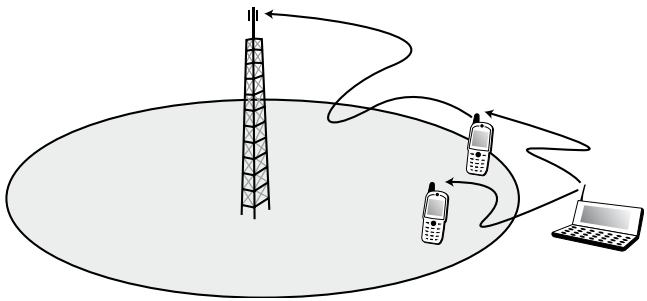


Figure 23.2

Extension de couverture par un réseau ad-hoc

Routage

Le routage est l'élément primordial d'un réseau ad-hoc. Il faut un logiciel de routage dans chaque nœud du réseau pour gérer le transfert des paquets IP. La solution la plus simple est évidemment d'avoir un routage direct, comme celui illustré à la figure 23.3, dans lequel chaque station du réseau peut atteindre directement une autre station, sans passer par un intermédiaire. Ce cas le plus simple correspond à une petite cellule, d'un diamètre inférieur à 100 m, comme dans un réseau 802.11 en mode ad-hoc.

Le cas classique du routage dans un réseau ad-hoc consiste à transiter par des nœuds intermédiaires. Ces derniers doivent posséder une table de routage apte à diriger le paquet vers le destinataire. Toute la stratégie d'un réseau ad-hoc consiste à optimiser les tables de routage par des mises à jour plus ou moins régulières. Si les mises à jour sont trop régulières, cela risque de surcharger le réseau. Cette solution présente toutefois l'avantage de maintenir des tables à jour et donc de permettre un routage rapide des paquets. Une mise à jour uniquement lors de l'arrivée d'un nouveau flot restreint la charge circulant dans le réseau mais décharge le réseau de nombreux flots de supervision. Il faut dans ce cas arriver à mettre en place des tables de routage susceptibles d'effectuer l'acheminement dans des temps acceptables.

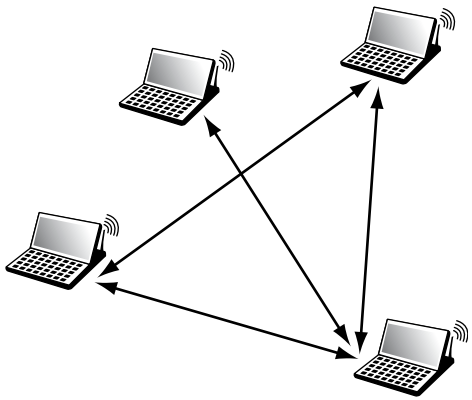


Figure 23.3

Communication directe entre machines d'un réseau ad-hoc

La figure 23.4 illustre le cas d'un réseau ad-hoc dans lequel, pour aller d'un nœud à un autre, il peut être nécessaire de traverser des nœuds intermédiaires. De nombreux écueils peuvent se trouver sur le chemin de la construction de la table de routage. Par exemple, en matière de transmission de signaux, il est possible que la liaison ne soit pas symétrique, un sens de la communication étant acceptable et pas l'autre. La table de routage doit en tenir compte. Les signaux radio étant sensibles aux interférences, l'asymétrie des liens peut par ailleurs se compliquer par l'évanouissement possible des liaisons.

Pour toutes ces raisons, les routes du réseau doivent être sans cesse modifiées, d'où l'éternelle question débattue à l'IETF : faut-il maintenir les tables de routage dans les nœuds mobiles d'un réseau ad-hoc ? En d'autres termes, vaut-il la peine de maintenir à jour des tables de routage qui changent sans arrêt ou n'est-il pas plus judicieux de déterminer la table de routage au denier moment ?

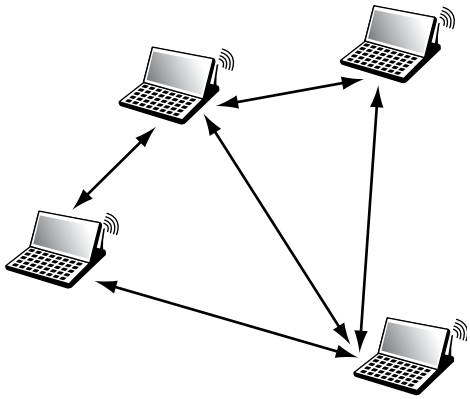


Figure 23.4
Routage par le biais de nœuds intermédiaires

Comme expliqué précédemment, les protocoles réactifs travaillent par inondation pour déterminer la meilleure route lorsqu'un flot de paquets est prêt à être émis. Il n'y a donc pas d'échange de paquets de contrôle en dehors de la supervision pour déterminer le chemin du flot. Le paquet de supervision qui est diffusé vers tous les nœuds voisins est de nouveau diffusé par les nœuds voisins jusqu'à atteindre le récepteur. Suivant la technique choisie, on peut se servir de la route déterminée par le premier paquet de supervision qui arrive au récepteur ou prévoir plusieurs routes en cas de problème sur la route principale.

Les protocoles proactifs se comportent totalement différemment. Les paquets de supervision sont émis sans arrêt dans le but de maintenir à jour la table de routage en ajoutant de nouvelles lignes et en supprimant certaines. Les tables de routage sont donc dynamiques et varient en fonction des paquets de supervision parvenant aux différents nœuds. Une difficulté consiste dans ce cas à calculer une table de routage qui soit compatible avec les tables de routage des différents nœuds de telle sorte qu'il n'y ait pas de boucle.

Une autre possibilité consiste à trouver un compromis entre les deux systèmes. Cela revient à calculer régulièrement des tables de routage tant que le réseau est peu chargé. De la sorte, les performances des flots utilisateur en transit ne sont pas trop modifiées. Lorsque le trafic augmente, les mises à jour sont ralenties. Cette méthode simplifie la mise en place d'une table de routage réactive lorsqu'une demande parvient au réseau.

Les protocoles proposés à la normalisation du groupe MANET sont récapitulés au tableau 23.1. Différentes métriques peuvent être utilisées pour calculer la meilleure route :

- Les vecteurs de distance donnent un poids à chaque lien et additionnent les poids pour déterminer la meilleure route, qui correspond à celle du poids le plus faible.

Métrique	Réactif	Proactif
Vecteur de distance	AODV (Ad-hoc On demand Distance Vector)	DSDV (Destination Sequence Distance Vector)
Routage à la source	DSR (Dynamic Source Routing)	
État du lien		OLSR (Optimized Link State Routing Protocol)

TABLEAU 23.1 • Protocoles ad-hoc

- Le routage à la source permet de déterminer la meilleure route comme étant celle qui permet au paquet de supervision d'arriver le premier au destinataire.
- Les états des liens indiquent les liens qui sont intéressants à prendre et ceux qui le sont moins.

En conclusion, si les études du groupe MANET sont pratiquement finies en ce qui concerne le routage, tout ou presque reste à faire pour la qualité de service, la sécurité et la consommation électrique.

La section suivante décrit brièvement les deux principaux protocoles de routage dans les réseaux ad-hoc normalisés par le groupe MANET.

OLSR

Le protocole OLSR (Optimized Link State Routing) est certainement le plus utilisé des protocoles de routage ad-hoc. Il est de type proactif.

Pour éviter de transporter trop de paquets de supervision, OLSR s'appuie sur le concept de relais multipoint, ou MPR (MultiPoint Relay). Les MPR sont des nœuds importants qui ont la particularité d'être les meilleurs points de passage pour atteindre l'ensemble des nœuds lors d'un processus d'inondation sans diffuser tous azimuts. L'état des liens n'étant envoyé que par les MPR, cela réduit d'autant les messages de supervision.

La connaissance de ses voisins est obtenue par les messages Hello qui sont émis en diffusion. Cela permet de déterminer quels sont les voisins et d'envoyer les informations d'état de lien nécessaires pour l'algorithme de routage. Le message Hello permet également d'indiquer les MPR à ses voisins. Ces messages Hello ne sont destinés qu'aux nœuds voisins et ne peuvent être routés vers un destinataire à deux sauts.

La structure du paquet Hello est illustrée à la figure 23.5.

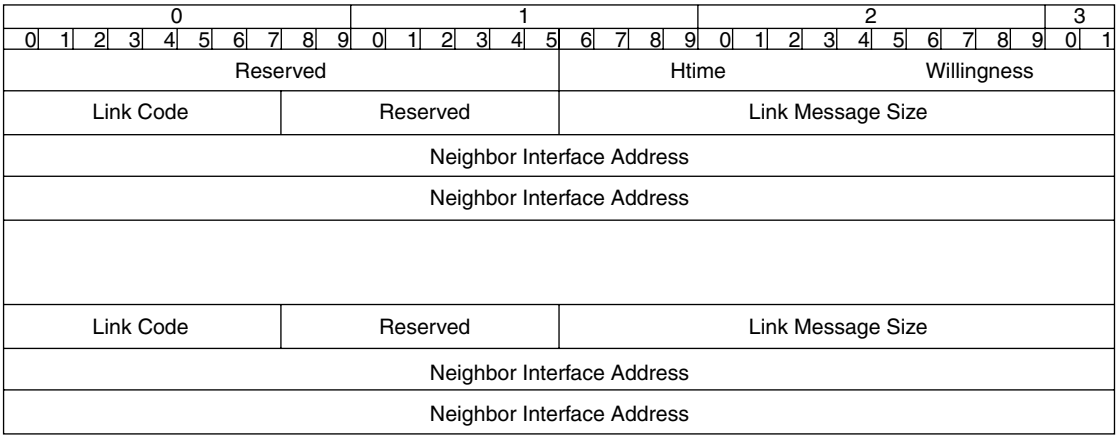


Figure 23.5

Structure du paquet Hello

Le champ Reserved ne contient que des 0, le champ Htime indique l'intervalle de temps entre Hello, le champ Willingness demande à un nœud de devenir un MPR, le champ Link Code permet de faire passer les informations d'état de lien entre l'émetteur et les récepteurs indiqués dans la liste des « Neighbor Interface Address ».

Les paquets TC (Topology Control) sont émis uniquement par les MPR, avec toujours une adresse de broadcast. L'information émise indique la liste de tous les voisins qui ont choisi ce nœud comme MPR et permet, par la connaissance de tous les MPR et l'état des liens, d'en déduire la table de routage. Ces messages sont diffusés sur tout le réseau avec une valeur de 255 dans le champ TTL. La structure du paquet TC est illustrée à la figure 23.6.

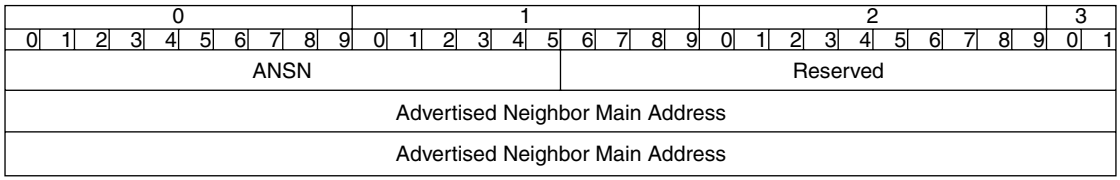


Figure 23.6

Structure du paquet TC

Le champ Reserved est toujours rempli de 0. Le champ ANSN (Advertised Neighbor Sequence Number) transporte un entier incrémenté à chaque changement de topologie. Cette astuce permet de ne pas prendre en compte des informations qui seraient trop anciennes. Les champs Advertised Neighbor Main Address transportent les adresses IP des nœuds à un saut.

Les paquets MID (Multiple Interface Declaration) sont utilisés lorsque les nœuds ont plusieurs interfaces et qu'il faut signaler l'ensemble des interfaces disponibles.

L'algorithme de sélection des MPR est le suivant. Grâce aux messages Hello, les nœuds peuvent déterminer s'ils sont reliés en full-duplex à leurs voisins. La détermination des MPR ne tient compte que des liens symétriques. Par rapport à un nœud donné, un premier ensemble est déterminé, celui de ses voisins à un saut, l'ensemble A. Pour déterminer les MPR, les messages Hello sont reroutés, ce qui permet de déterminer les nœuds à deux sauts, qui forment un autre ensemble bien déterminé, l'ensemble B. Chaque nœud détermine les liens symétriques avec ses voisins. Pour tous les nœuds de B qui n'ont qu'un et un seul lien symétrique avec un nœud de A, on définit ce nœud de A comme MPR, et on ne tient plus compte des nœuds de B reliés par ce MPR. On réitère le processus jusqu'à ce qu'il n'y ait plus de nœud non relié dans B. Les nœuds MPR sont alors tous déterminés.

AODV

AODV (Ad-hoc On-demand Distance Vector) a été le premier protocole normalisé par le groupe MANET, juste avant OLSR. Il est du type réactif. Ce protocole peut gérer à la fois les routages unicast et multicast.

Lorsqu'un flot de paquets est émis par un nœud, la première action est de déterminer la route par une technique d'inondation. Pour cela, le paquet de requête de connexion mémorise les

nœuds traversés lors de la diffusion. Lorsqu'un nœud intermédiaire reçoit une requête de connexion, il vérifie qu'il n'a pas déjà reçu une telle requête. Si la réponse est positive, un message est renvoyé vers l'émetteur pour indiquer l'abandon de cette route.

Le premier message qui arrive au destinataire détermine la route à suivre. La complexité du processus de détermination de la route doit être simplifiée au maximum en évitant les diffusions inutiles. Pour cela, chaque requête de demande d'ouverture d'une route est numérotée, afin d'éviter les duplications, et possède un TTL qui limite le nombre de transmissions dans le réseau.

L'avantage d'AODV est de ne pas créer de trafic lorsqu'il n'y a pas de message à transmettre. La détermination de la route est assez simple et n'implique que peu de calcul dans chaque nœud. Il est évident que les deux inconvénients majeurs résident dans le temps de mise en place de la route et de l'important trafic suscité pour mettre en place les routes.

Réseaux mesh

Les réseaux mesh (*meshed networks*) sont des réseaux de points d'accès formant un ensemble maillé. Les clients sont rattachés par un réseau sans fil aux points d'accès du réseau mesh, et les points d'accès sont reliés entre eux par des liaisons sans fil.

L'avantage de ces réseaux est qu'ils peuvent couvrir une zone géographique importante, sans nécessiter de pose de câbles. Par exemple, sur un grand campus, les points d'accès peuvent se mettre sur les toits des différents bâtiments sans que l'architecte du réseau ait à se préoccuper de relier les points d'accès à un système câblé de type Ethernet.

Plusieurs possibilités se font jour pour réaliser un réseau mesh :

- Utiliser la même fréquence que les terminaux, en considérant que les points d'accès sont traités comme des machines terminales. L'inconvénient est bien sûr d'utiliser de la bande passante enlevée aux autres machines terminales. De plus, il faut faire attention que les deux points d'accès ne soient pas trop éloignés et n'obligent l'émetteur et le récepteur à baisser leur vitesse. Cette solution est considérée comme la première génération de réseaux mesh.
- Utiliser des fréquences différentes. Par exemple, un réseau Wi-Fi 802.11b comportant trois fréquences disponibles, il est possible d'utiliser deux cartes de communication avec des fréquences différentes. L'inconvénient est bien sûr de perturber le plan de fréquences, surtout si le réseau est important et possède de nombreux points d'accès. Cette solution fait partie de la seconde génération de réseaux mesh.
- Toujours dans la deuxième génération, le réseau mesh fait appel à une norme différente pour relier les points d'accès entre eux. Par exemple, un réseau mesh 802.11g peut utiliser la norme IEEE 802.11a pour interconnecter les points d'accès.
- On considère que la troisième génération utilise trois fréquences au total. Une pour connecter les clients, et deux pour interconnecter les points d'accès. Dans ce cas, les connexions amont et aval d'un même nœud utilisent des fréquences différentes. Il faut généralement utiliser 802.11a qui possède jusqu'à huit fréquences différentes.

Les réseaux mesh posent des problèmes inédits aux réseaux sans fil, notamment les suivants : comment optimiser les batteries des points d'accès si ceux-ci ne sont pas reliés au courant électrique ? comment optimiser le routage pour ne pas perturber le trafic utilisateur aux points d'accès, surtout s'ils sont déjà saturés ? quelle densité de points d'accès faut-il utiliser, ce qui revient à se poser la question de la puissance des points d'accès ?

L'avantage de cette technologie est d'être capable de se reconfigurer facilement lorsqu'un point d'accès tombe en panne. Les clients peuvent se connecter à un autre point d'accès, quitte à augmenter légèrement la puissance des points d'accès voisins de celui en panne.

Le problème principal est de gérer le routage. Ce dernier est traité dans les points d'accès qui ne sont pas des machines très puissantes, et il faut de ce fait éviter les points d'accès qui supportent beaucoup de trafic provenant des clients raccordés. De nombreuses propositions ont été faites, en premier lieu celles provenant des réseaux ad-hoc.

À la suite d'une quinzaine de propositions, le groupe de travail IEEE 802.11s a également cet objectif. a retenu deux propositions le SEE-Mesh et le Wi-Mesh, qui se sont regroupés pour former une proposition unique. Cette proposition est devenue un standard en avril 2007, après de nombreuses discussions d'implémentation. Les points d'accès et les stations qui possèdent l'algorithme de routage 802.11s sont nommés Mesh Points (MP). Les liaisons radio permettent de les interconnecter. Le protocole par défaut est le HWMP (Hybrid Wireless Mesh Protocol). Ce protocole hybride provient d'une combinaison d'un protocole provenant d'AODV, le RM-AODV (Radio Metric-AODV) et d'un algorithme fondé sur les arbres. Un second protocole peut-être utilisé lorsque les MP l'acceptent : le protocole RA-OLSR (Radio Aware-OLSR).

Le groupe IEEE 802.11s définit également des solutions de sécurité pour les réseaux mesh. Pour cela, il faut définir une authentification mutuelle des MP, générer et contrôler les clés de session, permettre le chiffrement des données sur les lignes du réseau ad-hoc et détecter les attaques. Pour cela, il faut effectuer des authentifications avec le protocole IEEE 802.1x, que nous détaillons au chapitre 28. Les clés de session sont gérées par une PKI (Public Key Infrastructure). La confidentialité est assurée par la norme IEEE 802.11i, décrite au chapitre 22.

La diffusion massive de stations de travail de poche, telles que Pocket PC, d'une puissance comparable aux PC de bureau, va démultiplier le développement de ces réseaux sans fil, qui se présenteront comme l'entrée du réseau Internet. On donne parfois à un tel réseau, auquel on peut accéder de partout, à tout moment et à haut débit, le nom d'Internet ambiant

Dans un avenir proche, le changement intercellulaire sera possible dans les réseaux sans fil, permettant un déplacement plus important de l'équipement mobile. De surcroît, la téléphonie ne deviendra qu'une application particulière de cette nouvelle génération. On peut donc s'attendre à une diversification des stations terminales de poche capables de se connecter à des réseaux Internet ambiants disponibles dans tous les lieux de passage fréquentés, comme le cœur des villes, les gares, les aéroports, le métro, etc.

L'avantage des réseaux ad-hoc et mesh par rapport aux technologies 3G/4G est de n'utiliser une fréquence qu'une seule fois pour aller d'un point à un autre sur une liaison directe.

Dans le cas des réseaux de mobiles, il faut une première fréquence pour aller à l'antenne puis une autre fréquence pour aller de l'antenne au destinataire. Étant donné l'explosion des débits en mobilité, le gain réalisé par les réseaux ad-hoc et mesh est énorme. La plupart des groupes de travail dédiés aux réseaux de mobiles se penchent sur des solutions hybrides pour économiser à la fois de l'énergie et du spectre.

Réseaux satellite

Nous avons déjà examiné les réseaux satellite au chapitre 10 dans le cadre des réseaux d'accès : le satellite n'est là que pour mettre en relation un utilisateur et le routeur d'accès de l'opérateur. Nous examinons dans le présent chapitre les techniques d'accès et les protocoles utilisés, mais surtout les constellations de satellites, qui permettent d'aller directement du terminal émetteur au récepteur. Les constellations de satellites forment un réseau complet. Après beaucoup d'intérêt porté à ces constellations, elles n'ont pas reçu le succès attendu du fait d'une forte baisse des coûts des réseaux terrestres ajoutée à une non moins forte augmentation des débits. Ces constellations restent utilisées sur des marchés de niche et dans le cadre des communications militaires.

Les satellites de télécommunications de la première génération sont tous géostationnaires, c'est-à-dire qu'ils décrivent une orbite circulaire autour de la Terre dans un plan voisin de l'équateur, avec une vitesse angulaire égale à celle de la rotation de la Terre sur elle-même. Ils apparaissent ainsi comme sensiblement immobiles pour un observateur terrien, ce qui permet une exploitation simplifiée du satellite. Après avoir connu une éclipse éphémère pendant la montée en charge des constellations, ces systèmes géostationnaires reviennent à la mode de par leur capacité importante et la relative simplicité des communications due à la géostationarité des satellites.

L'orbite d'un satellite géostationnaire se situe à 36 000 km de la Terre, ce qui implique un trajet aller-retour entre la Terre et le satellite d'approximativement 0,27 s. Ce très long délai de propagation a un impact important sur les techniques d'accès au canal satellite. À cette altitude, parmi trois satellites placés à 120° les uns des autres sur l'orbite géostationnaire, au moins l'un d'entre eux est visible d'un point quelconque de la Terre.

Le signal reçu par le satellite à une fréquence *f1* est retransmis à une fréquence *f2* vers l'ensemble des stations terrestres. Il se produit ainsi une diffusion des signaux. Ces deux propriétés — toutes les stations écoutent toutes les transmissions, et toutes les stations peuvent émettre — permettent d'implanter des schémas de contrôle spécifiques. Il faut noter une certaine ressemblance de ce système avec les réseaux partagés de type LAN, dans lesquels le support est partagé entre plusieurs utilisateurs.

Les fonctionnalités des satellites incluent donc généralement l'accès multiple, c'est-à-dire que tous les utilisateurs peuvent s'adresser simultanément au satellite sans entente préalable entre eux, et la diffusion, par laquelle un signal réfléchi sur le satellite arrive à toutes les machines terminales situées dans sa zone de couverture.

Les caractéristiques des satellites géostationnaires sont les suivantes :

- La puissance d'émission des terminaux et du satellite doit être forte, à moins que l'antenne n'ait un diamètre important. L'importante distance à franchir entre la Terre et

le satellite affaiblit énormément les signaux. Le satellite doit donc émettre avec une puissance importante, ou bien l'antenne doit être suffisamment précise pour récupérer des signaux très faibles. Par exemple, un terminal ayant une antenne de 3 dBW (affaiblissement de 3 décibels par watt) exige du satellite une antenne de 10 m de diamètre.

- Le satellite doit disposer de batteries de grande capacité pour émettre à forte puissance, ce qui implique de grands capteurs solaires.
- La couverture des régions polaires pose problème, les zones situées au-dessus de 81° de latitude n'étant pas couvertes et celles situées entre 75° et 81° de latitude devant faire face à une capacité de communication fortement réduite.
- Les capacités de communication sont faibles. En effet, les ondes hertziennes utilisées étant inférieures à 20 GHz, il est difficile de réutiliser des fréquences car il y a une forte diffusion des ondes. De ce fait, la capacité de communication d'un satellite est faible en comparaison de celle des réseaux terrestres. Cependant, cette restriction est partiellement levée par les satellites géostationnaires de nouvelle génération, qui utilisent un très grand nombre d'émetteurs avec des fréquences très élevées, permettant de décomposer la zone visible du satellite en de petites cellules de quelques kilomètres de diamètre et de réutiliser des fréquences presque comme dans un réseau terrestre.
- Plus l'angle d'inclinaison est grand, plus la trajectoire des ondes est perturbée par les obstacles, ce qui rend les communications difficiles à partir de 50° de latitude. Par exemple, à Londres, une ville située au-dessus de 50° de latitude, les antennes doivent avoir un diamètre plus important que sous l'équateur pour recevoir un signal de même puissance.
- La communication de mobile à mobile entre deux stations qui ne sont pas situées dans la même zone de couverture requiert le passage par un réseau terrestre, les communications entre satellites géostationnaires étant fort complexes.

Ces caractéristiques nécessitent le recours à des satellites lourds, au lancement onéreux, alors que les satellites basse orbite, plus légers, peuvent être lancés par de petites fusées ou par grappes de 6 à 10. Comme nous allons le voir, le principal défaut des satellites basse orbite provient de leur mobilité par rapport à la surface terrestre. Un satellite en orbite à 700 km de la Terre tourne à une vitesse de 5 km/s.

Les orbites basses des LEOS (Low Earth Orbital Satellite) ou moyennes des MEOS (Medium Earth Orbital Satellite) profitent d'une meilleure réutilisation des fréquences. La distance à la Terre de 1 000 km, voire de 700 km, des LEOS permet de réaliser des cellules plus petites que celles des GEOS (Geostationary Earth Orbital Satellite). Pour des cellules de 50 km de diamètre, il est possible de réutiliser jusqu'à 20 000 fois une même fréquence.

La taille des cellules envisagées par les satellites GEOS est maintenant suffisamment petite pour concurrencer les LEOS pour la réutilisation des fréquences. Par l'utilisation de fréquences situées entre 20 et 40 GHz, on peut descendre à des tailles de cellules inférieures à 50 km de diamètre. On pourrait aussi utiliser ces fréquences pour des satellites LEOS, ce qui réduirait d'autant la taille des cellules, mais cette solution n'est pas acceptable dans le cadre des LEOS. Des cellules de l'ordre de 5 km de diamètre impliqueraient

une durée de recouvrement par le satellite de l'ordre d'une seconde. Il faudrait alors faire un handover toutes les secondes.

Compte tenu de la proximité des satellites LEOS avec la Terre, leurs principaux avantages sont un coût de lancement relativement modique et la faible puissance d'émission qu'ils réclament. Leur inconvénient majeur est occasionné par leur déplacement, puisqu'ils ne sont pas stationnaires. Les communications d'un utilisateur terrestre doivent donc régulièrement changer de satellite par des handovers, comme dans les réseaux de mobiles terrestres.

Suivant la trajectoire des satellites, l'inclinaison de l'orbite et l'orbite elle-même, il est possible de réaliser des réseaux spécifiques pour privilégier des régions particulières. La trajectoire correspond à la forme de l'orbite, qui peut être circulaire ou elliptique. Dans le cas d'une ellipse, la vitesse relative par rapport à la Terre varie, et le satellite peut se positionner pour rester plus longtemps au-dessus de certaines zones. L'inclinaison définit l'orbite par rapport au plan équatorial. Les orbites en rosette sont inclinées assez fortement par rapport au plan équatorial. Dans ce cas, les régions intermédiaires entre le pôle et l'équateur sont les mieux couvertes. Enfin, les orbites équatoriales favorisent bien sûr les pays situés autour de l'équateur.

Couches de protocoles des réseaux satellite

Les communications par l'intermédiaire d'un satellite ont des propriétés différentes de celles des réseaux terrestres. Les erreurs, par exemple, se produisent de façon fortement groupée en réponse à des phénomènes physiques, comme les éclairs magnétiques, sur les antennes d'émission ou de réception.

Au contraire des réseaux locaux, aucun protocole de niveau trame n'a été normalisé pour les réseaux satellite. Il en va de même pour le niveau paquet. Devant cette carence, les protocoles terrestres, que ce soit de niveau trame ou de niveau paquet, ont dû être repris et adaptés aux contraintes des satellites.

Protocoles de niveau liaison

Plusieurs procédures ont été proposées pour pallier le problème du délai d'accès au satellite. En effet, non seulement un temps égal à deux fois l'aller-retour au satellite est nécessaire avant de recevoir un acquittement, mais il faut ajouter les temps de traversée des stations terrestres et éventuellement des réseaux terrestres, qui sont loin d'être négligeables. Le délai aller-retour dépend en outre de la position de l'orbite sur laquelle se trouve le satellite.

Lorsque les capacités des liaisons sont importantes, les techniques ARQ (Automatic Repeat reQuest) classiques ne sont que peu efficaces, la quantité d'information à retransmettre devenant très grande en cas d'erreur. Les techniques sélectives engendrent des problèmes de dimensionnement des tailles des mémoires nécessaires pour attendre les paquets en cours de retransmission.

Un réseau utilisant un satellite géostationnaire ou sur une orbite moyenne se caractérise par un très long temps de propagation, comparativement au temps d'émission d'une

trame. C'est pour cette raison qu'un mode étendu est prévu dans les procédures classiques de reprise sur erreur. Une autre solution est d'allonger la taille des trames. Au niveau supérieur, le protocole TCP permet d'allonger les messages et la segmentation afin de générer de longs paquets IP. Cependant, les trames Ethernet, de 1500 octets, étant les plus longues de celles classiquement utilisées la solution est d'engendrer plusieurs connexions TCP en parallèle.

Par exemple, si le débit de la liaison satellite est de 10 Mbit/s, sachant qu'il faut au moins prévoir d'émettre sans interruption pendant un temps égal à deux allers-retours, la valeur minimale de la trame est de 20 Ko. Cette valeur très importante suppose une excellente qualité de la ligne physique de sorte que le bloc de données de 160 000 bits arrive avec un taux d'erreur bit inférieur à 10^{-10}.

Une première solution pour appréhender ces problèmes est offerte par la méthode des canaux virtuels, qui consiste à découper fictivement le canal unique du satellite en *M* canaux, de telle sorte que chaque session TCP puisse se dérouler avec une fenêtre de contrôle acceptable. La figure 23.7 illustre les divers éléments à mettre en œuvre pour faire fonctionner ce protocole. Les trames sont numérotées dans le dispatcheur, lequel affecte les trames dans les différents sous-canaux de façon circulaire. La trame numéro *x* est placée dans le sous-canal *i,* si $x = i$ (modulo *M*). Ensuite, les différents sous-canaux travaillent en parallèle, suivant une méthode TDMA statique dans la plupart des cas, mais qui peut être dynamique dans certaines conditions. Les trames arrivées dans les files d'attente des sous-canaux du récepteur sont remises à une file séquenceur, qui transmet les trames de façon ordonnée à la couche supérieure.

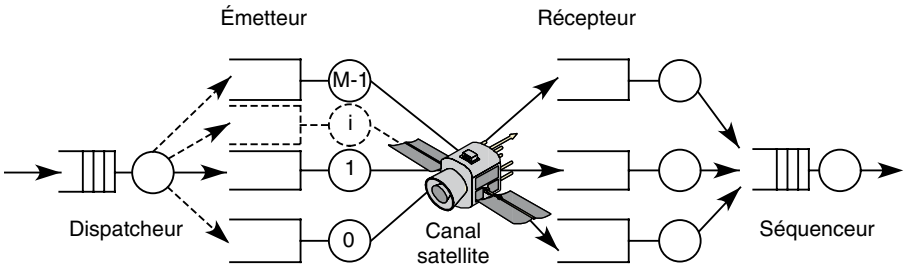


Figure 23.7

Protocole des sous-canaux virtuels

L'avantage de cette méthode est qu'elle permet de travailler sur *M* canaux indépendants simultanément. De ce fait, la fenêtre d'anticipation maximale est de *M* fois la fenêtre de chaque session, ce qui permet d'atteindre la valeur nécessaire à une bonne exploitation de la liaison. En outre, les reprises peuvent s'effectuer en parallèle. Jusqu'à *M* trames successives peuvent être en cours de retransmission. Comme les erreurs arrivent relativement groupées, la possibilité de reprendre en parallèle plusieurs trames qui se suivent est un avantage indéniable.

D'autres solutions de protocoles de liaison ont été proposées, concernant surtout la possibilité d'émettre plusieurs rejets sélectifs, c'est-à-dire sans attendre d'avoir reçu

l'acquittement de la trame en cours avant d'émettre une nouvelle requête de retransmission. Une solution également envisagée concerne l'utilisation de codes détecteurs et correcteurs d'erreurs. Cependant, un bilan de la liaison montre que la retransmission unique, sans correction, optimise généralement l'utilisation du canal. Cette propriété vient des taux d'erreur relativement faibles sur les liaisons satellite. Lorsque l'angle d'inclinaison devient prononcé, la solution optimale est moins évidente. En effet, le taux d'erreur augmente fortement lorsqu'on dépasse les 50° de latitude.

De même, pour accéder à des engins interplanétaires, les solutions à base de codage avec correction d'erreur sont indispensables. Dans ces protocoles de liaison, une autre voie a connu un certain succès un peu avant la fin des années 2000 avec les satellites ATM, qui possèdent une infrastructure de commutation embarquée dans le satellite. La normalisation des communications au travers de ces satellites ATM a été prise en compte dans le groupe S-ATM. De par la petite taille des trames ATM, leur nombre transmis sur un canal à haut débit peut devenir très important. Il est donc nécessaire de travailler sur des regroupements de trames ATM dans des supertrames de plus grande taille. Lorsqu'une erreur est détectée, la supertrame est retransmise et non la seule trame ATM, puisque, de toute façon, il n'y a aucun moyen de détection d'une erreur dans la trame ATM. La taille de la supertrame intermédiaire est à optimiser pour que le nombre de trames à retransmettre ne soit ni trop grand ni trop petit.

Protocoles de niveau réseau

Les réseaux satellite peuvent servir d'accès large bande à des réseaux terrestres ou réaliser des réseaux globaux lorsque des liaisons intersatellites sont mises en place.

Le satellite peut être transparent ou non, un commutateur ou un routeur embarqué permettant de décider de la route à suivre. Des architectures de niveau paquet ont été déterminées par le groupe de normalisation américain TR34.1 de la TIA/EIA.

Les applications qui transitent dans les satellites — qui de plus en plus sont en mode non transparent — appartiennent au monde Internet et transmettent de ce fait des paquets IP. Les solutions permettant de transférer ces paquets IP passent essentiellement par l'utilisation de routeurs ou de LSR (Label Switch Router) et de la technologie MPLS.

La difficulté majeure rencontrée dans ces environnements protocolaires est le contrôle de flux TCP par l'algorithme « slow-start and congestion avoidance ». Dès qu'un paquet IP est perdu ou en retard, le protocole TCP redémarre par une fenêtre de valeur 1. De nombreux algorithmes ont déjà été proposés pour pallier cette forte baisse du débit. La proposition TCP Reno permet une reprise rapide en cas de perte isolée de cellules grâce à un redémarrage de l'algorithme slow-start sur une valeur de la fenêtre bien supérieure à un. Les protocoles TCP SACK, TCP NewReno et autres modifications de TCP Reno ont été proposés pour résoudre les problèmes de reprise sur une perte de plusieurs paquets IP successifs. En fait, quelle que soit la qualité de l'algorithme utilisé, ce dernier est dépendant de nombreux paramètres ainsi que des caractéristiques du satellite et de la liaison. Globalement, TCP SACK et TCP NewReno travaillent correctement sur les constellations LEOS, TCP Reno sur les constellations MEOS et le TCP de base sur les satellites GEOS.

Le contrôle dans les constellations de satellites

Une autre façon d'aborder le problème du contrôle consiste à découper la boucle de réaction, c'est-à-dire la suite des commandes à effectuer pour contrôler un système, en plusieurs sous-boucles indépendantes. Cette solution a été proposée pour les communications par satellite utilisant le protocole TCP sous le nom de VD/VS (Virtual Destination, Virtual Source). La liaison satellite est isolée du reste de la boucle par deux routeurs, qui ne se connaissent que l'un l'autre. Ils forment la source et la destination virtuelle. Cependant, cette solution n'est pas conforme à la caractéristique de contrôle de bout en bout réclamée à ce niveau, la perte d'un paquet à l'intérieur du routeur n'étant pas découverte par le protocole TCP.

Une autre façon d'améliorer les performances consiste à ouvrir plusieurs connexions TCP pour une même application. Cette idée est similaire à celle qui a été indiquée dans le protocole de liaison des sous-réseaux virtuels, mais appliquée à un niveau plus élevé. L'avantage de cette solution est qu'elle reste compatible avec le protocole de base. Un exemple est fourni par le protocole XFTP, qui utilise cette propriété d'ouvrir plusieurs connexions simultanées plutôt qu'une seule.

Une autre solution consiste à choisir la classe ATM la mieux appropriée au service souhaité. Le monde ATM apporte une garantie de service mais en impliquant une interaction entre le point d'accès IP et le réseau ATM, de façon qu'il puisse y avoir continuité de la garantie de service vers le réseau utilisateur.

Le service GFR apporte une garantie supplémentaire en requérant une bande passante minimale et une taille de paquet maximale. Si l'émetteur émet à une vitesse inférieure à la limite et avec une taille de paquet inférieure à la taille maximale, une qualité de service correcte est obtenue. Si la vitesse d'émission dépasse le seuil déterminé dans le service GFR, pour obtenir une qualité de service, il est nécessaire de marquer une certaine proportion du flot avec le bit CLP = 1, de façon que les cellules CLP = 0 rentrent dans les conditions permettant d'obtenir une qualité de service. Avec la connaissance de la valeur du seuil minimal, il est possible d'adapter les valeurs des paramètres de contrôle de TCP pour obtenir une garantie de service. En fait, la gestion des mémoires tampons est particulièrement importante.

Une autre possibilité consiste à utiliser le service ABR sous la pile de protocoles TCP/IP. Le service ABR apporte une qualité de service pour les applications qui sont sensibles aux pertes mais pas au délai de transport. Dans ce cas, le contrôle de flux TCP s'applique assez bien pour réaliser la qualité de service demandée mais avec une utilisation des ressources qui peut être faible. La plupart de ces protocoles supposent que les flots IP ont une priorité de même niveau. Pourtant, plusieurs niveaux de priorités devraient naturellement être affectés aux applications, ce qui faciliterait la prise en charge des flots les plus prioritaires en leur fournissant une qualité de service garantie.

La capacité limitée du satellite pousse les routeurs à agréger les flots de même nature sur un circuit virtuel unique. La classification des flots peut être effectuée par un gestionnaire de qualité de service ou un service DiffServ géré par le routeur d'entrée dans le réseau. Suivant l'indication donnée par le champ ToS d'IPv4 ou la valeur du flow-label d'IPv6, une allocation spécifique peut être réalisée au moyen des cellules RM. L'ATM Forum appelle cette allocation ABR en boucle, ou Weighted Allocation. L'algorithme du max-min, utilisé sur les circuits virtuels ABR, travaille sur un critère d'équité. Cet algorithme a été étendu par des versions utilisant des poids, comme WMM (Weighted Max-Min), dans lesquelles la priorité intervient par un débit minimal déterminé par la valeur MCR (Minimum Cell Rate). L'ATM Forum définit cette solution comme une allocation proportionnelle au MCR. Cet algorithme est bien adapté aux communications par satellite, dans lesquelles le rapport délai sur débit est très grand.

Systèmes satellite

Un système satellite composé d'un seul satellite est beaucoup plus facile à gérer qu'une constellation de satellites, dans laquelle les satellites doivent se communiquer sans arrêt des données pour que leurs informations soient consistantes.

Les problèmes concernent d'abord l'utilisation optimisée du canal satellite, étant donné le coût des infrastructures. Viennent ensuite la gestion et le contrôle de l'ensemble. Il faut en outre un algorithme pour gérer les handovers.

Constellations de satellites

Malgré des échecs, les constellations de satellites offrent toujours des promesses alléchantes pour les communications interpersonnelles, en permettant des communications à tout moment et à tout endroit avec des terminaux de la taille de téléphones GSM.

Les constellations LEOS ont l'avantage de présenter un délai de propagation peu important. Elles requièrent de surcroît une faible puissance d'émission pour atteindre le terminal, de sorte que ce dernier peut être employé pour la communication directe d'un utilisateur mobile avec le satellite. Le retard dû à la propagation se situe aux alentours de 10 ms, ce qui est peu en comparaison des 250 ms pour un satellite GEOS. En revanche, la nécessité d'avoir un grand nombre de satellites pour recouvrir la Terre, ajoutée à la probabilité plus importante d'avoir des zones d'ombre et à l'augmentation de l'effet Doppler constitue des inconvénients certains.

Le problème majeur en matière de communications multimédias concerne la qualité de service dont les applications ont besoin. Cette qualité de service est aisément fournie dans un mode circuit, mais la mauvaise utilisation de la bande passante est inacceptable dans des systèmes coûteux tels que les constellations de satellites.

Le réseau mis en place sur la constellation utilise une technique de transfert de paquets par commutateur ATM ou routeur IP. La méthode de transfert ATM a été choisie par la plupart des opérateurs de constellations, mais la question reste ouverte avec l'arrivée de nouveaux concepts IP, tels que les gigarouteurs, capables de transmettre plusieurs gigabits par seconde, les techniques de réservation présentées précédemment, les nouvelles techniques de routage dépendant de la QoS, les nouveaux contrôles de flux, PoS (Packet Over SONET), etc. Il y a de fortes chances que le monde satellitaire adopte à son tour l'utilisation intensive du protocole IP et de ses dérivés.

Les constellations s'attaquent au problème réseau de deux façons très différentes, selon que :

- Le système n'est qu'un réseau d'accès.
- Le système est un réseau complet en lui-même.

Dans le premier cas, l'utilisateur se connecte au satellite pour entrer sur le réseau d'un opérateur fixe. Il n'est pas possible de passer d'un satellite à un autre, et à chaque satellite doit correspondre une station au sol connectée à un opérateur local. Dans la deuxième solution, il est possible de passer directement de l'émetteur au récepteur, en allant de satellite en satellite. Quelques stations d'accès à des opérateurs fixes sont également envisageables, mais surtout pour atteindre les clients fixes.

La configuration de la constellation est importante pour réaliser l'un ou l'autre type de réseau. Il faut notamment essayer de passer au-dessus des zones les plus demandées. Plusieurs catégories d'orbites sont possibles pour cela. Les liaisons intersatellites sont nécessaires lorsque le système n'est pas seulement un réseau d'accès. Le nombre de liaisons intersatellites à partir d'un satellite varie de deux à huit. La figure 23.8 illustre de telles liaisons.

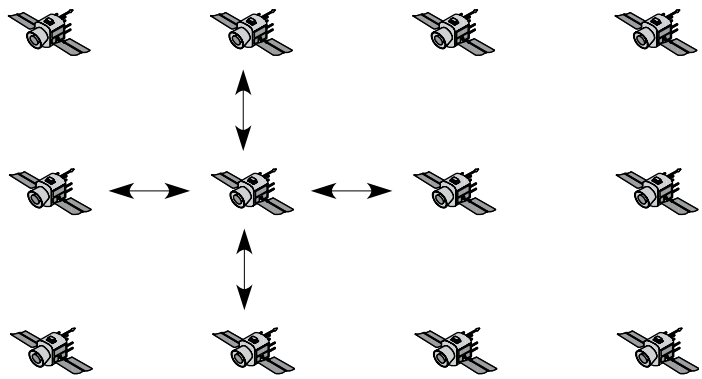


Figure 23.8

Exemple de liaisons intersatellites

Handovers satellitaires

Le handover correspond à un changement de cellule à la suite du déplacement soit du client, soit du satellite, qui, en tournant, finit par perdre son client de vue. Dans ce dernier cas, un autre satellite de la constellation prend le relais pour que la communication ne soit pas interrompue. Dans les constellations basse orbite, le satellite se déplace à la vitesse de 4 à 5 km/s, une vitesse bien supérieure à celle du client. Le nombre de handovers dus à un client qui se déplace peut être considéré comme négligeable et constitue en cela un avantage important. Comme la vitesse de défilement d'un satellite est constante et que le client est assimilé à un point fixe, les handovers sont prévisibles pour autant que le client ne termine pas brutalement sa communication.

En règle générale, on distingue deux catégories de handovers :

- Le handover dur (hard-handover), dans lequel il ne doit y avoir aucune coupure et où le relais sur la nouvelle cellule commence juste au moment où se termine la communication avec la cellule précédente.
- Le handover mou (soft-handover), dans lequel des éléments de communication commencent à transiter par la nouvelle cellule tandis que la cellule précédente est toujours en cours de communication.

Un satellite peut gérer plusieurs cellules — jusqu'à une centaine — grâce à de nombreuses antennes d'émission. Un handover intrasatellite correspond à un handover qui s'effectue entre deux cellules gérées par le même satellite. En revanche, un handover

intersatellite correspond à un client qui est pris en charge par une cellule dépendant d'un autre satellite. Le premier type de handover est assez simple, en ce sens qu'un seul et même satellite gère les deux cellules. Un handover intersatellite est nettement plus complexe, car il faut gérer la communication entre les deux satellites sans interruption.

Comme dans le monde du cellulaire terrestre, l'empreinte d'un satellite se divise en cellules pour augmenter la capacité globale du satellite par une amélioration de la réutilisation des fréquences. Chaque cellule correspond à une fréquence de l'antenne du satellite. Deux systèmes s'opposent dans la conception des handovers :

- L'antenne reste fixe sur le satellite, et la zone de couverture défile à vitesse constante sur la surface terrestre. C'est ce qu'on appelle un système à cellules défilantes, ou EMC (Earth-Mobile Cell).
- L'antenne est mobile et pointe vers une cellule fixe sur la surface terrestre. Lorsque le satellite ne peut plus pointer vers la cellule, c'est au satellite suivant sur l'orbite de prendre le relais. C'est la technique EFC (Earth-Fixed Cell).

Dans les systèmes à cellules défilantes, le handover s'effectue en fonction de la mobilité du satellite et non de la vitesse du mobile, qui peut être déclarée négligeable. Deux sortes de handovers peuvent se produire : le handover intrasatellite, c'est-à-dire entre deux cellules gérées par le même satellite, et le handover intersatellite, entre deux cellules gérées par deux satellites distincts. Le nombre de handovers pouvant survenir durant la conversation d'un utilisateur est déterminé par plusieurs facteurs : la durée de l'appel bien sûr, mais aussi la taille de la cellule et la vitesse du satellite, qui dépend de l'altitude.

Si l'on considère une constellation de satellites LEOS à 800 km d'altitude, dans laquelle l'angle d'élévation est de 10°, l'utilisateur effectue un handover intrasatellite (variant suivant la taille de la cellule) approximativement toutes les trente secondes et un handover intersatellite toutes les trois minutes. Les satellites MEOS ont un handover intersatellite toutes les heures et un handover intrasatellite environ toutes les dix minutes.

Un problème assez complexe concerne les politiques à choisir pour assurer qu'un client trouve toujours une place lors d'un handover. Plusieurs solutions ont été proposées, dont celle consistant à distinguer des clients GH (Guaranteed Handover) et des clients ordinaires, qui ne demandent pas cette assurance.

La réservation des canaux nécessaires à cette garantie est initialisée lors de l'ouverture de la demande. Un canal est alors réservé dans toutes les cellules qui seront visitées par l'utilisateur. La durée de cette procédure est déterminée par la durée du service GH, qui doit être connue à l'instant d'ouverture de la communication. Un canal n'est pas réservé dans toutes les cellules visitées, mais seulement dans celles que l'utilisateur GH visitera et situées à une distance inférieure à une valeur critique. Si aucun circuit n'est disponible dans une cellule visitée, l'appel est rejeté. Sinon, un canal est réservé dans chaque cellule.

Pour l'accès aux cellules dont la distance est supérieure à la distance critique, l'utilisateur GH attend d'être à la distance critique pour effectuer une réservation. Si un circuit est disponible, il est réservé. Sinon le client GH émet une demande de réservation qui est mise en file d'attente. Cette requête est bien sûr prioritaire par rapport aux demandes de réservation émanant des clients ordinaires. Enfin, pour que la probabilité d'échec soit

faible, le nombre global de client GH doit être raisonnable par rapport au nombre de canaux disponibles.

Une deuxième solution, dite EFC (Earth-Fixed Cell), concerne les cellules fixes par rapport à la Terre. Dans ce cas, la surface de la Terre est décomposée en cellules fixes correspondant aux faisceaux du satellite. Chaque faisceau continue de desservir sa cellule terrestre durant toute la durée de visibilité. Au moment de la disparition de la cellule, le satellite demande à un autre satellite de prendre le relais. En réalité, toutes les cellules sont réaffectées exactement au même instant à un autre satellite, et tous les handovers sont effectués au même moment.

Dans cette solution, les antennes du satellite sont directionnelles et doivent suivre la même cellule. Suite à des limitations physiques, l'angle d'élévation donne le temps exact pendant lequel la cellule est éclairée par le rayon, c'est-à-dire atteinte par les émissions provenant du satellite. Dans le cas EFC, il suffit qu'un client réussisse à s'approprier une fréquence pour la conserver jusqu'à ce qu'il la relâche. Dans ce cas, on peut considérer que le système se comporte comme un réseau terrestre fixe. Si l'on fait abstraction des instants de handovers, le système global n'est pas modifié.

Deux solutions peuvent être suivies pour réaliser les deux types de systèmes : mécanique et électronique. Quand le mouvement du satellite est suffisamment lent, ce qui est le cas des MEOS, la solution mécanique est acceptable. Pour les satellites LEOS, un suivi électronique est conseillé, étant donné la vitesse du satellite par rapport à la Terre.

Conclusion

Les réseaux avec relais sont très appréciés pour leur facilité de déploiement et d'utilisation. De plus, ils économisent grandement la bande passante nécessaire à l'acheminement de flux importants, car ils n'utilisent qu'une seule fréquence par transmission à la place de deux dès qu'il y a une antenne. Un autre avantage immédiat de ces réseaux est d'offrir une extension simple des réseaux d'accès en permettant d'atteindre une borne par le biais de machines intermédiaires.

De leur côté, les systèmes satellitaires ont connu un grand succès pour la diffusion des programmes de télévision. En revanche, les applications de télécommunications, qui fonctionnent très souvent avec des liaisons point-à-point, ont beaucoup plus de mal à trouver leur place dans ces systèmes. Cette situation est principalement due à la concurrence des opérateurs terrestres, qui offrent, avec les technologies cellulaires telles que le GSM, des services similaires à moindre prix. Les coûts des réseaux cellulaires terrestres sont devenus si bas que les constellations de satellites n'ont pu s'aligner sur la baisse des prix des minutes de communication.

Les systèmes satellitaires fonctionnent cependant parfaitement bien, et des études économiques permettront sans doute de trouver des créneaux pour lesquels ils se révéleront compétitifs.

24

L'Internet des choses

L'Internet des choses (Internet of Things) a démarré avec l'idée de raccorder à Internet des capteurs sans fil et filaire que l'on trouve dans le domicile, dans les bureaux et un peu partout dans la vie courante. Ensuite, son apport majeur a été suscité par les RFID (Radio-Frequency Identification), ou étiquettes électroniques. L'Internet des choses permet de raccorder tout ce qui est connectable, depuis les objets divers et variés jusqu'aux poussières électroniques. Le concept est simple, mais les problèmes sont nombreux, car les « choses » ne sont en général pas suffisamment sophistiquées pour gérer des communications et des traitements associés aux applications.

Nous commencerons par examiner les réseaux de capteurs, puis les réseaux de RFID et l'interface NFC (Near Field Communication), qui est de plus en plus utilisée dans la connectique des « choses » au réseau Internet, ainsi que HIP (Host Identity Protocol), qui pourrait devenir le standard pour les passerelles d'interconnexion entre les « choses » et Internet.

Les réseaux de capteurs

Un réseau de capteurs se définit comme un ensemble de capteurs connectés entre eux, chaque capteur étant muni d'un émetteur-récepteur. Les réseaux de capteurs forment une nouvelle génération de réseaux aux propriétés spécifiques, qui n'entrent pas dans le cadre des architectures classiques. Cependant, l'arrivée de l'Internet des choses a modifié la vision des réseaux de capteurs, qui peuvent bien sûr continuer à constituer un ensemble fermé, mais également s'ouvrir sur Internet. Des capteurs assez particuliers proviennent de ce que l'on appelle les poussières intelligentes (*smart dust*). Ces poussières, pratiquement invisibles, possèdent un équipement radio en plus des traitements liés au capteur interne.

La miniaturisation des capteurs pose des problèmes de communication et de ressources d'énergie. Il faut que le capteur soit suffisamment intelligent pour rassembler l'information requise et l'émettre à bon escient. De plus, le processeur du capteur ne doit pas être utilisé trop intensivement afin de consommer le moins d'énergie possible. Il doit donc incorporer des éléments réactifs plutôt que cognitifs. Enfin, pour assurer un bon débit, la portée des émetteurs-récepteurs doit être nécessairement faible, de l'ordre d'une dizaine de mètres. La mise en place d'un réseau de capteurs pose donc des problèmes de routage, de contrôle des erreurs et de gestion de l'alimentation.

Du point de vue de la communication, l'environnement des protocoles IP est trop lourd et engendre un débit trop important et une surconsommation. Les solutions qui ont été dérivées des réseaux de terrain, ou réseaux industriels temps réel, présentent un meilleur compromis entre efficacité et énergie consommée. Comme les capteurs peuvent être disposés par centaine au mètre carré, l'adressage IPv6 représente une première solution évidente pour gérer le problème des adresses. Cependant, l'environnement IP est lourd, et l'implémentation dans ces réseaux de capteurs d'une pile protocolaire TCP/IP ou même UDP/IP est souvent impossible.

Pour le moment, les problèmes de sécurité et de qualité de service sont mis au second plan par rapport aux problèmes de consommation. Un champ de recherche important est en tout cas ouvert pour rendre les réseaux de capteurs efficaces et résistants.

Les principaux standards radio concernent ZigBee, que nous avons présenté au chapitre 20. WiBree et 6LowPAN forment d'autres solutions. Wibree est une technologie très basse consommation d'une portée de 10 m et d'un débit de 1 Mbit/s. Cette solution a été développée par Nokia pour concurrencer à la fois ZigBee et Bluetooth. Elle a pourtant été intégrée à Bluetooth en 2009 pour donner un produit appelé Bluetooth LE (Low Energy).

Les réseaux 6LowPAN (IPv6 over Low power Wireless Personal Area Networks) proviennent d'un groupe de travail de l'IETF. L'objectif est clairement de permettre la continuité du protocole IP sur des machines peu puissantes et avec une puissance électrique limitée.

L'utilisation de la norme IPv6 pour obtenir un très grand nombre d'adresses pour les immenses réseaux de capteurs pose problème. En effet, les 16 octets occupés par l'adresse de l'émetteur ajoutés aux 16 octets d'adresse du récepteur plus les champs obligatoires entraînent une mauvaise utilisation de la liaison radio pour transporter les informations de supervision. Cela peut devenir réellement problématique du fait du peu d'énergie dont dispose le capteur. ZigBee, au contraire, limite la longueur de sa trame à 127 octets, ce qui peut aussi poser des problèmes si l'information à transporter venant d'un capteur est longue.

Les réseaux de capteurs forment des réseaux mesh, et il leur faut un protocole de routage. L'utilisation d'un protocole comme IEEE 802.11s associé à des adresses IPv6 serait catastrophique pour la longévité de la batterie des capteurs. Pour cette raison, les propositions actuelles sont beaucoup plus simples, avec des protocoles comme LOAD (6LowPAN Ad-hoc Routing Protocol), une simplification d'AODV, DyMO-Low (Dynamic MANET On-demand for 6LowPAN), une simplification de DyMO, du groupe de travail MANET, et Hi-Low (Hierarchical Routing over 6LowPAN), qui comporte un adressage hiérarchique.

Ces différents protocoles proviennent de propositions de l'IETF et donc de la normalisation des réseaux ad-hoc, mais en ne prenant pas en compte toutes les options.

Une autre caractéristique importante des protocoles des réseaux de capteurs concerne la découverte de service, qui doit permettre la mise en marche du réseau de façon automatique. L'IETF joue également un rôle important dans ce domaine, en proposant plusieurs solutions, dont une orientée vers les capteurs : LowPAN Neighbor Discovery Extension. Ce protocole est une réduction de la norme Neighbor Discovery concernant tous les éléments consommateurs d'énergie, comme les broadcast et la gestion des multicast.

Un réseau de capteurs particulier est proposé par les poussières intelligentes, dont l'objectif est de développer des capteurs en nanotechnologie et de les relier entre eux par un réseau de type ad-hoc ou mesh. La poussière intelligente tient dans un espace inférieur au millimètre cube, d'où son nom de poussière. Dans cette poussière, se trouvent tous les composants nécessaires pour réaliser un ordinateur communiquant : un processeur, de la mémoire, de la radio, une batterie, etc.

La problématique principale est ici encore la sauvegarde de l'énergie lors de l'exécution des fonctions du capteur. En particulier, la partie réseau doit mener à des communications dépensant très peu d'énergie. L'université de Berkeley a ainsi conçu un système d'exploitation et des protocoles spécifiques, nommés TinyOS et Tiny protocol. Le TinyOS a été écrit dans un langage C simplifié, appelé nesC, qui est une sorte de dialecte destiné à optimiser l'utilisation de la mémoire.

RFID

La RFID (Radio-Frequency Identification), ou radio-identification, a été introduite pour réaliser une identification des objets, d'où son autre nom d'étiquette électronique.

Les étiquettes électroniques sont interrogées par un lecteur, qui permet de récupérer l'information d'identification. Les étiquettes électroniques sont utilisées dans de nombreuses applications, allant du suivi d'animaux à des étiquettes pour magasin.

Il existe deux grands types d'étiquettes électroniques : les étiquettes passives et les étiquettes actives. Les étiquettes passives ne possèdent aucune ressource d'énergie. Elles sont allumées par un lecteur qui procure un champ électromagnétique suffisant pour générer un courrant électrique permettant l'émission par une onde radio des éléments binaires stockés dans une mémoire EEPROM constituant l'identification RFID. Une étiquette passive est illustrée à la figure 24.1. L'antenne doit être architecturée de sorte à recevoir le champ électromagnétique du lecteur et émettre son identité.

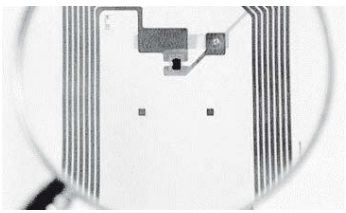


Figure 24.1
RFID passive

Une RFID passive peut être très petite. Les équipements nécessaires étant limités, des tailles d'un dixième de millimètre sur un dixième de millimètre sont suffisantes. Le prix d'une étiquette électronique dépend du nombre d'éléments fabriqués dans une même passe. Il est possible de descendre à cinq centimes d'euro.

Les étiquettes électroniques actives disposent d'une source d'alimentation électrique dans le composant. Le premier avantage très important de ces étiquettes tient à la qualité de la transmission. Une session peut être ouverte entre le lecteur et le RFID de telle sorte qu'une retransmission puisse être réalisée automatiquement en cas de problème. Un autre avantage est la transmission avec une portée de plusieurs mètres entre le RFID et le lecteur, au lieu de quelques centimètres. Un inconvénient pourrait être la durée de vie de la batterie. Cependant, pour une utilisation standard de quelques lectures par jour, il est possible de dépasser la dizaine d'années.

La RFID active peut posséder une mémoire plus importante pour le stockage d'attributs associés à la valeur de l'identité.

Une RFID active est illustrée à la figure 24.2.

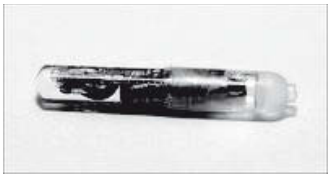


Figure 24.2
RFID active

Utilisation des RFID

Une application très connue des RFID est le passeport électronique. Le passeport électronique est défini dans le texte ICAO (International Civil Aviation Organization), Document 9303, Part 1, Volumes 1 et 2 (6e édition, 2006). Le composant de l'étiquette électronique contient les informations qui sont imprimées sur le passeport lui-même, ainsi qu'une photo numérisée du propriétaire du passeport.

Les titres de transport forment une seconde application des RFID. Par exemple, les tickets du métro parisien contiennent une étiquette électronique qui mémorise un ensemble d'informations comprenant la date et l'endroit de l'achat. Des solutions plus sophistiquées sont mises en œuvre dans les transports publics de Séoul, où l'étiquette devient active et contient de l'argent pour permettre l'utilisation d'un même ticket plusieurs fois.

Des barrières de péage pour autoroute utilisent également cette solution de RFID active, avec des portées de quelques mètres. L'étiquette active permet de soustraire le prix du péage de la somme d'argent stockée dans la mémoire. De même, des barrières de péage pour des remontées mécaniques dans de nombreuses stations de ski françaises utilisent des RFID actives.

Une autre application assez immédiate est le suivi des voitures pour détecter les voitures volées lors du passage près d'un lecteur.

Enfin, une des applications les plus connues concerne les inventaires et les achats dans les magasins. Les inventaires peuvent s'effectuer plus souvent et avec moins d'erreurs. Les achats posés dans un caddy peuvent de la même façon être lus par le lecteur et apporter une grande simplification à la procédure de paiement des achats dans un magasin.

La technologie RFID

Les fréquences de transmissions de la RFID sont indiquées au tableau 24.1. Elles sont déterminées par les organismes de normalisation locaux ou régionaux.

Fréquence pour les RFID	Commentaire
125 kHz (LF)	Première solution permettant une portée relativement importante pour les RFID passifs
13,56 MHz (HF)	Une des fréquences standardisées très utilisée pour les RFID passifs
400 MHz	Quelques utilisations spécifiques, comme la détection des voitures volées
865-868 MHz (UHF)	Bande de fréquences normalisées en Europe pour une utilisation intensive des RFID
902-928 MHz (UHF)	Bande de fréquences normalisée pour l'Amérique du Nord
2,4-2,483 5 GHz	Bande libre ISM dans laquelle devraient se développer de nombreuses applications RFID.

TABLEAU 24.1 • Fréquences de transmission des RFID

EPCglobal

Les RFID ont pour objectif de donner l'identité des objets auxquels ils sont adossés. La normalisation de cette indentification a été réalisée par le consortium EPCglobal. Deux générations sont disponibles : EPC Gen1 et EPC Gen2. Nous nous intéresserons surtout à cette deuxième génération, sortie mi-2006, qui a permis à la RFID de devenir une technique industrielle.

EPC Gen2 est l'acronyme d'EPCglobal UHF Class1 Generation 2. Cette spécification est sortie dans sa version 1.1 en mai 2006. Elle prend en charge le protocole entre le lecteur, d'une part, et la RFID et l'identification, d'autre part. L'objectif du protocole est de lire, écrire et tuer une RFID, de telle sorte que les lecteurs vendus par n'importe quel équipementier soient interchangeables.

La procédure de lecture est définie en utilisant un système à base de tranches temporelles (slots) muni d'un système anticollision. En effet, un lecteur pouvant allumer simultanément un grand nombre de RFID, des lectures simultanées des différentes étiquettes entraîneraient des collisions. Une signalisation permet de définir la fréquence, le codage utilisé (entre DSB-ASK, SSB-ASK et PR-ASK) et le débit du canal. Le système anticollision permet à chaque lecture simultanée que seulement la moitié des objets qui ont

pu transmettre puisse transmettre de nouveau dans la lecture suivante. Au bout d'un certain nombre de collisions, une seule RFID transmet avec succès. L'algorithme est conçu de telle sorte que chaque RFID passe ensuite à tour de rôle. La vitesse de lecture peut atteindre 640 Kbit/s.

L'identité de l'objet est déterminée par l'EPCglobal Electronic Product Code. La Gen1 utilise 96 bits tandis que la Gen2 passe à 256 bits de longueur. Un exemple de cette identification pour la Gen1 est illustré à la figure 24.3. La figure 24.4 indique les champs de l'identification dans la Gen2. Cette solution est beaucoup plus complexe, car elle fait appel à des filtres intermédiaires qui déterminent les longueurs des champs suivants. Il est à noter que le numéro de série passe de 36 à 140 bits, ce qui permet, pour un article donné, de ne jamais repasser par la valeur 0.

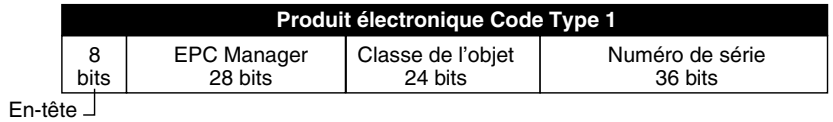


Figure 24.3

Structure de l'Electronic Product Code GEN1

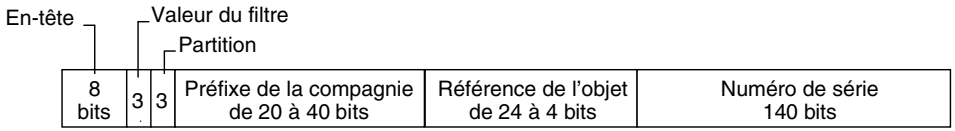


Figure 24.4

Structure de l'Electronic Product Code GEN2

Sécurité des RFID

La sécurité est un problème épineux du monde des RFID. En effet, la lecture d'une RFID passive peut se faire facilement à l'aide d'un lecteur d'une personne tierce. De même, la vie privée peut être mise à mal par le suivi et la traçabilité de tout ce qui concerne un individu.

Des solutions sont disponibles, comme le chiffrement de l'identifiant dans l'étiquette ou le changement de la valeur de l'étiquette après chaque lecture. Ces solutions reposent sur un middleware capable d'interpréter les valeurs des étiquettes ou de suivre les changements de valeur.

Les étiquettes actives peuvent ouvrir une session d'authentification permettant un échange avec le lecteur, qui joue alors le rôle de serveur d'authentification. Il faut dans ce cas un circuit électronique dans l'étiquette capable de chiffrer un texte émis par le serveur d'authentification. Cependant, la longueur des clés est si faible que la possibilité de les casser après une suite de tentatives d'authentification n'est pas négligeable. De nombreuses propositions ont été effectuées en utilisant l'algorithme anticollision, qui permet de sérialiser la lecture des étiquettes, pour l'authentification.

NFC (Near Field Comunication)

Le standard NFC est un cas particulier des communications RFID. Il permet de faire communiquer une RFID avec un lecteur sur une distance d'une dizaine de centimètres. Il s'agit d'une communication sans contact, avec, par exemple, une carte à puce ou un microcontrôleur sécurisé.

Les applications de ce type sont nombreuses et variées. La plus classique est le paiement sur téléphone mobile. Avec son mobile, un client peut recharger son compte par simple appel téléphonique ou transfert de donnée bas débit vers un serveur. Une fois le compte rechargé, le mobile sert de clé pour payer tout un ensemble de services. Pour l'utilisation du métro, par exemple, il suffit de passer le mobile près du lecteur pour que la communication radio valide l'achat du ticket.

Les débits de la communication NFC sont assez faibles : 106, 212, 424 et 848 Kbit/s. La gamme de fréquences est celle des 13,56 MHz. Les normes proviennent de l'ISO/IEC. Le Forum NFC a été crée par Philips et Sony.

La sécurité de la communication est assurée par la très petite distance entre l'émetteur et le récepteur et par la présence de la carte à puce.

HIP (Host Identity Protocol)

L'IETF a développé plusieurs mécanismes pour intégrer les choses dans l'Internet. HIP est une technologie d'identification qui fait partie de cet ensemble.

Le monde IP a deux grandes solutions de nommage : les adresses IP et le système de noms de domaine. HIP a pour objectif de séparer l'identificateur extrémité et la localisation des adresses IP. Il introduit pour cela un espace de nommage fondé sur une infrastructure PKI. Cet espace permet de gérer le multihoming d'une façon sécurisée. Les adresses IP sont remplacées par des identificateurs d'hôte chiffrés.

Conclusion

L'Internet des choses devient une réalité grâce aux RFID et aux capteurs. L'intégration de ces tout petits équipements est cependant loin d'être accomplie, car ils ne sont pas assez puissants pour supporter le protocole TCP/IP, assez gourmand en énergie. Pour y arriver, il faut faire appel à des passerelles très particulières, qui peuvent comprendre, d'un côté, les choses connectées et, de l'autre, Internet. Le protocole HIP pourrait devenir le standard de base de cette connectique.

Les poussières intelligentes (*smart dust*), qui proviennent du monde des nanotechnologies, forment une autre catégorie de choses en plein développement : sur l'équivalent d'une poussière, on trouve tous les composants nécessaires pour réaliser un petit ordinateur. La partie communication est prise en charge par un composant de type radio comportant une unité centrale, de la mémoire ainsi qu'un capteur miniature, de type

capteur de température ou de pression ou de tout autre élément de l'environnement humain. Un des exemples d'utilisation de cette technologie est le largage de plusieurs millions de poussières intégrant un thermomètre dans une forêt afin de détecter les incendies de forêt.

Partie VII

Contrôle, gestion et sécurité

Le contrôle et la gestion forment un ensemble de fonctionnalités indispensables à la vie d'un réseau. Le contrôle est un processus temps réel, mais pas la gestion. L'échelle de temps considérée est évidemment dépendante du type de processus. Comme il est parfois difficile de faire la différence entre contrôle et gestion, la tendance est de les regrouper dans un même plan, c'est-à-dire dans un réseau dont l'objectif est de réaliser une fonction, telle que transporter des données utilisateur, de la supervision ou des informations de gestion et de contrôle.

Le contrôle de congestion est sans conteste un contrôle puisque les nœuds doivent réagir instantanément sinon des paquets sont perdus. La planification est un processus de gestion puisque le temps pour prendre une décision peut être très grand par rapport à l'échelle de temps du réseau. La sécurité peut relever du contrôle, lorsqu'il faut réagir le plus rapidement possible pour éviter un arrêt du réseau, ou de la gestion, lorsqu'il faut mettre en place un mécanisme pour éviter des attaques.

Dans cette partie, nous allons faire le point sur les différentes solutions de gestion et de contrôle puis introduire la sécurité avec deux chapitres spécifiques, l'un orienté vers les protocoles généraux, l'autre vers le monde IP. Nous commencerons par les VLAN et les VPN, qui forment un ensemble d'instruments très importants dans le monde de la gestion et du contrôle.

25

VLAN et VPN

Un ensemble d'outils important pour le contrôle et la gestion de réseau provient des VLAN (Virtual LAN) et des VPN (Virtual Private Network). Les VLAN ont pour objectif de rassembler des machines dispersées géographiquement dans un réseau pour leur permettre de communiquer comme si elles étaient dans un même réseau local.

Les VPN ont un objectif assez différent, qui est de permettre à un opérateur de commercialiser des réseaux privés virtuels de telle sorte que le client pense qu'il dispose d'un réseau dédié. En fait, le réseau du client utilise des ressources du réseau de l'opérateur. L'avantage de l'opérateur est de multiplexer les ressources de son réseau entre tous ses clients. L'avantage du client est d'avoir un réseau personnel dont le coût est beaucoup plus abordable que s'il essayait de construire son propre réseau avec une infrastructure privée.

VLAN

On peut assimiler un VLAN à un VPN qui utiliserait comme réseau d'interconnexion le réseau local de l'entreprise au lieu du réseau d'un opérateur. La définition d'un VLAN peut prendre diverses formes, en fonction des éléments suivants :

- numéro de port ;
- protocole utilisé ;
- adresse MAC utilisée ;
- adresse IP ;
- adresse IP multicast ;
- application utilisée.

Un VLAN peut aussi être déterminé par une combinaison des critères précédents ainsi que par d'autres critères de gestion, comme l'utilisation d'un logiciel ou d'un matériel commun.

Les VLAN offrent une solution pour regrouper les stations et les serveurs en ensembles indépendants, de sorte à assurer une bonne sécurité des communications.

Ils peuvent être de différentes tailles, mais il est préférable de recourir à de petits VLAN, de quelques dizaines de stations tout au plus. Il faut en outre éviter de regrouper des stations qui ne sont pas situées dans la même zone de diffusion. Si c'est le cas, il faut gérer les tables de routage dans les routeurs d'interconnexion. Le champ permettant de réaliser cette diffusion vers l'ensemble des points d'accès du VLAN est situé dans la structure de trame illustrée à la figure 25.1.

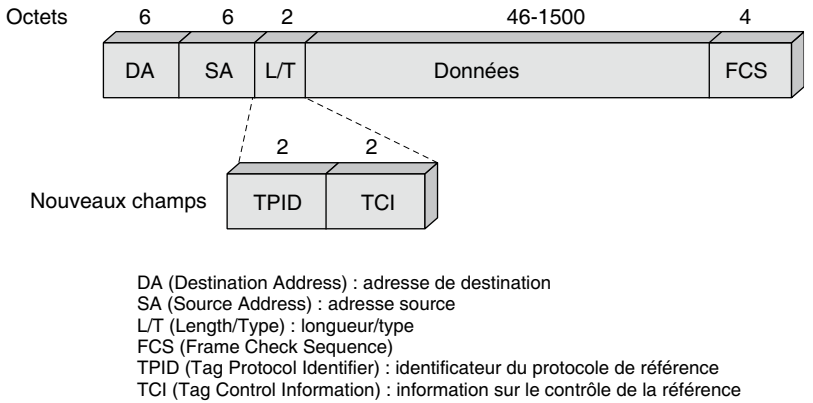


Figure 25.1

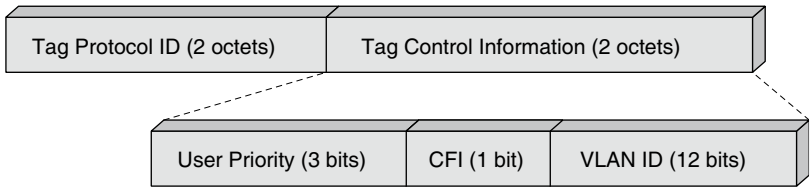
Nouveaux champs d'extension de la trame Ethernet pour les VLAN

La valeur du champ TPID (Tag Protocol IDentifier) n'a été définie que pour le cas Ethernet. Sa valeur est 0x8100.

Le champ TCI (Tag Control Information) est illustré à la figure 25.2. Il comprend :

- Un champ de niveaux de priorités sur trois éléments binaires, qui permet de déterminer jusqu'à huit niveaux de priorité.
- Un bit CFI (Canonical Format Indicator), qui indique que les données de la trame sont sous un format non canonique, c'est-à-dire non déterminé par des règles classiques.
- Un champ VLAN ID, qui identifie l'appartenance au VLAN de la trame et permet son routage vers les différents points du VLAN.

Les trois bits de priorité jouent un rôle de plus en plus important dans les VLAN avec qualité de service. Ils permettent de mettre en place une correspondance entre la gestion de la qualité de service DiffServ et le niveau trame du réseau Ethernet. Par exemple, un VLAN de téléphonie IP permet de réserver la plus haute priorité utilisateur, celle correspondant à la classe Expedited Forwarding (EF), de DiffServ, aux applications de téléphonie.



User Priority : priorité de l'utilisateur
CFI (Canonical Format Indicator) : identificateur du format canonique
VLAN ID (identificateur du VLAN)

Figure 25.2

Champ TCI de la trame Ethernet pour VLAN

Fonctionnement des VLAN

Le fonctionnement des VLAN est susceptible de varier selon les équipementiers et les normes. La manière de fonctionner d'un équipementier *X* peut être assez différente de celle d'une entreprise qui a programmé elle-même ses VLAN. Nous indiquons ci-après le fonctionnement le plus classique en essayant de pointer les modifications qui peuvent y être apportées.

Une règle assez utilisée est de permettre à une trame de n'être associée qu'à un seul VLAN. Outre cette règle assez générales, il est possible de refuser par programmation que la trame d'une machine appartenant à un VLAN puisse s'adresser à une machine qui n'est pas dans le VLAN. Cela permet de créer des groupes fermés et d'assurer ainsi une forte sécurité.

VLAN de niveau physique

Les VLAN de niveau physique (couche 1) fonctionnent sur des numéros de port physique. Une machine est rattachée à un port au travers de sa carte Ethernet. Un port est donc affecté à un VLAN unique. Cette solution très statique garantit une bonne étanchéité entre VLAN pour peu que les commutateurs soient dotés d'une programmation ne permettant pas aux trames Ethernet d'être acceptées ou nom en fonction de l'adresse VLAN. Elle manque cependant de souplesse puisqu'un utilisateur ne peut s'adresser qu'aux utilisateurs du même VLAN. Le concept est dans ce cas assez proche d'un VPN.

La figure 25.3 illustre le fonctionnement d'un VLAN de niveau physique. On voit que les machines sont rattachées entre elles par le biais des ports des deux commutateurs.

La mobilité d'une machine devient assez complexe puisqu'il faut associer le nouveau port au VLAN de la machine. De plus, si plusieurs utilisateurs se servent d'une même machine mais n'utilisent pas le même VLAN, la gestion devient particulièrement complexe puisqu'il faut reprogrammer le lien entre numéro de port et VLAN.

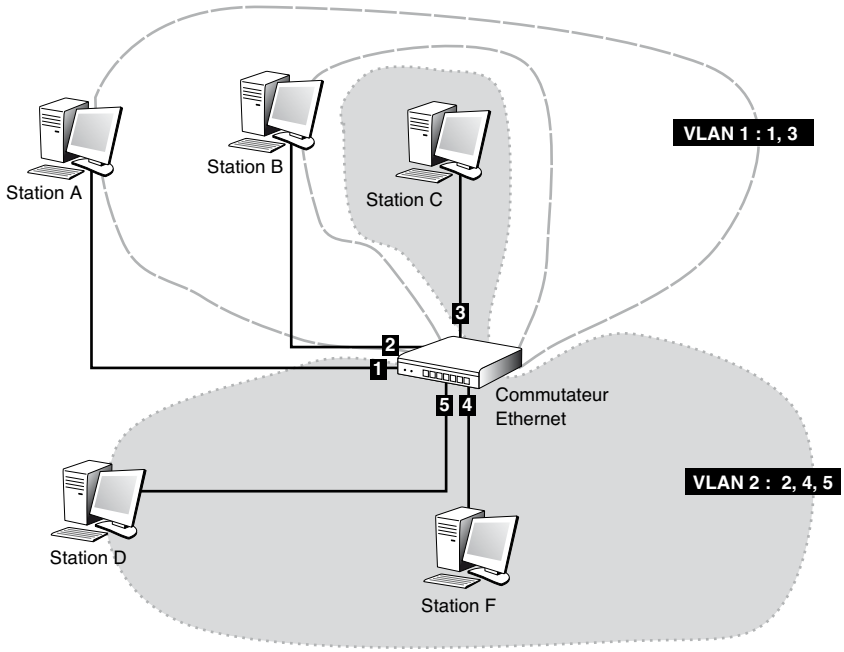


Figure 25.3

VLAN de niveau physique

VLAN de niveau trame

Pour réaliser des VLAN de niveau trame (couche 2, ou liaison), on affecte à chaque MAC un numéro de VLAN. En fonction de la table de commutation, qui associe des adresses MAC, pouvant être vues comme des références, à des ports de sortie, les trames sont acheminées vers les machines appartenant au VLAN. Les tables de commutation deviennent un peu plus complexes, puisque, associées à un même numéro de VLAN, il peut y avoir plusieurs adresses MAC et donc une émission de la trame sur plusieurs port de sortie du commutateur.

De nouveau, on peut accepter ou interdire par programmation qu'une machine associée à un VLAN puisse émettre hors de son VLAN. Un des avantages des VLAN de niveau trame est la plus grande souplesse qu'ils offrent pour gérer la mobilité des terminaux associés à des VLAN. Il suffit de reprogrammer les commutateurs pour modifier les tables de commutation. Cette reprogrammation peut s'effectuer automatiquement par apprentissage. Un exemple de VLAN de niveau trame est illustré à la figure 25.4.

VLAN de niveau paquet

Les VLAN de niveau paquet (couche 3, ou réseau) correspondent à des associations de numéros de VLAN et d'adresses IP. Une première difficulté provient de la façon d'accéder à l'adresse qui est encapsulée dans la zone de données de la trame. Le commutateur doit être capable de décapsuler la trame Ethernet, de retrouver le paquet et de déterminer l'adresse IP où

l'envoyer. Cette adresse IP permet d'associer le VLAN et de déterminer les ports de sortie du commutateur sur lesquels envoyer la trame reconstituée après réencapsulation du paquet dans la trame Ethernet. Un VLAN de niveau paquet est illustré à la figure 25.5.

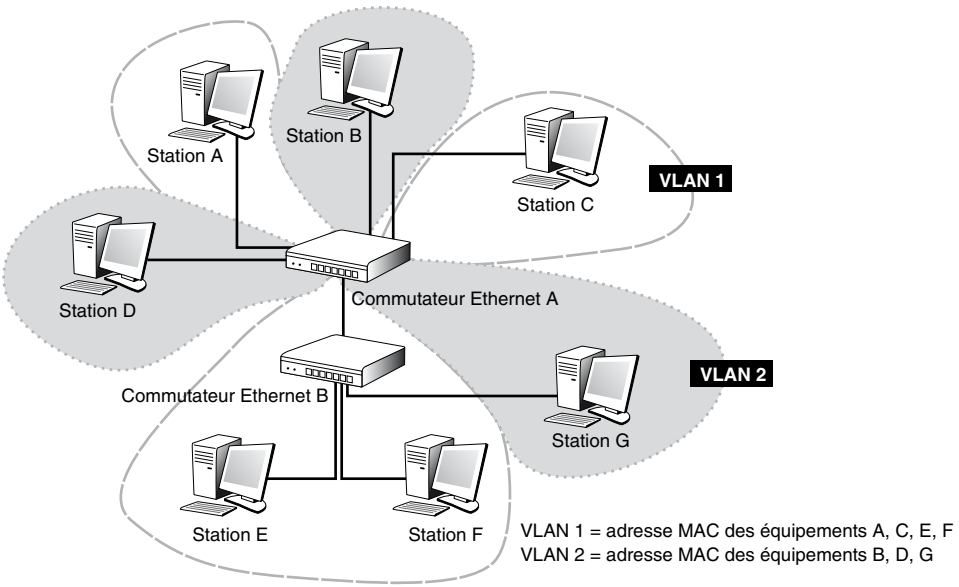


Figure 25.4
VLAN de niveau trame

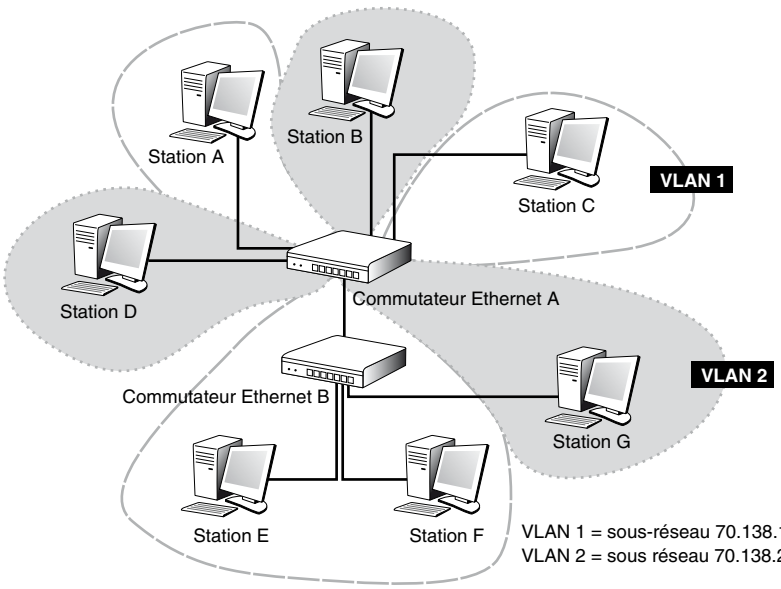


Figure 25.5
VLAN de niveau paquet

Autres VLAN

Les VLAN peuvent être associés à d'autres informations. Une des solutions classiques est l'utilisation de VLAN dans les réseaux Wi-Fi lorsque le point d'accès est capable de gérer plusieurs SSID, c'est-à-dire plusieurs noms de réseau. Le client voit ces réseaux comme des réseaux différents les uns des autres, et il se connecte à un réseau particulier, c'est-à-dire un SSID spécifique.

Au SSID correspond en général un VLAN, ce qui implique que la trame est envoyée uniquement aux machines associées à ce VLAN. Si la programmation du réseau se fait classiquement en empêchant la sortie du VLAN, le client connecté au réseau Wi-Fi ne pourra atteindre que les machines du VLAN.

Une application classique de cette solution est de permettre à des visiteurs étrangers à une entreprise de se connecter au réseau de l'entreprise. Cependant, par l'intermédiaire du VLAN, les trames des visiteurs vont directement sur une machine de sortie de l'entreprise pour leur permettre d'avoir un accès à Internet. Les VLAN qui ne sont pas ceux des visiteurs disposent d'une sécurité WPA, alors que le point d'accès est ouvert aux visiteurs (hotspot).

Un autre type de VLAN utile dans certains cas correspond à une classification protocolaire ou applicative. Par exemple, en fonction du protocole utilisé par un utilisateur, le VLAN associé peut permettre de diffuser les messages à tous ceux qui utilisent le même protocole. Par exemple, un protocole de signalisation téléphonique peut permettre de diffuser les trames à toutes les machines utilisant la signalisation téléphonique.

La difficulté principale avec ce type de VLAN réside dans la reconnaissance de l'information qui permet de déterminer le VLAN. Cela peut être le numéro de port de l'application (80 pour l'application HTTP). Encore faut-il que ce numéro puisse être récupéré à partir des trames ATM, puisqu'il se trouve au niveau TCP et dans certaines trames seulement. Il faut donc être capable de déterminer l'application sur la première trame, puis de tracer les trames suivantes sur les adresses MAC extrémité et enfin de vérifier régulièrement que l'application n'a pas changé.

VPN

Les VPN (Virtual Private Network), ou réseaux privés virtuels, forment une classe particulière de réseaux partagés. Dans de tels réseaux, les ressources d'un réseau réel peuvent se trouver distribuées à un instant donné entre plusieurs réseaux, de telle sorte que chaque sous-réseau puisse croire que le réseau réel appartient à lui seul.

Cette section décrit les différentes catégories de réseaux privés virtuels permettant d'introduire des fonctions susceptibles d'améliorer la gestion d'une entreprise. Ces catégories proviennent soit du type de réseau mis en place, soit du niveau d'architecture, trame ou paquet, soit encore du type de fonction recherchée (sécurité, qualité de service, etc.). Ces différentes catégories ne sont pas indépendantes mais se recoupent. Par exemple, un VPN IP est à la fois un VPN permettant de créer un réseau virtuel IP et un VPN de niveau paquet. De même, un VPN IPsec est à la fois un VPN de niveau paquet et un VPN de sécurité. Les VPN MPLS sont plus complexes, car ils appartiennent à la fois au niveau trame et au niveau paquet.

Architecture des VPN

Un réseau privé virtuel peut être défini comme un ensemble de ressources susceptibles d'être partagées par des flots de paquets ou de trames provenant de machines autorisées. Les VPN peuvent utiliser des technologies et des protocoles quelconques. La gestion de ces ressources nécessite un haut niveau d'automatisation pour obtenir la dynamique nécessaire au fonctionnement d'un VPN. Pour obtenir cette dynamique, les ressources permettant d'acheminer les paquets au destinataire doivent être gérées avec efficacité.

Les informations de gestion à prendre en compte pour cela sont les suivantes :

- Informations de topologie, permettant de déterminer les points d'accès vers les sites qui doivent être interconnectés par le VPN.
- Informations d'adressage, permettant la localisation des points d'accès et des sites qui doivent être interconnectés par le VPN.
- Informations de routage, qui permettent d'atteindre les sites du VPN.
- Informations de sécurité, pour l'établissement et l'activation des filtres laissant ou non passer les paquets.
- Informations de qualité de service, en d'autres termes les paramètres déterminés dans le SLS (Service Level Specification) pour le contrôle des ressources nécessaires à la qualité de service.

Catégories de VPN

Les catégories de VPN permettent de différencier ces derniers suivant différents critères, tels que le type de réseau mis en place, comme les VPN d'entreprise, le niveau auquel est géré le VPN, niveau trame ou niveau paquet, le protocole utilisé ou le type de fonction recherché, comme la sécurité ou la qualité de service. Toutes ces catégories se recoupent fortement, comme nous allons le voir.

Deux grandes catégories permettent toutefois de classifier les VPN en fonction de celui qui gère le réseau :

- Les VPN d'entreprise, qui forment le réseau logique d'interconnexion de plusieurs sites d'une entreprise, permettent en outre à des utilisateurs hors des sites de se connecter sur ce réseau logique.
- Les VPN d'opérateurs, qui forment le réseau physique et permettent de constituer des réseaux logiques pour les entreprises.

Dans la première catégorie, on trouve les VPN IPsec, les VPN SSL et les VPN d'encapsulation permettant de réaliser des tunnels entre les points d'accès aux différents sites d'une entreprise. Dans la deuxième catégorie, on trouve les VPN qui font appel à des chemins de niveau 2 pour être mis à la disposition des entreprises.

Les VPN classés par niveau de protocole sont les VPN de niveau trame, de niveau paquet et de niveau applicatif.

Ce chapitre introduit d'abord les VPN d'entreprise et d'opérateurs puis examine les propriétés des VPN par niveau de protocole et par fonctionnalité.

VPN d'entreprise

Les entreprises doivent prendre en charge un nombre croissant d'utilisateurs, qui peuvent être fixes, connectés par un réseau sans fil ou reliés à un réseau de mobiles. Un VPN d'entreprise répond à ces exigences en constituant un réseau capable de desservir ces différents utilisateurs grâce à l'apport de fonctionnalités spécifiques.

Les VPN d'entreprise et les CPE-VPN (Customer Premise Equipment-VPN) sont des réseaux de données privés qui permettent de partager les infrastructures de télécommunications d'un opérateur entre plusieurs entreprises clientes, tout en maintenant une confidentialité des transmissions par l'utilisation de tunnels et de procédures de sécurité. Ces solutions sont totalement différentes des réseaux privés ou des réseaux loués, dans lesquels l'infrastructure n'appartient qu'à l'entreprise qui l'a achetée ou qui loue les lignes de communication. Les infrastructures ne sont pas partagées avec d'autres utilisateurs.

Un CPE-VPN ne s'occupe que des liaisons intersites tandis qu'un VPN d'entreprise est plus large, incluant la possibilité pour un client se trouvant à l'extérieur de l'entreprise de se connecter aux différents sites de l'entreprise.

Le rôle des VPN d'entreprise est de permettre à une société de posséder un réseau en propre, comme si l'infrastructure lui appartenait, à un coût très inférieur à celui de l'achat d'un réseau privé. Fonction essentielle de ces réseaux, la sécurité doit permettre aux différents usagers qui se partagent les ressources d'être protégés des écoutes. Cette catégorie de VPN a été la première à s'imposer.

La gestion globale de VPN de ce type peut être effectuée dans la partie du réseau appartenant à l'entreprise. L'opérateur qui fournit les ressources pour l'interconnexion des réseaux de l'entreprise ne fait que diriger les paquets d'un site à un autre par le biais d'un tunnel, sans que le client puisse voir par où passent les paquets entre l'entrée du tunnel et la sortie. Ce qui se passe entre l'entrée et la sortie ne concerne pas le client. Le filtrage des paquets est effectué par les machines d'accès, qui appartiennent au client et se situent à l'entrée et à la sortie du tunnel. L'opérateur du réseau utilisé pour réaliser le VPN n'offre aucun service supplémentaire. Il se contente de vendre des tunnels dans son réseau. La gestion et la sécurité des VPN sont effectuées par l'utilisateur.

Le réseau d'interconnexion, qui est de plus en plus souvent le réseau Internet, est utilisé comme réseau d'opérateur. Cela permet d'obtenir des interconnexions à partir de n'importe quel point du globe à un coût très bas. Les limites de cette catégorie de VPN résident dans l'impossibilité d'offrir de la qualité de service sur Internet.

Une nouvelle génération de VPN d'entreprise est apparue au milieu des années 1990 avec l'arrivée d'opérateurs de VPN offrant des fonctionnalités supplémentaires. Dans ces nouveaux réseaux, un SLA (Service Level Agreement) est négocié entre l'opérateur et l'entreprise pour définir précisément les droits de chacun et les performances attendues dans le VPN. La partie technique du SLA est le SLS. Si l'entreprise souhaite faire transiter de la parole téléphonique, le SLS propose un temps de transfert dans le réseau de l'opérateur inférieur à une cinquantaine de millisecondes. La demande de l'entreprise peut porter sur d'autres propriétés, comme la sécurité ou la mobilité. La gestion du

VPN est généralement effectuée par l'opérateur et non plus par le réseau du client. Nous revenons sur ce type de VPN dans la suite du chapitre.

VPN d'opérateurs

Les opérateurs ont réagi rapidement à la demande de VPN des entreprises. Après avoir mis en place des réseaux loués, qui n'appartenaient qu'à l'entreprise cliente, ils ont proposé des solutions de partage des infrastructures en sécurisant suffisamment les connexions de site à site par des protocoles de type IPsec ou SSL. L'avantage de cette offre à partir d'un réseau partagé est de permettre à un client extérieur aux sites de l'entreprise de se connecter de façon sécurisée, comme s'il était dans l'entreprise.

Au départ, les VPN d'opérateurs provenaient de la mise en place de tunnels PPTP, L2F, L2TP mais aussi MPLS, que nous examinons plus en détail à la section suivante. Ils ont ensuite offert les services sur mesure que nous connaissons actuellement, que ce soit pour la sécurité, la qualité de service ou la gestion de la mobilité. La négociation avec l'opérateur s'effectue par le biais d'un SLA, sa partie technique, le SLS, indiquant les performances attendues du VPN. Par exemple, si la société veut y faire transiter sa téléphonie privée, il faut que le temps de traversée des tunnels ne dépasse pas la cinquantaine de millisecondes.

Pour réaliser ces diverses fonctionnalités, l'opérateur doit posséder un réseau dont il sait lui-même apprécier la qualité de service. C'est la raison pour laquelle la plupart des opérateurs de VPN mettent en place des réseaux MPLS sur lesquels une ingénierie de performance est disponible.

VPN de niveaux trame, paquet et application

Les VPN de niveau trame, de niveau paquet et de niveau application datent de la fin des années 1990. Ils sont caractérisés par des tunnels, qui permettent le transit des trames, pour les VPN de niveau trame, des paquets, pour les VPN de niveau paquet, ou des messages, pour les VPN de niveau application. Les avantages et les inconvénients de ces VPN sont semblables à ceux des architectures des niveaux correspondants.

Un VPN peut donc se définir par le niveau d'architecture déterminé par la technologie employée. Par exemple, si le VPN est constitué de réseaux Ethernet, il est de niveau trame (couche 2). Si le VPN est constitué de réseaux IP, c'est un VPN de niveau paquet (couche 3). Si le VPN est mis en place pour une application comme HTTP, le VPN est de niveau application (couche 7).

Les sections qui suivent détaillent ces différentes catégories de VPN.

VPN de niveau trame

Les premiers VPN d'entreprise mis en place étaient de niveau trame. Leur rôle était de transporter des trames d'un port d'entrée vers un port de sortie, comme illustré à la figure 25.6.

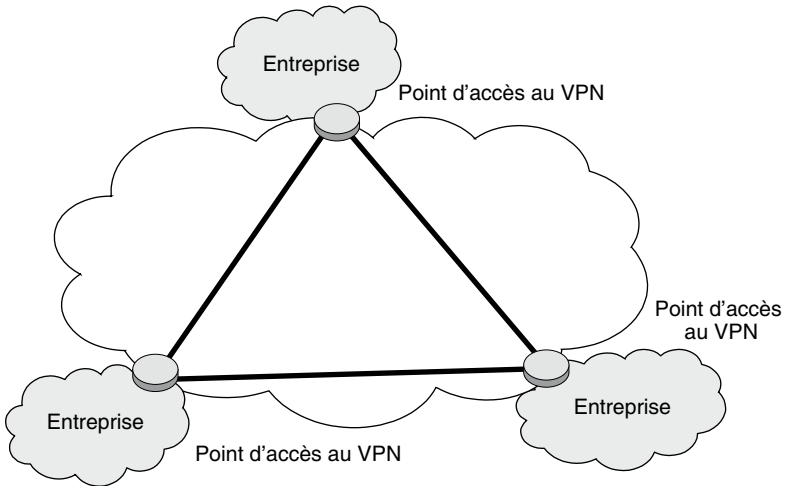


Figure 25.6

Exemple de VPN de niveau trame

Dans ce type de VPN, les trois accès à l'utilisateur sont interconnectés par des circuits virtuels permanents de niveau trame, qui peuvent provenir d'un relais de trames ou d'un réseau ATM. Les fonctions de filtrage, pour ne laisser entrer que les trames des utilisateurs du VPN, sont assurées par les points d'accès appartenant à l'entreprise. L'opérateur ne fait que fournir les circuits virtuels qui acheminent les paquets IP encapsulés dans les trames LAP-D d'un relais de trames ou les cellules d'un réseau ATM. Éventuellement, l'opérateur peut introduire un centre de gestion capable de configurer les points d'accès de l'utilisateur et d'apporter une intelligence au VPN.

De nombreux autres types de tunnels peuvent être mis en œuvre pour réaliser ces VPN, mais ces solutions sont plutôt en décroissance aujourd'hui. On peut citer en premier lieu le protocole PPTP (Point-to-Point Tunneling Protocol), surtout poussé par Microsoft et utilisant des techniques d'authentification du client qui se connecte par des techniques telles que MS-Chap. L'objectif de cette solution est de connecter un client à son entreprise par le biais d'un tunnel prenant son départ dans le réseau du FAI. Le paquet IP est encapsulé dans une trame PPP, laquelle peut être chiffrée puis elle-même encapsulée dans la trame d'un protocole qui forme un tunnel, par exemple, L2TP. Cette dernière encapsulation utilise le protocole GRE (Generic Routing Encapsulation) normalisé par l'IETF dans les RFC 1701 et 1702.

Une autre solution de tunnel, proposée par Cisco Systems avec L2F (Layer 2 Forwarding), définie par la RFC 2341, reste peu utilisée. Une dernière solution, plus fortement utilisée, est le tunnel L2TP (Layer 2 Tunneling Protocol), développé à partir de 1999 et normalisé par l'IETF dans la RFC 2661. L'objectif de cette solution est d'étendre les deux techniques de tunnel précédentes en permettant l'accès par modem ADSL. Dans cette solution, des trames PPP sont encapsulées dans des trames L2TP. La version L2TPv3

étend l'identification de tunnel de 16 à 32 bits. Cela permet d'augmenter le nombre de tunnels et de s'adapter ainsi beaucoup mieux aux réseaux à très haut débit.

Une nouvelle génération de VPN de niveau trame, les VPN Ethernet, a fait son apparition au début des années 2000 pour réaliser des VPN peu onéreux et offrant une grande souplesse d'utilisation. Les VPN Ethernet sont conçus autour des réseaux Ethernet, que ces derniers soient partagés ou commutés. Ces VPN ressemblent aux VPN de niveau paquet (*voir ci-après*), dans lesquels les paquets IP sont remplacés par des trames Ethernet. Les équipements Ethernet peuvent être dispersés sur toute la planète tout en appartenant à un même VPN, le point d'accès étant l'équipement lui-même, muni de son adresse Ethernet.

Les VPN de niveau trame sont aujourd'hui délaissés au profit des VPN de niveau paquet, qui offrent plus de souplesse, comme nous allons le voir.

VPN de niveau paquet

Le niveau paquet (couche 3) étant aujourd'hui un niveau IP, les VPN de niveau paquet sont appelés VPN IP. Cette génération de VPN date du début des années 2000. Elle permet de rassembler toutes les propriétés que l'on peut trouver dans les réseaux intranet et extranet, notamment le système d'information d'une entreprise distribuée. La solution IP permet d'intégrer à la fois des terminaux fixes et des terminaux mobiles.

Un VPN IP est illustré à la figure 25.7. Les entreprises A, B et C ont des VPN de niveau IP. Leurs points d'accès sont des routeurs IP, qui laissent entrer et sortir de l'entreprise les paquets IP destinés aux autres succursales.

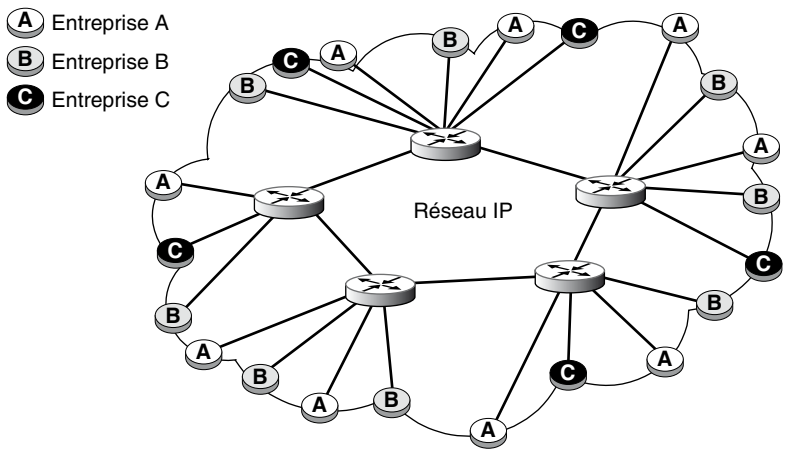


Figure 25.7
Exemple de VPN IP

Sur cette figure, les clients d'un même VPN utilisent le réseau IP pour aller d'un point d'accès à un autre point d'accès appartenant au VPN. La qualité de service et la sécurité sont prises en charge par l'utilisateur. Comme la sécurité est un élément essentiel de ces

réseaux, la première génération de VPN IP a utilisé le protocole IPsec pour réaliser les communications. Ce protocole permet de créer des tunnels chiffrés en proposant à l'utilisateur de choisir ses algorithmes de chiffrement et d'authentification. Les points d'accès des VPN communiquent entre eux par l'intermédiaire de ces tunnels chiffrés.

Une difficulté nouvelle pour l'opérateur consiste à configurer les nœuds dynamiquement, de sorte à rendre le service défini par l'ensemble des SLA. Une solution qui se développe, que nous examinons un peu plus loin, repose sur la configuration par politique. Avant d'examiner cette technique de configuration, nous allons introduire les autres types de VPN.

VPN MPLS

Une grande tendance du début des années 2000 en matière de VPN a consisté à utiliser des réseaux MPLS. La souplesse de MPLS autorise l'utilisation de fonctionnalités de niveau trame et paquet.

MPLS met en place des tunnels, appelés LSP (Label Switched Path), qui ne sont autres que des circuits virtuels. Ces LSP sont toutefois beaucoup plus souples d'usage que des circuits virtuels et offrent en outre une qualité de service. La figure 25.8 illustre le premier modèle de VPN MPLS utilisé, le modèle *overlay* (recouvrement). Il ressemble aux VPN d'entreprise en ce qu'il confie à un opérateur externe la mise en place d'un réseau à partir d'une infrastructure partagée. Sur la figure, deux entreprises se partagent un réseau d'opérateur avec des LSP différents. L'une des entreprises possède un point d'accès, sur lequel arrivent deux LSP, provenant de deux autres sites, pour des raisons de fiabilité : si l'un des points d'accès tombe en panne, le second continue à offrir le service. La restriction fondamentale de ce modèle réside dans la scalabilité, ou passage à l'échelle, qui est extrêmement coûteuse, puisque, si dix sites existent déjà et que l'on veuille en ajouter un onzième, il faut mettre en place dix nouveaux LSP.

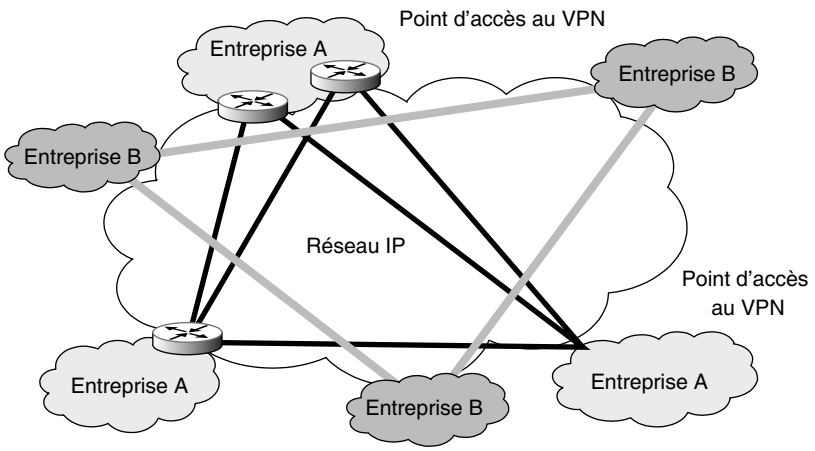


Figure 25.8
Exemple de VPN MPLS overlay

Une deuxième solution de VPN MPLS, appelée *peer model*, rend possible le passage à l'échelle, ou scalabilité, en facilitant l'augmentation du nombre de sites à interconnecter. Ce modèle doit permettre à l'opérateur de VPN d'augmenter le nombre de VPN jusqu'à atteindre plusieurs centaines de milliers de sites, si nécessaire. Une autre fonction sous-jacente de ces VPN Peer concerne la possibilité pour l'opérateur d'offrir de nouveaux services sur mesure à l'utilisateur et de prendre en charge son infrastructure réseau, surtout si l'utilisateur n'a pas de fortes compétences dans le domaine du routage Internet.

Cette solution combine les apports de plusieurs technologies :

- Les informations de routage sont distribuées partiellement.
- Les tables de routage sont multiples.
- Les adresses utilisées sont du nouveau type VPN IP.

La figure 25.9 illustre un VPN Peer. La différence essentielle avec le modèle overlay provient du routeur d'accès à MPLS. Dans l'overlay, le point d'accès au réseau MPLS se trouve dans le réseau utilisateur. Dans le modèle VPN Peer, le routeur d'accès se trouve chez l'opérateur, de sorte qu'un flot provenant d'un client du VPN peut se diriger à volonté vers n'importe quel point du VPN en utilisant le réseau MPLS.

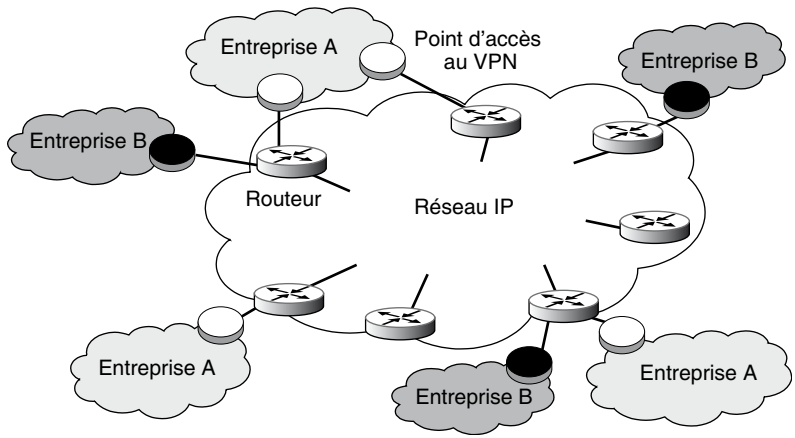


Figure 25.9
Exemple de VPN MPLS Peer

Le premier algorithme de routage à mettre en œuvre pour router les paquets doit assurer une connectivité entre les sites. Ce routage peut n'être défini que pour l'entreprise A, l'entreprise B pouvant avoir un autre protocole de routage ou travailler avec un autre algorithme pour déterminer le routage. L'algorithme de routage le plus classique dans les VPN MPLS utilise le protocole BGP (Border Gateway Protocol).

Quatre étapes définissent la distribution des éléments de routage :

1. Les informations de routage proviennent du client et sont envoyées vers le point d'accès de l'opérateur. Les protocoles RIP (Routing Information Protocol), OSPF (Open Shortest Path First) et BGP peuvent être utilisés par le client du VPN.

2. Au point d'entrée de l'opérateur, les informations de routage sont exportées dans l'algorithme BGP de l'opérateur.
3. Au point de sortie, les informations BGP sont rassemblées pour être transmises vers l'utilisateur.
4. Toujours au point de sortie, les informations de routage sont exportées vers l'utilisateur sous une forme propre à l'utilisateur.

Cette solution permet de transporter sur un VPN MPLS BGP les informations d'un point du VPN vers n'importe quel autre point du VPN. Grâce à ce mécanisme, des tables de routage spécifiques peuvent être mises en place pour chaque VPN.

Un problème d'adressage est posé par le fait que le routage BGP utilisé par l'opérateur suppose que l'adresse IP soit unique pour un utilisateur. Or ce n'est pas vrai puisqu'un client peut utiliser plusieurs VPN simultanément dans un même réseau d'opérateur. Une solution à ce problème consiste à rendre les adresses utilisées sur plusieurs VPN uniques pour chaque VPN en créant à cet effet de nouvelles adresses, dites adresses VPN IP. Ces adresses sont construites par concaténation d'un champ de longueur fixe, appelé Route Distinguisher, et d'une adresse IP standard. Le rôle de ce champ est de rendre unique l'adresse globale d'un utilisateur vis-à-vis de l'opérateur. Pour être sûr que cette adresse globale est unique, le Route Distinguisher contient trois champs : le type, sur 2 octets, le numéro du système autonome, sur 2 octets également, et un numéro déterminé par l'opérateur du VPN, sur 4 octets. Pour l'algorithme BGP, il n'y a aucune différence entre travailler sur la seule adresse IP ou sur l'adresse VPN IP.

Ces VPN MPLS BGP des opérateurs offrent une grande souplesse à leurs clients. Un de leurs grands avantages est qu'ils peuvent utiliser des LSP avec des classes de priorités. Cela permet à un utilisateur de travailler avec des classes de services correspondant à ces priorités. Ces VPN procurent en outre à l'opérateur des fonctionnalités spécifiques, allant de la configuration au traitement d'applications de diverses natures. L'avantage pour l'entreprise est de pouvoir externaliser de nombreux services auprès de l'opérateur de VPN.

VPN de niveau application

Le niveau application (couche 7) peut également être utilisé pour mettre en place des VPN. Dans ce cas, seule l'application concernée est transportée dans le tunnel. Le plus classique de ces VPN est le VPN SSL, qui utilise un tunnel SSL. SSL (Secure Sockets Layer) a été créé par Netscape pour protéger le transport de pages Web entre un client et un serveur. Présenté en détail au chapitre 28, SSL a été étendu à plusieurs reprises par les versions v2 puis v3. Une déclinaison importante a été apportée ensuite par TLS (Transport Layer Security), qui peut être considéré comme la version v3.1 de SSL.

SSL assure l'authentification du serveur de telle sorte que le client sache qu'il s'adresse au bon serveur. Cette authentification s'appuie sur un chiffrement asymétrique, par le biais de certificats à clé publique (*voir le chapitre 28*). SSL s'appuie essentiellement sur HTTP, mais d'autres protocoles peuvent l'utiliser, comme HTTPS (HyperText Transfer Protocol Secure sockets), LDAPS, Telnet, IMAPS, POP3S, etc.

On compare souvent les VPN IPsec et SSL. Il existe en effet beaucoup de similitudes entre eux, mais également d'importantes différences, en particulier le fait qu'ils ne sont pas situés au même niveau de l'architecture : paquet pour IPsec et application pour SSL. Un VPN SSL ne prend en compte que les applications qui lui sont associées et a l'avantage d'être plus léger qu'un VPN IPsec, lequel ne fait pas de distinction entre les applications et peut prendre en charge tous les types de flux.

VPN fonctionnels

Les VPN peuvent se concevoir pour réaliser des tâches particulières, comme la sécurité ou la qualité de service, mais aussi des tâches beaucoup plus spécifiques, comme le partage d'une ressource. Le cas le plus classique pour l'opérateur de VPN est d'offrir les fonctions de portail d'accès, de logiciel applicatif, de machine de calcul ou de PABX IP.

VPN de sécurité

Les VPN utilisent une infrastructure d'interconnexion qui peut être publique ou privée. L'infrastructure publique se ramène essentiellement à Internet. La sécurité étant évidemment moins forte dans ce cas, la mise en place de pare-feu et de modules de chiffrement et d'identification est impérative.

La sécurité d'un VPN est assurée dans le cas classique par les tunnels qui sont mis en place entre les points d'accès du VPN. Un simple circuit virtuel propose déjà une sécurité importante, puisqu'il est assez difficile pour un utilisateur externe de prendre la place d'un autre en utilisant les références adéquates.

Pour bénéficier d'une sécurité complète, il faut une authentification des équipements aux deux extrémités puis une autorisation et enfin un chiffrement. Ces différentes fonctions peuvent être réalisées par l'intermédiaire de serveurs AAA (Authentication, Authorization, Accounting) par l'intermédiaire de protocoles tels que RADIUS ou Diameter (*voir le chapitre 27*).

Les échanges au sein de l'opérateur de VPN peuvent être sécurisés en utilisant des tunnels dans lesquels trames, paquets ou messages sont chiffrés. Les circuits virtuels étant déjà des sortes de tunnels, il suffit de chiffrer les paquets avant de les émettre. Une solution pour cela consiste à utiliser IPsec, qui donne un cadre normalisé à la fois au tunnel et au chiffrement.

Les pare-feu forment une autre pièce essentielle de l'accès sécurisé au réseau de l'utilisateur en empêchant les flux non désirés d'entrer dans le réseau du client du VPN. Les pare-feu ont pour rôle de filtrer les flux en les reconnaissant. La méthode la plus classique de filtrage consiste à examiner la valeur du port, transportée par les protocoles TCP et UDP, et à en déduire si le type d'application est acceptable ou non par le VPN.

VPN de qualité de service

Les VPN peuvent procurer une qualité de service aux applications de l'utilisateur. Pour cela, il faut que le réseau de l'opérateur puisse effectuer une différenciation du trafic. Cela

revient, d'une part, à reconnaître le trafic et à le classer et, d'autre part, à mettre à disposition du VPN un mécanisme capable de gérer la qualité de service.

Ce mécanisme peut être d'un des quatre types suivants :

- Le réseau de l'opérateur est surdimensionné, et les paquets du client voient le réseau comme étant vide et donc le traversent rapidement.
- Le réseau obéit à la gestion de qualité de service DiffServ et classifie les flots grâce à des classificateurs.
- Le réseau est de type MPLS, et divers LSP, correspondant aux qualités de service, sont ouverts. L'avantage de cette solution est la forte sécurisation de la qualité de service.
- Le réseau est géré par politique, et la qualité de service est garantie par une configuration automatique des routeurs.

La qualité de service est souvent négociée entre l'utilisateur et l'opérateur de VPN par un SLA, qui permet de définir de façon explicite à la fois les attentes de l'utilisateur et les engagements de l'opérateur. Les SLA portent souvent sur des temps de transit au travers du réseau de l'opérateur ou sur des taux de perte de paquet mais aussi sur des paramètres plus spécifiques, comme le moment d'ordre 2 du temps de réponse. Par exemple, pour un VPN capable de faire transiter de la parole téléphonique, il faut un temps de transit limité, qui ne dépasse pas 50 ms. Il faut de surcroît s'assurer que les 50 ms représentent un temps maximal de traversée, et non un temps moyen. Avec un temps moyen de 50 ms et une très forte variance du temps de réponse, il serait impossible de réaliser de la téléphonie sur IP.

La qualité de service est de plus en plus proposée par les VPN et demandée par les utilisateurs.

Configuration d'un VPN par politique

Une difficulté rencontrée par les opérateurs concerne la configuration de leur réseau pour permettre aux différentes entreprises connectées d'obtenir les performances qu'elles sont en droit d'attendre après négociation de leur SLA.

Une solution à ce problème se fonde sur la gestion par politique, décrite en détail à l'annexe S.

Conclusion

La gestion et le contrôle de réseau représentent un objectif que remplissent aussi bien les VLAN que les VPN. Quasiment tous les réseaux se servent de l'un ou de l'autre et bien souvent des deux. Les VLAN visent beaucoup plus le contrôle des réseaux d'entreprise en permettant de créer des sous-ensembles capables d'avoir une certaine étanchéité à l'égard des autres VLAN et de construire le réseau d'une entreprise en fonction des contraintes et caractéristiques de l'entreprise.

Les VPN concernent davantage les opérateurs, qui peuvent ainsi proposer à leurs clients différents types de VPN, classiques, comme les VPN d'entreprise, ou spécialisés. Les VPN forment un paradigme, qui permet à l'ensemble des entreprises, même les plus petites, de s'offrir un réseau privé. Dans le même temps, ils deviennent de plus en plus sophistiqués et permettent de prendre en charge le contrôle et la gestion des réseaux d'entreprise. Ils sont de ce fait promis à un grand avenir.

La technologie Ethernet Carrier Grade permet d'encapsuler les VPN et d'apporter ainsi à la fois de la sécurité et de la qualité de service.

26

La gestion de réseau

La gestion de réseau correspond aux actions de gestion qui permettent de prendre en charge la configuration, la sécurité, les pannes, l'audit des performances, la comptabilité. La prise en charge de toutes ces fonctions n'est pas un mince problème. De nombreux travaux de normalisation ont été effectués dans ce domaine, mais tous n'ont pas encore abouti. Cependant, une architecture de gestion de réseau et certains protocoles et services ont déjà été adoptés comme standards. Deux grandes tendances se font jour depuis plusieurs années : associer la gestion de service à la gestion de réseau et rapprocher la gestion de réseau et le contrôle de réseau.

La gestion de réseau recouvre de nombreuses opérations, telles que l'initialisation des paramètres de configuration du système, la gestion des erreurs, les statistiques, les diagnostics, la gestion des alarmes et leur rapport, la reconfiguration, la gestion des ressources, la sécurité, etc. Ces activités sont présentées plus précisément par la suite.

Pour interconnecter deux systèmes de gestion, une norme doit être respectée, qu'elle soit de droit ou de fait. Dans les normes de droit, on retrouve la normalisation provenant de l'ISO, que l'on appelle CMIS/CMIP, et celle de l'UIT-T, qui porte le nom de TMN (Telecommunications Management Network), en français RGT (réseau de gestion des télécommunications). Ces deux normes ne sont pas tant concurrentes que complémentaires.

La norme la plus utilisée est SNMP (Simple Network Management Protocol), qui provient de l'environnement Internet. Les grands constructeurs ont quant à eux développé des plates-formes qui permettent d'avoir :

- un service de transport entre les différents processus applicatifs ;
- des adaptateurs de protocoles traduisant les messages échangés ;

- des piles de protocoles de communication ;
- des services supplémentaires internes, comme les annuaires.

Nous examinons à l'annexe S la gestion par politique, qui, sans avoir vraiment percé, demeure très importante dans les orientations actuelles.

Du côté du contrôle, nous insisterons beaucoup plus sur la signalisation, c'est-à-dire la façon de signaler au réseau un événement potentiel à prendre en compte, comme l'ouverture d'un chemin pour y transporter des trames.

Fonctions de base de la gestion de réseau

Suivant le type de système, les tâches de gestion varient et doivent donc être identifiées et analysées. Des services et des protocoles de gestion sont nécessaires pour gérer les ressources logicielles et matérielles d'un réseau.

L'identification et la mise en œuvre des tâches de gestion sont complexes en raison de la nature distribuée du système. On peut citer les fonctions suivantes :

- Démarrage et arrêt du réseau. Fonction de base liée à la configuration du réseau et à l'initialisation des paramètres.
- Traitement des alarmes. Permet au réseau de réagir à n'importe quel dysfonctionnement, comme la perte du contrôle d'accès, par exemple.
- Redémarrage du réseau. Nécessaire à la reprise d'activité suite à une panne du coupleur, d'une liaison, etc.
- Reconfiguration du réseau. Fonction liée à l'ajout ou à la suppression de points d'accès de terminaux. Par exemple, des éléments du réseau doivent pouvoir être mis hors circuit en cas de mauvais fonctionnement.
- Contrôle de la qualité. Fonction liée aux techniques de contrôle, aux caractéristiques opérationnelles du réseau et à la gestion des rapports de changement d'états.

Les moniteurs de gestion peuvent être matériels ou logiciels. Les moniteurs matériels s'occupent des phénomènes rapides, tandis que les moniteurs logiciels sont plutôt orientés application.

Les moniteurs de gestion doivent prendre en charge les fonctions suivantes :

- Tests et diagnostics. Les erreurs du système doivent être détectées. Un message de diagnostic peut être émis pour signaler qu'une erreur s'est produite et qu'un traitement peut avoir lieu. On doit pouvoir mettre un élément du système en état de diagnostic afin d'exécuter des séquences de tests.
- Compte rendu d'alarmes. Fonction destinée à notifier à l'opérateur du système tout mauvais fonctionnement.
- Contrôle du réseau. Fonction liée à l'allocation et à la désallocation des ressources et à leur contrôle (prévention des abus et des famines, manque de ressource, etc.).

Le système de gestion peut contrôler tous les changements. Il est aussi responsable des allocations de noms et d'adresses et des associations entre elles.

Le modèle de référence OSI a contribué au développement de réseaux hétérogènes. Cette hétérogénéité se traduit par l'interconnexion de matériels issus de constructeurs différents (Bull, IBM, DEC, HP, etc.) et par l'interconnexion de réseaux de différents types, par exemple un réseau grande distance (X.25 ou autre) relié à un réseau local (Ethernet, etc.).

L'échange d'informations entre systèmes hétérogènes a été rendu possible par l'intermédiaire de la normalisation de l'ISO. De plus, dans son rôle de transporteur de l'information, un réseau doit garantir une certaine qualité de service (débit, temps de réponse, etc.) à ses utilisateurs. Afin d'assurer une qualité de service, il est nécessaire de gérer convenablement de multiples composants (nœud, ligne, abonné, application, etc.). Cette gestion est à la charge d'entités spécifiques, les entités de gestion. L'ensemble de ces entités et leurs activités constituent la gestion de réseau.

Chaque fournisseur de réseau propose des outils permettant de mettre en place une telle gestion. Toutefois, la répartition de ces fonctions par rapport aux sept couches du modèle OSI est entièrement à l'appréciation du constructeur. De ce fait, si l'on dispose de deux systèmes hétérogènes, il est très difficile de faire coopérer les différents outils de gestion de réseau de chaque système.

Les deux architectures qui se sont développées en premier, il y a une vingtaine d'années, proviennent du modèle Internet, avec SNMP, et du modèle de référence OSI normalisé par l'ISO. Le modèle ISO est aujourd'hui en chute libre, mais il reste un modèle au même titre que le modèle de référence. Au contraire, SNMP a pris totalement le devant de la scène en se présentant sous diverses formes que nous allons étudier dans ce chapitre.

Gestion ISO

La gestion ISO consiste à faire remonter dans un processus appelé SMAP (System Management Application Process) toutes les informations de gestion par l'intermédiaire d'une entité d'application de la couche 7, appelée SMAE (System Management Application Entity), et à les traiter à ce niveau.

Ces informations se présentent sous la forme d'objets dont la syntaxe est normalisée sous le nom d'ASN.1. D'autres choix auraient pu être faits, comme une entité de gestion, à chaque niveau de la hiérarchie ISO, capable de prendre les décisions de gestion de ce niveau, mais tel n'est pas le cas. En outre, toutes les informations de gestion sont mémorisées dans une base de données, appelée MIB (Management Information Base). Cette MIB est, d'une part, remplie par les informations provenant des couches de protocoles à gérer et, d'autre part, consultée par le processus de gestion SMAP. L'entité SMAE récupère les informations demandées par le SMAP par une interface nommée SMI (System Management Interface). Cette architecture est illustrée à la figure 26.1, qui montre également la gestion de couche qui s'effectue, avec des processus de gestion associés à chaque couche.

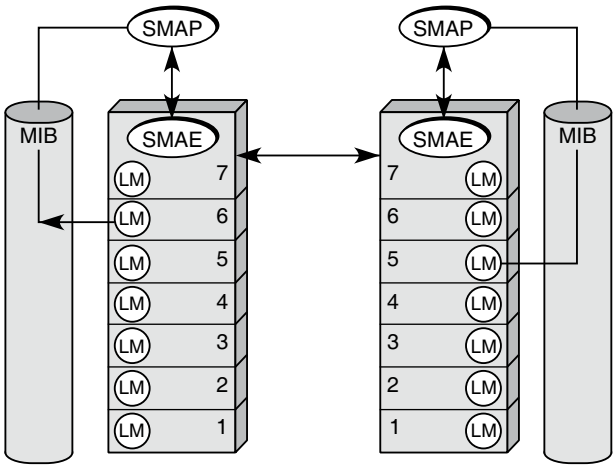


Figure 26.1
Modèle de gestion ISO

La gestion ISO comprend trois types d'activités :

- la gestion système, ou Systems-Management ;
- la gestion de couche, ou Layer Management (LM sur la figure 26.1) ;
- la gestion d'opération de couche (Layer Operation).

La gestion système définit l'échange de l'ensemble des informations de gestion concernant les ressources (objets gérés) utilisées dans un système ouvert. Ces échanges se font au niveau 7 de l'architecture du modèle de référence entre entités d'application pour la gestion système SMAE (System Management Application Entity), comme illustré à la figure 26.2.

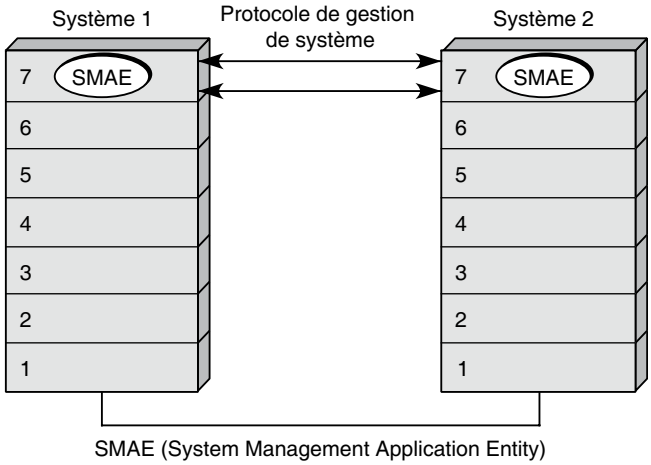


Figure 26.2
Échanges de niveau gestion de système

La gestion de couche, schématisée à la figure 26.3, définit les échanges d'informations concernant la gestion d'une couche *N* particulière. Ces informations ne concernent que les ressources propres à cette couche (mémoires tampons, temporisateurs, connexions, etc.). Cette gestion de couche correspond à des protocoles spécifiques, utilisés uniquement pour la gestion.

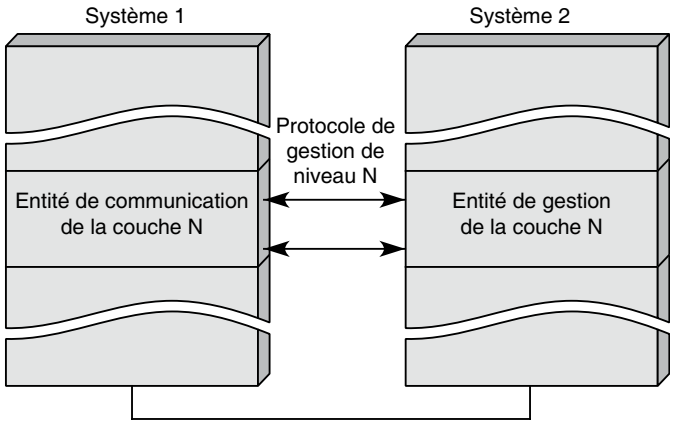


Figure 26.3

Échanges de niveau gestion de couche

Plusieurs instances de communication sont concernées par ces échanges, qui peuvent se faire soit *via* des protocoles de système (au niveau application), soit *via* des protocoles de gestion spécifiques de la couche concernée. On peut citer comme exemple de ces derniers le NCMS (Network Connection Management Subprotocol), qui est un additif au protocole de transport OSI et qui spécifie un sous-protocole de gestion de connexions de réseau.

La gestion d'opération de couche couvre les échanges d'informations relatives à une instance de communication (une opération) dans une couche donnée. Cela englobe les données véhiculées par les protocoles de communication OSI. Ces échanges d'opération de couche sont illustrés à la figure 26.4. En voici deux exemples :

- les trames U dans le protocole HDLC ;
- les données de tarification dans les paquets X.25.

Nous revenons plus loin sur la gestion système, puisque les seules normes développées à l'heure actuelle sont relatives à ce type d'activité.

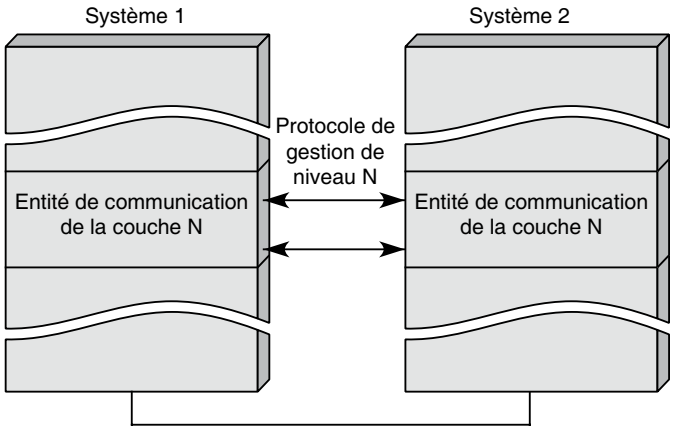


Figure 26.4

Échanges au niveau d'une opération de couche

Problématique de la gestion ISO

La gestion des réseaux est devenue primordiale dans les environnements réseau. De ce fait, la plupart des constructeurs de réseaux offrent un système de gestion plus ou moins compatible avec la normalisation ISO.

La figure 26.5 résume le fonctionnement de la gestion ISO. Les protocoles de couches viennent déposer leurs informations dans la MIB, qui peut être interrogée par les processus de gestion.

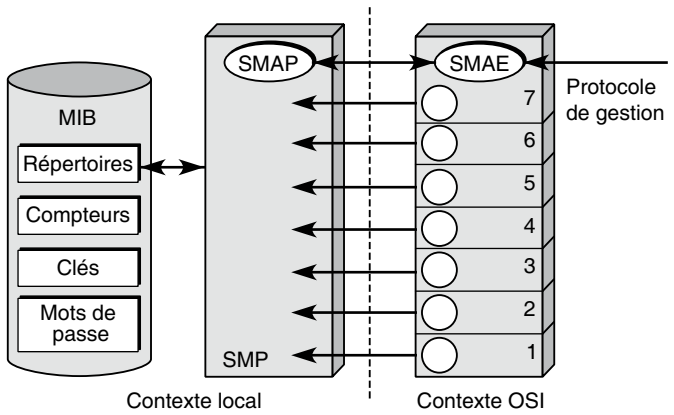


Figure 26.5

Architecture de la gestion ISO

Cette architecture est conçue pour être générale, ce qui constitue son défaut par rapport à la simplicité de SNMP. En effet, les objets dans la gestion ISO peuvent devenir très

complexes mais surtout spécifiques pour une implémentation donnée du modèle. De ce fait, la plupart des produits compatibles ISO ne sont que faiblement compatibles entre eux puisque les objets sont spécifiques, tout en étant conformes à la norme.

TMN

La présente section donne un bref aperçu du TMN (Telecommunications Management Network) en s'appuyant sur la série de recommandations M.3000 de l'UIT-T. Cet organisme de normalisation décrit une architecture physique et fonctionnelle capable de prendre en charge la gestion de tous les types de réseaux de télécommunications.

Le TMN est une norme de l'UIT-T applicable aux réseaux publics et privés, aux réseaux à commutation de circuits et de paquets et aux équipements associés. Même si, dans la recommandation M.3010, l'architecture du TMN est conceptuellement définie comme une base de travail pour tous les types de réseaux, dans les faits, le TMN est plutôt orienté vers l'administration des réseaux à circuits commutés que l'on rencontre dans les environnements de télécommunications. En effet, il n'est pas évident que l'architecture du TMN couvre rigoureusement toutes les possibilités de configuration physique susceptibles d'être rencontrées.

Le TMN détermine une structure de fonctions, de protocoles et de messages que l'administrateur de réseau peut sélectionner. Ces ensembles forment les spécifications d'un système TMN. En revanche, le TMN ne spécifie pas le système d'administration de réseau. Il ne renseigne en rien sur l'implémentation du système et ne spécifie pas la manière dont les fonctions TMN sont mises en œuvre. Seule est disponible une liste de fonctions qui peuvent être utilisées par l'administration de réseau. De plus, le TMN est applicable uniquement pour l'administration des ressources de communication. Cela signifie qu'il ne l'est pas pour l'administration des applications.

Le TMN identifie cinq catégories de fonctions de gestion, définies dans la recommandation X.700 : la gestion des fautes, la gestion comptable, la gestion de configuration, la gestion des performances et la gestion de la sécurité.

Cette architecture propose un découpage en couches des fonctions de gestion. Quatre grandes catégories ont été déterminées par l'UIT-T :

- Business Management
- Service Management
- Network Management
- Element Management

Le premier niveau concerne les besoins de l'entreprise et de la gestion de l'entreprise au niveau global. Le niveau de gestion de service se préoccupe des points d'accès aux utilisateurs et de l'administration des services offerts aux utilisateurs. Ces services peuvent aussi s'adresser aux fournisseurs de services. Le niveau de gestion gère les éléments du réseau, le mot élément étant pris ici au sens d'un ensemble d'éléments de base. Le dernier niveau gère cet ensemble d'éléments de base pris individuellement, comme les lignes, les multiplexeurs, les commutateurs, etc.

Architecture du TMN

Le TMN offre une structure de réseau définie, qui permet l'interconnexion de différents types de systèmes d'exploitation et des équipements de télécommunications regroupés en architectures hétérogènes. Cela rend possible l'administration de différents réseaux et fournit un ensemble de normes à respecter par les constructeurs des équipements de télécommunications. De façon conceptuelle, c'est un réseau indépendant, qui interface les réseaux de télécommunications en différents points pour en recevoir les informations et en contrôler les opérations.

Le TMN utilise les architectures normalisées existantes, comme le modèle OSI ou celui de l'UIT-T pour l'ATM. Dans le cas du modèle OSI, on retrouve naturellement l'architecture de gestion normalisée par l'ISO avec l'environnement CMIP/CMIS. Pour le modèle UIT-T, qui est beaucoup plus large que le modèle OSI, la partie spécifique concernant la gestion des équipements s'effectue avec CMIS/CMIP.

Architecture physique

Le TMN se fonde conceptuellement sur un réseau de communication de données, appelé DCN (Data Communication Network), séparé du réseau de télécommunications à gérer, comme illustré à la figure 26.6.

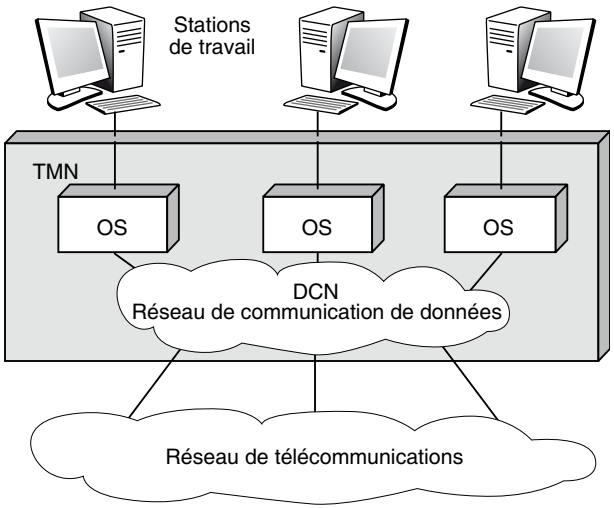


Figure 26.6

Architecture physique du TMN

Le TMN est divisé en cinq catégories de blocs fonctionnels principaux :

- OSF (Operations System Function), ou bloc fonctionnel des systèmes d'exploitation, traite les informations d'administration prises en charge et contrôle la réalisation des différentes fonctions d'administration de télécommunications. En d'autres termes, un bloc OSF offre des applications d'administration. Il existe trois types d'OSF : les OSF

de base, qui gèrent les éléments de réseau, les OSF du réseau, qui réalisent les fonctions de TMN relatives au réseau en coopérant avec les OSF de base, et les OSF de service, qui fournissent les moyens de gérer les services de télécommunications.

- NEF (Network Element Function), ou bloc fonctionnel d'élément de réseau, qui communique avec un TMN dans le but d'être géré. Il peut être considéré comme un objet administré.
- MF (Mediation Function), ou bloc fonctionnel de médiation, qui opère sur l'information transitant entre les blocs NEF et OSF dans le but d'établir une communication entre les fonctions primitives et le stockage des données. Il doit également adapter, filtrer et condenser l'information du NEF d'une manière conforme à la demande de l'OSF. Parmi les exemples de MF, citons les convertisseurs de protocole, les contrôleurs de communication, les gestionnaires de prise de décision, les éléments de stockage des données, etc.
- DCF (Data Communication Function), ou bloc fonctionnel de communication de données, qui offre les moyens de transporter les informations relatives à l'administration des télécommunications entre les blocs fonctionnels. Son existence est souvent supposée implicite.
- WSF (Work Station Function), ou bloc fonctionnel du poste de travail, qui offre les moyens de communication entre les blocs fonctionnels et l'utilisateur.

Un sixième bloc fonctionnel, le bloc d'adaptation, a été ajouté pour permettre une meilleure intégration dans un environnement hétérogène. Ce bloc propose une interface permettant la connexion des éléments de réseau ne supportant pas les interfaces normalisées. Il propose de raccorder des réseaux s'appuyant sur un système de gestion propriétaire. Ce bloc peut être considéré comme similaire à NEF.

Les blocs fonctionnels ci-dessus sont connectés de façon hiérarchique, comme illustré à la figure 26.7. Les points de référence de cette figure, indiqués par les valeurs f, g, q, x, sont expliqués dans la suite.

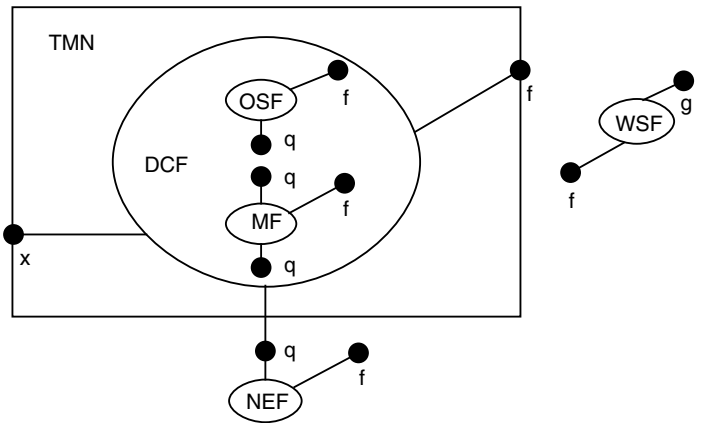


Figure 26.7

Architecture fonctionnelle du TMN

Les points de références définissent un point conceptuel d'échange d'information entre des blocs ayant des fonctions distinctes. Un point de référence devient une interface quand les blocs de fonctions connectés sont réalisés dans des équipements séparés. Il existe cinq types de points de référence : q, f, g, x et m.

- Les points de référence q connectent les blocs de fonctions entre NEF et MF, MF et MF, MF et OSF, OSF et OSF, soit directement, soit via le DCF. Plus précisément, l'interface q1 se place entre NEF et MF, q2 entre deux MF et q3 entre les équipements se connectant à un OSF.
- Les points f connectent les stations WSF.
- Les points g sont des points entre les WSF et les utilisateurs.
- Les points x connectent un TMN à un autre réseau d'administration incluant d'autres TMN.
- Les points m permettent le raccordement d'éléments non-TMN vers un bloc d'adaptation QAF. Cette interface est en dehors du champ du TMN.

Comme illustré à la figure 26.8, l'architecture physique du TMN, schématisée ici avec les interfaces, est calquée sur l'architecture fonctionnelle.

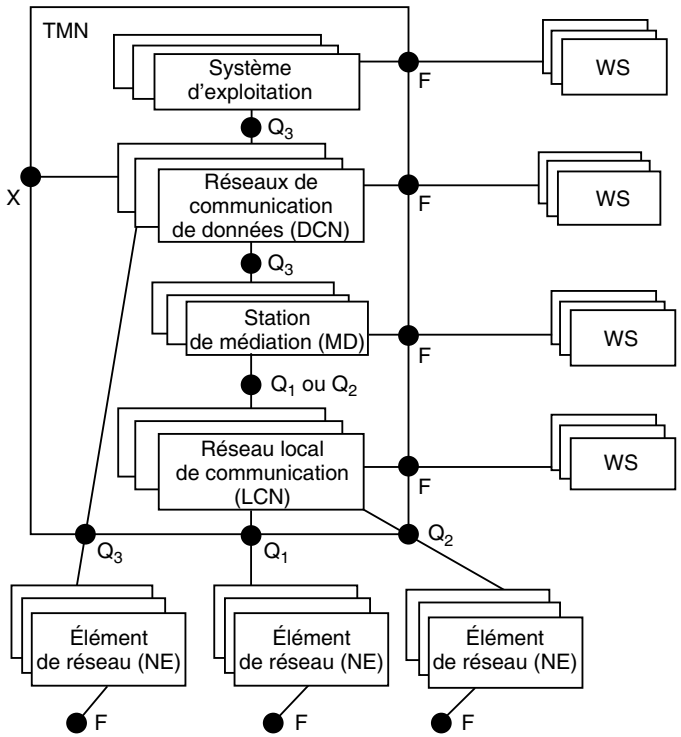


Figure 26.8

Architecture physique du TMN

Les interfaces normalisées sont définies en correspondance avec les points de référence. Elles sont signalées par des lettres majuscules pour les différencier des points de référence. L'interface Q est appliquée au point de référence q, F au point f, X au point x, etc. La figure 26.9 montre un exemple de relations entre une configuration physique et une configuration de référence dans laquelle le DCF est implicite.

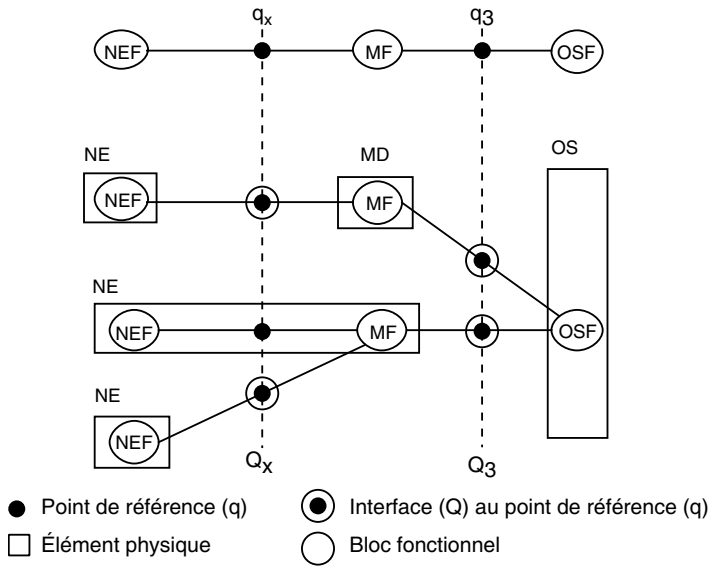


Figure 26.9

Exemples de relations entre une configuration physique et une configuration de référence

Q3 est l'interface qui normalise les équipements les plus complexes, comme les nœuds de commutation. Les spécifications de cette interface suivent diverses recommandations de l'UIT-T. La recommandation G.503 recommande l'utilisation de l'interface D au niveau physique ainsi qu'au niveau trame et X.25 au niveau trame. Pour les niveaux supérieurs, on se réfère aux protocoles de la gestion OSI.

Le système d'exploitation est le système qui exécute les OSF. Les NE sont constitués des équipements de télécommunications (groupe ou partie d'équipement) et des équipements qui exécutent les NEF. Ils comportent une ou plusieurs interfaces standards de type Q. Le LCN est un réseau de communication dans un environnement TMN. Il supporte le DCF en un point de référence de type q_1 ou q_2. Le DCN est un réseau de communication dans un environnement TMN, qui supporte le DCF en un point de référence de type q_3. Le MD est le matériel actif qui exécute les OSF, et le WS le matériel actif qui exécute le WSF.

Dans le TMN, les éléments physiques doivent contenir plus d'un bloc fonctionnel. Il est aussi possible que les objets administrés (NE) contiennent plus d'un bloc fonctionnel.

Architecture fonctionnelle

L'architecture fonctionnelle du TMN offre les moyens de transporter et de traiter les informations relatives à l'administration des réseaux de communication. Elle définit les points de référence, les interfaces et les protocoles. Elle offre aussi une description des fonctions nécessaires à l'administration d'un réseau de télécommunications. Ainsi, il existe une liste des fonctions de base utilisées par les fonctions d'application du TMN.

Les fonctions générales du TMN constituent le support pour les applications du TMN. Elles peuvent être considérées comme équivalentes aux services d'information d'administration commune de l'administration OSI. Les cinq aires fonctionnelles correspondantes sont souvent appelées FCAPS par référence à leurs cinq initiales :

- Fault Management, ou gestion des fautes, qui regroupe les alarmes, la localisation des fautes et les tests.
- Configuration Management, ou gestion des configurations, qui comporte la définition de la configuration, le statut de la configuration, l'installation, l'initialisation, les inventaires, les reprises, la restauration, etc.
- Accounting Management, ou gestion de la comptabilité, qui comprend la récupération, l'émission et la modification des factures.
- Performance Management, ou gestion des performances, qui inclut l'obtention et la récupération d'informations de performance, le filtrage de ces informations, la gestion du trafic, etc.
- Security Management, ou gestion de la sécurité, qui nécessite un contrôle d'accès au réseau et aux applications ainsi qu'à des composants du TMN.

Les applications TMN sont des applications d'administration utilisant l'infrastructure du TMN et s'exécutant sur le réseau d'administration. Elles ne doivent pas être confondues avec les applications de communication, qui s'exécutent sur le réseau de communication.

Le rôle de l'UIT-T est de spécifier toutes les interfaces du TMN. Ces spécifications permettent d'assurer la compatibilité des dispositifs interconnectés pour accomplir une fonction d'application du TMN donnée, indépendamment du type du dispositif ou du fournisseur. À cet effet, des protocoles de communication compatibles et une méthode de représentation des données (acceptable pour les messages) sont nécessaires. Cela inclut en outre la définition des messages génériques compatibles avec les fonctions d'application TMN.

Le modèle informationnel de la gestion TMN

Le TMN doit permettre à des informations de gestion traversant les points de référence d'avoir un modèle commun défini par le modèle informationnel. Une approche orientée objet a été choisie en commun avec l'ISO. En suivant cette approche, les ressources sont représentées comme des classes d'objets gérés. Les règles définies par l'ISO pour la gestion système et la représentation des objets sont reprises par l'UIT-T. Les classes d'objets gérés sont spécifiées dans la notification internationale de gestion ISO GDMO (Guidelines for the Definition of Managed Objects).

Le modèle informationnel d'un réseau générique GNMI (Generic Network Information Model) a pour rôle d'identifier et de standardiser les classes d'objets gérés qui se retrouvent dans tous les réseaux de télécommunications. Cette approche devrait permettre de définir des services de gestion indépendants de la technologie utilisée et de la manière de réaliser le réseau physique. Le modèle GNMI détermine les classes de base qui sont utilisées dans les architectures de réseau d'opérateur.

Pour conclure cette section sur l'architecture TMN, indiquons qu'elle est fortement utilisée, en particulier chez les opérateurs, même si souvent la gestion d'équipements spécifiques est effectuée par SNMP. En fait, les solutions de gestion utilisées dans les grands réseaux mettent en jeu, la plupart du temps, à la fois le TMN et SNMP.

Gestion Internet avec SNMP

SNMP (Simple Network Management Protocol) est un protocole simple de gestion de réseau développé par un groupe de travail de l'IETF dans le cadre de la définition d'un système de gestion pour les réseaux utilisant les protocoles TCP/IP. Trois versions se sont succédé dans le temps : SNMPv1, SNMPv2 et SNMPv3.

Le protocole de gestion SNMPv1 est très répandu dans le domaine des réseaux locaux, principalement pour le contrôle de réseaux locaux interconnectés. C'est aujourd'hui un standard de fait quasi incontournable pour les réseaux qui n'appartiennent pas au monde des télécoms.

SNMP a été approuvé par l'IAB (Internet Activities Board), responsable des spécifications de TCP/IP. Plusieurs documents définissent ce standard, parmi lesquels :

- RFC 1155 SMI (Structure of Management Information)
- RFC 1156 MIB (Management Information Base)
- RFC 1157 SNMP Protocol
- RFC 1158 MIB II (Management Information Base II)

Dans ce cadre, trois composants essentiels ont été définis :

- Le protocole SNMP, situé au niveau application de l'architecture en couches de TCP/IP, définit la structure formelle des communications.
- La base d'informations de gestion, ou MIB (Management Information Base), regroupe l'ensemble des variables relatives aux matériels et aux logiciels supportés par le réseau et définit les objets de gestion dans l'environnement TCP/IP.
- Les spécifications de la structure de l'information de gestion SMI définissent comment sont représentées dans la MIB les informations relatives aux objets de gestion (ressources) et comment sont obtenues ces informations.

Architecture de SNMP

Toutes les stations du réseau possèdent une base de ressources. Une station de gestion, la NMS (Network Management Station), contient une base maître qui représente toutes les ressources du réseau et les informations de gestion associées.

La structure des paquets SNMP est définie par la syntaxe ASN.1 (Abstract Syntax Notation 1). L'environnement SNMP est destiné à surveiller la performance d'un réseau, à détecter et à analyser ses fautes ainsi qu'à configurer ses éléments.

Les premiers produits implémentant SNMP sont apparus à la fin des années 1980 dans de petites entreprises du marché TCP/IP, parmi lesquelles Cisco Systems, qui était alors minuscule, Advanced Computer Communications et Proteon Inc. Depuis, la quasi-totalité des constructeurs informatiques, dont IBM et Hewlett Packard, ont intégré le support de SNMP dans leur architecture globale de gestion de réseau.

Les systèmes SNMP possèdent deux éléments-clés :

- L'agent logiciel, qui fonctionne dans les stations gérées. Ces stations sont généralement des nœuds de réseau IP, qui peuvent être des systèmes hôtes (stations de travail, serveurs, etc.), des équipements de transmission (multiplexeurs, etc.), des sondes ou des routeurs. Chaque agent comprend une MIB, base d'objets gérés, et des variables.
- La station de gestion de réseau (manager), système hôte qui contient le protocole de gestion de réseau et les applications de gestion. Elle est généralement composée d'un calculateur contenant une console et une base de données représentant tous les périphériques gérés du réseau et toutes les variables MIB de ces agents. Elle permet de récolter et d'analyser les données relatives aux équipements physiques connectés au réseau (ponts, routeurs, hubs) et de les gérer. Un agent peut être géré par plusieurs stations centrales. Certains agents, appelés agents proxy, permettent à un système de gestion SNMP de gérer des nœuds ne supportant pas la suite des protocoles Internet, c'est-à-dire des nœuds dialoguant avec un protocole propriétaire ou ISO.

La figure 26.10 illustre l'architecture SNMP.

La syntaxe des informations de gestion, intitulée SMI (Structure of Management Information), définit comment chaque élément d'information, concernant les périphériques gérés et les agents, est représenté dans la base d'information de gestion.

La syntaxe utilisée est un sous-ensemble de celle définie par la norme ASN.1.

Seuls quatre types de données sont utilisés :

- Integer : type de données qui n'accepte que des valeurs entières.
- Octet String : suite de 0 ou de plusieurs octets pouvant accepter des valeurs comprises entre 0 et 255.
- Object Identifier : suite de numéros référençant un objet enregistré par une autorité compétente.
- Null.

Deux types de données structurées sont autorisés : les listes et les tables à deux dimensions.

La MIB (Management Information Base) contient l'ensemble des variables gérées suivantes :

- Jeu de variables ayant trait à la fois au matériel et au logiciel.
- Jeu de points de test et de contrôle qu'un système supportant la gestion SNMP est censé vérifier.

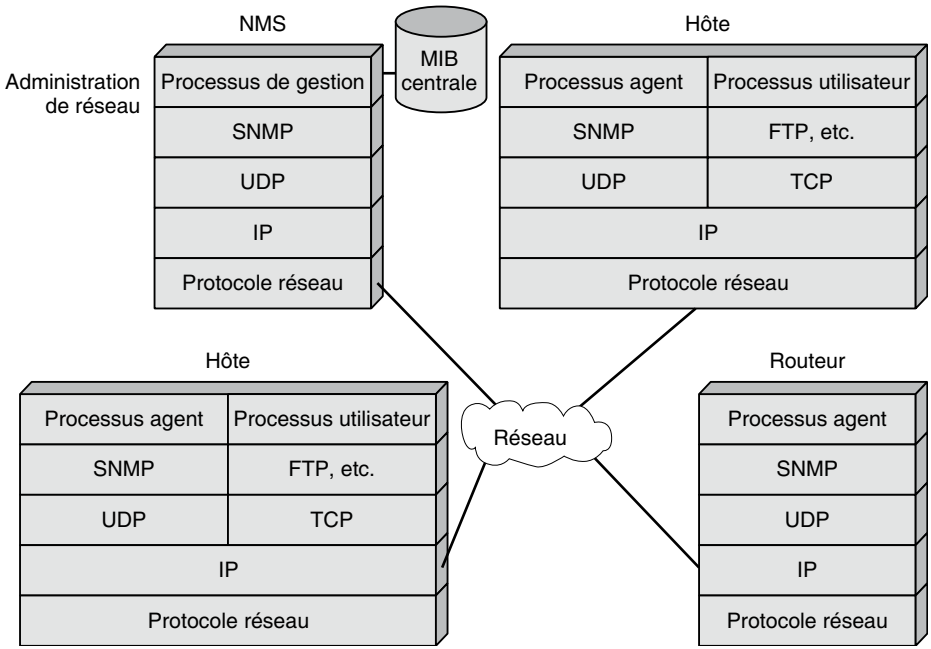


Figure 26.10

Architecture SNMP

La MIB attribue des noms aux éléments selon une hiérarchie d'enregistrements définie par l'ISO pour le nommage des objets réseau. Il en résulte une structure dans laquelle les variables ayant une relation logique sont regroupées en table. Par exemple, les variables concernant la vitesse, le taux d'erreur et les adresses d'interfaces de communication sont placées dans une table interface. Les objets de la MIB sont classés en une structure hiérarchisée de classes d'objets.

Le premier niveau de cette hiérarchie de classes d'objets de la MIB, ou MIB 1, comprend les huit groupes d'objets suivants :

- system : pour la gestion du nœud lui-même ;
- interfaces : pour les ports et interfaces réseau ;
- address translation : pour la traduction d'adresses IP ;
- IP (Internet Protocol) ;
- ICMP (Internet Control Message Protocol) ;
- TCP (Transmission Control Protocol) ;
- UDP (User Datagram Protocol) ;
- EGP (Exterior Gateway Protocol).

Suivant le type d'équipement à gérer, seuls certains groupes d'objets peuvent être implémentés.

Cette structure propose un grand nombre d'entrées permettant de décrire la majorité des objets réseau, mais certains fabricants ont défini leur propre MIB. Des entrées propres aux constructeurs ont donc été prévues dans cette organisation. De nombreuses extensions ont été effectuées au cours du temps, et des objets spécifiques de chaque nouveau protocole forment aujourd'hui le corps de plusieurs RFC.

La MIB 2 comprend, outre ce qui a été défini pour la MIB 1, des attributs ou objets, et deux groupes supplémentaires d'objets ont été définis : transmissions et SNMP. La MIB 2 gère environ 200 variables.

Une autre version, RMON MIB (Remote MOnitor Network Management Information Base), permet d'étendre les possibilités de SNMP. Elle autorise les moniteurs distants à contrôler les flux de trafic circulant à travers le réseau et est notamment utilisée pour les sondes.

RMON a été ratifié par l'IETF en novembre 1991 (RFC 1271). Le standard RMON couvre neuf groupes de données :

- Les statistiques, telles que le taux de collision pour un réseau Ethernet.
- Les historiques, qui décrivent le comportement du réseau pendant certaines périodes.
- Les alarmes.
- Les données relatives à la gestion des hôtes (enregistrement des hôtes sur le réseau, etc.).
- Les données se rapportant à la gestion de N hôtes, qui regroupent les statistiques d'hôtes faisant partie d'un groupe vérifiant un critère commun relatif à une donnée statistique.
- Les matrices de trafic, qui contiennent des données relatives aux communications entre groupes d'adresses.
- Les filtres.
- Les paquets capturés, qui contrôlent les données envoyées aux stations de gestion.
- Les événements générés par les agents.

RMON définit des variables relatives au contrôle du trafic sur les réseaux de niveau trame tels qu'Ethernet. Le protocole SNMP est le langage que les agents et les stations de gestion (managers) utilisent pour communiquer. C'est un protocole asynchrone de type question-réponse.

Les stations de gestion interrogent les agents pour observer leur fonctionnement et leur envoient des commandes pour leur faire exécuter certaines tâches. Les agents adressent les informations requises aux stations de gestion. Certains événements du réseau, tels que des erreurs de transmission, peuvent déclencher des alarmes envoyées aux stations de gestion. Cependant, l'envoi de messages de façon spontanée de l'agent vers le manager est limité. Les managers effectuent une interrogation périodique des agents de manière à vérifier leur état.

Si SNMP a l'avantage d'être simple, ses capacités à l'égard de la sécurité sont toutefois limitées, principalement en ce qui concerne l'authentification.

Les requêtes SNMP

Le protocole SNMP est un protocole sans connexion, qui utilise principalement le protocole UDP. Un système SNMP supporte trois types de requêtes : GET, SET et TRAP :

- get. La commande get request permet aux stations de gestion (managers) d'interroger les objets gérés et les variables de la MIB des agents. La commande get next request permet aux stations de gestion de recevoir le contenu de l'instance qui suit l'objet nommé. Grâce à cette commande, les stations de gestion peuvent balayer les tables des MIB. La commande get response est le message retourné par les entités interrogées (agents) en réponse aux commandes de type get request, get next request et set request.
- set. La commande set request permet aux stations de gestion de modifier la valeur d'un objet de la MIB ou d'une variable et de lancer des périphériques. set request autorise, par exemple, un manager à mettre à jour une table de routage.
- trap. La commande trap permet à un agent de notifier un événement. Cette alarme, envoyée lors de la détection d'une anomalie par l'agent (initialisation de l'agent, arrêt de l'agent, dépassement d'un seuil, etc.), n'est pas confirmée par le manager. À l'exception des messages d'alarme (traps), chaque message SNMP contient, entre autres :
  - un identificateur de requête ;
  - une liste de variables (noms et valeurs) ;
  - un champ pour les types d'erreurs ;
  - un index d'erreur signalant le numéro de la variable en erreur.

Tous les agents ne supportent pas obligatoirement toutes les commandes. Ainsi, SET REQUEST n'est pas toujours implémentée, car le protocole SNMP n'étant pas pourvu de dispositifs de protection, un mauvais usage de cette commande peut endommager des objets du réseau.

SNMP ne stocke et ne restitue que des types de données simples et ne travaille pas, à la différence de CMIP, sur des structures de données complexes. La plupart des fournisseurs d'outils d'interconnexion ont intégré SNMP dans leur offre. Le protocole SNMP est largement utilisé pour la gestion des matériels d'interconnexion de réseaux locaux, tels que ponts, routeurs, passerelles, hubs, etc.

SNMPv2 et SNMPv3

Une version plus avancée de SNMP, SNMPv2, a été proposée à l'IETF, mais elle n'a pas engendré de produits en grand nombre, et l'on peut même parler dans son cas d'échec cuisant. En revanche, la version SNMPv3 est bien acceptée par les entreprises, et de nombreuses implémentations sont disponibles sur le marché.

Le tableau 26.1 recense les principales RFC et normes du monde IP pour la gestion de réseau des domaines SNMPv2 et v3.

SNMPv2 essaie principalement de limiter les flots d'information de contrôle par une nouvelle commande GETBULK et une commande GET améliorée. Pour prendre en charge la coopération entre managers, SNMPv2 introduit deux nouvelles caractéristiques : une commande INFORM et une MIB manager à manager. Un manager utilise une commande INFORM pour envoyer une information non sollicitée à un autre manager. Il peut, par exemple, signaler un débit excessif sur une ligne de communication. Cette information est consignée dans la nouvelle MIB manager à manager.

RFC	Titre de la RFC
RFC 1901	Introduction to community-based SNMPv2
RFC 1902	Structure of management information for SNMPv2
RFC 1903	Textual conventions for SNMPv2
RFC 1904	Conformance statements for SNMPv2
RFC 1905	Protocol operations for SNMPv2
RFC 1906	Transport mappings for SNMPv2
RFC 1907	Management Information Base for SNMPv2
RFC 1908	Coexistence between version 1 and version 2 of the internet-standard Network Management Framework
RFC 2573	SNMPv3 applications
RFC 2263	SNMPv3 applications
RFC 2273	SNMPv3 applications
RFC 2574	User-based Security Model (USM-SNMPV3)

TABLEAU 26.1 • RFC du domaine SNMPv2 et SNMPv3

En septembre 1996, l'IETF a formé un nouveau comité dans le but d'examiner les problèmes de sécurité dans SNMP. Début 1997, ce comité a proposé une nouvelle génération, appelée SNMPng, qui rassemble les possibilités de SNMPv2 en incluant de nouveaux éléments de sécurité. Après un certain nombre d'améliorations supplémentaires, ce protocole SNMPng s'est transformé en SNMPv3, standard du domaine depuis la parution des RFC correspondantes, en 1998.

SNMPv3 est composé de trois modules :

- Message Processing and Control, qui définit la création et les fonctions d'analyse des messages.
- Local Processing, qui s'occupe des contrôles d'accès et de l'exécution des données.
- Security, qui permet l'authentification et le chiffrement ainsi que la prise en compte de contraintes de temps de certains messages SNMP.

L'amélioration la plus importante apportée par SNMPv3 concerne la sécurité, notamment l'authentification, le secret et le contrôle d'accès.

Comparaison de CMIP et de SNMP

CMIP et SNMP doivent, à terme, coexister. L'objectif de SNMP, qui était d'obtenir une gestion correcte à un coût raisonnable, a été atteint. Sa facilité d'utilisation et sa simplicité d'implémentation ont favorisé son rapide développement dans le monde TCP/IP. Cette simplicité pose néanmoins quelques problèmes lorsqu'il s'agit de gérer de nouveaux équipements et logiciels non conformes aux standards SNMP, les fournisseurs étant contraints d'écrire des extensions propriétaires.

Contrairement à CMIP, SNMP est un protocole de type datagramme, c'est-à-dire un protocole travaillant dans un mode sans connexion. De plus, les systèmes SNMP reposent

sur IP, et donc sur un autre protocole de type datagramme. Cependant, SNMP peut être utilisé dans des environnements autres qu'IP, par exemple, pour la gestion de ponts 802.1. CMIP, quant à lui, se doit de fournir un cadre d'architecture pour systèmes distribués et une application de gestion. Sa portée, qui est plus ambitieuse que celle de SNMP, a provoqué de nombreuses critiques, car elle engendre une forte complexité ainsi qu'une implémentation délicate.

Une autre différence importante entre SNMP et CMIP réside dans la façon de représenter l'information. CMIP distingue les notions d'objets et d'attributs, alors que SNMP ne possède pas la notion d'attribut : un objet peut être un système à gérer comme une caractéristique qui décrit ce système. Un attribut peut correspondre à l'état du système ou à un paramètre décrivant comment le système devrait fonctionner dans des conditions optimales. À chaque objet est associée une description unique, et un objet ne peut pas être défini à partir d'un autre.

CMIP utilise six primitives et effectue une distinction très nette entre un objet et ses attributs. CMIP et SNMP fournissent tous deux des directives sur la définition des objets de gestion et permettent aux fournisseurs d'ajouter tout ce qu'un système a besoin de savoir pour contrôler un objet. Le fait que SNMP ne fasse pas la distinction entre objet et attribut a de fâcheuses conséquences : la réutilisation d'un attribut ou d'une définition pour présenter une information générique est impossible, d'où la difficulté de gérer de nouveaux objets. Sous CMIP, un certain nombre d'objets totalement différents peuvent avoir un attribut commun, par exemple l'état opérationnel. SNMP n'est pas apte à supporter la notion d'héritage, contrairement à CMIP, et ne fournit pas le concept d'évolution d'un objet. En revanche, SNMP autorise les fournisseurs à définir de nouveaux objets et à les stocker de façon que les systèmes de ces fournisseurs puissent être gérés. Cette aide a sans doute contribué au développement de SNMP.

SNMP et CMIP sont tous deux spécifiés en ASN.1, mais SNMP est restrictif en ce qui concerne le codage des éléments complexes, comme les listes. De même, les deux protocoles comportent un certain nombre d'options qui permettent aux fournisseurs d'étendre les informations transportées par ces protocoles.

Les deux protocoles ont trois primitives en commun :

- get, qu'un système gérant envoie à un agent en vue d'obtenir la valeur d'un objet.
- set, utilisé pour initialiser la valeur d'un attribut.
- event-report, ou trap dans la terminologie SNMP, qui permet de signaler une occurrence d'un événement important concernant un objet.

Les performances de SNMP et de CMIP sont à peu près équivalentes. Leur fiabilité dépend essentiellement de la qualité de développement du logiciel et du mécanisme de transport des données. L'architecture CMIP est plus ouverte aux extensions, dans la mesure où elle peut davantage accepter de nouvelles définitions d'objets. La distinction entre objet et attributs rend cependant les extensions plus difficiles que dans SNMP. Enfin, la place mémoire nécessaire pour stocker les informations de gestion donne sans aucun doute un avantage à SNMP, qui est beaucoup plus concis que CMIP.

Le protocole CMOT (Common Management Information Services and Protocol Over TCP/IP), promu par un groupement de constructeurs réunis sous le nom de Netman, devrait offrir le moyen de gérer les éléments d'un réseau TCP/IP à partir de logiciels de gestion ISO. Le protocole CMOT implémente les prémices de la gestion définies par l'ISO, tels ROSE et ACSE.

Une couche présentation a été développée et intégrée à CMOT de façon que ROSE et ACSE puissent s'y référer. Cette couche de présentation, LPP (Lightweight Presentation Protocol), travaille au-dessus d'UDP ou de TCP et assure la présentation des messages dans l'environnement TCP/IP.

Cette version de SNMP pallie un certain nombre d'inconvénients de la précédente. Elle permet notamment de diminuer le nombre de paquets générés sur le réseau et offre la possibilité à une station d'être à la fois manager et agent.

Gestion par le Web

SNMP est devenu le protocole standard pour la gestion de réseau en se développant au début en parallèle à la version ISO, représentée par CMIP/CMIS, puis en prenant pratiquement l'ensemble du marché. Cependant, le processus de décision n'est pas inclus dans le protocole de gestion. L'ajout d'un environnement Web permet d'intégrer la gestion dans le système d'information des entreprises. C'est l'un des rôles de l'architecture de gestion WBEM (Web-Based Enterprise Management).

WBEM provient d'une initiative de plus de soixante-quinze sociétés visant à définir une architecture de gestion complète pour l'entreprise. Les composants principaux de cette architecture sont les suivants :

- Modèle de données simple et extensible pour définir et manipuler les états du système.
- Architecture côté client utilisée pour implémenter le modèle comme un ensemble d'objets.
- Modèle de distribution globale et de propagation des informations entre les clients et les sites où les actions de gestion sont décidées.

Le processus de normalisation a été réalisé sous l'égide du DMTF (Distributed Management Task Force) et de l'IETF. Le premier modèle adopté, en avril 1997, est le CIM (Common Information Model). Son principe de fonctionnement consiste à réutiliser l'environnement Web pour gérer le réseau.

Deux nouveaux modules de gestion sont ajoutés :

- CIMOM (CIM Object Manager), pour interpréter les requêtes en utilisant le modèle d'information.
- HMMP (HyperMedia Management Protocol), un protocole d'encodage qui permet le transport d'informations de gestion dans d'autres protocoles, tels que TCP/IP.

WBEM (Web-Based Enterprise Management)

Comme expliqué précédemment, WBEM permet de gérer les réseaux et les applications à partir d'un navigateur Web. WBEM décrit une architecture, un protocole, un schéma de gestion et un gestionnaire d'objets. Il doit permettre de prendre en charge les cinq aires de gestion et de donner naissance à un modèle de données adapté à la gestion de systèmes, de réseaux et d'applications. La proposition utilise le HTML pour la description des informations et HTTP.

Illustrés à la figure 26.11, les principaux composants de WBEM sont les suivants :

- HMMS (HyperMedia Management Schema), qui définit un schéma, ou une description, des données indépendant de leur implémentation et acceptant les données de différentes sources.
- HMMP (HyperMedia Management Protocol), qui définit un protocole permettant d'accéder aux données de gestion et fournit des solutions de gestion indépendantes de la plate-forme et de la distribution.
- HMOM (HyperMedia Object Manager), qui propose une définition générique pour les applications de gestion. Ce composant permet d'agréger les données de gestion et utilise un ou plusieurs protocoles pour fournir une représentation uniforme au navigateur utilisant HTML.

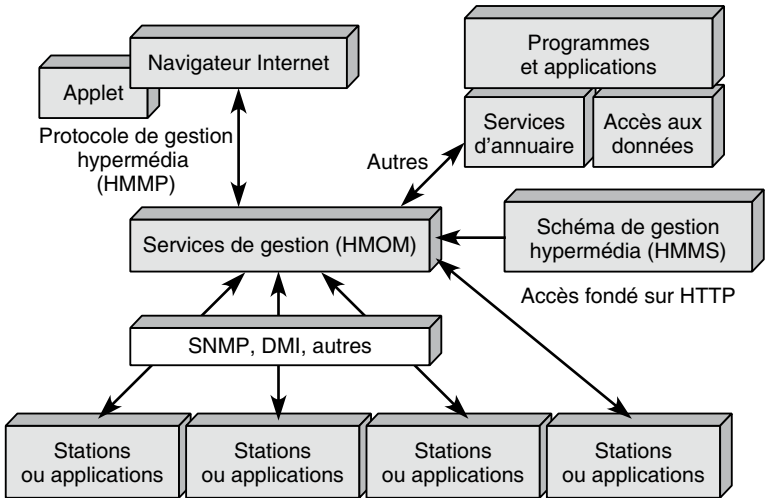


Figure 26.11

Composants de l'architecture WBEM

JMAPI (Java Management API)

Dans la perspective de l'unification de la gestion de réseau à travers le Web, JMAPI (Java Management API) a été définie par le consortium Java afin de simplifier la gestion. L'initiative JMAPI a principalement consisté en une extension du noyau de Java pour y intégrer des mécanismes permettant de développer des logiciels de gestion de réseau fondés sur le Web.

JMAPI est un ensemble de classes dérivées permettant d'accéder aux services de gestion SNMP sous-jacents. Grâce à cette approche, il est possible de s'affranchir des problèmes de portabilité des applications et d'obtenir des capacités étendues d'affichage.

Au niveau le plus haut, JMAPI propose une interface de navigateur, un module de gestion et des équipements à gérer. L'interface utilisateur du navigateur est le mécanisme par lequel un administrateur peut accéder aux opérations de gestion. Le module de gestion définit les mécanismes qui prennent en charge les objets gérés. Il inclut des interfaces objet pour les agents, des interfaces de notification et des interfaces avec les objets gérés.

L'architecture JMAPI est illustrée à la figure 26.12.

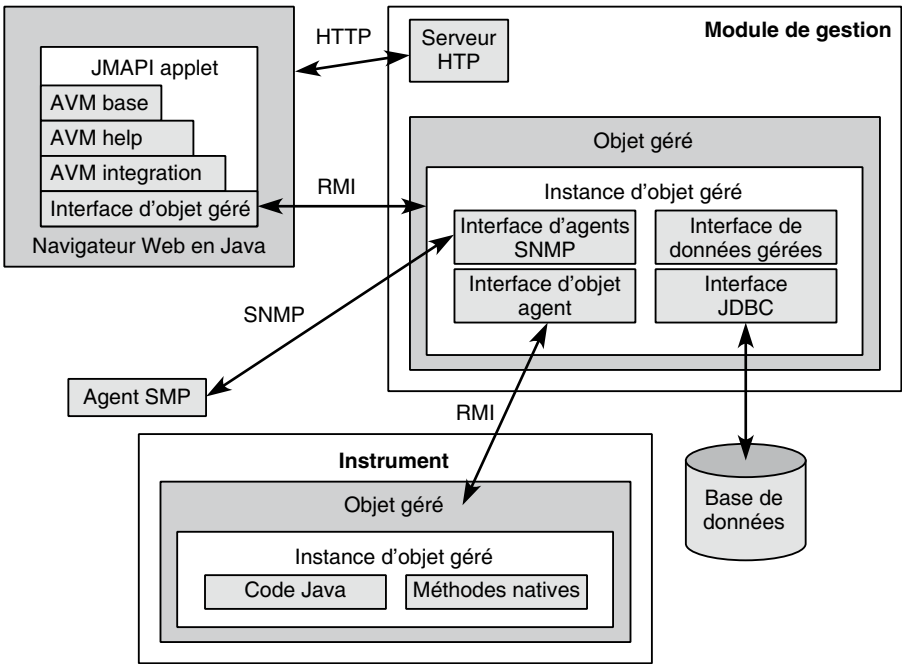


Figure 26.12
Architecture JMAPI

Tout l'intérêt de JMAPI est de distribuer géographiquement différents composants du système et de rendre possible les interactions entre composants grâce à RMI (Remote Method Invocation). Dans ce cas, le gestionnaire de réseau devient complètement indépendant du protocole de gestion spécifique, et l'on peut dès lors télécharger différentes applets au niveau du site agent pour réaliser des tâches de gestion sans surcharger le réseau.

Ce type d'intégration est illustré à la figure 26.13.

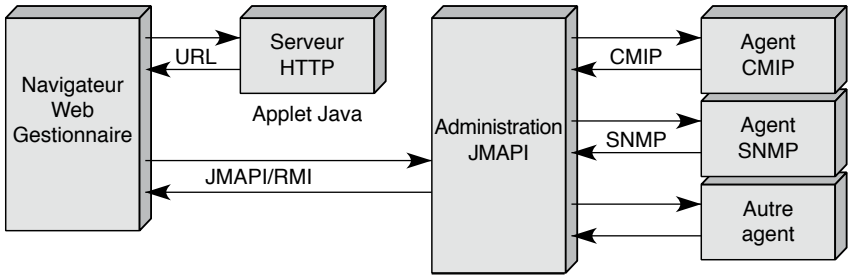


Figure 26.13

Exemple d'intégration de Java dans le modèle agent-manager

Dans son utilisation actuelle, l'approche JMAPI ne définit pas un nouveau modèle de gestion mais offre un niveau intermédiaire permettant de s'affranchir de l'hétérogénéité des systèmes et des protocoles de gestion sous-jacents. L'approche fondée sur Java offre un environnement de développement d'applications de gestion homogène, cachant entièrement l'hétérogénéité sous-jacente, tout en permettant une extensibilité et une portabilité simples.

Gestion par le middleware

Nous allons maintenant examiner comment le middleware, c'est-à-dire un logiciel intermédiaire entre les équipements et les processus de décisions, peut aider à la réalisation d'un système de gestion de réseau intégré en prenant l'exemple du middleware CORBA.

Dans le cadre de la gestion de réseau, l'architecture CORBA (Common Object Request Broker Architecture) a pour principal intérêt d'offrir aux applications de gestion une abstraction suffisante vis-à-vis des technologies système sous-jacentes. Elle permet ainsi de concentrer l'intelligence sur les services de gestion plutôt que sur la manière d'interagir avec le système ou la communication entre applications. Néanmoins, il est nécessaire de spécialiser ces environnements de manière à introduire un ensemble de fonctionnalités communes spécifiques de la gestion de réseau et permettant de mieux maîtriser le cycle de vie des services de gestion.

Cette gestion est illustrée à la figure 26.14.

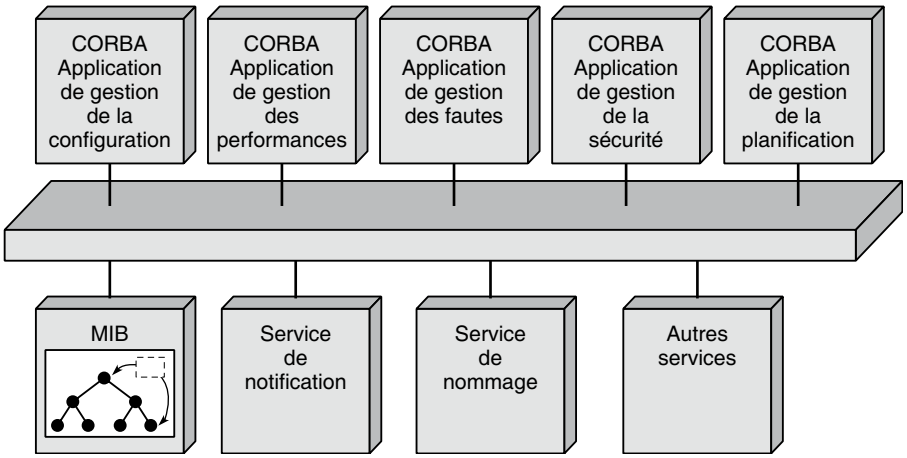


Figure 26.14

CORBA et la gestion de réseau

L'intégration de l'existant est un aspect crucial de la gestion de réseau, du fait notamment du parc logiciel et matériel déjà présent et du délai d'adoption par les constructeurs d'une nouvelle approche. Dans cette optique, de nombreuses initiatives ont été lancées afin de définir des mécanismes de migration du modèle agent-manager de CMIP/CMIS vers un modèle client-serveur CORBA.

Ces différentes initiatives ont abouti à la spécification de mécanismes permettant d'intégrer soit des objets issus de la normalisation ISO dans des environnements CORBA, soit des objets CORBA dans un environnement ISO. Ces deux approches correspondent à des processus d'intégration distincts : l'encapsulation ou la passerelle, comme illustré à la figure 26.15.

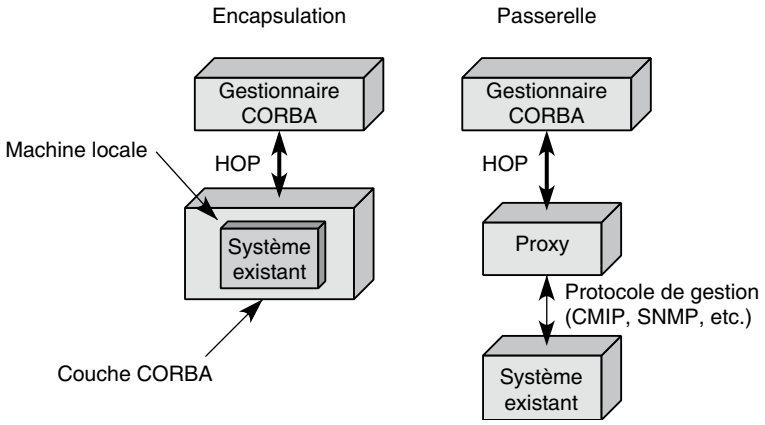


Figure 26.15

Intégration des objets de gestion par encapsulation ou passerelle

Ces travaux ont été repris par le groupe de travail XoJIDM (Joint Inter-Domain Management) de l'X-Open et du NM Forum et le groupe de télécommunications de l'OMG (Object Management Group) afin d'uniformiser les différentes approches d'intégration.

Les passerelles ont pour rôle de mettre en place des mécanismes de conversion dynamique. Ces mécanismes permettent la mise en correspondance de modèles d'information de gestion définis dans des environnements différents. Les modèles d'information les plus importants mis en correspondance sont CORBA et SNMP/SMI (System Management Interface), ainsi que CORBA et GDMO (Guidelines for the Definition of Managed Objects). Dans ce cadre, plusieurs architectures de passerelles ont été proposées, qui permettent au concepteur de systèmes de gestion de s'affranchir des protocoles et des services sous-jacents afin de collecter des informations sur les éléments physiques ou logiques du réseau. Cette architecture est illustrée à la figure 26.16.

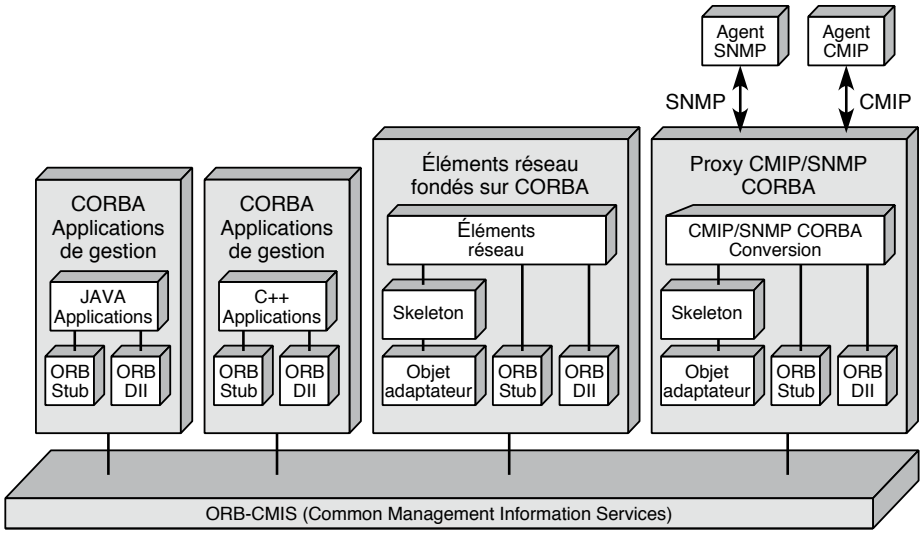


Figure 26.16

Intégration de CORBA dans le modèle agent-manager

Architecture Java/CORBA des systèmes de gestion

L'intégration de CORBA et de Java dans le même middleware offre à la gestion de réseau des perspectives séduisantes. Cette intégration, déjà réalisée dans certains middlewares, permet de résoudre les problèmes d'interopérabilité entre des applications Java et des applications développées dans d'autres langages. Il est notamment possible de rapprocher le processus de traitement des informations de gestion du système cible, par exemple le nœud du réseau lui-même, de façon à diminuer le trafic et à distribuer le contrôle. L'introduction des technologies agent dans la gestion de réseau en est facilitée. Les agents ne sont autres que des programmes autonomes possédant une certaine intelligence (agents intelligents) et pouvant se déplacer (agents mobiles) et communiquer entre eux à travers le réseau. Cette approche peut être utilisée dans le cadre de la gestion de réseau afin de disposer d'une plus grande efficacité dans le contrôle.

Dans ce contexte, le gestionnaire a la possibilité de déléguer complètement certaines tâches et de les distribuer sur le réseau sans avoir à contrôler d'une manière centralisée le déroulement des processus. Une fois les tâches achevées, les agents reviennent vers le centre de gestion pour rendre compte de l'exécution de la tâche ou des tâches qui leur ont été assignées. Les agents sont supportés dans leur déplacement par des interfaces CORBA, tandis que Java fournit la base de l'environnement d'exécution sur les nœuds du réseau. Dans ce cadre, l'OMG a spécifié les interfaces permettant de mettre en place les fonctionnalités des agents mobiles fondées sur CORBA.

Le modèle DME

DME (Distributed Management Environment) est un modèle d'architecture pour la gestion des réseaux locaux. Mis au point par l'OSF (Open Software Foundation), qui regroupe la plupart des grands constructeurs informatiques (IBM, DEC, Bull, Hewlett Packard, etc.), DME a pour but de résoudre le problème de la gestion de réseaux hétérogènes en proposant un environnement de traitement réparti.

Plusieurs points ont permis les avancées suivantes :

- DCE (Distributed Computing Environment), qui est un environnement développé pour le traitement distribué en milieu hétérogène.
- DME, qui s'appuie sur DCE et permet de gérer les ressources d'un environnement réseau contenant des systèmes, des éléments de réseau et des applications. Il s'agit d'un environnement assez complexe, qui inclut de nombreux composants :
  - Une interface utilisateur de gestion, qui permet d'obtenir une vue unique des objets de l'environnement.
  - Un ensemble de services destinés à la gestion des objets de l'environnement (logiciels, matériels, impression, configuration, etc.).
  - Des services de gestion permettant la mise en œuvre d'un modèle de gestion.
  - Des services d'objets qui gèrent les objets de l'environnement, tels un gestionnaire de requêtes inclus dans DME pour localiser et enregistrer les objets stockés dans les serveurs d'objets.
  - Des serveurs d'objets.
  - Des services de gestion d'événements provenant de requêtes du modèle OSI ou d'architectures non compatibles par l'intermédiaire d'un langage de description. Les communications sont fournies à distance par des RPC (Remote Procedure Call) ou en local par des IPC (Inter Process Communication).
  - Des protocoles de gestion, notamment une interface CMIP, une interface SNMP et un protocole de gestion spécifique de l'OSF, qui utilise les RPC pour communiquer.
  - Des outils de développement, qui comprennent des langages et des compilateurs ainsi que des appels système. Ces appels système, ou API (Application Programming Interface), reposent le plus souvent sur une architecture orientée objet. Pour les applications de gestion, l'API définie par l'OSF se fonde sur le protocole CMIS.

DME est une plate-forme de développement complète, qui doit pouvoir s'interfacer avec tous les grands standards d'aujourd'hui et de demain.

SLA (Service Level Agreement)

Les réseaux deviennent de plus en plus complexes. Le développement des services s'appuie sur des modèles de plus en plus élaborés, comme si l'imagination concernant le développement de nouveaux services était illimitée.

Les utilisateurs souhaitent avoir accès à des services personnalisés, à travers des terminaux ou des technologies d'accès variés, tout en exigeant des garanties pour les services qu'ils achètent. La réalisation de ces attentes implique la coopération et la coordination entre les fournisseurs de services Internet, ou FAI, les fournisseurs d'applications, ou ASP (Application Service Provider), et les opérateurs réseau, ou NSP (Network Service Provider). Cela implique d'assurer tout à la fois la qualité de service demandée, la gestion de la mobilité et la prise en compte de la sécurité. Pour garantir les droits et définir les obligations de l'utilisateur et du fournisseur de service, un contrat, appelé SLA, est écrit dans un langage de niveau business, compréhensible par ces derniers.

Les sections qui suivent examinent les différentes parties qui constituent un SLA ainsi qu'un ensemble de paramètres pour la qualité de service, la mobilité et la sécurité pouvant être négociés dynamiquement entre l'utilisateur et le fournisseur.

SLA, SLO et SLS

Les réseaux sont caractérisés par l'intégration de plusieurs technologies réseau en une unique technologie sous IP pour permettre le développement de nouveaux services en utilisant des modèles plus complexes. Ces services ne sont plus fournis par un seul fournisseur mais par plusieurs entités business que sont l'opérateur réseau, le fournisseur d'applications (ASP) et le fournisseur d'accès à Internet (FAI). L'ASP et le FAI peuvent être des clients de l'opérateur réseau. La relation entre ces entités n'intéresse généralement pas l'utilisateur final, qui se préoccupe plutôt du niveau de garantie des services qu'il paye.

Comme expliqué précédemment, la négociation entre l'utilisateur final et le fournisseur de service est spécifiée dans un SLA. Le SLA est ensuite traduit en objectifs, nommés SLO (Service Level Objectives). Chaque SLO est à son tour traduit en un ensemble de paramètres formant un SLS (Service Level Specification), comme illustré à la figure 26.17. Le SLO représente les objectifs à réaliser dans le cadre d'un SLA tandis que le SLS représente une interprétation technique du SLO et sert de guide opératoire afin d'aider le fournisseur à implémenter un objectif. Un SLA peut contenir plusieurs SLO pour plusieurs objectifs, tels le SLO pour la mobilité, le SLO pour la sécurité, le SLO pour la qualité de service, etc. Chaque SLO peut contenir à son tour plusieurs SLS.

Figure 26.17

Relations entre SLA, SLO et SLS

Paramètres d'un SLS de QoS

Cette section décrit les paramètres d'un SLS de qualité de service. Nous verrons un peu plus loin les paramètres à ajouter pour la gestion de la mobilité et de la sécurité.

Temps de service

Le temps de service, encore appelé service schedule, indique les temps de début et de fin de service. Ce paramètre spécifie le temps pendant lequel la QoS négociée doit être garantie. Le temps de service peut être l'instant précis du début et le temps précis de la fin du service. Par exemple, le service commence à 13 heures le 20 septembre 2005 et se termine à 17 heures le même jour. Le temps de service peut aussi être déterminé par des horaires périodiques spécifiés par l'heure du jour, le jour de la semaine, la date du mois et le mois de l'année. Par exemple, le service commence tous les jours de lundi à vendredi, de 8 heures à 17 heures, entre septembre et juin de chaque année.

Scope

Le scope est défini comme le point d'entrée et le point de sortie d'un domaine, par exemple, l'interface du routeur d'entrée par lequel le trafic entre dans le domaine et l'interface du routeur de sortie par lequel le trafic sort du domaine.

Paramètres de QoS

Les paramètres de QoS suivants sont définis :

- Délai. Délai de transmission d'un paquet IP entre le point d'entrée et le point de sortie du domaine.
- Gigue. Variation du délai de transmission des paquets IP entre le point d'entrée et le point de sortie du domaine.
- Taux de perte. Pourcentage des paquets perdus pendant la transmission des paquets IP entre le point d'entrée et le point de sortie du domaine.
- Débit. Nombre de paquets par seconde sur une interface.

Profil du trafic

Le profil du trafic, aussi appelé descripteur du trafic, est défini par les paramètres suivants :

- paramètres du token-bucket utilisé pour identifier les paquets dans le profil et hors profil ;
- taille maximale du paquet (MTU) ;
- taille minimale du paquet ;
- débit moyen et débit crête.

Traitement en excès

Le traitement en excès spécifie le traitement que le réseau applique aux paquets hors profil. Ce paramètre peut avoir les valeurs suivantes :

- Dropping. Le réseau jette les paquets hors profil.

- Shaping. Le réseau lisse les paquets hors profil pour les mettre dans le profil (in-profile).
- Remarking. Le réseau marque les paquets hors profil pour modifier la classe de service de ces paquets ou pour qu'ils puissent être rejetés avec une probabilité plus grande en cas de congestion.

Identification du trafic

L'identification du trafic, ou Flow Identification, est définie par les paramètres suivants :

- adresse IP de la source et de la destination ;
- numéro de port TCP ou UDP de la source et de la destination ;
- identification de protocole ;
- valeur du DSCP ;
- valeur de l'identificateur de flot (flow-label).

Identification du client

L'identification du client est utilisée pour les fonctions AAA (Authentication, Authorization, Accounting).

Marquage

Le paramètre de marquage spécifie la priorité qui est donnée aux paquets. Par exemple, dans DiffServ la valeur du DSCP est utilisée pour faire le marquage des paquets à l'entrée du réseau.

Mode de négociation

Le mode de négociation définit la manière avec laquelle la négociation est appliquée. En règle générale, il y a deux modes de négociation, le mode prédéfini (predefined-SLS mode) et le mode non prédéfini (non-predefined-SLS mode). Dans le mode non prédéfini, il n'y a pas de contrainte sur les valeurs des paramètres de SLS envoyées par le client. Dans le mode prédéfini, le fournisseur de service propose aux clients des SLS avec des paramètres à une valeur ou une plage de valeurs déterminées à l'avance. Dans ce cas, le client doit choisir le SLS le plus approprié à ses besoins.

Intervalle de renégociation

L'intervalle de renégociation spécifie l'intervalle de temps pendant lequel un SLS négocié ne peut être renégocié.

Fiabilité

La fiabilité est définie par deux paramètres principaux :

- Le temps d'indisponibilité moyen du réseau par an (Mean Down Time).
- Le temps maximal de réparation (Time To Repair) lorsque le service tombe en panne.
- Disponibilité d'un réseau d'opérateur.

- Dans un réseau d'opérateur, la fiabilité est une qualité essentielle. Nous avons représenté au tableau 30.1 les temps d'indisponibilité d'un réseau en fonction du taux de disponibilité, c'est-à-dire la proportion du temps pendant lequel le réseau est disponible. La première colonne indique le taux de disponibilité et les colonnes suivantes le temps d'indisponibilité du réseau par mois et par an.
- Les réseaux de télécommunications pour la téléphonie sont actuellement des réseaux « cinq neuf », c'est-à-dire avec un taux de disponibilité de 99,999. Ce taux représente des coupures du service téléphonique égales au total à 5 minutes par an. Actuellement, les réseaux des FAI n'offrent que « trois neuf » et donc un temps de panne de l'ordre de 9 heures par an, un temps beaucoup trop important pour un service téléphonique de qualité. Les opérateurs de télécommunications en mode IP doivent donc faire un énorme effort pour atteindre des taux de deux ordres supérieurs.
- Plusieurs solutions pour atteindre des taux de disponibilité acceptables pour les applications utilisateur sont envisageables et même déjà en grande partie implémentées dans les grands réseaux d'opérateurs. La solution la plus utilisée est la réservation de chemins supplémentaires, ou chemins de back-up. Les chemins supplémentaires peuvent être soit réservés et disponibles en permanence, soit réservés mais utilisés par des flots qui cèdent leur place aux flots à sauvegarder.

1	90 %	36,5 j/an	3 j/m	
2	99 %	3,65 j/an	7,3 h/m	
3	99,9 %	8,8 h/an	44 min/m	Bon ISP
4	99,99 %	53 min/an	4,4 min/m	
5	99,999 %	5 min/an	25 s/m	Téléphone
6	99,9999 %	32 s/an	3 s/m	

TABLEAU 26.2 • Taux d'indisponibilité d'une ligne ou d'un réseau

- Une protection 1:N indique qu'une ligne en back-up est réservée pour N lignes en cours d'utilisation, la ligne en back-up pouvant elle-même être utilisée. Une protection 1+N indique qu'une ligne en back-up est réservée pour N lignes en cours d'utilisation, la ligne en back-up ne pouvant être utilisée que par les lignes à protéger. Plus généralement, une protection M:N ou M+N indique que M lignes en back-up sont réservées pour N lignes actives.
- Pour arriver au « cinq neuf » dans un grand réseau où les paquets doivent passer par plusieurs routeurs, il faut protéger très fortement les chemins. En effet, le taux de panne pour une liaison en fibre optique de 1 000 kilomètres est de l'ordre de 0,3 p. 1000. Les pannes peuvent avoir de nombreuses raisons, dont la plus importante est la coupure pour travaux de génie civil. Si l'on compte un temps de réparation de 12 heures par panne, qui est déjà une valeur excellente, une redondance de 1:1 ne suffit pas à atteindre les « cinq neuf » car la probabilité que les chemins primaire et secondaire soient tous deux en panne est supérieure à 5 minutes par an. Il faut donc que la ligne de protection soit elle-même protégée.

- Dans les réseaux traditionnels, la boucle locale est protégée dans le cadre de SONET par une reconfiguration qui s'effectue en 50 ms. Dans le réseau cœur, il y a toujours un chemin de rechange pour un chemin en panne. Quant à la partie entre le réseau métropolitain et l'utilisateur, sa fiabilisation s'effectue comme pour la téléphonie classique par le biais d'une alimentation indépendante du réseau électrique. Dans ce cas, il est facile d'atteindre les 99,999 %. Cependant, le prix de revient de cette fiabilisation du réseau est assez important, et les opérateurs IP hésitent du fait de la concurrence acharnée sur les prix.

Conclusion

Le tableau 26.3 compare les caractéristiques des principaux protocoles conduisant à une gestion de réseau.

	CMIP	SNMP	DMI	HTTP
Modèle informationnel	Orienté objet	Orienté objet	Orienté objet	Hypermédia
Langage	GDMO	SMI	MIF	HTML
Architecture	Manager-agent, manager-manager	Manager-agent, manager-manager	Manager-agent	Client-serveur
Primitive	M-Get, M-Set, M-Action, M-Create, M-Delete, M-Event-Report	Get, Set, action implicite (effets secondaires), Trap	Get, Set, action implicite, Add, Delete, Event	Get, Post, Link Ne supporte pas la primitive Trap.
Mode de communication	Orienté transactions Requête/réponse	Requête/réponse	Requête/réponse	Requête/réponse asynchrone
Adressage	Par filtrage	Par arbre	Par attribut	URL
Application de gestion	Cinq aires fonctionnelles	Non spécifiée	Non spécifiée	Plug-in Java
Organisme de standardisation	ITU-T, ISO/OSI	IETF	DMTF	IETF

TABLEAU 26.3 • Comparaison des solutions proposées pour la gestion de réseau

Le système de gestion nécessite une définition de sa structure, de son fonctionnement et des protocoles d'échange. La gestion de ressources distribuées est une tâche complexe, qui requiert une bonne fiabilité, certaines opérations devant pouvoir être réalisées en dépit d'une quelconque panne. De plus, des contraintes de temps réel sont souvent à prendre en compte.

Ce chapitre a présenté l'environnement de gestion OSI, ainsi que les autres solutions constructeur disponibles sur le marché. SNMP est le protocole aujourd'hui de loin le plus utilisé. Ayant été développé pour gérer les architectures TCP/IP, la vogue de l'environnement TCP/IP lui a fortement profité. L'avantage de SNMP par rapport à la normalisation ISO est sa simplicité, puisque c'est un environnement inspiré de la normalisation ISO mais simplifié. On ne trouve que trois primitives dans SNMP, au lieu de six dans CMIP :

GET, SET et EVENT. De plus, le logiciel SNMP a été fortement simplifié par rapport à celui de l'ISO car il n'est pas possible d'adresser un attribut d'un objet de gestion, ce qui est possible dans l'architecture OSI. Enfin, des architectures plus globales s'appuyant sur le succès du Web se mettent en place et devraient prendre le devant de la scène dans ce domaine.

Enfin, la gestion de réseaux continue à progresser surtout dans le sens de la généralisation : il faut gérer les éléments de réseau mais également de plus en plus les applications qui tournent autour ainsi que l'ingénierie, la planification et la sécurité du réseau sous surveillance. Le nom de OSS (Operation Support System) a été adopté pour cette généralisation de la gestion de réseaux.

27

Le contrôle de réseau

Dans ce chapitre, nous commencerons par examiner les contrôles de flux et de congestion puis détaillerons la supervision de réseau et les signalisations du niveau application, en particulier SIP (Session Initiation Protocol).

Le contrôle de flux et de congestion apporte sans conteste des propriétés indispensables aux réseaux. Il peut revêtir différentes formes :

- La supervision, qui permet de mettre en place les chemins pour la commutation ou de réacheminer les paquets en cas de rupture du chemin.
- Les décisions temps réel pour réagir à des problèmes dans les couches basses des réseaux.
- Les protocoles pour permettre à certaines applications de s'exécuter, comme faire sonner l'équipement d'un correspondant pour indiquer un appel.

Les techniques de contrôle et de gestion de flux sont capitales dans le monde des réseaux. Les réseaux à transfert de paquets ou de cellules sont comme des autoroutes : s'il y a trop de trafic, plus personne ne peut avancer. Il faut donc contrôler le réseau et les flux qui y circulent. Le contrôle de flux est préventif, puisqu'il limite les flots d'information à la capacité de transport du support physique. Le contrôle de congestion a pour objet d'éviter la congestion dans les nœuds et de résoudre les embouteillages lorsqu'ils sont effectifs.

Les deux termes, contrôle de flux et contrôle de congestion, peuvent être définis de manière plus précise :

- Le contrôle de flux est un accord entre deux entités, la source et la destination, pour limiter le débit de transmission du service en considérant les ressources disponibles dans le réseau.
- Le contrôle de congestion représente l'ensemble des actions entreprises afin d'éviter et d'éliminer les congestions causées par manque de ressources.

Le contrôle de congestion

On a remarqué que, dans un réseau à commutation de paquets, quand bien même chaque source respectait son contrat de trafic, des congestions pouvaient apparaître en raison de la superposition de plusieurs trafics. Diverses publications ont proposé des méthodes de rejet sélectif de cellules pour soulager le réseau en cas de congestion. Par exemple, quand le bit CLP (Cell Loss Priority) de l'en-tête de la cellule est marqué (CLP = 1), la cellule est détruite en priorité lorsqu'une congestion est détectée. Ces méthodes peuvent être utiles pour décongestionner le réseau sans pour autant dégrader de manière significative la qualité de service. Cependant, il peut en résulter un gaspillage des ressources du réseau et des nœuds intermédiaires, particulièrement lorsque la durée de congestion est très longue.

Comme nous venons de le voir, si le bit de priorité de perte de cellule est marqué (CLP = 1), la cellule peut être rejetée en cas de congestion. Le CLP peut être marqué soit par les terminaux source, indiquant que la cellule a des informations non essentielles, soit par la méthode UPC/NPC, signifiant que la cellule viole la limite de trafic négociée avec la méthode CAC.

La technique par priorité

Une solution pour le contrôle de flux, que nous n'avons pas encore examinée, consiste à associer une priorité à un circuit virtuel et à traiter les cellules suivant cet ordre de priorité. Cette priorité peut être fixe ou varier dans le temps. On a dans ce dernier cas affaire à des priorités variables. Différentes publications ont montré que la méthode d'ordonnancement de la priorité dans un nœud de commutation pouvait engendrer un taux d'utilisation des ressources du nœud assez élevé. La méthode la plus simple est celle de la priorité fixe. Par exemple, la classe de service sensible au délai (service AAL-1 et AAL-2) est toujours prioritaire par rapport à la classe de service sensible à la perte (service AAL-3/4 ou AAL-5).

Contrairement à la méthode de priorité fixe, dans la méthode de priorité variable, la priorité varie selon le point de contrôle. Par exemple, les services sensibles au délai sont prioritaires pour les cellules sortant de la mémoire tampon. Les services sensibles aux pertes sont prioritaires pour les cellules entrant dans la mémoire tampon : si une cellule sensible à la perte demande à entrer dans une mémoire lors du débordement de cette dernière, une cellule sensible au délai est rejetée.

Il existe plusieurs méthodes de priorité variable :

- Dans la méthode QLT (Queue Length Threshold), la priorité est donnée aux cellules sensibles aux pertes, si le nombre de cellules présentes dans la file dépasse un seuil, sinon les cellules sensibles au délai ont la priorité.
- Dans la méthode HOL-PJ (Head Of Line with Priority Jumps), plusieurs classes de priorité sont prises en compte. La plus grande priorité est donnée à la classe de trafic qui requiert des délais stricts. La priorité non préemptive est donnée aux cellules de haute priorité. Enfin, les cellules de basse priorité peuvent transiter vers une file d'attente plus prioritaire, lorsque le délai maximal d'attente est atteint.

- Dans la méthode push-out, ou partage partiel de tampons, le rejet sélectif est réalisé dans les éléments de commutation. Une cellule non marquée peut entrer dans un tampon saturé si des cellules marquées sont en attente de transmission. Une des cellules marquées est rejetée et la cellule non marquée entre dans le tampon. Si le tampon ne compte que des cellules non marquées, la cellule non marquée arrivante est rejetée. Dans la méthode de partage partiel du tampon, lorsque le nombre de cellules dans le tampon atteint un seuil donné, seules les cellules non marquées peuvent entrer dans ce tampon.

La méthode de push-out peut être améliorée de différentes façons. Par exemple, au lieu de détruire la cellule marquée la plus vieille ou la plus récente dans la file d'attente, il serait possible de détruire les cellules marquées en plus grand nombre, correspondant à un même message. En effet, si l'on détruit une cellule, toutes les cellules appartenant au même message sont détruites à l'arrivée ; donc, autant les détruire directement dans le réseau. C'est le but de ce push-out amélioré.

Le contrôle de congestion réactif

Le contrôle de congestion réactif est nécessaire lorsque des rafales simultanées provoquent des surcharges instantanées dans les nœuds. La congestion peut se développer à la suite d'une incertitude sur le trafic ou à cause d'une modélisation incorrecte du comportement statistique des sources de trafic.

L'UIT-T a inclus le mécanisme EFCI/BCN dans ses recommandations. Le rôle du mécanisme EFCI (Explicit Forward Congestion Indication) est de transporter les informations de congestion le long du conduit virtuel entre l'émetteur et le récepteur. Les cellules qui passent dans un nœud surchargé sont marquées dans l'en-tête. Dans le nœud de destination, la réception de cellules dont les indicateurs de congestion sont marqués (PTI = 010 ou 011) signale la présence d'une congestion dans certains nœuds du chemin. Le mécanisme BCN (Backward Congestion Notification) permet de renvoyer les informations sur la congestion au nœud émetteur. Celui-ci peut réagir en diminuant son trafic. La notification vers l'émetteur s'effectue par le flux OAM F4. Cette méthode nécessite un mécanisme de contrôle de flux efficace, réactif à la congestion interne.

Dans les réseaux traditionnels, le mécanisme de contrôle de flux par fenêtre a été le plus souvent utilisé. Plusieurs études récentes proposent des méthodes adaptatives de contrôle de flux par fenêtre. La taille de la fenêtre est calculée par le destinataire ou augmentée automatiquement par l'arrivée d'un acquittement. Ces méthodes sont développées pour les services de données et peuvent être liées au contrôle d'erreur. Le très long délai de propagation par rapport au temps d'émission rend cependant difficile l'utilisation d'un mécanisme de contrôle de flux par fenêtre. De plus, ces méthodes partent d'hypothèses fortes, telles que la connaissance de l'état du réseau ou bien le temps de propagation suffisamment court pour effectuer un aller-retour de l'information de gestion.

Gestion rapide des ressources

Il est possible d'exercer un contrôle en adaptant les réservations de ressources dans le réseau au trafic entrant. Évidemment, ce contrôle est très délicat à mettre en place étant donné l'écart entre les vitesses de transmission et les délais de propagation. La méthode FRP (Fast Reservation Protocol) a été fortement soutenue par la France auprès des organismes de normalisation de l'ATM et a été adoptée au milieu des années 1990. Elle se décline en deux variantes, FRP/DT (Fast Reservation Protocol/Delayed Transmission) et FRP/IT (Fast Reservation Protocol/Immediate Transmission). Dans le premier cas, la source n'émet qu'après avoir réservé les ressources nécessaires à la transition du flux des cellules, et ce au niveau de tous les nœuds intermédiaires. Dans la seconde version, les cellules sont précédées d'une cellule de demande d'allocation de ressources et sont suivies par une cellule de libération des ressources.

Le contrôle de flux dans les réseaux IP

Les réseaux IP présentés ont leur propre contrôle de flux, que nous allons examiner en détail. Ces contrôles suivent l'orientation classique des réseaux informatiques : on essaie de donner beaucoup d'importance à la station de travail, qui, de fait, contient les mécanismes de contrôle. En particulier, le protocole TCP, qui se trouve dans la station terminale, gère le contrôle de trafic.

Le contrôle de flux dans TCP

Les principes du contrôle de flux ont été arrêtés à la fin des années 1980 et constituent ce que l'on appelle le TCP Tahoe. De nouveaux algorithmes ont été ajoutés dans les années 1990, en particulier les mécanismes de prévention des congestions par le biais de l'algorithme RED (Random Early Discard). TCP Reno est le nom de l'implémentation intégrant ces nouvelles fonctionnalités.

Le principe de base du contrôle est fondé sur l'algorithme slow-start. Le contrôle s'effectue par une fenêtre, qui augmente ou diminue suivant la valeur du délai aller-retour des paquets dans le réseau. La fenêtre augmente de façon exponentielle jusqu'à ce qu'une perte soit constatée. La dernière valeur acceptable avant la perte est appelée seuil de saturation, et l'on détermine une valeur SS_threshold (Slow-Start_threshold) égale à la moitié de ce seuil de saturation arrondi à la valeur inférieure. Après la perte, la valeur de la fenêtre est remise à 1 puis se met de nouveau à augmenter.

À partir de là, la croissance se fait en deux phases. La première phase, le slow-start de nouveau, commence par une fenêtre de taille 1, correspondant à un segment TCP. À chaque réception d'un acquittement, la fenêtre double de valeur. Même en partant d'un flux faible au départ, on arrive rapidement à un débit important, surtout si le délai aller-retour, ou RTT (Round Trip Time), du réseau est court. Cette procédure est maintenue jusqu'à ce que la fenêtre atteigne la limite SS_threshold, indiquant un nouveau processus de croissance de la fenêtre, qui devient beaucoup plus limitée, puisqu'on approche de la

limite de saturation de la connexion. On passe alors dans une phase dite de Congestion Avoidance.

La fenêtre évolue de façon linéaire, augmentant d'un segment supplémentaire chaque fois qu'un ensemble de segments est reçu correctement. À chaque nouvelle perte de paquet, le seuil de saturation détermine une nouvelle valeur du SS_threshold, et l'algorithme redémarre par un slow-start. La figure 27.1 illustre un exemple d'accroissement de la fenêtre de contrôle dans TCP Tahoe. La taille de la fenêtre ne peut dépasser la taille maximale définie par l'utilisateur au début de la connexion. S'il n'y a pas de perte de paquet lorsque la fenêtre atteint cette valeur maximale, la fenêtre devient fixe jusqu'à ce qu'une perte survienne.

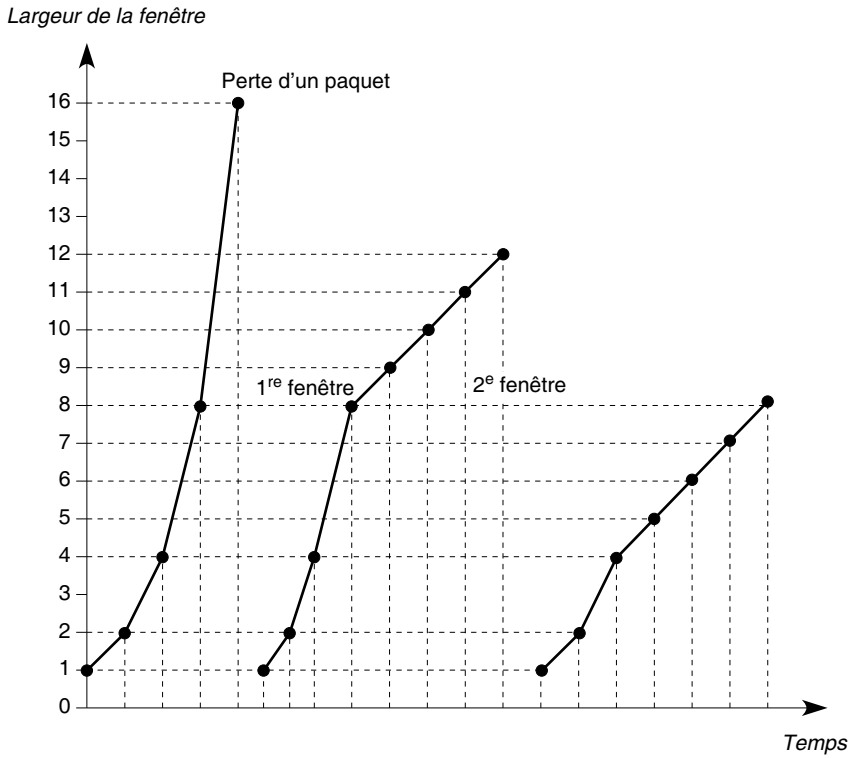


Figure 27.1

Exemple d'accroissement de la fenêtre de contrôle dans TCP Tahoe

L'interprétation correcte de la valeur du RTT reçu lorsqu'un acquittement se présente constitue une difficulté majeure. En effet, le récepteur a pu mettre un certain temps à émettre ce paquet, même si le réseau n'est pas congestionné. L'estimation d'une perte de paquet représente un autre problème. Un acquittement qui arrive déséquencé peut constituer un motif d'alarme, même si ce n'est pas forcément une indication de perte puisque le paquet qui n'a pas été acquitté a très bien pu passer par un autre chemin.

Pour une bonne estimation de la perte, il faut demander au récepteur d'envoyer un acquittement à chaque segment reçu. L'acquittement du dernier paquet en séquence correctement reçu permet de déterminer l'état de la communication. Lorsque le récepteur reçoit un paquet qui n'est pas en séquence, il émet un acquittement du dernier paquet en séquence de telle sorte que l'émetteur, à la réception d'un acquittement qu'il a déjà reçu, peut avoir une première intuition qu'un paquet est perdu. Comme le routage peut fausser la détection, le même acquittement doit être reçu trois fois avant que le paquet soit déclaré perdu. Cette solution permet de retransmettre beaucoup plus rapidement les segments perdus que celle consistant en l'attente d'un temporisateur, qui doit forcément être long pour tenir compte des aléas du réseau.

Des améliorations ont été apportées à cet algorithme, en particulier dans TCP Reno, qui propose de ne pas repasser par la phase du slow-start. Celle-ci requiert en effet un certain temps pour transporter un seul segment, ce qui repousse d'autant la détection de trois acquittements successifs identiques à des temps importants. En revanche, en cas d'erreurs multiples, les performances des deux algorithmes sont fortement dégradées, si bien que de nouveaux algorithmes ont dû être proposés, comme TCP NewReno, pour éviter les redémarrages sur le temporisateur déclenché à l'émission de chaque segment et arrivant à échéance lorsque le paquet n'a pas été acquitté dans un temps donné.

Les nouvelles versions de TCP ont fait surgir un nouveau problème, à savoir l'utilisation d'un protocole de reprise de type Go-back-n, qui demande la retransmission à partir du premier segment perdu, même si des segments postérieurs ont été bien reçus. L'équivalent dans le modèle de référence est le Reject du protocole HDLC. Pour améliorer les performances, surtout si la liaison est longue ou le débit très élevé, il convient d'utiliser des acquittements sélectifs comme le SREJ, le rejet sélectif du protocole HDLC. La version de TCP qui intègre ce protocole est TCP SACK (RFC 2018). Les acquittements négatifs indiquent le numéro de séquence du premier et du dernier octet à retransmettre.

Le contrôle de flux dans IP

Les algorithmes de contrôle de flux et de qualité de service peuvent être mis en place au niveau IP et plus précisément dans les routeurs IP. Nous allons en décrire quelques-uns.

L'algorithme RED (Random Early Discard) permet aux extrémités de réduire leur trafic par la perte d'un ou de plusieurs paquets lorsqu'une situation de congestion semble menacer. En effet, comme nous l'avons vu, TCP réduit sa fenêtre dès la perte d'un paquet. L'idée est donc de forcer la perte d'un paquet pour réduire le débit, d'où le nom de la méthode : on perd un paquet sans attendre sa perte par saturation. Dans la définition de RED, il faut se méfier des pointes de trafic instantanées qui pourraient pousser à la perte d'un paquet, alors même que cette pointe ne serait que ponctuelle. À cet effet, l'algorithme RED travaille avec deux seuils. En dessous du premier seuil, tout va bien. Le premier seuil franchi, le nœud peut commencer à perdre quelques paquets sélectionnés pour réduire le trafic de certaines sources. Au-dessus du deuxième seuil, tous les flots passant par le routeur IP sont concernés.

Les protocoles RSVP et ICMP, qui sont présentés au chapitre 18, peuvent également apporter une garantie de service. Pour compléter ces protocoles dans le but d'obtenir une qualité de service plus grande, l'IETF a créé plusieurs groupes de travail pour présenter des algorithmes plus élaborés. Nous allons examiner trois de ces groupes.

Le service IntServ intègre deux niveaux de service différents avec des garanties de performance. C'est un service orienté flot, c'est-à-dire que chaque flot peut faire sa demande spécifique de qualité de service. Pour obtenir une garantie précise, le groupe de travail IntServ a considéré que seule une réservation de ressources était capable d'apporter à coup sûr les moyens de garantir la demande. Deux sous-types de services sont définis : le service IntServ, avec une garantie totale ou avec une garantie partielle, et le service best-effort. Ces deux types correspondent aux services rigides avec contraintes à respecter et aux services dits élastiques, dans lesquels les flots n'ont pas de contraintes fortes.

Le service IntServ pose le problème du passage à l'échelle, ou scalabilité Le contrôle IntServ se faisant sur la base de flots individuels, les routeurs du réseau IntServ doivent garder en mémoire les caractéristiques de chaque flot. Une autre difficulté concerne le traitement des différents flots dans les nœuds IntServ : quel flot traiter avant tel autre lorsque des milliers de flots arrivent simultanément avec des classes et des paramètres associés tous distincts ?

Comme il n'y a pas de réponse précise à tous ces problèmes, une autre grande technique de contrôle, DiffServ, essaie de trier les flots en un petit nombre bien défini, en multiplexant les flots de même nature dans des flots plus importants mais toujours en nombre limité.

Le rôle de DiffServ est d'agréger les flots en quelques classes offrant des services spécifiques. La qualité de service est assurée par des traitements effectués dans les routeurs spécifiés par un indicateur situé dans le paquet. Les points d'agrégation, auxquels les trafics entrants sont agrégés en un seul flot, sont placés à l'entrée du réseau. Le contrôle de flux dans les réseaux Ethernet

À partir du moment où une commutation est mise en place, il faut ajouter un contrôle de flux puisque les paquets Ethernet peuvent s'accumuler dans les nœuds de commutation. Ce contrôle de flux est effectué par le paquet Pause. C'est un contrôle de type back-pressure, dans lequel l'information de congestion remonte jusqu'à la source, nœud par nœud. À la différence des méthodes classiques, le nœud amont est informé d'une demande d'arrêt des émissions, avec précision du temps pendant lequel il doit rester silencieux. Cette période de temps peut être brève, si le nœud est peu congestionné, ou longue, si le problème est important. Le nœud amont peut lui-même estimer, suivant la longueur de la période de pause qui lui est imposée, s'il doit faire remonter un signal Pause ou non vers ses nœuds amont.

Cette technique doit permettre de faire remonter jusqu'à la source les informations du réseau. Cependant, de nombreuses difficultés doivent être contournées par le logiciel de supervision. Par exemple, il faut éviter qu'au travers d'une boucle une information d'arrêt ne revienne à la station qui l'a émise, car on aurait alors une situation de deadlock, ou blocage.

La figure 27.2 illustre le fonctionnement du contrôle de flux dans un réseau Ethernet. Dans cet exemple, le nœud central s'aperçoit qu'il approche de la saturation, et il envoie vers son nœud de droite une commande Pause de 200 ms lui demandant de ne plus rien lui envoyer pendant 200 ms. Il envoie également vers le nœud du dessus une commande Pause de 100 ms et vers le nœud du dessous une commande Pause pour lui pour demander d'arrêter ses transmissions pendant 200 ms. Enfin, il émet une commande Pause vers le nœud à sa gauche en lui demandant de ne plus rien lui envoyer pendant un temps de 50 ms. Toujours dans ce schéma, le nœud de droite, qui reçoit une commande Pause de 200 ms, s'aperçoit que lui-même risque d'avoir des problèmes de saturation s'il ne peut plus rien émettre vers sa gauche pendant 200 ms. Il décide donc d'envoyer deux commandes Pause de 100 et de 50 ms aux deux nœuds qui sont en amont de lui.

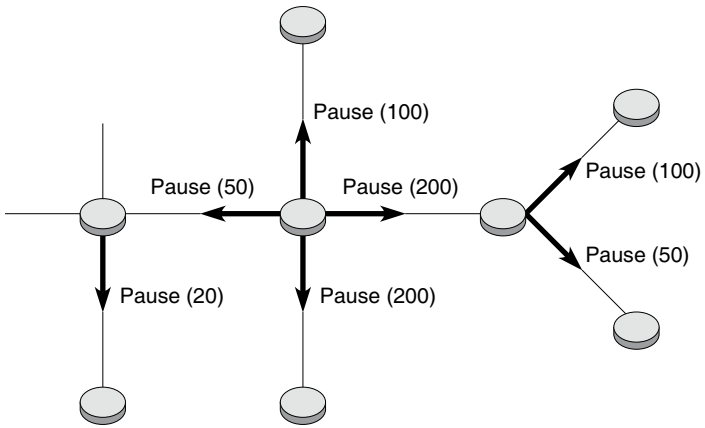


Figure 27.2
Contrôle de flux dans Ethernet

Comme nous venons de le voir, Ethernet s'étend vers le domaine des WAN privés en utilisant les techniques de commutation. Pour les réseaux locaux partagés, la tendance actuelle est plutôt à l'augmentation des débits, avec le Gigabit Ethernet et le 10 Gigabit Ethernet.

Une autre solution de contrôle de flux a été introduite dans Ethernet par le MEF (Metro Ethernet Forum), qui est en tout point similaire au relais de trame, que nous présentons à la section suivante.

La signalisation

Le transport de l'information de commande, ou signalisation, est un aspect capital de l'infrastructure des réseaux. On peut même dire que l'avenir des réseaux réside dans la capacité de les piloter et d'automatiser leur configuration. L'objectif est de signaler une information, par exemple celle de déclencher les processus de mise en place de l'infrastructure, afin qu'une application puisse se dérouler.

La signalisation est depuis longtemps étudiée par les organismes de normalisation, et plus particulièrement par l'UIT-T. Elle a beaucoup évolué au cours des dix dernières années et elle continue à s'adapter aux bouleversements du monde IP. Par exemple, la signalisation SIP (Session Initiation Protocol) est devenue en quelques années la plus importante dans le monde des réseaux. Elle est notamment utilisée à des fins de convergence dans l'IMS (IP Multimedia SubSystem).

Ce chapitre ne vise pas à dresser un panorama exhaustif des protocoles de signalisation. Nous en abordons un grand nombre dans l'ensemble de l'ouvrage, en les introduisant directement dans les chapitres traitant des architectures ou des protocoles de service concernés. Le présent chapitre se contente d'introduire quelques notions de base et de les accompagner d'un certain nombre d'exemples éloquents, qui, même s'ils sont introduits par ailleurs dans l'ouvrage, représentent des cas importants.

Nous commençons par donner les raisons d'être de la signalisation et présenter les principales fonctions dont elle s'occupe. Nous introduisons ensuite les exemples de signalisation les plus importants, avec les protocoles RSVP et SIP.

Caractéristiques de la signalisation

La signalisation désigne les moyens à mettre en œuvre pour transmettre une information telle que l'ouverture ou la fermeture d'un chemin. Elle existe dans tous les réseaux, y compris ceux qui, comme IP, souhaitent la réduire au minimum afin de préserver la simplicité du système. La signalisation doit donc être capable de fonctionner selon toutes les techniques du monde des réseaux, en particulier des réseaux IP.

La signalisation demande généralement un mode routé. En effet, il faut indiquer à qui la signalisation est adressée et, pour cela, exhiber l'adresse complète du récepteur dans le paquet de signalisation. Tous les réseaux commutés ont donc besoin d'un réseau routé pour mettre en œuvre la signalisation.

La signalisation est capable de prendre en charge des services à différents niveaux de l'architecture. Par exemple, elle doit être capable d'effectuer une négociation de SLA (*voir le chapitre 26 pour la définition des SLA*), de demander l'authentification d'un utilisateur, de collecter des informations sur les ressources disponibles, etc. Le protocole de signalisation doit être extensible de façon à permettre l'arrivée de nouveaux services de façon simple. Le protocole de signalisation doit de plus être modulaire et flexible, afin de répondre aux besoins de chaque application particulière. La modularité facilite l'ajout de nouveaux modules lors des phases de développement.

Fonctionnement de la signalisation

Un protocole de signalisation comporte deux modes de fonctionnement : dans la bande (*inband*) et hors bande (*outband*). Dans le premier cas, les messages de signalisation sont transportés dans le chemin de données, tandis que dans le second ils sont indépendants du chemin suivi par les données.

Une autre caractéristique de la signalisation est la possibilité de couplage (*path-coupled*) ou au contraire de découplage du chemin (*path-decoupled*). Dans le premier cas,

la signalisation suit les données dans la bande ou hors bande en empruntant la même succession de nœuds. Par exemple, le protocole RSVP est *path-coupled* et le protocole SIP est *path-decoupled*.

La signalisation doit être capable de fonctionner à la fois dans les modes interdomaines et intradomaines. La signalisation doit également pouvoir fonctionner en modes bout-en-bout, bordure à bordure et end-to-edge (signalisation entre un end-host et un edge-node).

Dans l'environnement Internet hétérogène actuel, il existe un grand nombre de protocoles de signalisation, plus ou moins adaptés aux différentes applications. Cette grande diversité a poussé l'IETF à créer le groupe de travail NSIS (Next Step in Networking) afin de proposer une nouvelle norme unique destinée à rassembler toutes les précédentes.

D'une façon générale, un protocole de signalisation doit pouvoir coopérer avec d'autres protocoles. Pour ce faire, il doit être capable de transporter les messages d'autres protocoles de signalisation. Il est aussi possible de définir des interfaces permettant de transformer un message concernant un protocole en un message concernant un autre protocole.

La signalisation doit supporter la gestion de toutes les ressources du réseau. Elle prend en charge le transport des informations permettant d'exprimer les demandes des applications en termes de réservation et d'allocation de ressources. Pour ce faire, la signalisation interagit avec des entités spécifiques, telles que les serveurs de gestion de ressource, comme les *bandwidth brokers*, ou serveurs de bande passante. Enfin, la signalisation doit supporter la négociation de SLA entre un utilisateur et un fournisseur ou entre fournisseurs et la configuration des entités dans le réseau selon le nouveau SLA.

La signalisation peut supporter le monitoring des services et les états des entités dans le réseau et prendre en charge la facturation des services.

Afin de valider les demandes de service d'un utilisateur, la signalisation est aussi utilisée pour réaliser une authentification. Elle permet en ce cas de transporter les informations nécessaires à cette interaction. Ce transport doit être suffisamment générique pour autoriser les mécanismes existants et à venir.

Sécurité

La signalisation joue un rôle très important dans la sécurisation d'un réseau. En premier lieu, elle doit être elle-même sécurisée. Les primitives doivent pouvoir s'authentifier pour garantir qu'elles ne proviennent pas d'attaquants. La signalisation doit aussi implémenter des moyens de protection des messages de signalisation contre leur modification malicieuse. Elle doit en outre permettre de détecter qu'un ancien message est réutilisé, afin d'éviter le rejeu, et de cacher les informations de topologie du réseau. Elle peut enfin supporter des mécanismes de confidentialité des informations, tels que le chiffrement.

Les protocoles de signalisation peuvent coopérer avec les protocoles d'authentification et les agréments de clés (Key Agreement) pour négocier les associations de sécurité.

La signalisation doit aussi posséder des moyens pour négocier des mécanismes de sécurité selon les besoins des applications et des utilisateurs.

Mobilité

La signalisation joue un rôle important dans la gestion de la mobilité. Elle intervient dans les diverses actions à effectuer quand le mobile change de cellule, quand il effectue un roaming, lorsqu'il négocie son SLA ou bien pour la mise en place d'une application.

Quand un handover a lieu, la signalisation doit être capable de rétablir la connexion et de reconstituer rapidement et efficacement les états installés dans la nouvelle station de base. Le processus de rétablissement peut être local ou de bout en bout. Si le réseau mobile est surchargé, la signalisation des handovers doit avoir une priorité plus élevée que celle d'une signalisation démarrant une nouvelle connexion.

Charge du réseau

Dans une situation normale, le trafic de signalisation occupe une part peu importante du trafic du réseau. Cependant, dans certaines situations de congestion, de panne ou de problème, le trafic de signalisation peut augmenter de façon significative et créer une sévère congestion de la signalisation dans le réseau. Par exemple, une erreur de routage d'un paquet de signalisation peut entraîner une explosion en chaîne des messages de notification. Un protocole de signalisation doit être capable de maintenir la stabilité de la signalisation.

La signalisation doit être robuste, efficace et consommer le moins possible de ressource dans le réseau. Ce dernier doit être capable de fonctionner, même dans le cas d'une forte congestion.

Le réseau doit être capable d'assigner une priorité aux messages de signalisation. Cela permet de réduire les délais de transit des signalisations correspondant à des applications fortement prioritaires. Il faut également faire attention aux attaques par déni de service, qui peuvent saturer le réseau par des messages de signalisation de haute priorité.

Le protocole de signalisation doit permettre de regrouper des messages de signalisation. Cela peut concerner, par exemple, le regroupement des messages de rafraîchissement, comme RSVP, afin d'éviter de rafraîchir individuellement les états de réservation, ou soft-state.

La signalisation doit pouvoir passer l'échelle (scalabilité), c'est-à-dire s'appliquer à un petit réseau aussi bien qu'à un immense réseau de plusieurs millions de nœuds. Elle doit aussi être capable de prendre en charge et de modifier les différents mécanismes de sécurité en fonction des besoins en performance des applications.

Le protocole RSVP

Le protocole RSVP (Resource reSerVation Protocol) est conçu pour supporter la réservation unicast et multicast de ressources de bout en bout. Repris dans l'environnement IntServ (Integrated Services), RSVP est un protocole de signalisation modulaire, qui offre la possibilité de définir de nouveaux objets pour des extensions à venir. Il supporte le soft-state, fonctionne en mode path-coupled et fait la réservation en mode receiver-initiator, c'est-à-dire depuis le récepteur vers l'émetteur.

Des extensions de RSVP ont été proposées pour permettre la livraison fiable de messages de signalisation (message ACK/NACK) et le regroupement des messages de rafraîchissement dans un seul message SREFRESH. Une autre proposition d'extension permet l'agrégation des demandes de réservation de ressources pour augmenter la performance et la scalabilité du protocole.

Caractéristiques

Une caractéristique importante de RSVP est de permettre la réservation de ressources dans un mode multicast. Il est difficile d'utiliser le mode émetteur vers récepteur pour prendre en charge la réservation de ressources en multicast puisqu'on ne connaît pas les caractéristiques du récepteur au démarrage de la demande de réservation. C'est la raison pour laquelle RSVP fonctionne en mode récepteur vers émetteur.

Dans ce mode, c'est le récepteur des données qui déclenche et maintient la réservation des ressources dans le réseau. En d'autres termes, l'émetteur envoie une demande au récepteur, lequel déclenche la primitive de réservation de ressources et l'envoie vers l'émetteur. Le paquet portant cette primitive effectue la réservation dans les nœuds traversés en allant du récepteur vers l'émetteur. La raison de ce choix tient à la nécessité d'effectuer une réservation adéquate puisque la primitive de réservation connaît les caractéristiques de l'émetteur et du récepteur, et pas seulement celles de l'émetteur. Par exemple, si l'émetteur demande un débit de 1 Mbit/s mais que le récepteur ne puisse recevoir qu'un débit de 128 Kbit/s, il est inutile de réserver une bande passante de 1 Mbit/s, 128 Kbit/s suffisant.

Le maintien d'une réservation repose sur la notion de soft-state au niveau des nœuds intermédiaires et d'extrémité. Les soft-states sont des états périodiquement réactivés, permettant de mettre à jour dynamiquement le chemin à réserver en fonction des arrivées et des départs de participants et des changements de route. L'état de réservation peut donc être périssable, grâce à l'usage d'un temporisateur.

Les autres caractéristiques importantes de RSVP sont les suivantes :

- RSVP transporte et maintient des paramètres de contrôle de trafic (QoS) et de contrôle de politique (Policy Control) qui lui sont opaques. En fait, RSVP véhicule des structures d'objets définissables en dehors de lui.
- RSVP est pris en charge aussi bien par IPv4 qu'IPv6. Les composants du protocole sont définis pour cela pour IPv4 comme pour IPv6. Par exemple, les objets FILTER_SPEC sont définis différemment en IPv4 et en IPv6.
- RSVP est unidirectionnel. Il n'établit donc de réservation pour les flux de données que dans un seul sens. La réservation de ressources pour des transferts bidirectionnels requiert deux sessions RSVP indépendantes.
- RSVP n'est pas un protocole de routage. La signalisation RSVP utilise des protocoles de routage qui déterminent le chemin vers la destination. Précisons que RSVP fournit un mode opératoire transparent aux routeurs qui ne le supportent pas. Les routeurs non RSVP-aware routent les paquets IP qui transportent les messages RSVP comme des paquets normaux.

Fonctionnement

Le protocole de signalisation RSVP met en place une connexion logique appelée session. Une session RSVP est définie par les trois éléments suivants :

- adresse IP destination (unicast ou multicast) ;
- identifiant du protocole sur IP ;
- port destination (optionnel pour IPv4), TCP ou UDP.

Le modèle RSVP se fonde sur l'échange de deux messages fondamentaux, les messages Path et Resv (*voir figure 27.3*) :

- Le message Path (à l'initiative de l'émetteur) permet à l'émetteur du flux de données de spécifier les caractéristiques du trafic qu'il va générer.
- Le message Resv (à l'initiative du récepteur) permet à un récepteur ayant préalablement reçu un message Path de spécifier la QoS requise et de déclencher la réservation sur le chemin. Ce message suit le même chemin que celui du message Path mais dans le sens inverse.

Les principaux messages qui ont été définis dans RSVP sont les suivants :

- Message d'erreur :
  - PathErr, envoyé à l'émetteur qui a créé l'erreur.
  - ResvErr, envoyé vers le récepteur pour notifier une erreur en fusionnant les demandes de réservation.
- Message de confirmation de réservation :
  - ResvConf, utilisé pour indiquer le succès de la réservation si le récepteur ne reçoit pas le message ResvErr.
- Message de suppression :
  - PathTear, envoyé vers le récepteur pour supprimer l'état Path qui a été établi par le message Path.
  - ResvTear, envoyé vers l'émetteur pour supprimer l'état Resv qui a été établi par le message Resv.

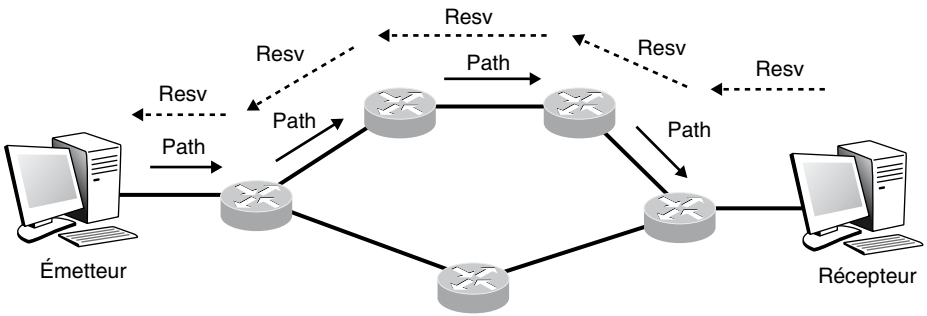


Figure 27.3

Fonctionnement du protocole RSVP

Format des messages de RSVP

Un message RSVP est constitué d'un en-tête commun et d'un nombre variable d'objets en fonction du type du message :

<RSVP message>::=<En-tête commun><ensemble des objets RSVP>

Comme illustré à la figure 27.4, l'en-tête du message RSVP est structuré de la façon suivante :

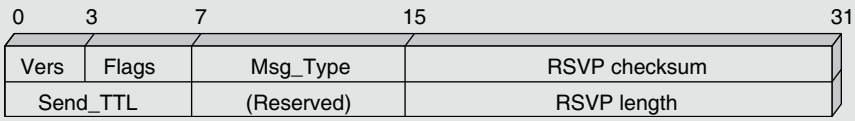


Figure 27.4

En-tête du message RSVP

- Vers (4 bits) : version du protocole.
- Flags (4 bits) : drapeau.
- Msg_Type :
  - Path
  - Resv
  - PathErr
  - ResvErr
  - PathTear
  - ResvTear
  - ResvConf
- RSVP Checksum (16 bits).
- Send_TTL : contient au départ la valeur du champ TTL du datagramme IP qui transporte le message RSVP. Grâce à ce champ, il est possible de détecter la traversée de routeurs non-RSVP. En effet, ceux-ci décrémentent le champ TTL IP et pas celui de RSVP, alors que les routeurs RSVP modifient les deux valeurs.
- RSVP Length (16 bits) : indique la longueur du message RSVP en octets.

La structure d'un objet RSVP (*voir figure 27.5*) suit celle de TLV (Type/Length/Value).

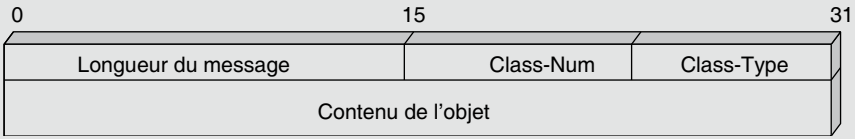


Figure 27.5

Structure d'un objet RSVP

- Longueur (16 bits) : indique la longueur de l'objet RSVP en octets.
- Class-Num : identifie la classe de l'objet.

Les classes qui sont définies sont récapitulées au tableau 27.1.

Numéro de la classe d'objet	Description
0 NULL	Ignoré par le récepteur
1 SESSION	Contient l'adresse IP destination, le protocole ID sur IP et le port de destination (obligatoire dans tous les messages).
3 RSVP_HOP	Transporte l'adresse IP du nœud RSVP qui a émis le message.
4 INTEGRITY	Données d'authentification
5 TIME_VALUES	Fréquence de rafraîchissement utilisée par le créateur du message
6 ERROR_SPEC	Spécifie une erreur dans un message PathErr, ResvErr ou ResvConf.
7 SCOPE	Transporte une liste des émetteurs de données vers lesquels les informations dans le message doivent être transmises.
8 STYLE	Style de réservation
9 FLOW_SPEC	Définit la QoS demandée.
10 FILTER_SPEC	Définit un sous-ensemble de paquets d'une session qui doit recevoir la QoS demandée (spécifié dans FLOW_SPEC) dans un message RESV.
11 SENDER_TEMPLATE	Contient l'adresse IP de l'émetteur et autre information pour identifier l'émetteur.
12 SENDER_TSPEC	Définit la caractéristique de trafic de l'émetteur de données.
13 ADSPEC	Transporte des données de OPWA.
14 POLICY_DATA	Transporte l'information de politique.
15 RESV_CONFIRM	Transporte l'adresse IP du récepteur qui a demandé la confirmation.

TABLEAU 27.1 • Classes d'objets RSVP

SIP (Session Initiation Protocol)

SIP est un protocole de signalisation dont la première version est apparue sous forme de draft à l'IETF en 1997 dans le groupe de travail MMUSIC. Repris dans le groupe SIP en 1999, il a été normalisé en mars 1999 sous la RFC 2543. La RFC 3261 décrit une nouvelle version de SIP dont l'objet est de réviser la RFC 2543, devenue de ce fait obsolète, en corrigeant ses erreurs et en apportant des détails sur les scénarios d'utilisation. Des compléments au protocole ont été définis dans les RFC 3262 à 3265.

SIP a pour objectif l'établissement, la modification et la terminaison de sessions multimédias entre deux terminaux. Il ne définit pas le corps de ses messages. Le corps, qui contient la description du média (vidéo, audio, codeur, etc.), est décrit par le protocole SDP (Session Description Protocol). Outre la description du flux, SIP peut transporter les médias utilisés dans une session, ou *session media*, en particulier des informations de QoS ou de sécurité. Le média de session est dissocié des échanges SIP.

Héritant du modèle HTTP, le mode d'échange est de type client-serveur, avec une relation d'égal à égal entre les deux. Les messages SIP sont des requêtes, aussi appelées méthodes, qui engendrent des messages en retour, les réponses. SIP peut fonctionner au-dessus de

plusieurs protocoles de transport. UDP est pour l'instant le plus utilisé, mais l'utilisation de TCP est aussi définie, ainsi que le transport par d'autres protocoles, tel SCTP (Stream Control Transmission Protocol). Avec UDP, SIP assure la fiabilité à partir d'accusés de réception positifs et de temporisateurs.

SIP est conçu pour être évolutif. Seules les fonctions de base sont obligatoires, des extensions pouvant être supportées ou non par les différentes entités qui s'échangent leur capacité.

Deux modes de communication sont possibles, le réseau décidant du mode :

- Mode direct : les deux entités SIP représentant les terminaux communiquent directement.
- Mode indirect : des entités intermédiaires faisant partie du réseau relaient les messages échangés.

Entités

SIP comporte plusieurs catégories d'entités, dont les plus classiques sont les entités utilisatrices et les entités réseau. Ces entités s'échangent des messages.

Entités utilisatrices

Les entités utilisatrices sont appelées agents utilisateur, ou UA (User Agent) ou encore plus simplement terminal utilisateur. Les UA ouvrent, modifient et terminent les sessions pour le compte de l'utilisateur. Concrètement, dans l'application multimédia du terminal utilisateur, il s'agit de la partie du programme qui permet de recevoir et d'établir les sessions. Elle regroupe deux composantes, l'une qui agit en tant que client (UAC) et initialise les sessions à la demande de l'utilisateur, l'autre qui agit en tant que serveur (UAS) et qui est responsable de la réception de toutes les sessions à destination de l'utilisateur. Les UA conservent des informations sur l'état de la session et sont dits pour cela *stateful*.

L'association des requêtes et des réponses entre deux entités de type UA constitue un dialogue.

Par analogie, on peut remarquer que la même chose se produit avec le protocole HTTP dans une application Web : un utilisateur exploite son navigateur comme client pour envoyer des requêtes et contacter une machine serveur, laquelle répond aux requêtes du client. La différence essentielle par rapport aux applications classiques utilisant HTTP est qu'en téléphonie un terminal doit être à la fois utilisé pour joindre un interlocuteur et pour appeler. Chaque terminal possède donc la double fonctionnalité de client et de serveur.

Lors de l'initialisation d'un appel, l'appelant exploite la fonctionnalité client de son terminal (UAC), tandis que celui qui reçoit la communication exploite sa fonctionnalité de serveur (UAS).

La communication peut être clôturée indifféremment par l'User Agent Client ou l'User Agent Server.

De nombreuses implémentations de clients SIP sont disponibles sur les plates-formes les plus courantes, Windows, Linux ou Mac. Elles sont le plus souvent gratuites, sous licence GPL.

Entités réseau

SIP définit trois entités logiques de type serveur faisant partie du réseau et agissant pour étendre son fonctionnement.

Serveur proxy (proxy server)

Le serveur proxy a une fonction de relais. Il accepte les requêtes ou les réponses SIP en provenance d'un terminal ou d'un autre serveur proxy et les fait suivre. Ce serveur peut conserver des états de l'avancement des sessions pour lesquelles il intervient. Il est dit dans ce cas *stateful.* Dans le cas inverse, il est dit *stateless.*

Le serveur proxy (parfois appelé serveur mandataire) permet d'initialiser une communication à la place de l'appelant. Il joue le rôle d'intermédiaire entre les terminaux des interlocuteurs et agit pour le compte de ces derniers. Le serveur proxy remplit les différentes fonctions suivantes :

- localiser un correspondant ;
- réaliser éventuellement certains traitements sur les requêtes ;
- initialiser, maintenir et terminer une session vers un correspondant.

Lorsqu'un utilisateur demande à un serveur proxy de localiser un correspondant, ce dernier effectue la recherche, mais, au lieu de retourner le résultat au demandeur, comme le ferait un serveur de redirection, il utilise cette réponse pour effectuer lui-même l'initialisation de la communication en invitant le correspondant à ouvrir une session.

Bien que fournissant le même type de service de localisation qu'un serveur de redirection, un serveur proxy va donc plus loin que la simple localisation en initialisant la mise en relation des correspondants de façon transparente pour le client. Il peut acheminer tous les messages de signalisation des terminaux, de l'initialisation de la communication à sa terminaison, en passant par sa modification. En contrepartie, le serveur proxy est une entité beaucoup plus sollicitée que le serveur de redirection, et donc plus lourde.

Chaque terminal peut et devrait en principe disposer d'un tel serveur sur lequel se reposer pour interpréter, adapter et relayer les requêtes. En effet, le serveur proxy peut reformuler une requête du terminal UAC afin de la rendre compréhensible par le serveur auquel s'adresse l'UAC. Cela accroît la souplesse d'utilisation du terminal et simplifie son usage.

Les serveurs proxy jouent aussi un rôle collaboratif, puisque les requêtes qu'ils véhiculent peuvent transiter d'un serveur proxy à un autre, jusqu'à atteindre le destinataire. Notons que le serveur proxy ne fait jamais transiter de données multimédias, et qu'il ne traite que les messages SIP.

On distingue deux types de serveurs proxy :

- Proxy statefull, qui maintient pendant toute la durée des sessions l'état des connexions.
- Proxy stateless, qui achemine les messages indépendamment les uns des autres, sans sauvegarder l'état des connexions.

Les proxy *stateless* sont plus rapides et plus légers que les proxy *statefull,* mais ils ne disposent pas des mêmes capacités de traitement sur les sessions.

Serveur d'enregistrement (Registrar Server)

Les UA de son domaine viennent s'enregistrer auprès de lui. Il renseigne ensuite le service de localisation, qui, lui, n'est pas défini par SIP. Le protocole généralement utilisé pour accéder à ce service est LDAP.

Deux UA peuvent communiquer entre eux sans passer par un serveur d'enregistrement, à la condition que l'appelant connaisse l'adresse IP de l'appelé. Cette contrainte est fastidieuse, car un utilisateur peut être mobile et donc ne pas avoir d'adresse IP fixe, par exemple s'il se déplace avec son terminal ou s'il se connecte avec la même identité à son travail et à son domicile. En outre, l'adresse IP peut être fournie de manière dynamique par un serveur DHCP.

Le serveur d'enregistrement offre un moyen de localiser un correspondant avec souplesse, tout en gérant la mobilité de l'utilisateur. Il peut en outre supporter l'authentification des abonnés.

Dans la pratique, lors de l'activation d'un terminal dans un réseau, la première action initialisée par celui-ci consiste à transmettre une requête d'enregistrement auprès du serveur d'enregistrement afin de lui indiquer sa présence et sa position de localisation courante dans le réseau. C'est la requête REGISTER, que nous détaillons plus loin, que l'utilisateur envoie à destination du serveur d'enregistrement. Celui-ci sauvegarde cette position en l'enregistrant auprès du serveur de localisation.

L'enregistrement d'un utilisateur est constitué par l'association de son identifiant et de son adresse IP. Un utilisateur peut s'enregistrer sur plusieurs serveurs d'enregistrement en même temps. Dans ce cas, il est joignable simultanément sur l'ensemble des positions qu'il a renseignées.

Serveur de redirection (Redirect Server)

Le serveur de redirection répond à des requêtes en donnant les localisations possibles de l'UA recherché. Ce serveur de redirection agit comme un intermédiaire entre le terminal client et le serveur de localisation. Il est sollicité par le terminal client pour contacter le serveur de localisation afin de déterminer la position courante d'un utilisateur.

L'appelant envoie au serveur de redirection une requête de localisation d'un correspondant. Il s'agit en réalité d'un message d'invitation, qui est interprété comme une requête de localisation. Le serveur de redirection joint le serveur de localisation afin d'effectuer la requête de localisation du correspondant à joindre. Le serveur de localisation répond au serveur de redirection, lequel informe l'appelant en lui fournissant la localisation trouvée. Ainsi, l'utilisateur n'a pas besoin de connaître l'adresse du serveur de localisation.

Serveur de localisation (Location Server)

SIP fait aussi référence à une quatrième entité, qui n'entre pas dans les dialogues SIP mais offre le service de localisation sur lequel les entités logiques SIP viennent s'appuyer. Ce serveur joue donc un rôle complémentaire par rapport au serveur d'enregistrement en permettant la localisation de l'abonné.

Le serveur de localisation contient la base de données de l'ensemble des abonnés qu'il gère. Cette base est renseignée par le serveur d'enregistrement. Chaque fois qu'un utilisateur s'enregistre auprès du serveur d'enregistrement, ce dernier en informe le serveur de localisation.

Presque toujours, le serveur de localisation et le serveur d'enregistrement sont implémentés au sein d'une même entité. On parle alors souvent non pas de serveur de localisation, mais de service de localisation d'un serveur d'enregistrement, tant ces fonctionnalités sont proches et dépendantes.

Les serveurs de localisation peuvent être collaboratifs. Le fonctionnement d'un serveur d'enregistrement est analogue à celui d'un serveur DNS dans le monde Internet : pour joindre un site Internet dont on ne connaît que le nom, il faut utiliser un serveur DNS, qui effectue la conversion (on parle de résolution) du nom en adresse IP. Ce serveur a connaissance d'une multitude d'adresses, qu'il peut résoudre parce qu'elles appartiennent à son domaine ou qu'il a la capacité d'apprendre dynamiquement en fonction des échanges qu'il voit passer. Dès qu'un nom lui est inconnu, il fait appel à un autre DNS, plus important ou dont le domaine est plus adéquat. De la même manière, les serveurs de localisation prennent en charge un ou plusieurs domaines et se complètent les uns les autres.

Un exemple d'échange entre entités SIP est illustré à la figure 27.6.

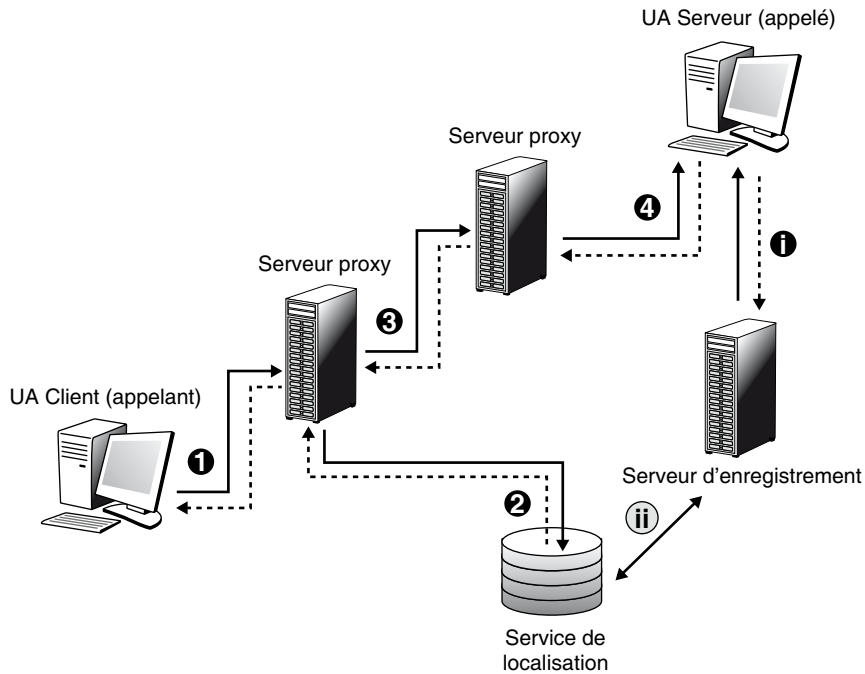


Figure 27.6

Exemple d'échange entre entités SIP lors d'un établissement de session

Messages

Il existe deux catégories de messages SIP, les requêtes et les réponses. Les messages sont codés en langage textuel. Le message comprend trois parties, comme illustré à la figure 27.7.

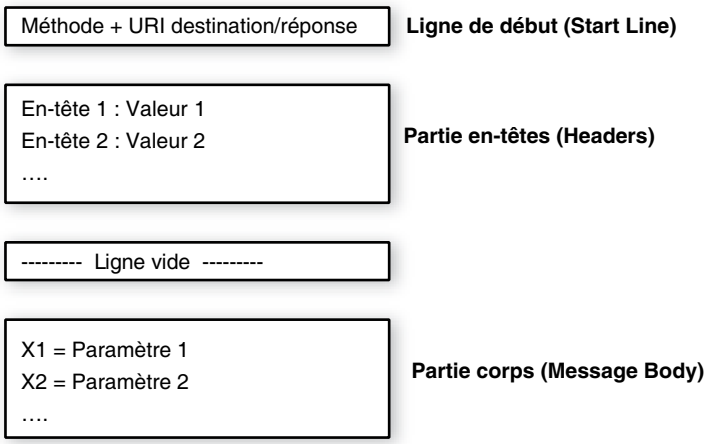


Figure 27.7
Structure des messages SIP

Les messages initialisés par les UAC (User Agent Client) à destination d'un ou de plusieurs UAS (User Agent Server) sont appelés requêtes ou méthodes, par analogie avec HTTP.

SIP n'utilise que six méthodes fondamentales pour formuler ses requêtes. Cela indique très nettement la volonté de simplicité de ses concepteurs. Ces méthodes sont détaillées dans la RFC 3261. Elles doivent être supportées par tous les terminaux et serveurs sollicités. À ces méthodes fondamentales, ont été ajoutées des méthodes supplémentaires, destinées à diverses améliorations, qui ne sont pas forcément implémentées par tous les terminaux.

Notons que l'établissement d'un appel peut ne faire intervenir que trois de ces méthodes fondamentales (INVITE, ACK et BYE).

Initialiser une session avec `INVITE`

La méthode INVITE permet d'initialiser une communication en invitant un correspondant à y participer. Elle peut aussi être utilisée pour une conférence afin d'inviter plusieurs interlocuteurs à communiquer au sein d'une même session.

Le corps du message de cette méthode fournit à l'appelé les paramètres de session souhaités et supportés par l'appelant. Ce dernier spécifiera, par exemple, le codec souhaité et le type de flux requis (voix, vidéo, etc.). En règle générale, l'appelant ne se contente

pas d'une seule proposition mais offre de multiples possibilités de paramètres. Ses préférences sont définies par l'ordre dans lequel apparaissent ses propositions.

Notons qu'une autre utilisation classique de cette méthode consiste à renégocier dynamiquement de nouveaux paramètres de session. Par exemple, si, durant une session déjà établie, l'un des interlocuteurs souhaite enrichir la voix par la vidéo, il fait sa demande par une requête d'invitation.

Confirmer les paramètres de session avec ACK

La méthode ACK correspond à un acquittement de l'appelant, qui peut être utilisé dans deux cas de figure :

- Elle fait suite à l'acceptation d'un appel par l'appelé. Avec la méthode d'invitation, l'émetteur a fait connaître au récepteur les paramètres qu'il supporte et ses préférences. En réponse, le récepteur en a fait autant. Au final, l'émetteur compare les paramètres supportés par les deux terminaux et indique par la méthode ack ceux qui seront utilisés. Dans le corps de ce message, la méthode décrit l'ensemble des paramètres de session à adopter au cours de la session. Si le corps de la méthode d'acquittement est vide, les paramètres proposés par l'appelant pourront être adoptés pour la session.
- Elle fait suite à une réponse de localisation fournie par un serveur de redirection. Une fois la détermination de la position de l'appelé effectuée, le serveur de redirection retourne le résultat à l'UAC (User Agent Client). Celui-ci valide la réception de ce résultat par la méthode ack.

S'informer sur le serveur avec OPTIONS

La méthode OPTIONS permet d'interroger un serveur SIP, y compris l'entité UAS (User Agent Server) sur différentes informations. Elle comporte globalement deux volets : l'état du serveur et ses capacités.

Par exemple, cette méthode offre la possibilité de savoir si un utilisateur que l'on souhaite appeler est présent, c'est-à-dire disponible pour initialiser une communication. Cette réponse est pratique en ce qu'elle donne des informations sur un serveur, sans avoir à initialiser une communication pour autant. Autrement dit, la requête ne fait pas sonner le poste du récepteur, puisqu'elle n'établit pas d'appel, mais agit comme un indicateur de présence.

Avec cette méthode, il est possible d'obtenir des informations sur un serveur relativement aux types de médias supportés (audio, vidéo, données), aux codecs supportés, aux méthodes supportées et aux options d'appels, si le serveur en a diffusé. Le serveur qui reçoit cette requête répond par son état et ses capacités.

Terminer une session avec BYE

La méthode BYE permet de libérer une communication. Cette requête peut être émise indifféremment par l'appelant ou par l'appelé. Elle n'attend pas d'acquittement, puisqu'une terminaison d'appel peut être décidée unilatéralement.

Abandonner une demande avec CANCEL

Cette méthode annule une requête dont la réponse n'est pas encore parvenue au demandeur. Elle ne permet pas d'interrompre une session, mais indique que la réponse n'est plus attendue et qu'il n'est donc pas nécessaire de traiter la requête.

Par exemple, une demande de recherche d'un utilisateur peut solliciter plusieurs serveurs de localisation en parallèle, qui vont tous rechercher la présence de l'abonné dans leur base de données et retourner le résultat de la recherche. Dès qu'un serveur a trouvé l'abonné, les autres serveurs n'ont plus besoin de poursuivre leur recherche. Un message d'annulation leur est donc envoyé.

Autre exemple, si un utilisateur envoie un message d'invitation INVITE et qu'il attende la réponse de l'appelé, il peut à tout moment émettre un message CANCEL afin d'annuler l'invitation sans avoir à attendre la réponse de l'appelant.

La méthode CANCEL est nécessairement acquittée par un message ACK pour signifier que l'annulation est prise en compte.

Enregistrer sa localisation avec REGISTER

Cette méthode permet d'enregistrer son adresse IP auprès d'un serveur d'enregistrement. Elle permet donc d'assurer le service de localisation.

L'information enregistrée correspond à une entrée dans la base spécifiant la correspondance d'une adresse SIP avec une adresse IP.

Cette entrée a une durée de vie limitée. Passé ce délai, le serveur de localisation la supprime de sa base de données. Par défaut, la durée est d'une heure. Périodiquement, chaque terminal doit rafraîchir cette entrée pour la conserver en base ou, s'il est mobile, la modifier le cas échéant.

Une autre manière de gérer la durée de vie de l'enregistrement est d'utiliser le champ *expire* de la méthode afin d'imposer une durée de validité fixe, qu'il n'est pas nécessaire de mettre à jour. Le risque dans ce cas est que si l'abonné se déconnecte du réseau sans l'indiquer au serveur d'enregistrement, il reste considéré comme actif dans le réseau (une tentative infructueuse de communication est initialisée).

Méthodes complémentaires

Plusieurs méthodes complémentaires ont été définies comme des extensions aux méthodes précédentes afin d'enrichir les communications SIP. Leur implémentation n'est toutefois pas systématique, et certains terminaux peuvent ne pas en supporter certaines. Néanmoins, ces méthodes apportent des fonctionnalités pratiques. Les huit méthodes d'extension classiquement utilisées sont les suivantes :

- info. Décrite dans la RFC 2976, cette méthode donne des informations complémentaires sur la session en cours (puissance de réception, qualité du son, codecs utilisés, etc.). Seules des données informatives sont envoyées en réponse à cette commande, ce qui ne modifie aucunement la session en cours.
- refer. Décrite dans la RFC 3515, cette méthode permet d'indiquer au récepteur du message une ressource. Elle autorise de la sorte différents services de relais, en particulier la redirection d'appel.

- update. Décrite dans la RFC 3311, cette méthode met à jour les paramètres d'une session multimédia.
- prack. Décrite dans la RFC 3262, cette méthode fournit une sécurisation des réponses provisoires. PRACK est l'acronyme de Provisional Reliable ACK.
- message. Décrite dans la RFC 3428, cette méthode est utilisée pour l'envoi de messages instantanés. Le contenu de cette méthode peut être fait en MIME, ce qui offre une liberté pour le transport des différents types de contenus.
- subscribe. Décrite dans la RFC 3265, cette méthode permet de demander une notification d'événement. Un client envoyant au serveur cette requête réclame d'être informé lorsque certains événements surviennent. Par exemple, un utilisateur peut souhaiter être averti lorsqu'un de ses contacts termine sa communication en cours. Il interroge alors le serveur pour lui demander d'être prévenu lorsque le contact devient disponible. Si le serveur accepte cette demande, il notifie les événements correspondant à l'abonnement de l'utilisateur pendant toute la durée spécifiée dans le champ expires inséré dans l'en-tête du message. Au-delà de cette durée, la notification n'est plus active. La notification est effectuée par le serveur au moyen de la commande notify.
- notify. Décrite dans la RFC 3265, cette méthode permet de recevoir une notification pour les événements auxquels on a souscrit. Lorsqu'un client a envoyé une demande de notification d'événement par la méthode subscribe, le serveur concerné lui envoie les notifications réclamées par la méthode notify.
- publish. Décrite dans la RFC 3903, cette méthode permet d'afficher l'état d'une requête à laquelle on a souscrit par la méthode subscribe.

Scénarios de session

Différents scénarios d'établissement de médias de session sont possibles. La figure 27.8 illustre un scénario qui met en évidence une caractéristique majeure de SIP : lors de sa réponse, l'UAS peut déclencher un échange direct des messages SIP à venir (a) ; de leur côté, les serveurs proxy peuvent obliger les messages SIP qui vont suivre à passer par eux (b).

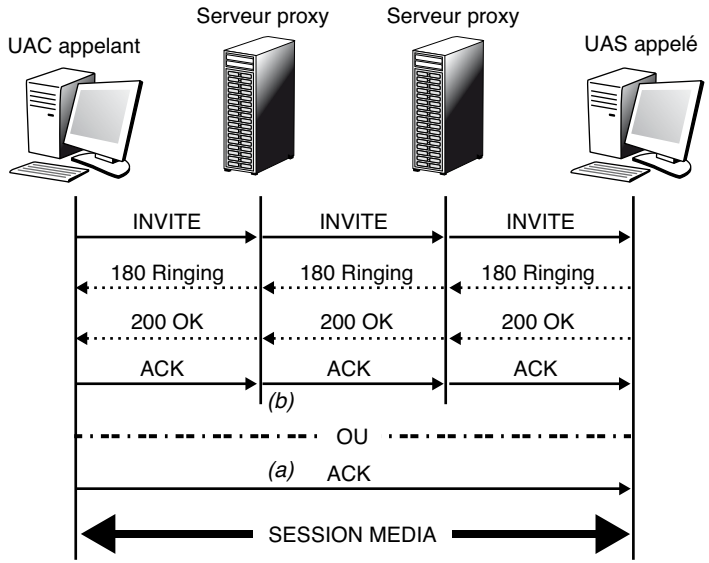


Figure 27.8
Exemple d'établissement de session SIP

SDP (Session Description Protocol)

SDP est une syntaxe de description de médias normalisée dans la RFC 2327 d'avril 1998. Cependant, comme nous le verrons un peu plus loin, SDP n'offre pas de possibilité complète de négociation de capacité de média. Issue du groupe MMUSIC de l'IETF précédant SIP, sa première application a été la description de sessions multicast combinée avec le protocole d'annonce de session multimédia SAP (Session Announcement Protocol), qui officie très largement dans le réseau multicast expérimental MBONE (Multicast Backbone).

SDP est ensuite devenu le protocole naturel de description des médias de session intégrés à l'établissement de session réalisé avec le protocole SIP.

La syntaxe de description de SDP suit un codage textuel. Une description de session est en fait une suite ordonnée de lignes, appelées fields, représentées par une lettre. Le nombre de fields est volontairement limité de façon à faciliter le décodage (*via* un parser). Le seul moyen d'étendre SDP est de définir de nouveaux attributs.

Le format général d'un field est *x* = paramètre1 paramètre2… paramètre*N*.

Les principales informations caractérisant le média de session sont les suivantes :

- adresse IP (ou nom d'hôte) : adresse de réception du flux média ;
- numéro de port pour la réception des flux ;
- type de média : audio, vidéo, tableau blanc, etc. ;
- schéma d'encodage (PCM A-LAW, MPEG-2, etc.

Le format du champ caractérisant le média de session est m = media port transport format-list, avec :

- media : audio, vidéo, application, données, contrôle ;
- port : numéro de port de réception du média ;
- transport : RTP/AVP (Audio Video Profiles) ou UDP ;
- format-list : liste d'informations complémentaires sur le média, ou Media Payload Type.

Plusieurs types de payload peuvent être listés. S'ils sont listés, il s'agit d'un choix proposé. Pour ouvrir *n* canaux audio il faut présenter *n* champs media.

Échange des caractéristiques du média de session

Le besoin de qualité de service nécessaire à la session est déduit des caractéristiques du média de session. Ces caractéristiques définies par SDP et présents dans le corps des messages SIP sont les suivantes :

- extrémités d'échange de flux : adresses IP source et destination et numéros de ports source et destination ;
- type de média échangé : audio, vidéo, etc. ;
- mode de codage utilisé : liste des codecs utilisés pour chaque flux, par exemple G.711 ou G.723.1.

Lors de l'initialisation d'une session SIP, seules les caractéristiques du média de l'émetteur sont connues. Elles sont déterminées par l'UAC en fonction de la demande de l'application utilisateur, application de téléphonie sur IP, par exemple. L'UAC qui initialise la demande d'établissement de session ne connaît pas *a priori* les informations concernant la partie caractéristique du média de l'UAS qu'il sollicite. Après l'arrivée de la sollicitation à l'UAS, la faisabilité de l'établissement de session est déterminée et, dans l'affirmative, les caractéristiques du média de session sont identifiées.

Il ne faut pas perdre de vue qu'un média de session classique résulte de l'échange de deux flux de média :

- flux de média de l'initiateur vers le sollicité ;
- flux de média du sollicité vers l'initiateur.

Dans cette version de SIP (RFC 2543), l'échange des caractéristiques du média de session donne très peu de latitude pour la négociation. En effet, l'UAS qui reçoit les caractéristiques du média de session souhaité dispose du type de média et de la liste des codecs relatifs proposés par l'UAC de départ. Il est précisé que la station qui initialise la communication indique dans sa liste des codecs ceux avec lesquels il veut recevoir le flux média et le fait qu'il aimerait émettre ce flux. Dans sa réponse, l'UAS précise sa liste de codecs, qui peut être ou non un sous-ensemble de la liste de l'émetteur. Il indique lui aussi la liste des codecs avec lesquels il veut recevoir le flux média. La RFC SDP précise que, lorsqu'une liste de codecs est donnée, elle spécifie les codecs qui peuvent être utilisés pendant la session avec un ordre de préférence, le premier étant considéré comme le codec par défaut de la session.

Dans le meilleur des cas, l'UAS sollicité accepte la liste des codeurs qui lui sont proposés (flux sollicité → initiateur). Inversement, l'UAC initiateur accepte celle qui lui est proposée (flux initiateur → sollicité). Pour qu'une session puisse avoir lieu, il faut au minimum que chacun accepte le premier codeur spécifié dans la liste qui lui est proposée. Autrement, la session ne peut avoir lieu.

L'échange des caractéristiques de média est illustré à la figure 27.9.

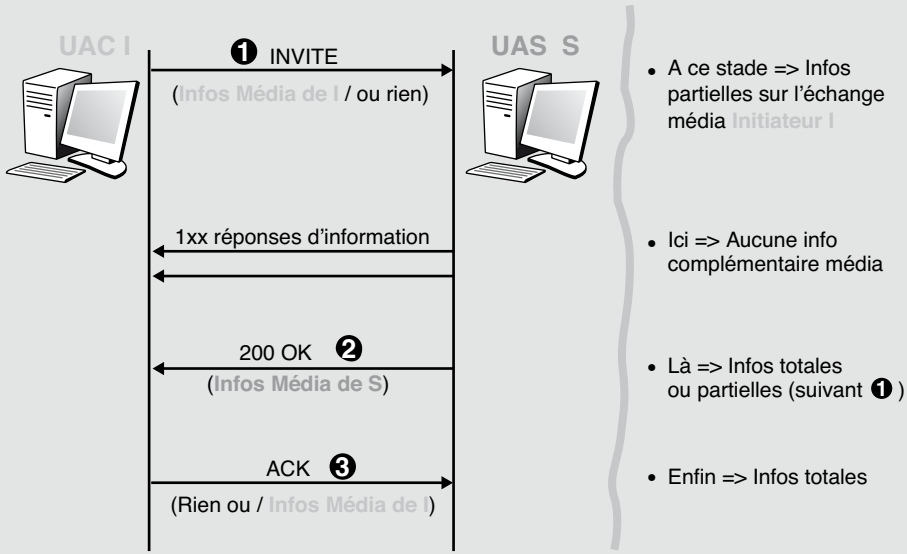


Figure 27.9

Échange des caractéristiques de média dans le protocole SIP

La figure 27.10 présente un exemple mettant en évidence les extensions qui ont été apportées en 2002. Ces nouvelles possibilités ont un impact important. En effet, les informations caractérisant le média ne se trouvent plus uniquement dans les messages principaux de l'établissement de session INVITE, 200 OK et ACK mais dans les messages provisoires, tel 180 RINGING, et les messages intermédiaires de modification UPDATE. Cela rend toutefois l'intégration plus complexe.

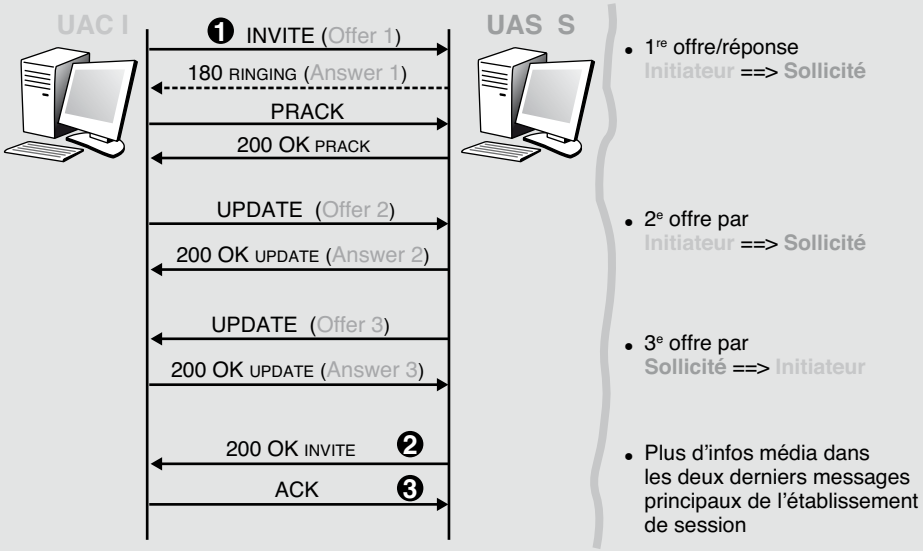


Figure 27.10

Échange des caractéristiques média dans SIP

GIMPS (General Internet Messaging Protocol for Signaling)

Nous avons examiné dans ce chapitre les principales caractéristiques des protocoles de signalisation. Nous avons vu quelques exemples avec les protocoles de signalisation les plus connus, comme RSVP, H.323, SIP, MGCP et COPS, qui se situent à différents niveaux de l'architecture : le niveau 3 pour RSVP et COPS, qui cherchent à effectuer une allocation de ressources de niveau 3, et le niveau 7 pour SIP.

Le nombre de protocoles de signalisation du monde IP est très important du fait que la normalisation s'est effectuée en suivant les services de niveaux réseau et application et que chaque technologie a introduit ses propres protocoles de signalisation. Le groupe de travail NSIS (Next Step In Signaling) de l'IETF essaie d'introduire un protocole de signalisation unique. Plus exactement, il s'agit d'un protocole de signalisation à deux niveaux, le premier au niveau transport, qui introduit la normalisation de la structure du paquet de signalisation transportant les différentes catégories de signalisation, et le second au niveau de la couche application pour la signalisation du service.

L'architecture du protocole GIMPS, qui semble devoir être le prochain protocole normalisé, est décrite à la figure 27.11.

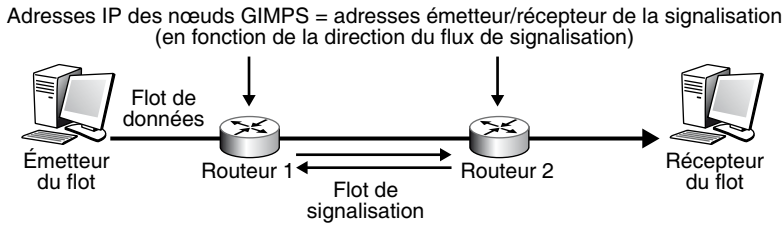


Figure 27.11

Architecture du protocole GIMPS

Conclusion

Le contrôle est primordial dans un réseau à transfert de paquets, car il permet, par exemple, de réagir à la moindre congestion. Il sert en outre à tout un ensemble de régulations, dont celle de la qualité de service, en attribuant des priorités plus ou moins fortes aux différents flux.

Le monde IP s'est beaucoup préoccupé du contrôle de flux. En effet, lorsque le nombre de machines terminales émettant en même temps devient important, il faut mettre en place un contrôle assez fin pour qu'il n'y ait pas de congestion dans un des routeurs du réseau. De nombreux efforts restent encore à faire pour contrôler de façon adéquate les millions de flots d'Internet afin que tous les utilisateurs soient satisfaits du comportement du réseau.

Les techniques de contrôle s'appliquent également aux ouvertures de chemins dans les techniques de commutation. On parle aussi de signalisation dans ce cas.

Les contrôles précédents concernent les couches basses des architectures. Dans les niveaux supérieurs les contrôles sont tout aussi importants, car ils permettent d'ouvrir des sessions, comme dans la téléphonie.

En résumé, il existe un très grand nombre de formes de contrôles, et la normalisation est assez en retard par rapport à la gestion de réseau. Le groupe de travail NSIS (Next Step In Signaling) a été lancé pour essayer de normaliser la signalisation dans les réseaux du futur. Après un démarrage difficile, ce groupe de normalisation n'a pas encore pu imposer une norme commune, mais les avancées déjà réalisées sont un bon signe pour le futur.

28

La sécurité et l'identité

La sécurité est une fonction incontournable des réseaux. Puisqu'on ne voit pas son correspondant directement, il faut l'authentifier. Puisqu'on ne sait pas par où passent les données, il faut les chiffrer. Puisqu'on ne sait pas si quelqu'un ne va pas modifier les informations émises, il faut vérifier leur intégrité. Nous pourrions ajouter une longue suite de requêtes du même genre qui doivent être prises en charge par les réseaux.

Globalement, on peut diviser la sécurité en deux parties : la sécurité à l'ouverture de la session et la sécurité lors du transport de l'information. Les techniques pour réaliser ces deux formes de sécurité sont extrêmement diverses, et il s'en invente de nouvelles tous les jours. De même, les pirates, à chaque attaque contrée, vont un peu plus loin pour contourner les défenses. Ce jeu de poursuite n'est pas de nature à faciliter la présentation des mécanismes de sécurité. Dans cet ouvrage, nous nous limitons à l'environnement réseau, sans nous pencher sur la sécurité physique des terminaux ou des logiciels.

Ce chapitre propose une vue générale des éléments de sécurité dans un réseau, en suivant la proposition de l'ISO en matière de sécurité. Cette proposition a été effectuée en même temps que le modèle de référence. Nous présentons ensuite les mécanismes de sécurité les plus classiques, tels que l'autorisation, l'authentification, le chiffrement, la signature, etc. Le chapitre suivant s'intéresse plus particulièrement au monde IP et aux protocoles qui implémentent les mécanismes décrits dans ce chapitre.

La sécurité du transport de l'information est une préoccupation primordiale dans le domaine des réseaux. Pendant de longues années, la sécurité d'un équipement demandait une isolation complète de l'environnement extérieur, et aucune communication avec une machine externe n'était possible. C'est encore très souvent le cas aujourd'hui.

Ce chapitre examine les mécanismes fondamentaux de sécurité mis en œuvre dans les réseaux, ainsi que les algorithmes de chiffrement et d'authentification.

Nous décrirons également les problèmes posés par l'identification et donnerons quelques pistes importantes dans les développements actuels. Enfin, nous introduirons la carte à puce comme élément de sécurité puisque ces cartes forment l'un des éléments, si ce n'est l'élément, le plus résistant en matière de sécurité de réseau. La téléphonie mobile avec le GSM l'a choisie et son extension est en cours dans de nombreux environnements réseau.

Les services de sécurité

En informatique, le terme sécurité recouvre tout ce qui concerne la protection des informations. L'ISO s'est attachée à prendre toutes les mesures nécessaires à la sécurité des données durant leur transmission. Ces travaux ont donné naissance à un standard d'architecture international, ISO 7498-2 (*OSI Basic Reference Model-Part 2: Security Architecture*). Cette architecture est très utile pour tous ceux qui veulent implémenter des éléments de sécurité dans un réseau car elle décrit en détail les grandes fonctionnalités et leur emplacement par rapport au modèle de référence.

Trois grands concepts ont été définis :

- Les fonctions de sécurité, qui sont déterminées par les actions pouvant compromettre la sécurité d'un établissement.
- Les mécanismes de sécurité, qui définissent les algorithmes à mettre en œuvre.
- Les services de sécurité, qui représentent les logiciels et les matériels mettant en œuvre des mécanismes dans le but de mettre à la disposition des utilisateurs les fonctions de sécurité dont ils ont besoin.

La figure 28.1 recense les services de sécurité et les niveaux de l'architecture OSI où ils doivent être mis en œuvre.

Cinq types de service de sécurité ont été définis :

- La confidentialité, qui doit assurer la protection des données contre les attaques non autorisées.
- L'authentification, qui doit permettre de s'assurer que celui qui se connecte est bien celui qui correspond au nom indiqué.
- L'intégrité, qui garantit que les données reçues sont exactement celles qui ont été émises par l'émetteur autorisé.
- La non-répudiation, qui assure qu'un message a bien été envoyé par une source spécifiée et reçu par un récepteur spécifié.
- Le contrôle d'accès, qui a pour fonction de prévenir l'accès à des ressources sous des conditions définies et par des utilisateurs spécifiés.

Dans chacun de ces services, il peut exister des conditions particulières, indiquées à la figure 28.1.

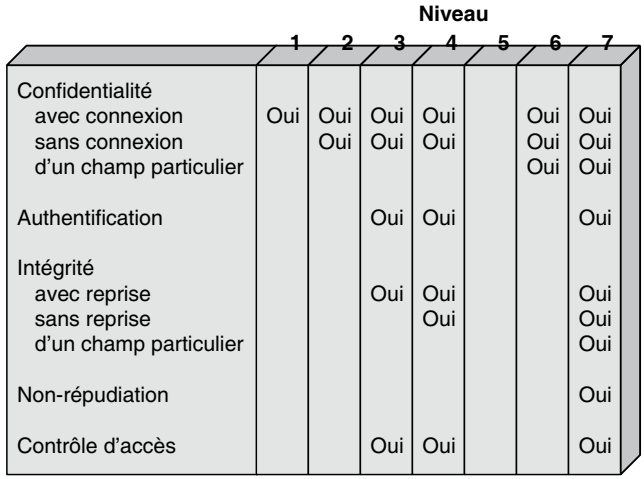


Figure 28.1

Sécurité et niveaux de l'architecture OSI

Si l'on reprend les cinq services de sécurité présentés précédemment en étudiant les besoins de l'émetteur et du récepteur et en les répertoriant, on obtient le processus suivant :

1. Le message ne doit parvenir qu'au destinataire.
2. Le message doit parvenir au bon destinataire.
3. L'émetteur du message doit pouvoir être connu avec certitude.
4. Il doit y avoir identité entre le message reçu et le message émis.
5. Le destinataire ne peut contester la réception du message.
6. L'émetteur ne peut contester l'émission du message.
7. L'émetteur ne peut accéder à certaines ressources que s'il en a l'autorisation.

Le besoin 1 correspond à un service de confidentialité, les besoins 2 et 3 à un service d'authentification, le besoin 4 à un service d'intégrité des données, les besoins 5 et 6 à un service de non-répudiation, et le besoin 7 au contrôle d'accès.

Les mécanismes de chiffrement

Le chiffrement est un mécanisme issu d'une transformation cryptographique. Le mécanisme inverse du chiffrement est le déchiffrement. La normalisation dans ce domaine est quelque peu complexe, pour des raisons essentiellement politiques. De ce fait, l'ISO a supprimé ce type de normalisation de son cadre de travail à la suite de la publication des algorithmes DES (Data Encryption Standard). L'ISO est alors devenue une simple chambre d'enregistrement des algorithmes de chiffrement.

La première norme ISO du domaine, ISO 9979, se préoccupe du problème relatif aux « procédures pour l'enregistrement des algorithmes cryptographiques ». Une trentaine d'algorithmes sont aujourd'hui déposés à l'ISO ou chez d'autres organismes de normalisation. Les principaux mécanismes de chiffrement normalisés par l'ISO sont les suivants :

- Le mécanisme de bourrage de trafic consiste à envoyer de l'information en permanence en complément de celle déjà utilisée de façon à empêcher les fraudeurs de repérer si une communication entre deux utilisateurs est en cours ou non.
- L'authentification utilise un mécanisme de cryptographie normalisé par la série de normes ISO 9798 à partir d'un cadre conceptuel défini dans la norme ISO 10181-2. Dans cette normalisation, des techniques de chiffrement symétrique et à clés publiques sont utilisées.
- L'intégrité est également prise en charge par l'ISO. Après avoir défini les spécifications liées à la normalisation de l'authentification dans la norme ISO 8730, cet organisme a décrit le principal mécanisme d'intégrité, le CBC (Cipher Block Chaining), dans la norme ISO 8731. La norme ISO 9797 en donne une généralisation. La norme ISO 8731 décrit un second algorithme, le MAA (Message Authenticator Algorithm).
- La signature numérique est un mécanisme appelé à se développer de plus en plus. Pour le moment, la normalisation s'adapte aux messages courts, de 320 bits ou moins. C'est l'algorithme RSA, du nom de ses inventeurs (Rivest, Shamir, Adleman), qui est utilisé dans ce cadre (ISO 9796). Le gouvernement américain possède son propre algorithme de signature numérique, le DSS (Digital Signature Standard), qui lui a été délivré par son organisme de normalisation, le NIST (National Institute for Standards and Technology).
- La gestion des clés peut également être mise en œuvre dans les mécanismes de sécurité. Elle comprend la création, la distribution, l'échange, le maintien, la validation et la mise à jour de clés publiques ou secrètes. En matière d'algorithmes symétriques, la norme ISO 8732 fait référence. De même, la norme ISO 11166 fait référence pour les algorithmes asymétriques.

Les mécanismes de sécurité pour la messagerie électronique ont été définis par l'UIT-T, dans la série de recommandations X.400. Cette série fournit la description des menaces et les clés d'utilisation de l'algorithme cryptographique RSA pour résoudre ces problèmes.

Le second apport de l'UIT-T en matière de sécurité concerne les annuaires et fait l'objet de la recommandation X.509. Les annuaires électroniques peuvent également être le lieu de dépôt des clés publiques, et l'UIT-T a introduit des concepts de certificats de clés publiques et des mécanismes de gestion de ces certificats.

Les algorithmes de chiffrement

Les algorithmes de chiffrement permettent de transformer un message écrit en clair en un message chiffré, appelé cryptogramme. Cette transformation se fonde sur une ou plusieurs clés. Le cas le plus simple est celui d'une clé unique et secrète, que seuls l'émetteur et le récepteur connaissent.

Les systèmes à clés secrètes sont caractérisés par une transformation f et une transformation inverse f^{-1}, qui s'effectuent à l'aide de la même clé. C'est la raison pour laquelle on appelle ce système « à chiffrement symétrique ». Cet algorithme est illustré à la figure 28.2.

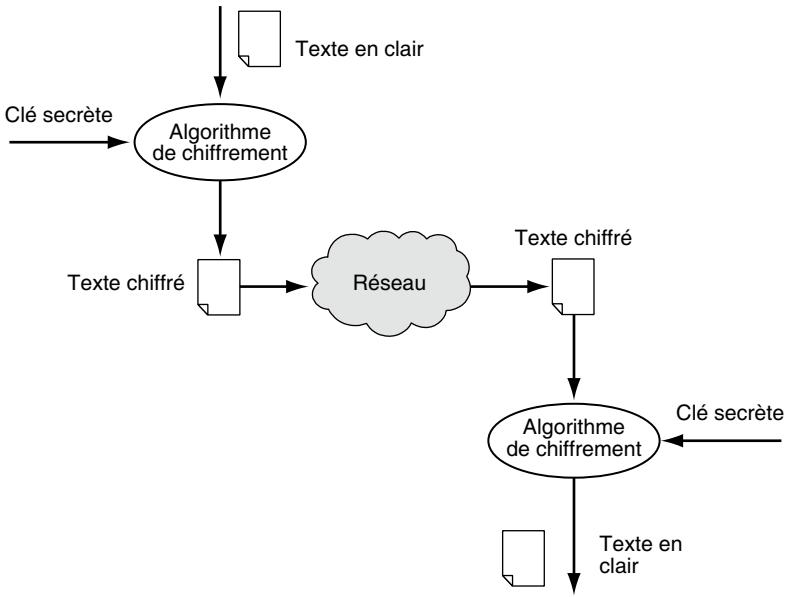


Figure 28.2

Algorithme de chiffrement symétrique

Le plus connu des algorithmes de chiffrement est le DES. Pour chaque bloc de 64 bits, le DES produit un bloc chiffré de 64 bits. La clé, d'une longueur de 56 bits, est complétée par un octet de détection d'erreur. De cette clé de 56 bits, on extrait de manière déterministe 16 sous-clés de 48 bits chacune. À partir de là, la transformation s'effectue par des sommes modulo 2 du bloc à coder et de la sous-clé correspondante, avec des couplages entre les blocs à coder.

Les algorithmes à sens unique sont ceux dont la transformation en sens inverse est quasiment impossible à effectuer dans un laps de temps admissible. Diffie-Hellman constitue un premier exemple de ce type d'algorithme. Soit X et Y un émetteur et un récepteur qui veulent communiquer. Ils se mettent d'accord sur deux valeurs non secrètes, μ et p. L'émetteur X choisit une valeur a secrète et envoie à Y la valeur $x = \mu_a \bmod p$. De même, Y choisit une valeur b secrète et envoie à X une valeur $y = \mu_b \bmod p$. Si les valeurs μ et p sont suffisamment grandes, le fait de retrouver a ou b à partir de x ou y est à peu près impossible. X et Y décident que la clé commune est le produit ab et que le message chiffré est obtenu par $\mu_{ab} \bmod p$.

Les algorithmes de chiffrement à clé publique sont des algorithmes asymétriques. Le destinataire est le seul à connaître la clé de déchiffrement. La sécurité s'en trouve accrue puisque même l'émetteur ne connaît pas cette clé. L'algorithme le plus classique et le plus utilisé est RSA, qui utilise la quasi-impossibilité d'effectuer la fonction d'inversion d'une fonction puissance. La clé permettant de déchiffrer le message et que seul le destinataire connaît est constituée de deux nombres, p et q, d'environ 250 bits chacun. La clé publique est $n = pq$. Comme n est très grand, il est quasiment impossible de trouver toutes les factorisations possibles. La connaissance de n ne permet pas d'en déduire p et q. À partir de p et de q, on peut choisir deux nombres, e et d, tels que $ed = 1 \bmod (p - 1)(q - 1)$. De même, la connaissance de e ne permet pas de déduire la valeur de d.

L'algorithme de chiffrement s'effectue de la façon suivante : si M est le message à chiffrer, le message chiffré est obtenu par $M_e \bmod n$ et l'algorithme de déchiffrement par $(M_e)_d$.

La figure 28.3 illustre le fonctionnement de l'algorithme asymétrique.

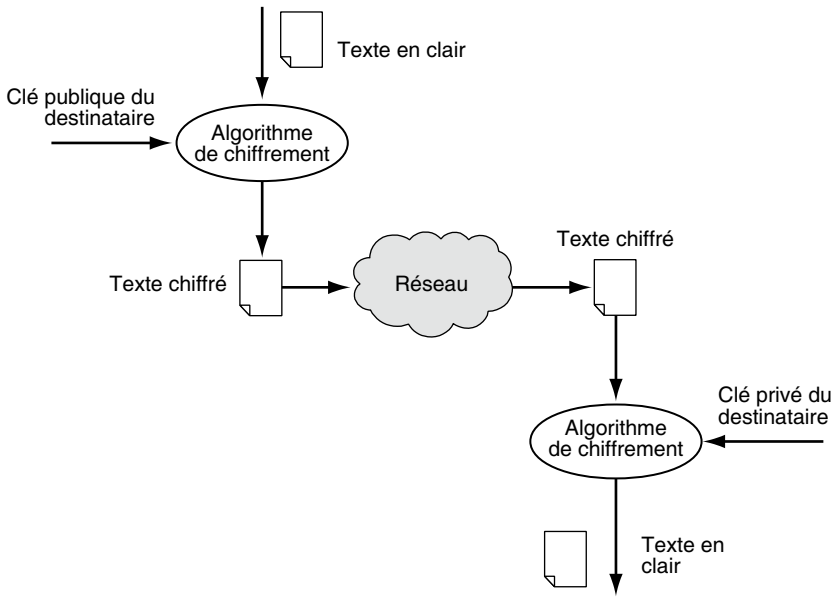


Figure 28.3

Algorithme de chiffrement asymétrique

Les signatures électroniques font également partie de la panoplie des mécanismes indispensables à la transmission de documents dans un réseau. La signature a pour fonction d'authentifier l'émetteur. Celui-ci code le message de signature par une clé qu'il est le seul à connaître. La vérification d'une signature s'effectue par le biais d'une clé publique. En utilisant l'algorithme RSA, l'émetteur signe le message M par $M_e \bmod n$, et le récepteur porte cette valeur à la puissance d pour vérifier que $(M_e)_d = M$. Si cette égalité se vérifie, la signature est authentifiée.

Solutions de chiffrement

Le chiffrement représente la méthode suivie pour que l'information ne puisse pas être lue par une autre personne que le destinataire. Les techniques de chiffrement que l'on utilise sont toutes *a priori* violables, mais il faudrait pour cela utiliser une machine de calcul extrêmement puissante et la faire tourner pendant plusieurs années.

Nous allons introduire les principaux algorithmes qui permettent de chiffrer une suite d'éléments binaires en la transformant en une nouvelle suite d'éléments binaires, qui, elle, ne peut être lue sans la clé de déchiffrement :

- DES, de 1977, à clés symétriques. Les données sont codées par blocs de 64 bits avec une clé de 56 bits. Cet algorithme est très utilisé dans les applications financières. Il est également utilisé dans un chaînage dit par bloc CBC (Cipher Block Chaining). Il existe de nombreuses variantes de l'algorithme DES, comme 3DES, qui utilise trois niveaux de chiffrement, ce qui implique une clé de chiffrement sur 168 bits.
- RC4, RC5 (Rivest's Code #4, #5), de 1987, à clés symétriques. Ce sont des algorithmes propriétaires, diffusés par la société RSA Security Inc. Ils utilisent des clés de longueur variable pouvant atteindre 2 048 bits. Ils sont surtout utilisés au niveau applicatif lorsqu'une application a besoin d'être fortement sécurisée. Ils demandent une puissance de calcul importante, qui ne pourrait être maintenue sur un flot continu à haut débit à des niveaux inférieurs de l'architecture.
- IDEA (International Data Encryption Algorithm), de 1992, à clés symétriques. Cet algorithme développé en Suisse est surtout utilisé pour la messagerie sécurisée PGP, que nous détaillons un peu plus loin dans ce chapitre.
- Blowfish, de 1993, à clés symétriques.
- AES (Advanced Encryption Standard), de 1997, à clés symétriques.
- RSA (Rivest, Shamir, Adleman), de 1978, à clés asymétriques (RFC 2437).
- Diffie-Hellman, à clés asymétriques.
- El Gamal, à clés asymétriques.

L'ensemble des techniques que nous venons d'énumérer est difficile à mettre en œuvre dès que le débit d'une application, d'un flot ou d'un lien augmente. C'est la raison pour laquelle, les techniques symétriques et asymétriques sont utilisées conjointement. Pour cela, on recourt à des clés de session, qui ne sont valables que pour une communication déterminée. Les informations de la session sont codées grâce à une clé secrète permettant de réaliser un chiffrement avec beaucoup moins de puissance qu'une clé asymétrique. Seule la clé secrète est codée par un algorithme de chiffrement asymétrique pour être envoyée au destinataire.

Les certificats

Une difficulté qui s'impose à la station d'un réseau qui communique avec beaucoup d'interlocuteurs consiste à se rappeler de toutes les clés publiques dont elle a besoin pour récupérer les clés secrètes de session. Pour cela, il faut utiliser un service sécurisé et

fiable, qui délivre des certificats. Un organisme offrant un service de gestion de clés publiques est une autorité de certification, appelée tiers de confiance. Cet organisme émet des certificats au sujet de clés permettant à une entreprise de les utiliser avec confiance.

Un certificat est constitué d'une suite de symboles (document M) et d'une signature. Le format de certificat le plus courant provient du standard X.509 v2 ou v3. La syntaxe utilisée est l'ASN.1.

L'authentification

L'authentification a pour objectif de vérifier l'identité des processus communicants. Plusieurs solutions simples sont mises en œuvre pour cela, comme l'utilisation d'un identifiant (*login*) et d'un mot de passe (*password*). L'authentification peut s'effectuer par un numéro d'identification personnel, comme le numéro inscrit dans une carte à puce, ou code PIN (Personal Identification Number).

Des techniques beaucoup plus sophistiquées, comme les empreintes digitales ou rétiniennes, se développent de façon industrielle en ce début des années 2000. Cependant, leur utilisation est assez complexe et ne peut être mise en place que dans un contexte particulier, comme un centre de recherche de l'armée.

L'authentification peut être simple ou mutuelle. Elle consiste essentiellement à comparer les données provenant de l'utilisateur qui se connecte à des informations stockées dans un site protégé. Des attaques sur les sites mémorisant les mots de passe forment une classe importante de piratage.

L'intégrité des données

L'intégrité des données consiste à prouver que les données n'ont pas été modifiées. Elles ont éventuellement pu être copiées, mais aucun bit ne doit avoir été changé.

Une première possibilité pour garantir l'intégrité des données transportées dans un paquet est de les chiffrer. En effet, si les données sont impossibles à déchiffrer par le récepteur, c'est qu'elles ont été modifiées. Cette solution permet à la fois de garantir la confidentialité et l'intégrité.

Une seconde possibilité provient des techniques de signature. Une signature, déterminée par l'ensemble des éléments binaires composant un message, est nécessaire pour en assurer l'intégrité. Le chiffrement joue le rôle de signature dans la première possibilité. Une signature plus simple que le chiffrement est suffisante dans le cas d'une demande d'intégrité uniquement. Pour cela, on utilise des fonctions de hachage, qui calculent une empreinte digitale qu'il suffit de vérifier au récepteur pour prouver que la suite d'éléments binaires n'a pas été modifiée. Pour que l'empreinte ne puisse être modifiée par hasard lors de la transmission, c'est-à-dire pour que le pirate ne puisse à la fois déterminer l'algorithme de hachage utilisé et recalculer une nouvelle valeur de l'empreinte sur la suite d'éléments binaires modifiés, une fonction de chiffrement doit être appliquée à la signature.

Les plus célèbres techniques de signature sont les suivantes :

- MD5 (Message Digest #5), de 1992, défini dans la RFC 1321. Ce sont des fonctions conçues par Ron Rivest qui produisent des empreintes de 128 bits.
- SHA-1 (Secure Hash Algorithm), de 1993, pour les fonctions de hachage. Cette technique permet de réaliser une empreinte de 160 bits.

La non-répudiation

Les services de non-répudiation consistent à empêcher le démenti qu'une information a été reçue par une station qui l'a réclamée. Ce service permet de donner des preuves, comme on peut le faire par télex. De manière équivalente, on peut retrouver la trace d'un appel téléphonique, de telle sorte que le récepteur de l'appel ne puisse répudier cet appel.

La fonction de non-répudiation peut s'effectuer à l'aide d'une signature à clé privée ou publique ou par un tiers de confiance qui peut certifier que la communication a bien eu lieu.

Caractéristiques des algorithmes de sécurité

Cette section présente quelques caractéristiques des algorithmes de sécurité, en commençant par les algorithmes de chiffrement, puis analyse leurs performances temporelles.

Les algorithmes de chiffrement

Les algorithmes de chiffrement les plus classiques sont DES, 3DES et AES qui est aujourd'hui le plus utilisé.

Nombre de rounds

La plupart des algorithmes de chiffrement par clés symétriques utilisent le chiffrement en utilisant deux transformations : une substitution et une permutation. Un « round » est complété lorsque ces deux transformations sont effectuées une fois.

En règle générale, on considère que plus le nombre de round est élevé, plus la sécurité apportée est grande. En revanche, plus le nombre de round est élevé, plus on consomme de ressources, si bien que les temps de réponse peuvent s'en ressentir. C'est la raison pour laquelle AES est devenu très prisé. Cet algorithme ne demande pas un effort de calcul aussi important que les algorithmes DES, tout en étant plus sûr.

Le nombre de round n'est cependant pas toujours le critère le plus important. Certains algorithmes sont beaucoup plus puissants que d'autres, tout en ayant beaucoup moins de rounds.

DES et 3DES

DES applique 16 rounds. 3DES, qui est une succession de trois algorithmes DES, applique $3 \times 16 = 48$ rounds.

Algorithme	Nombre de round
DES	16 rounds
3DES	48 rounds

AES

AES applique 10 rounds avec une clé de 128 bits, 12 rounds avec une clé de 192 bits et 14 rounds avec une clé de 256 bits.

Algorithme	Nombre de round
AES	10 rounds pour une clé de 128 bits 12 rounds pour une clé de 192 bits 14 rounds pour une clé de 256 bits

Longueur de la clé

En règle générale, plus la clé est longue, plus l'algorithme est résistant à une attaque exhaustive. La force d'un algorithme symétrique, dédié à la confidentialité ou à l'intégrité, peut être mesurée en termes de *work factor* associé à une attaque « exhaustive », ou attaque de force brute. Cette attaque consiste à tester toutes les clés possibles. Si une clé a une longueur de n bits, il existe 2^n possibilités de clés différentes, et il faudrait en moyenne 2^{n-1} essais pour trouver la valeur de la bonne clé. On considère que plus la clé est grande, plus la probabilité de la trouver est faible et donc plus grande est la sécurité. La sécurité correspond ici à la résistance de l'algorithme symétrique à une attaque exhaustive.

DES et 3DES

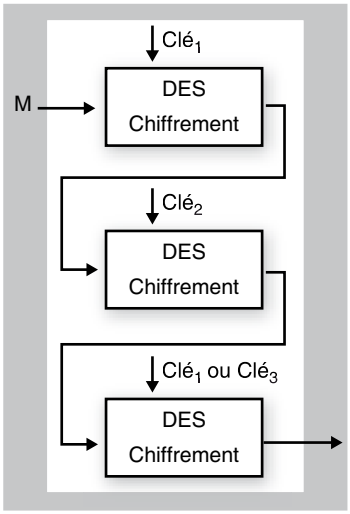


Figure 28.4

Principe de fonctionnement de 3DES

DES utilise une clé de 56 bits. 3DES, qui est illustré à la figure 28.4, étant une succession de trois DES, si K1 = K3, 3DES utilise une clé de $2 \times 56 = 112$ bits. Si K1 ≠ K3, c'est une clé de $3 \times 56 = 168$ bits.

Algorithme	Longueur de la clé secrète
DES	56 bits
3DES	112 ou 168 bits

AES

L'algorithme AES peut utiliser une clé sécrète de 128, 192 ou 256 bits.

Algorithme	Longueur de la clé secrète
AES	128, 192 ou 256 bits

La performance temporelle

Le temps de traitement de l'algorithme de chiffrement influe sur les caractéristiques temporelles du flux à sécuriser. Un algorithme lent ne permet pas de chiffrer le flux d'une application temps réel sur certaines machines, alors même qu'il peut apporter davantage de sécurité qu'un algorithme plus rapide mais moins sûr. On peut utiliser le nombre de round de l'algorithme pour lui associer un facteur de performance temporelle. Si l'on considère une confidentialité utilisant DES et 3DES, nous pouvons décrire le niveau de sécurité et les performances comme indiqué au tableau 28.1.

Nombre de round	Longueur de la clé secrète	Niveau de sécurité	Performance (rapidité pour QoS)
16 (DES)	56 bits	★	★★
48 (3DES)	112 bits (2 clés)	★★	★
48 (3DES)	168 bits (3 clés)	★★★	★

TABLEAU 28.1 • Performance des algorithmes DES

Pour une confidentialité utilisant uniquement l'AES, à la fois plus sûr et plus rapide que le DES, nous obtenons les performances décrites au tableau 28.2.

Nombre de round	Longueur de la clé secrète	Niveau de sécurité	Performance (rapidité pour QoS)
10	128 bits	★	★★★
12	192 bits	★★	★★
14	256 bits	★★★	★

TABLEAU 28.2 • Performance de l'algorithme AES

Si nous tentons de classifier les niveaux de sécurité des algorithmes DES, 3DES et AES, nous obtenons les valeurs décrites au tableau 28.3.

Nombre de round	Niveau de sécurité	Performance (rapidité pour QoS)
DES	★	★★
3DES (112)	★★	★
3DES (168)	★★★	★
AES (128)	★★★★	★★★★★
AES (192)	★★★★★	★★★★
AES (256)	★★★★★★	★★★

TABLEAU 28.3 • Classification des niveaux de sécurité des algorithmes DES et AES

Des compromis sont nécessaires pour décider du niveau de confidentialité à apporter et de la rapidité de l'algorithme à utiliser. Ce choix peut dépendre de la puissance des machines qui chiffrent et déchiffrent.

Les algorithmes d'authenticité

Les services d'intégrité des données et d'authentification de leur origine sont deux services inséparables. C'est pourquoi on les rassemble sous le terme d'authenticité. La solution la plus classique est d'utiliser un chiffrement permettant à la fois de vérifier l'intégrité et de chiffrer les données. Par exemple, l'authenticité apportée par IPsec s'effectue par l'ajout d'un code d'authentification de message, ou HMAC (Hashing Message Authentication Code).

Dans le cas d'IPsec, qui est le protocole de sécurité le plus utilisé avec SLL, les algorithmes que doit fournir par défaut toute implémentation sont HMAC-MD5 et HMAC-SHA-1. La sécurité fournie par l'algorithme HMAC est directement liée à l'algorithme de hachage sous-jacent, tels MD5 pour HMAC-MD5, SHA-1 pour HMAC-SHA-1, etc.

Dans SHA-1, la fonction de compression demande 4 rounds, chacun constitué de 20 étapes, soit 80 étapes. Dans MD5, la fonction de compression demande 4 rounds, chacun constitué de 16 étapes, soit 64 étapes. On peut dire que pour le chiffrement d'un texte donné, SHA-1 est un peu plus lent que MD5. Chacune de ces fonctions prend en entrée une clé secrète en plus des données auxquelles on souhaite appliquer le hachage. La taille de ces clés est différente selon l'algorithme utilisé.

Pour établir un niveau entre ces différents algorithmes, on peut se fonder sur la force de chacun. La force de l'algorithme est mesurée en terme de facteur de travail associé à une force d'attaque brute, donc liée à la longueur de la clé secrète. Les attaques par force brute sont plus difficiles si SHA-1 est utilisé. Pour cela, SHA-1 est considéré comme étant plus sûr que MD5.

Les niveaux de service d'authenticité

Les niveaux d'authenticité peuvent être classés en fonction de la longueur de la clé secrète et des performances de l'algorithme. Cette classification est récapitulée au tableau 28.4.

Algorithme	Longueur de la clé secrète	Niveau d'authenticité	Performance (rapidité pour QoS)
MD5	128 bits	★	★★
SHA-1	160 bits	★★	★

TABLEAU 28.4 • Niveaux des services d'authenticité

SHA-1 est considéré comme plus sûr que MD5, mais le choix de MD5 au lieu de SHA-1 dans un HMAC peut se justifier pour la performance.

Protection contre le rejeu

Malgré le chiffrement, il est possible d'effectuer une attaque par rejeu, c'est-à-dire en rejouant une séquence de paquets à laquelle l'attaquant ne comprend rien mais qui correspond à ce que le serveur attend. En d'autres termes, il est possible pour un attaquant de recopier des trames pendant une authentification et de réutiliser les mêmes trames ultérieurement.

La protection contre le rejeu repose sur un numéro de séquence. Elle se présente souvent sous forme d'option : l'utilisateur peut, sur demande explicite, bénéficier d'une protection contre le rejeu en numérotant ses paquets dans le champ Chiffrer du paquet de telle sorte qu'une recopie ne puisse être utilisée puisque le récepteur attend un numéro de série parfaitement déterminé entre l'émetteur et le récepteur.

Les algorithmes d'authentification

Comme nous l'avons vu à plusieurs reprises, l'authentification est une fonction de sécurité essentielle. Le protocole d'authentification utilisé le plus souvent provient de la norme IEEE 802.1x. Cette norme est très générale et s'applique aussi bien aux réseaux terrestres qu'aux réseaux hertziens.

Nous détaillons ici la procédure IEEE 802.1x mais renvoyons au chapitre suivant pour la description des algorithmes les plus utilisés, qui appartiennent au monde IP.

IEEE 802.1x s'appuie essentiellement sur le protocole EAP, que nous examinons beaucoup plus en détail au chapitre 29. EAP est un protocole d'authentification général, qui supporte de multiples méthodes d'authentification, telles que Kerberos, TLS, MS-Chap, SIM, etc. De nouveaux mécanismes d'authentification peuvent ainsi être définis au-dessus d'EAP. Seul le champ type du paquet EAP, codé sur un octet, limite le nombre de mécanismes d'authentification. Le standard EAP a été conçu comme protocole générique pour le transport du trafic des protocoles d'authentification. Il est construit autour d'un modèle de communication demandant un défi (challenge), auquel une réponse doit être apportée pour qu'il y ait authentification.

Comme illustré à la figure 28.5, quatre types de messages EAP permettent de réaliser l'authentification d'un client sur un serveur :

- EAP Request : demande d'authentification ;
- EAP Response : réponse à une requête d'authentification ;

- EAP Success : pour indiquer le succès de l'authentification ;
- EAP Failure : pour informer le client du résultat négatif de l'authentification.

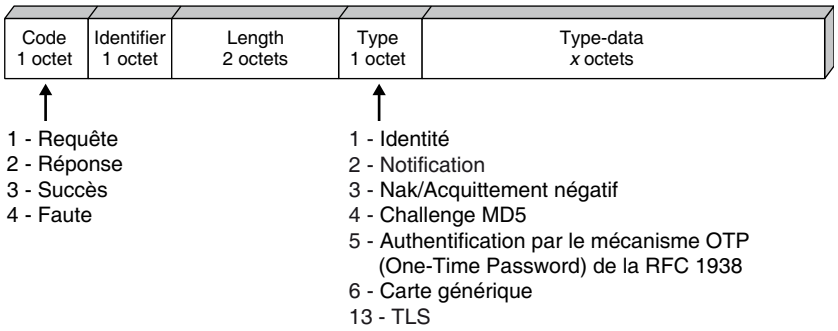


Figure 28.5

Format d'un paquet EAP

La norme IEEE 802.1x met en présence un supplicant, que l'on appelle client, un authenticator, qui est un contrôleur de communication, et un serveur d'authentification. Le client est un équipement terminal relié par une liaison filaire ou sans fil. Le contrôleur est un équipement intermédiaire qui peut être intégré dans un routeur ou dans un commutateur. Il peut aussi s'agir d'un contrôleur Wi-Fi ou même d'un point d'accès Wi-Fi compatible avec la norme IEEE 802.11. Ces points d'accès compatibles sont généralement haut de gamme et réservés au monde professionnel. Le contrôleur est un organe qui possède un port contrôlé, lequel peut être ouvert ou fermé en fonction de la réussite ou non de l'authentification. Le serveur d'authentification est le plus souvent de type RADIUS (*voir le chapitre 29*).

La figure 28.6 illustre cette configuration.

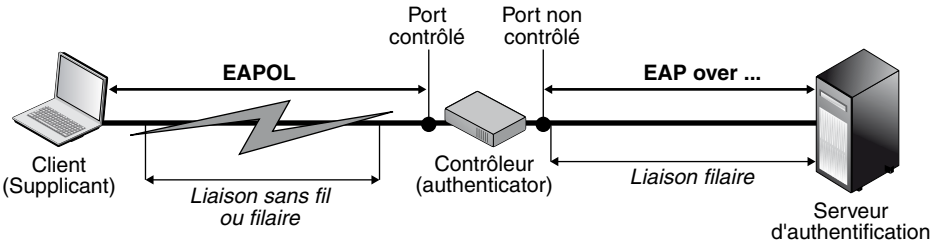


Figure 28.6

Configuration d'une authentification IEEE 802.1x

IEEE 802.1x utilise le protocole EAP pour mettre en communication le client et le serveur d'authentification *via* le contrôleur. Le protocole EAP est encapsulé dans une trame émise sur la connexion avec ou sans fil entre le client et le contrôleur et adaptée à la communication entre le contrôleur et le serveur d'authentification.

L'authentification EAP se déroule de la manière suivante :

1. Lorsque la phase d'établissement de la liaison est terminée, le serveur d'authentification envoie une demande d'identité.
2. Le client envoie un paquet EAP RESPONSE dans lequel il fournit son identité et les méthodes d'authentification qu'il supporte. La phase d'authentification débute à cet instant.
3. Le serveur envoie un défi au client.
4. Le client y répond par un message EAP RESPONSE, dans lequel il envoie le défi chiffré avec sa clé secrète.
5. Le serveur met fin à la phase d'authentification par l'intermédiaire d'un paquet de succès ou d'échec.

Si la phase d'authentification s'est bien déroulée, le serveur d'authentification peut transmettre une clé de chiffrement au client, lequel l'utilise pour chiffrer les données émises. Cette dernière phase est optionnelle pour le protocole EAP, car elle dépend du protocole d'authentification utilisé.

Le protocole EAP étant extensible, tout mécanisme d'authentification peut être encapsulé à l'intérieur des messages EAP, comme l'illustre la figure 28.7. Au niveau supérieur de la figure se trouvent les méthodes d'authentification, comme TLS, MS-Chap, SIM, etc. Vient ensuite le niveau d'encapsulation de la méthode d'authentification de la trame EAP. La trame EAP elle-même est encapsulée dans une trame de transport. Cette encapsulation peut s'effectuer soit dans une trame EAP over RADIUS, soit dans une trame EAPoL (EAP over LAN), qui est utilisée dans les réseaux locaux, en particulier les réseaux locaux sans fil de type Wi-Fi.

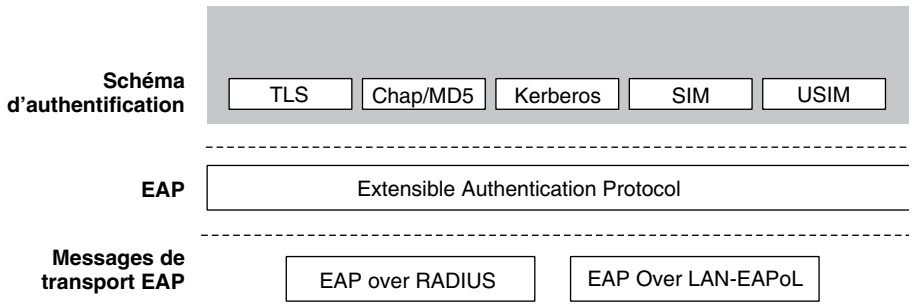


Figure 28.7
Architecture d'EAP

Un autre atout d'EAP est qu'il est conçu pour fonctionner au-dessus de la couche liaison. Il ne nécessite donc pas le niveau IP mais inclut son propre support pour la livraison et la retransmission. Développé pour être utilisé avec PPP, c'est un protocole générique qui supporte la majorité des normes de niveau liaison.

Autres mécanismes d'authentification

D'autres mécanismes d'authentification, plus simples dans leur conception et liés à des environnements différents, sont couramment utilisés. Les sections suivantes présentent brièvement les deux plus connus, OTP et Kerberos. OTP (One-Time Password) introduit un changement du mot de passe à chaque tentative d'authentification. C'est pourquoi on l'appelle mécanisme à mot de passe valable une seule fois. Kerberos est fondé sur une architecture client serveur à chiffrement symétrique.

OTP (One-Time Password)

Fondé sur un algorithme de hachage répété récursivement afin de générer des mots de passe à usage unique, OTP a fait l'objet de plusieurs tentatives de sécurisation par carte à puce.

L'algorithme OTP fonctionne de la façon suivante :

1. Dans le cas des mots de passe défi/réponse, le serveur envoie un défi aléatoire (random challenge) au client.
2. Le client manipule ce défi en introduisant son secret et envoie la réponse au serveur.
3. Le serveur effectue le même travail et compare les résultats.

L'inconvénient de ce mécanisme est qu'il est possible pour un attaquant de rejouer le même mot de passe une fois que celui-ci a été intercepté. Pour y remédier, on utilise une liste de mots de passe, chacun d'eux n'étant valable que pour une tentative d'authentification. Une telle liste est constituée de mots de passe générés et utilisés séquentiellement par le client à chaque tentative d'authentification. Les mots de passe étant indépendants, il est impossible de prévoir un mot de passe à partir de ceux utilisés précédemment.

La procédure S/KEY

Dans la procédure S/KEY, qui est un cas particulier de la méthode OTN, une liste de mots de passe à usage unique de 64 bits de longueur est générée par le serveur à partir du mot de passe de l'utilisateur. Cela permet au client d'utiliser le même mot de passe sur des machines différentes. La taille des mots de passe OTP est un bon compromis entre sécurité et facilité d'emploi pour l'utilisateur.

Les 8 octets du mot de passe de l'utilisateur sont concaténés avec une séquence aléatoire, ou *seed*. Une fonction de hachage MD4 est appliquée au résultat de la concaténation, puis le résultat obtenu est réduit à 8 octets par un XOR des deux moitiés. Ce résultat, appelé *s*, est fourni en entrée de l'étape suivante.

Le premier mot de passe à usage unique est produit en exécutant n fois la fonction de hachage sur s. Le mot de passe OTP de rang i (p_i) est produit en appliquant la fonction de hachage $n - i$ fois. Les deux équations suivantes indiquent le calcul du premier mot de passe (exécution de n fois la fonction de hachage sur s) et du i-ème mot de passe (exécution de n-i fois la fonction de hachage sur s) :

$$p_0 = f_n(s)$$
$$p_i = f_{n-i}(s)$$

Un attaquant qui a surveillé l'utilisation du mot de passe p_i n'est pas en mesure de générer le prochain mot de passe de la séquence (p_{i+1}) puisque la fonction de hachage est irréversible.

Quand un client tente d'être authentifié, la séquence d'octets aléatoires et la valeur courante de *i* sont passées au client. Le client retourne le prochain mot de passe. Le serveur sauvegarde dans un premier temps une copie de ce mot de passe puis lui applique la fonction de hachage :

$$p_i = f(f_{n-i-1}(s)) = f(p_{i+1})$$

Si l'égalité ci-dessus n'est pas vérifiée, la requête échoue. Dans le cas contraire, le fichier de mots de passe est mis à jour avec la copie du mot de passe OTP qui a été sauvegardé. Cette mise à jour avance la séquence de mots de passe.

Ce mécanisme empêche les attaques par rejeu mais n'a malheureusement aucun effet sur les attaques actives.

Kerberos

Kerberos est un algorithme d'authentification fondé sur une cryptographie. L'utilisation de cet algorithme ne permet pas à une personne qui écoute le dialogue d'un client à l'insu de ce dernier de se faire passer pour lui plus tard. Ce système permet à un processus client travaillant pour un utilisateur donné de prouver son identité à un serveur sans avoir à envoyer de données dans le réseau.

Kerberos a été développé à partir des années 1980 et en est aujourd'hui à la version v5, qui peut être considérée comme le standard Kerberos. L'idée sous-jacente est que le processus client doit prouver qu'il possède la clé de chiffrement qui est connue des seuls utilisateurs de base et du serveur.

La suite simplifiée des requêtes qui vont être échangées est illustrée à la figure 28.8.

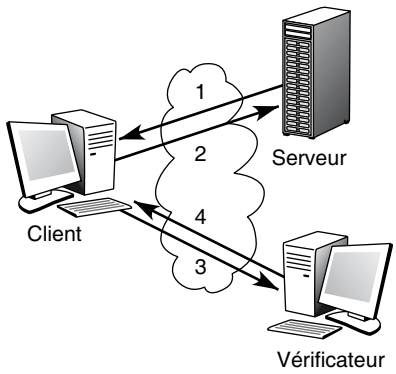


Figure 28.8

Suite simplifiée des requêtes Kerberos

Le client et le processus client ne connaissent pas la clé de chiffrement de base utilisée pour l'authentification. Quand un client doit répondre à une demande d'authentification, il se met en contact avec le serveur pour générer une nouvelle clé de chiffrement et se la faire envoyer de façon sécurisée. Cette nouvelle clé est appelée clé de session. Le serveur utilise un ticket Kerberos pour envoyer la clé de session au vérificateur par l'intermédiaire du client.

Le ticket Kerberos est un certificat provenant, comme nous venons de le voir, du serveur d'authentification. Il est chiffré avec la clé de base que ne connaît pas le client. Le ticket contient des informations, parmi lesquelles la clé de session qui est utilisée pour l'authentification, le nom de l'utilisateur de base et un temps d'expiration après lequel la clé de session n'est plus valide. Puisque le ticket est chiffré avec la clé de base, connue seulement du serveur et du vérificateur, il est impossible au client de modifier le ticket sans que cela passe inaperçu.

À la figure 28.8, la demande 1 de vérification génère la réponse 2, qui délivre un ticket de vérification et la clé de session. Les messages 3 et 4 permettent l'authentification en prouvant que le client connaît la clé de session incluse dans le ticket. À la réception du ticket Kerberos, le vérificateur le déchiffre, extrait la clé de session et utilise celle-ci pour déchiffrer le nom du serveur. Si la même clé a été utilisée pour chiffrer le nom du serveur et le déchiffrer, la vérification de la zone de détection d'erreur, ou checksum, donne un résultat positif.

Cette solution peut paraître insuffisante, puisqu'un utilisateur malveillant peut intercepter les requêtes et les rejouer à la place du vérificateur. Pour cette raison, le vérificateur doit s'assurer que le temporisateur d'utilisation du ticket n'est pas dépassé. À ce stade, il est supposé que l'identité du client a été authentifiée par le vérificateur. Le client peut aussi demander à vérifier l'identité du serveur. Une authentification mutuelle est alors effectuée.

Exemples d'environnements de sécurité

Un environnement de sécurité fait référence à un ensemble d'équipements qui peuvent se faire confiance grâce à des mécanismes de sécurité qui leur permettent d'entrer dans le même cercle de confiance. Les sections suivantes présentent quelques exemples de mécanismes permettant d'introduire des éléments de sécurité.

PGP (Pretty Good Privacy)

PGP est un algorithme permettant de sécuriser la messagerie électronique en lui apportant authentification et confidentialité. PGP permet le chiffrement et la signature de documents par le biais d'un chiffrement symétrique avec IDEA ou DES, d'une fonction de hachage MD5 ou SHA-1 et d'une clé RSA.

Le texte à envoyer est chiffré par l'algorithme IDEA. La signature utilise MD5. L'algorithme RSA est utilisé pour l'échange de la clé privée nécessaire à IDEA. L'authentification par signature implémente une fonction de hachage SHA-1, et la confidentialité un des nombreux algorithmes disponibles, comme IDEA, 3DES, Diffie-Helman, RSA, etc.

L'infrastructure PKI

La distribution sécurisée de clés publiques est une question cruciale pour un système global sécurisé, à laquelle l'infrastructure PKI (Public Key Infrastructure) offre une solution.

Les principales fonctions réalisées par une infrastructure PKI pour la gestion des certificats sont les suivantes :

- Enregistrement de demandes et vérification des critères pour l'attribution d'un certificat. L'identité du demandeur est vérifiée ainsi que le fait qu'il soit bien en possession de la clé privée associée.
- Création des certificats.
- Diffusion des certificats entraînant la publication des clés publiques.
- Archivage des certificats pour assurer la sécurité et la pérennité.
- Renouvellement des certificats en fin de période de validité.
- Suspension des certificats : cette fonction peut être utile si le propriétaire estime ne pas avoir besoin temporairement de son certificat. Cependant, n'étant pas aisée à mettre en œuvre, elle est essentiellement administrative, et il n'existe pas de standard d'implémentation.
- Révocation de certificats pour péremption, perte, vol ou compromission de clés.
- Création et publication des listes de révocation des certificats. Il y a révocation du certificat en cas de fin de validité ou de clé privée divulguée, perdue ou compromise. Il n'existe aucun protocole standard qui permette d'effectuer une révocation automatiquement. Il faut donc recourir à des moyens administratifs. Ceux-ci doivent être implémentés avec un maximum de sécurité, le demandeur de la révocation devant en particulier prouver qu'il est bien le propriétaire de la clé publique ou privée devenue inutilisable. Les listes de révocation doivent, d'une part, être protégées afin d'éviter toute corruption et, d'autre part, être accessibles en permanence et le plus à jour possible. Pour un fonctionnement correct, les listes de révocation nécessitent une synchronisation des horloges de tous les acteurs concernés.
- Délégation de pouvoir à d'autres entités reconnues de confiance. Toute communauté de personnes peut créer sa propre infrastructure PKI. Dans ce cas, une étude de faisabilité est nécessaire en s'appuyant sur de nombreux critères.

Un critère important lors du déploiement d'une PKI est le format des certificats numériques utilisés. Le format le plus largement accepté est le X.509 de l'UIT-T. En plus d'une clé publique, un certificat contient généralement un nom, une adresse et d'autres informations décrivant le porteur de la clé secrète.

Tous les certificats sont signés par la banque de données qui enregistre les clés publiques des membres de la communauté. Pour devenir membre de la communauté, un abonné doit réaliser deux choses :

- Fournir au service d'annuaire une clé publique et des informations d'identification, de telle sorte que les autres personnes soient capables de vérifier la signature de son certificat.

- Obtenir la clé publique du service d'annuaire de façon à permettre une vérification de la signature des autres personnes.

Un certificat étant signé, il est non falsifiable. Son authenticité ne dépend pas du canal par lequel il a été reçu mais est intrinsèque.

Une autorité de certification (AC) émet, gère et révoque les certificats. La clé publique du certificat de l'AC doit être reconnue de confiance par tous les utilisateurs finals. Les certificats émis aux utilisateurs finals sont appelés certificats utilisateur (end-user certificates), et ceux émis pour validation entre les différents AC certificats d'AC (CA-certificates).

Une seule autorité de certification pour le monde entier ne serait pas appropriée. Il est nécessaire que l'architecture PKI soit distribuée, les AC étant autorisées à certifier d'autres AC. L'AC peut déléguer son autorité à une autorité subordonnée en émettant un certificat d'AC, créant ainsi une hiérarchie de certificats. La séquence ordonnée de certificats, de la dernière branche à la racine, est appelée chemin ou chaîne de certification. Chaque certificat contient le nom de l'émetteur du certificat, c'est-à-dire le nom du certificat directement supérieur dans la chaîne. En règle générale, il peut y avoir un nombre arbitraire d'AC sur le chemin entre deux utilisateurs. Pour obtenir la clé publique de son correspondant, un utilisateur doit vérifier le certificat de chaque AC. Ce procédé est appelé validation du chemin de certification.

Quand plusieurs AC sont utilisées, la manière dont les AC sont organisées est très importante pour construire l'architecture PKI. Certaines PKI utilisent un modèle hiérarchique, appelé hiérarchie générale, où chaque AC certifie ses pères et ses fils. D'autres PKI utilisent une variante de la hiérarchie générale dans laquelle les AC certifient seulement leurs fils et l'AC racine dans tous les chemins de certification.

Dans une architecture « top-down », tous les utilisateurs doivent utiliser la plus haute AC comme racine. Cela nécessite que tous les utilisateurs obtiennent une copie de la clé publique de l'AC la plus haute avant d'utiliser la PKI. Tous les utilisateurs doivent pleinement avoir confiance dans l'AC racine, ce qui la rend impraticable pour une PKI globale. La certification croisée (cross-certification) aide à réduire la longueur du chemin, au risque d'en compliquer la découverte. La figure 28.9 illustre un exemple de chemin de certification.

Dans l'optique d'une communication extérieure à l'entreprise, l'interopérabilité des PKI est essentielle. Les principaux efforts de normalisation en ce sens émanent des laboratoires RSA, avec les normes PKCS (Public-Key Cryptography Standards). Ces normes font office de standard et sont unanimement adoptées, notamment pour la cryptographie et l'échange de clés. Parallèlement, l'IETF produit des normes plus générales, avec les RFC PKIX (Public Key Cryptography eXtension). Cependant, certains aspects demeurent encore insuffisamment normalisés, comme les politiques et les pratiques de certification ou les paramètres des certificats.

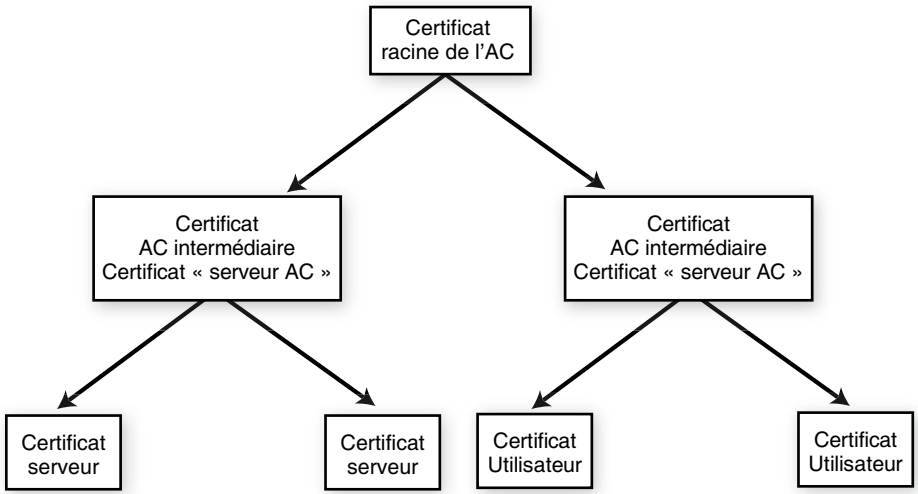


Figure 28.9

Exemple de chemin de certification

PKCS (Public-Key Cryptography Standards)

PKCS est un ensemble de standards pour la mise en place des IGC (infrastructure de gestion des clés). Coordonnés par RSA, ces standards définissent les formats des éléments de cryptographie :

- PKCS#1, RSA Cryptography Specifications Version 2, RFC 2437 ;
- PKCS#2, inclus dans PKCS#1 ;
- PKCS#3, Diffie-Hellman Key Agreement Standard Version 1.4 ;
- PKCS#4, inclus dans PKCS#1 ;
- PKCS#5, Password-Based Cryptography Standard Version 2 ;
- PKCS#6, Extended-Certificate Syntax Standard Version 1.5 ;
- PKCS#7, Cryptographic Message Syntax Standard Version 1.5, RFC 2315 ;
- PKCS#8, Private-Key Information Syntax Standard Version 1.2 ;
- PKCS#9, Selected Attribute Types Version 2.0 ;
- PKCS#10, Certification Request Syntax Version 1.7 ou CSR (Certificate Signing Request), RFC 2314 ;
- PKCS#11, Cryptographic Token Interface Standard Version 2.10 ;
- PKCS#12, Personal Information Exchange Syntax Standard Version 1.0 ;
- PKCS#13, Elliptic Curve Cryptography Standard Version 1.0 ;
- PKCS#14, Pseudorandom Number Generation Standard Version 1.0 ;
- PKCS#15, Cryptographic Token Information Format Standard Version 1.1.

Les virus

Les virus sont des programmes, généralement écrits en langage machine, susceptibles de s'introduire dans un ordinateur et de s'y exécuter. L'exécution peut produire de nombreux effets, allant du blocage d'une fonction à la destruction des ressources de l'ordinateur, comme l'effacement de la mémoire ou du disque dur, en passant par l'émission de messages incontrôlés.

Les logiciels antivirus ont pour fonction de détecter la présence de virus sur une machine et de les détruire. Cependant, comme nous allons le voir, certains virus sont résistants, et les logiciels antivirus peuvent avoir du mal à les détecter.

On dénombre un très grand nombre de techniques de virus, notamment les suivantes :

- Boot sector virus, ou virus travaillant sur le programme de démarrage. Ce programme se met en route au moment de la mise en marche de la station terminale. Le virus se trouve sur le disque dur et peut se dupliquer sur les disquettes ou les CD. Suivant son origine, le virus bloque un certain nombre de fonctions, parfois de façon aléatoire afin de ne pas se faire détecter. Il peut aussi empêcher tout démarrage de la machine en ne permettant pas à une instruction importante du programme de démarrage de se dérouler.
- File infected virus. Ce sont les plus courants. Ils s'attachent à un programme exécutable particulier et, en s'exécutant, bloquent la mise en route du programme, tout en s'attachant à d'autres programmes.
- Polymorphic virus. Le rôle de ces virus est de ne pas se faire détecter, tout en causant un certain nombre d'ennuis à l'utilisateur. Ils se modifient en passant à un autre programme, de telle sorte qu'ils sont parfois très difficiles à détecter puisque non répertoriés dans une forme spécifique à un programme.
- Stealth virus, que l'on peut traduire par virus furtifs. Comme les précédents, ils tentent de ne pas se faire détecter facilement tout en occasionnant des dégâts aux programmes auxquels ils s'accrochent. Une des méthodes qu'ils emploient le plus fréquemment consiste à s'incruster dans les programmes en prenant la place de quelques lignes de code de telle sorte que la taille exacte du programme reste inchangée.
- Encrypted virus. Ces virus forment une famille très délicate à repérer puisqu'ils sont chiffrés et que les antivirus n'ont pas la possibilité de les déchiffrer pour les détecter. Ces virus doivent pouvoir être déchiffrés pour être mis en œuvre. Ils nécessitent donc un environnement qui leur est adapté. Ils utilisent généralement les techniques de chiffrement utilisées classiquement dans les systèmes d'exploitation qu'ils attaquent.
- Worms, ou vers. Ces virus sont de nature différente. Ce sont eux-mêmes des programmes qui transportent des virus. Beaucoup d'attaques sur les messageries s'effectuent en attachant un vers au message. L'utilisateur à qui l'on a fait croire à l'utilité de ce programme l'ouvre et l'exécute. Le virus attaché peut alors commencer à infecter la machine.
- Trojan horses, ou chevaux de Troie. Ces virus bien connus sont des programmes qui s'introduisent à l'intérieur de l'ordinateur et donnent des renseignements à l'attaquant externe. Le code du cheval de Troie est généralement encapsulé dans un programme système nécessaire au fonctionnement de l'ordinateur.

- Time bomb virus. Ces virus sont liés à l'horloge du système et se déclenchent à une heure déterminée à l'avance.
- Logical bombs, ou bombes logiques. Ces virus se déclenchent lorsqu'un certain nombre de conditions logiques sont vérifiées.

Il est de plus en plus difficile de détecter les virus, les pirates essayant de les encapsuler dans des programmes innocents. Les parades à ces attaques sont nombreuses, quoique jamais complètement efficaces. La solution la plus simple consiste à se doter d'un antivirus mis à jour régulièrement.

L'identité

L'identité est devenue une fonctionnalité primordiale des réseaux. Il existe aujourd'hui beaucoup de façons de s'identifier avec logins et mots de passe, tous différents les uns des autres. La plupart des internautes essaient d'avoir un seul login et un seul mot de passe, qu'ils tentent d'appliquer partout, mais c'est en général compliqué, car les sites imposent des nombres de caractères déterminés. De plus, cela peut être dangereux car le vol du mot de passe signifie pour l'attaquant la possibilité de se connecter à tous les sites de l'internaute. Pour simplifier ce processus et le sécuriser, diverses solutions se sont imposées dont la plus importante est Open-ID.

Les systèmes de gestion des identités

De nombreux systèmes de gestion des identités ont été proposés dans la littérature. Les principaux systèmes ouverts sont OpenID et Liberty Alliance. La solution de base recommande une authentification unique, ou SSO (Single Sign-On). Regardons les idées cachées derrière ces deux systèmes.

Commençons par OpenID, qui est un bon exemple de système de gestion des identités. C'est un système à authentification unique, c'est-à-dire que le client s'authentifie auprès du serveur OpenID, lequel se charge de mettre le client en relation avec divers fournisseurs de services. En fait, le modèle OpenID se fonde sur des liens de confiance entre les fournisseurs d'identité OpenID et les fournisseurs de service. Le système est décrit à la figure 28.10.

Le modèle OpenID fonctionne de la façon suivante : on commence par créer un compte OpenID. Pour cela, l'internaute choisit un nom d'utilisateur et un mot de passe. Différentes informations peuvent compléter le compte. Il est cependant possible de remplacer le nom d'utilisateur et le mot de passe par un jeton sécurisé de type cate à puce, comme expliqué à la section suivante dédiée à la sécurité par carte à puce.

L'internaute fait une demande au fournisseur de service en indiquant son identité OpenID. Le fournisseur de service prend contact avec le fournisseur d'identité pour mettre en place une session qui est acceptée grâce au lien de confiance tissé entre le fournisseur d'identité OpenID et le fournisseur de services. Il faut ensuite que le client s'authentifie fortement auprès du serveur d'identité pour que la liaison sécurisée antre le client et le serveur Web se mette en place.

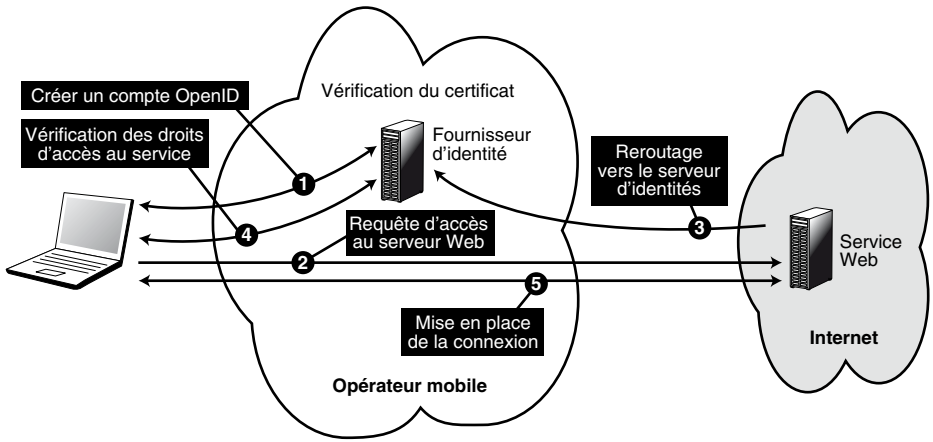


Figure 28.10
Le modèle OpenID

Liberty Alliance est un projet dont l'objectif est de définir un certain nombre de protocoles pour réaliser un système de gestion des identités. La solution est assez radicalement différente d'OpenID puisque c'est l'utilisateur qui gère l'identification unique qui est la même auprès des fournisseurs de service. Les fournisseurs de services appartiennent tous à un cercle vertueux, ou *Circle of Trust*. Cette solution permet au client de maîtriser beaucoup mieux ses données personnelles.

Vie privée

La défense de la vie privée a toujours été importante, mais Internet n'y a pas toujours porté une grande attention. Aujourd'hui, cette fonction est prise en charge dès que possible. Malheureusement peu de protocoles s'y intéressent vraiment. Dans la défense de la vie privée, il est délicat d'authentifier toutes les personnes connectées sans que cette connexion soit connue des autres. Nous pouvons appeler cette propriété, l'anonymat traçable : cela indique que le client travaille anonymement sur Internet, mais que le système est capable, en cas de nécessité, de retrouver la personne en question. Il faut donc à la fois permettre l'anonymat et faire que cet anonymat puisse être levé en cas d'abus. Une solution possible est l'utilisation d'un couple de cartes à puce.

Le serveur d'authentification est constitué de plusieurs cartes à puce et peut être dimensionné avec autant de cartes que nécessaire. L'authentification forte s'effectue d'une façon duale avec la carte à puce. L'avantage de cette solution est l'anonymat permis par les deux cartes à puce de l'émetteur et du serveur. Les connexions peuvent cependant être traçables pour un superadministrateur (la justice, par exemple).

Cette solution peut être envisagée aussi bien pour une set-top-box d'un client individuel que pour un cybercafé ou une très grande entreprise : il passe l'échelle sans problème. Dans le cas d'une set-top-box, il suffit, par exemple, d'une interface USB pour mettre un micro-serveur d'authentification correspondant à une seule carte à puce. Dans le cas d'une grande entreprise, le serveur est constitué d'un ensemble de cartes à puce pouvant monter à plusieurs dizaines voire plusieurs centaines d'utilisateurs.

La sécurité par carte à puce

La sécurité, capitale pour les réseaux d'aujourd'hui, le sera encore plus à l'avenir. Avec Internet, il faut inventer de nouveaux procédés garantissant la non-divulgation de nombreux éléments, comme la localisation, le nom de ceux qui sont authentifiés, etc. Parmi les différentes solutions envisageables, nous allons détailler la carte à puce, qui se répand de plus en plus en dehors des opérateurs de mobiles.

La figure 28.11 illustre une carte contenant tous les éléments physiques d'un ordinateur classique, à savoir un microprocesseur, une mémoire ROM, une mémoire RAM, une mémoire persistante, généralement de l'EEPROM, un bus de communication et une entrée/sortie. Jusqu'à l'apparition des nouvelles cartes à puce USB, le canal de communication était un goulet d'étranglement, mais ce n'est plus le cas désormais.

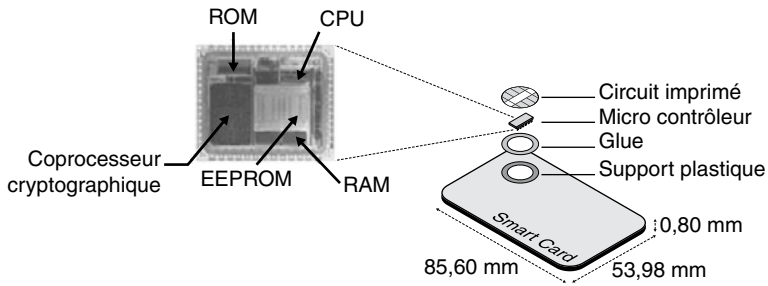


Figure 28.11

Architecture matérielle de la carte à puce

Le cœur de la plupart des cartes à puce repose sur un microprocesseur 8 bits d'une puissance de calcul de l'ordre de 1 à 3 MIPS (million d'instructions par seconde) à une fréquence de 3,5 MHz. Ce type de microprocesseur met 17 ms pour exécuter l'algorithme de chiffrement DES (Data Encryption Standard), par exemple. Il est à noter que la puissance du processeur de la carte à puce augmente à une telle vitesse que de nouvelles cartes de sécurité pourront supporter des algorithmes beaucoup plus lourds.

Les architectures 32 bits fondées sur des processeurs RISC à 1 million de transistors constituent la nouvelle génération de microprocesseurs, d'une puissance de calcul de l'ordre de 30 MIPS à 33 MHz. De tels microprocesseurs ne mettent qu'environ 50 µs pour exécuter un DES et 300 ms pour un chiffrement RSA avec une clé de 2 048 bits.

Outre le processeur, les différents types de mémoire sont les éléments principaux du microcontrôleur. Ils servent à enregistrer des programmes et des données. Les microcontrôleurs de carte à puce sont des ordinateurs à part entière. Ils possèdent généralement entre 1 et 8 Ko de mémoire RAM, entre 64 et 256 Ko de mémoire ROM et entre 16 et 128 Ko d'EEPROM.

La quantité de mémoire EEPROM disponible sur une carte à puce a été longtemps limitée du fait que l'EEPROM n'était pas conçue spécifiquement pour les cartes à puce et que ses limites physiques de miniaturisation étaient atteintes. La mémoire Flash a permis de s'affranchir de cette contrainte. C'est ainsi que l'on a vu apparaître de premiers prototypes de carte à puce à 1 Mo de mémoire persistante de type Flash.

La protection de la carte à puce est principalement assurée par le système d'exploitation. Le mode d'adressage physique pour l'accès aux données n'est disponible qu'après que la carte a été personnalisée et remise à l'utilisateur. L'accès aux données s'effectue au travers d'une structure logique de fichiers sécurisés par des mécanismes de contrôle d'accès.

La carte à puce est beaucoup utilisée dans les réseaux de téléphonie mobile (cartes SIM) ou par la mise en place des infrastructures à clés publiques (PKI). Cette technologie a permis aux opérateurs d'exploiter leur réseau en limitant très fortement le nombre de fraudes, assurant par là même une rentabilité financière. Elle est également le support légal de la signature électronique reconnue par de nombreux pays.

La carte à puce EAP traite directement le protocole EAP dans la puce sécurisée. Les principales applications visées sont EAP-SIM et EAP-TLS. Les avantages d'un EAP-TLS effectué dans une carte à puce sont nombreux. L'authentification est tout d'abord indépendante d'un éditeur de logiciel, par exemple Microsoft. De plus, la sécurité fournie est bien meilleure qu'avec EAP-TLS réalisé en logiciel par le processeur d'un ordinateur personnel puisqu'il est toujours possible pour un logiciel espion introduit dans le PC de capturer les clés. L'avantage de la carte à puce est que l'ensemble des calculs s'effectue dans la carte et qu'il ne sort de la carte à puce qu'un flux chiffré. Les clés secrètes ne sortent jamais de la carte à puce.

Schématiquement, une carte EAP assure les quatre services suivants :

- Gestion d'identités multiples. Le porteur de la carte peut utiliser plusieurs réseaux sans fil. Chacun d'eux nécessite un triplet d'authentification, EAP-ID (valeur délivrée dans le message eap-response.identity), EAP-Type (type de protocole d'authentification supporté par le réseau) et crédits cryptographiques, c'est-à-dire l'ensemble des clés ou paramètres utilisés par un protocole particulier (EAP-SIM, EAP-TLS, MS-CHAP-V2, etc.). Chaque triplet est identifié par un nom (l'identité), dont l'interprétation peut être multiple (SSID, nom d'un compte utilisateur, mnémonique, etc.).
- Affectation d'une identité à la carte. L'identité de la carte est une fonction du réseau visité. La carte peut posséder en interne plusieurs identités et s'adapter au réseau auquel le PC et la carte à puce sont connectés.
- Traitement des messages EAP. La carte à puce étant doté d'un processeur et de mémoires, elle peut exécuter du code et traiter des messages EAP reçus et en envoyer en réponse.

- Calcul de la clé unicast. En fin de session d'authentification, le tunnel EAP peut-être utilisé pour la transmission d'informations diverses, comme des clés ou des profils. Il est possible de faire transiter une clé de session, par exemple, et de la mettre à disposition du terminal désirant accéder aux ressources du réseau sans fil.

La figure 28.12 illustre une procédure d'authentification entre un serveur d'authentification et une carte à puce EAP. Le flot des primitives traverse les logiciels du PC, c'est-à-dire d'abord le logiciel EAP, qui ne réalise qu'une transition des paquets EAP vers le serveur RADIUS d'un côté et vers la carte à puce de l'autre, puis le système d'exploitation de la machine, qui prend en charge l'interface avec la carte à puce, et enfin l'interface IEEE 802.11 de la liaison sans fil.

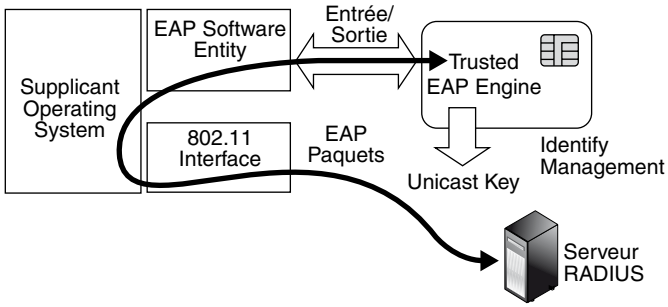


Figure 28.12

Procédure d'authentification par carte à puce EAP

Pour parfaire la sécurité, il est possible d'insérer des cartes à puce également du côté serveur en sorte que l'algorithme EAP-TLS du serveur d'authentification se déroule également dans la carte à puce. Avec les nouvelles cartes à puce pouvant stocker jusqu'à 1 Go, il est possible de mémoriser les logs nécessaires à la traçabilité. Il est évident que plus il y a de clients, plus le nombre de cartes à puce doit être augmenté.

Un exemple de cette sécurisation forte est illustré à la figure 28.13.

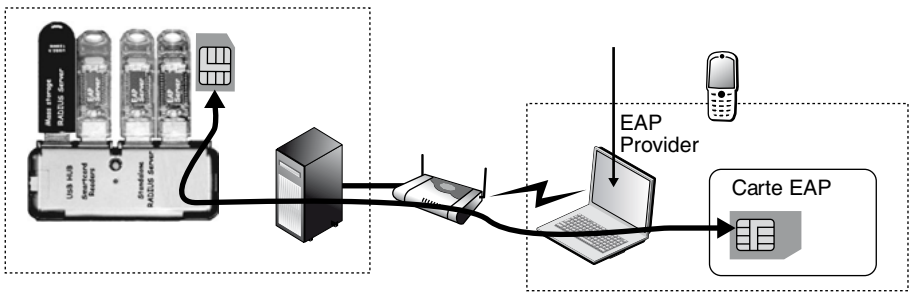


Figure 28.13

Une architecture forte de sécurisation

Conclusion

Pour définir la sécurité, on peut partir de la couche application en disant qu'une application est sécurisée si l'utilisateur qui s'en sert a été identifié et authentifié, si les données transportées n'ont pas été modifiées, si les données n'ont pu être interceptées et si elles ont une valeur juridique.

À partir de cette définition, on peut considérer que la sécurité consiste en cinq types d'opération :

- identification d'un utilisateur ;
- authentification d'un utilisateur ;
- intégrité des données ;
- confidentialité des données ;
- non-répudiation.

Les outils à mettre en œuvre pour assurer ces opérations proviennent de différents horizons et progressent rapidement pour tenter de rattraper le retard sur les attaquants, qui ont toujours une longueur d'avance. Le chapitre suivant examine les algorithmes de sécurité les plus utilisés dans le monde IP.

29

La sécurité dans l'environnement IP

Les échanges de données s'effectuent soit entre un client et un serveur, soit en peer-to-peer, c'est-à-dire directement d'un client à un autre client. En règle générale, le client se sert d'un identifiant déterminé par un login et un mot de passe mis en clair sur le réseau. Le client est donc identifié, et il obtient l'autorisation d'accéder au serveur grâce à son mot de passe. Cependant, cette solution peut se révéler bien faible face à des pirates. L'absence d'authentification de la provenance des paquets IP rend possible de nombreuses attaques, comme les dénis de service *(denial of service),* c'est-à-dire le refus ou l'impossibilité pour un serveur de fournir l'information demandée.

Il existe de nombreuses familles d'attaques dans le réseau Internet. Ce chapitre commence par donner un certain nombre d'exemples de ces attaques avant d'examiner les parades possibles.

Les attaques par Internet

Les attaques concernent deux grands champs : celles qui visent les équipements terminaux et celles qui visent le réseau Internet lui-même. Elles ne sont pas totalement décorrélées puisque les attaques des machines terminales par Internet utilisent souvent des défauts d'Internet.

Les attaques du réseau Internet lui-même consistent à essayer de dérégler un équipement de routage ou un serveur, comme les serveurs DNS, ou à obstruer les lignes de communication. Les attaques des machines terminales consistent à prendre le contrôle de la machine pour effectuer des opérations non conformes. Très souvent, ces attaques

s'effectuent par le biais des logiciels réseau qui se trouvent dans la machine terminale. Cette section explicite quelques attaques parmi les plus classiques.

Les attaques par ICMP

Le protocole ICMP (Internet Control Message Protocol) est utilisé par les routeurs pour transmettre des messages de supervision permettant, par exemple, d'indiquer à un utilisateur la raison d'un problème. Un premier type d'attaque contre un routeur ou un serveur réseau consiste à générer des messages ICMP en grande quantité et à les envoyer vers la machine à attaquer à partir d'un nombre de sites important.

Pour inonder un équipement de réseau, le moyen le plus simple est de lui envoyer des messages de type ping lui demandant de renvoyer une réponse. On peut également inonder un serveur par des messages de contrôle ICMP d'autres types.

Les attaques par TCP

Le protocole TCP travaille avec des numéros de port qui permettent de déterminer une adresse de socket, c'est-à-dire d'un point d'accès au réseau. Cette adresse de socket est formée par la concaténation de l'adresse IP et du numéro de port. À chaque application correspond un numéro de port, par exemple 80 pour une application HTTP.

Une attaque par TCP revient à utiliser un point d'accès pour faire autre chose que ce pour quoi il a été défini. En particulier, un pirate peut utiliser un port classique pour entrer dans un ordinateur ou dans le réseau d'une entreprise. La figure 29.1 illustre une telle attaque. L'utilisateur ouvre une connexion TCP sur un port correspondant à l'application qu'il projette de dérouler. Le pirate commence à utiliser le même port en se faisant passer pour l'utilisateur et se fait envoyer les réponses. Éventuellement, le pirate peut prolonger les réponses vers l'utilisateur de telle sorte que celui-ci reçoive bien l'information demandée et ne puisse se douter de quelque chose.

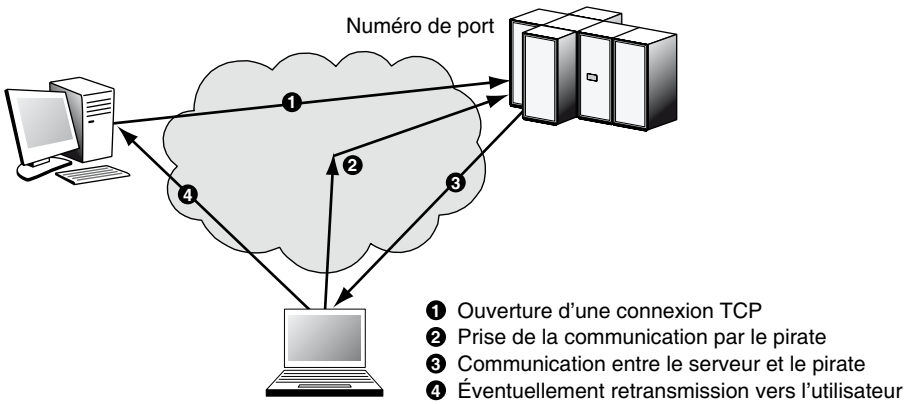


Figure 29.1

Attaque par le protocole TCP

Nous verrons en fin de chapitre comment les pare-feu, ou firewalls, essaient de parer ce genre d'attaque en bloquant certainzs ports.

Les attaques par cheval de Troie

Dans l'attaque par cheval de Troie, le pirate introduit dans la station terminale un programme qui permet de mémoriser le login et le mot de passe de l'utilisateur. Ces informations sont envoyées à l'extérieur par le biais d'un message vers une boîte aux lettres anonyme.

Diverses techniques peuvent être utilisées pour cela, allant d'un programme qui remplace le gestionnaire de login jusqu'à un programme pirate qui espionne ce qui se passe dans le terminal.

Les attaques par dictionnaire

Beaucoup de mots de passe étant choisis dans le dictionnaire, il est très simple pour un automate de les essayer tous. De nombreuses expériences ont démontré la facilité de cette attaque et ont mesuré que la découverte de la moitié des mots de passe des employés d'une grande entreprise s'effectuait en moins de deux heures.

Une solution simple pour remédier à cette attaque est de complexifier les mots de passe en leur ajoutant des lettres majuscules, des chiffres et des signes comme !, ?, &, etc.

Les autres attaques

Le nombre d'attaques possibles est bien trop grand pour que nous puissions les citer toutes. De plus, de nouvelles procédures d'attaque s'inventent chaque jour.

Les attaques par écoute consistent, pour un pirate, à écouter une ligne de communication et à interpréter les éléments binaires qu'il intercepte. Les attaques par fragmentation utilisent le fait que les informations de supervision se trouvent dans la première partie du paquet à un emplacement parfaitement déterminé. Un pirate peut modifier la valeur du bit de fragmentation, ce qui a pour effet de faire croire que le message se continue alors qu'il aurait dû se terminer. Le pare-feu voit donc arriver une succession de fragments qui suivent les fragments de l'utilisateur sans se douter que ces fragments complémentaires ont été ajoutés par le pirate.

Les algorithmes de routage sont à la base de nombreuses attaques. En effectuant des modifications sur les tables de routage, le pirate peut récupérer de nombreuses informations qui ne lui sont pas destinées ou dérouter les paquets, lesquels, par exemple, vont effectuer des boucles et saturer le réseau.

De la même façon, de nombreuses attaques sont possibles en perturbant un protocole comme ARP (Address Resolution Protocol), soit pour prendre la place d'un utilisateur, soit en captant des données destinées à un autre.

Les parades

Les parades aux attaques sont nombreuses. Elles relèvent autant du comportement humain que de techniques spécifiques. Nous allons examiner les principales : l'authentification, l'intégrité du flux, la non-répudiation, la confidentialité du flux et la confidentialité au niveau de l'application.

L'authentification

Une première parade visant à empêcher qu'un autre terminal que celui prévu ne se connecte ou bien qu'un terminal ne se connecte sur un serveur pirate est offerte par les méthodes d'authentification. L'authentification peut être simple, et ne concerner que l'utilisateur, ou mutuelle, et impliquer à la fois le client et le serveur.

Dans des applications de type Telnet, e-mail ou LDAP, le client s'authentifie avec un mot de passe auprès du serveur pour établir ses droits. Dans une application de commerce électronique (HTTP), il est nécessaire d'authentifier le serveur puis le client, généralement à l'aide d'un mot de passe. Le protocole HTTP ne possédant pas de moyen efficace d'authentification du client, la société Netscape a introduit vers 1995 la notion de cookie, destinée à identifier un flux de requêtes HTTP disjointes.

L'intégrité du flux de données

L'intégrité d'un flux de données demande qu'il ne puisse y avoir une altération des informations transportées. Un pirate pourrait en effet modifier une information pour tromper le récepteur. Il est à noter qu'intégrité ne signifie pas confidentialité. En effet, il est possible que l'information ne soit pas confidentielle et qu'elle puisse être recopiée, sans que cela pose de problème à l'utilisateur. Cependant, l'utilisateur veut que son information arrive intègre au récepteur.

La solution classique à ce genre de problème consiste à utiliser une empreinte. À partir de l'ensemble des éléments binaires dont on souhaite assurer l'intégrité, on calcule une valeur, qui ne peut être modifiée sans que le récepteur s'en rende compte. Les empreintes regroupent les solutions de type empreinte digitale, signature électronique, analyse rétinienne, reconnaissance faciale et, d'une manière générale, tout ce qui permet de signer de façon unique un document. Ces différentes techniques de signature proviennent de techniques d'authentification puisque, sous une signature, se cache une authentification.

Dans les réseaux IP, la pratique de la signature électronique est de plus en plus mise en œuvre pour faciliter le commerce et les transactions financières.

La non-répudiation

La non-répudiation consiste à empêcher l'éventuel refus d'un récepteur d'effectuer une tâche suite à un démenti de réception. Si la valeur juridique d'un fax est reconnue, celle d'un message électronique ne l'est pas encore. Pour qu'elle le soit, il faut un système de non-répudiation. Les parades visant à éviter qu'un utilisateur répudie un message reçu

proviennent essentiellement d'une signature unique sur le message et sur son accusé de réception, c'est-à-dire une signature qui ne serait valable qu'une seule fois et serait liée à la transmission du message qui a été répudié. Un système de chiffrement à clés publiques peut être utilisé dans ce contexte.

Une autre solution, qui se développe, consiste à passer par un notaire électronique, qui, par un degré de confiance qui lui est attribué, peut certifier que le message a bien été envoyé et reçu.

Une difficulté importante de la non-répudiation dans une messagerie électronique provient de la vérification que le récepteur en a pris possession et a lu le message. Il n'existe pas de règle aujourd'hui sur Internet pour envoyer des messages de type lettre recommandée. Le récepteur peut, par exemple, recevoir le message dans sa boîte aux lettres électronique mais ne pas le récupérer. Il peut également recopier le message dans la boîte aux lettres de son terminal et le supprimer sans le lire.

Les techniques de non-répudiation ne sont pas encore vraiment développées dans le monde IP. En effet, cette fonction de sécurité est souvent jugée moins utile que les autres. Cependant, elle est loin d'être absente. En effet, dans le commerce électronique elle est capitale pour qu'un achat ne puisse être décommandé sans certaines conditions déterminées dans le contrat d'achat. Cette fonction serait également utile dans des applications telles que la messagerie électronique, où l'on aimerait être sûr qu'un message est bien arrivé.

Même si la non-répudiation n'est pas implémentée de façon automatique, elle est proposée dans de nombreuses applications qui en ont besoin.

La confidentialité

La confidentialité désigne la capacité de garder une information secrète. Le flux, même s'il est intercepté, ne doit pas pouvoir être interprété. La principale solution permettant d'assurer la confidentialité d'un flux consiste à le chiffrer. Les systèmes de chiffrement ont été présentés au chapitre 38.

Aujourd'hui, étant donné la puissance des machines qui peuvent être mises en jeu pour casser un code, il faut utiliser de très longues clés. Les clés de 40 bits peuvent être percées en quelques secondes et celles de 128 bits en quelques minutes sur une plus ou moins grosse machine en fonction de l'algorithme de chiffrement utilisé. Une clé RSA de 128 bits a été cassée en quelques heures par un ensemble de machines certes important mais accessible à une entreprise.

Pour casser une clé, il faut récupérer des données chiffrées, parfois en quantité importante, ce qui peut nécessiter plusieurs heures d'écoute, voire plusieurs jours si la ligne est à faible débit. Une solution à ce problème de plus en plus souvent utilisée consiste à changer de clé régulièrement de telle sorte que l'attaquant n'ait jamais assez de données disponibles pour casser la clé.

Dans la réalité, il est plus facile de pirater une clé que d'effectuer son déchiffrement. Une parade pour contrer les pirates réside dans ce cas dans un contrôle d'accès sophistiqué des bases de données de clés.

La confidentialité est aujourd'hui un service fortement utilisé dans le monde IP. IPsec en est un très bon exemple, et nous le détaillons un peu plus loin dans ce chapitre. De nouvelles méthodes, comme le chiffrement quantique, sont à l'étude et pourraient déboucher sur des méthodes encore plus sûres.

IPsec (IP sécurisé)

Le monde TCP/IP permet d'interconnecter plusieurs millions d'utilisateurs, lesquels peuvent souhaiter que leur communication reste secrète. Internet transporte de plus un grand nombre de transactions de commerce électronique, pour lesquelles une certaine confidentialité est nécessaire, par exemple pour prendre en charge la transmission de numéros de carte bancaire.

L'idée développée dans les groupes de travail sur la sécurité du commerce électronique dans le monde IP consiste à définir un environnement contenant un ensemble de mécanismes de sécurité. Les mécanismes de sécurité appropriés sont choisis par une association de sécurité. En effet, toutes les communications n'ont pas les mêmes caractéristiques, et leur sécurité ne demande pas les mêmes algorithmes.

Chaque communication se définit par sa propre association de sécurité. Les principaux éléments d'une association de sécurité sont les suivants :

- algorithme d'authentification ou de chiffrement utilisé ;
- clés globales ou spécifiques à prendre en compte ;
- autres paramètres de l'algorithme, comme les données de synchronisation ou les valeurs d'initialisation ;
- durée de validité des clés ou des associations ;
- sensibilité de la protection apportée (secret, top secret, etc.).

La solution IPsec introduit des mécanismes de sécurité au niveau du protocole IP, de telle sorte qu'il y ait indépendance vis-à-vis du protocole de transport. Le rôle de ce protocole de sécurité est de garantir l'intégrité, l'authentification, la confidentialité et la protection contre les techniques rejouant des séquences précédentes. L'utilisation des propriétés d'IPsec est optionnelle dans IPv4 et obligatoire dans IPv6.

Une base de données de sécurité, appelée SAD (Security Association Database), regroupe les caractéristiques des associations par l'intermédiaire de paramètres de la communication. L'utilisation de ces paramètres est définie dans une autre base de données, la SPD (Security Policy Database). Une entrée de la base SPD regroupe les adresses IP de la source et de la destination, ainsi que l'identité de l'utilisateur, le niveau de sécurité requis, l'identification des protocoles de sécurité mis en œuvre, etc.

Le format des paquets IPsec est illustré à la figure 29.2. La partie la plus haute de la figure correspond au format d'un paquet IP dans lequel est encapsulé un paquet TCP. La partie du milieu illustre le paquet IPsec. On voit que l'en-tête IPsec vient se mettre entre l'en-tête IP et l'en-tête TCP. La partie basse de la figure montre le format d'un paquet dans un tunnel IPsec. La partie intérieure correspond à un paquet IP encapsulé dans un paquet IPsec de telle sorte que le paquet IP intérieur soit bien protégé.

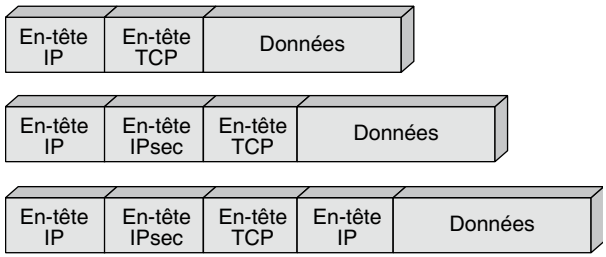


Figure 29.2
Format des paquets IPsec

Dans un tunnel IPsec, tous les paquets IP d'un flot sont transportés de façon totalement chiffrée. Il est de la sorte impossible de voir les adresses IP ni même les valeurs du champ de supervision du paquet IP encapsulé. La figure 29.3 illustre un tunnel IPsec.

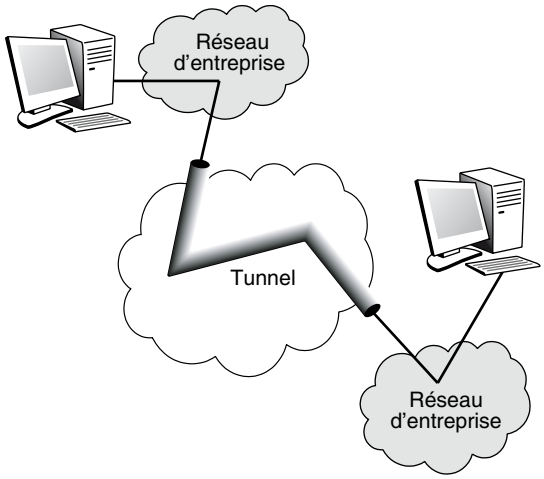


Figure 29.3
Tunnel IPsec

L'en-tête d'authentification

L'en-tête d'authentification est ajouté immédiatement derrière l'en-tête IP standard. À l'intérieur de l'en-tête IP, le champ indiquant le prochain protocole inclus dans le paquet IP (champ Next-Header) prend la valeur 51. Cette valeur précise que les champs IPsec et d'authentification sont mis en œuvre dans le paquet IP. L'en-tête IPsec possède lui-même un champ indiquant le protocole encapsulé dans le paquet IPsec. En d'autres termes, lorsqu'un paquet IP doit être sécurisé par IPsec, il repousse la valeur de l'en-tête suivant, qui était dans le paquet IP, dans le champ en-tête suivant de la zone d'authentification d'IPsec et met la valeur 51 dans l'en-tête de départ.

La figure 29.4 présente en détail l'en-tête d'authentification. Comme indiqué précédemment, cet en-tête commence par la valeur indiquant le protocole transporté. Le champ LG (Length), sur un octet, indique la taille de l'en-tête d'authentification. Vient ensuite une zone réservée, sur 2 octets, qui prend place avant le champ sur 4 octets, donnant un index des paramètres de sécurité, qui décrit le schéma de sécurité adopté pour la communication.

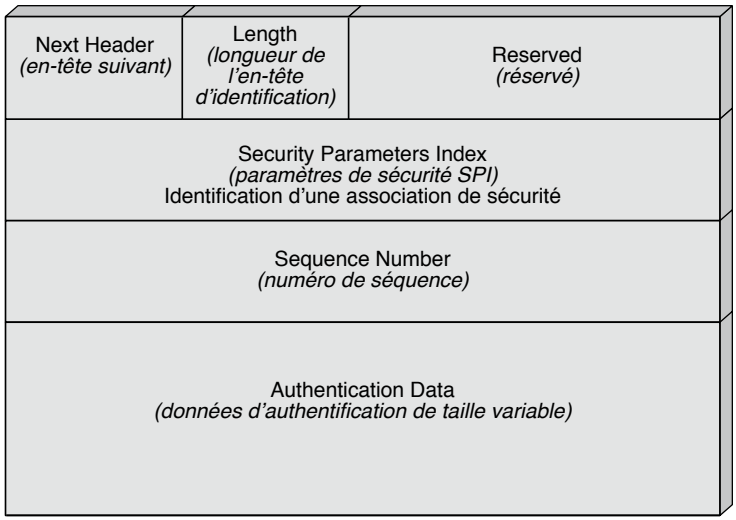


Figure 29.4
Format de l'en-tête d'authentification

Le champ numéro de séquence, qui contient un numéro de séquence unique, est nécessaire pour éviter les attaques de type rejeu, dans lesquelles le pirate rejoue exactement la même séquence de messages que l'utilisateur par une copie pure et simple. Par exemple, si vous consultez votre compte en banque et qu'un pirate recopie vos messages, même chiffrés, c'est-à-dire sans les comprendre, il peut, à la fin de votre session, rejouer la même succession de messages, qui lui ouvrira les portes de votre compte.

L'en-tête d'authentification se termine par les données associées à ce schéma de sécurité. Il transporte le type d'algorithme de sécurité, les clés utilisées, la durée de vie de l'algorithme et des clés, une liste des adresses IP des émetteurs qui peuvent utiliser le schéma de sécurité, etc.

L'en-tête d'encapsulation de sécurité

Pour permettre une confidentialité des données, tout en garantissant une authentification, IPsec utilise une encapsulation dite ESP (Encapsulating Security Payload), c'est-à-dire une encapsulation de la charge utile de façon sécurisée. La valeur 50 est transportée dans le champ en-tête suivant (Next-Header) du paquet IP pour indiquer cette encapsulation ESP.

La figure 29.5 illustre ce processus d'encapsulation. On s'aperçoit que l'encapsulation ESP ajoute trois champs supplémentaires au paquet IPsec : l'en-tête ESP, qui suit l'en-tête IP de départ et porte la valeur 50, le Trailer, ou en-queue, ESP, qui est chiffré avec la charge utile, et le champ d'authentification ESP de taille variable, qui suit la partie chiffrée sans être lui-même chiffré.

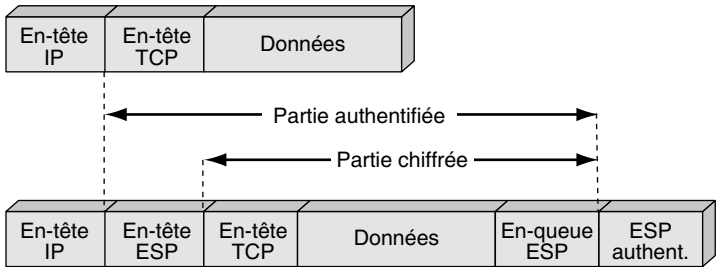


Figure 29.5

Processus d'encapsulation ESP

Le paquet ESP est repris à la figure 29.6 de façon un peu plus détaillée en ce qui concerne les champs internes, à partir du champ ESP d'en-tête.

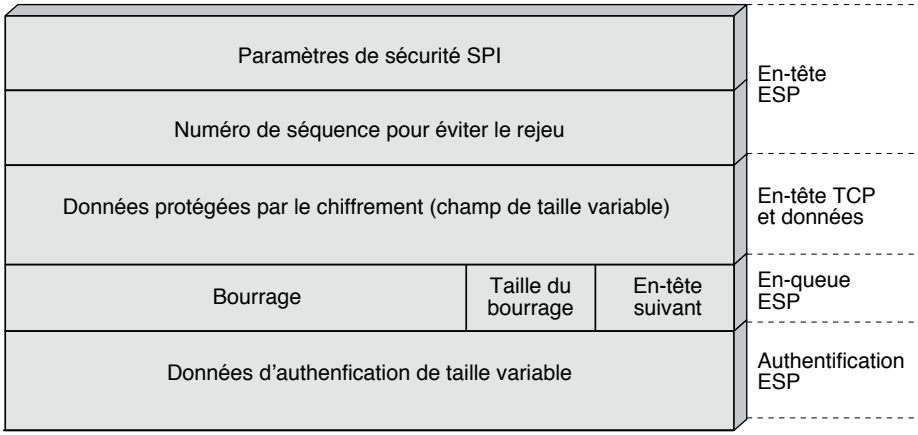


Figure 29.6

Format de l'en-tête ESP

La première partie de l'encapsulation reprend les paramètres SPI (Security Parameter Index) et numéro de séquence que nous avons déjà décrits dans l'en-tête d'authentification. Vient ensuite la partie transportée et chiffrée. L'en-queue ESP comporte une zone de bourrage optionnelle, allant de 0 à 255 octets, puis un champ longueur du bourrage (Length) et la valeur d'un en-tête suivant.

La zone de bourrage a plusieurs raisons d'être. La première provient de l'adoption d'algorithmes de chiffrement, qui exigent la présence d'un nombre de 0 déterminé après la zone chiffrée. La deuxième raison vient de la place de l'en-tête suivant, qui doit être aligné à droite, c'est-à-dire prendre une place en fin d'un mot de 4 octets. La dernière raison est que, pour contrer une attaque, il peut être intéressant d'ajouter de l'information sans signification susceptible de leurrer un pirate.

Les compléments d'IPsec

Dans IPsec, le chiffrement ne s'effectue pas sur l'ensemble des champs, car certains champs, que l'on appelle *mutable,* changent de valeur à la traversée des routeurs, comme le champ TTL (durée de vie). Dans le calcul du champ d'authentification, le processus ne tient pas compte de ces champs mutables.

Les algorithmes de sécurité qui peuvent être utilisés dans le cadre d'IPsec sont déterminés par un certain nombre de RFC :

- HMAC avec MD5 : RFC 2403
- HMAC avec SHA-1 : RFC 2404
- DES en mode CBC : RFC 2405
- TripleDES avec CBC : RFC 2451
- AES avec CBC : RFC 3602

La sécurité dans IPv6

Le protocole IPv6 contient les mêmes fonctionnalités qu'IPsec. On peut donc dire qu'il n'existe pas d'équivalent d'IPsec dans le contexte de la nouvelle génération IP.

Les champs de sécurité sont optionnels. Leur existence est détectée par les valeurs 50 et 51 du champ en-tête suivant (Next-Header). Globalement, la sécurité offerte par IPv6 est donc exactement la même que celle offerte par IPsec. Elle est toutefois plus simple à mettre en œuvre puisque le protocole de sécurité est dans le protocole IPv6 lui-même. On peut en déduire que la sécurisation des communications sera beaucoup plus simple avec la nouvelle génération de réseau qui utilisera IPv6.

Cela pose toutefois d'autres problèmes. Si tous les flux sont chiffrés, par exemple, il n'y a plus moyen de reconnaître les numéros de port ou les adresses source et destination, et les applications deviennent transparentes. Toutes les appliances intermédiaires, comme les pare-feu ou les contrôleurs de qualité de service, deviennent inutilisables. L'information sur le type d'application véhiculé ne se trouve qu'à la source ou à la destination, et c'est là qu'il faut venir la rechercher. De nouvelles architectures de contrôle sont donc à prévoir avec l'arrivée d'IPv6, ce qui constitue une raison de repousser cette arrivée dans beaucoup d'entreprises.

SSL (Secure Sockets Layer)

SSL est un logiciel permettant de sécuriser les communications sous HTTP ou FTP. Ce logiciel a été développé par Netscape pour son navigateur et les serveurs Web.

Le rôle de SSL est de chiffrer les messages entre un navigateur et le serveur Web interrogé. Le niveau d'architecture où se place SSL est illustré à la figure 29.7. Il s'agit d'un niveau compris entre TCP et les applicatifs.

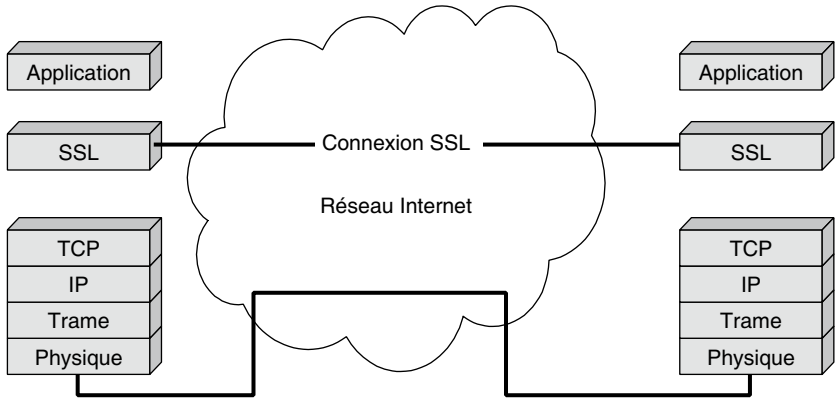


Figure 29.7
Architecture SSL

Les signatures électroniques sont utilisées pour l'authentification des deux extrémités de la communication et l'intégrité des données.

L'initialisation d'une communication SSL commence par un handshake, c'est-à-dire une poignée de main, qui permet l'authentification réciproque grâce à un tiers de confiance. La communication se continue par une négociation du niveau de sécurité à mettre en œuvre et peut se dérouler avec un chiffrement associé au niveau négocié à la phase précédente.

Les inconvénients du protocole SSL proviennent de l'utilisation d'un tiers de confiance et de la nécessité d'ouvrir le port associé à SSL dans les pare-feu. Nous verrons ultérieurement dans ce chapitre la signification exacte de l'expression « ouvrir un port ».

Le protocole SSL a vu son champ d'action dépasser la simple sécurisation d'une communication Web. Il est notamment utilisé dans le commerce électronique pour sécuriser la transmission du numéro de carte de crédit. Un autre protocole, S-HTTP (Secure HTTP), assez semblable à SSL, a été développé pour sécuriser les communications sous HTTP, mais il est beaucoup moins utilisé.

HTTPS est un autre protocole très utilisé, qui intègre à la fois HTTP et SSL et qui est décrit dans le RFC 2660.

L'authentification de SSL s'appuie sur la cryptographie asymétrique par le biais de certificats à clé publique. Un client peut s'authentifier automatiquement auprès d'un serveur SSL en utilisant la paire de clés publiques nécessaire. SSL peut utiliser différents mécanismes de chiffrement. En règle générale, la négociation entre le client et le serveur SSL permet de définir le meilleur algorithme commun. Classiquement, un serveur SSL utilise une clé publique RSA pour établir un ensemble de clés secrètes partagées utilisées avec un algorithme de chiffrement RC4 pour le chiffrement des données et MD5 pour l'intégrité.

Le protocole SSLv3 propose une architecture plus évoluée, qui contient un générateur de clés, des fonctions de hachage et des algorithmes de chiffrement et de gestion de certificats. Cette architecture est représentée à la figure 29.8.

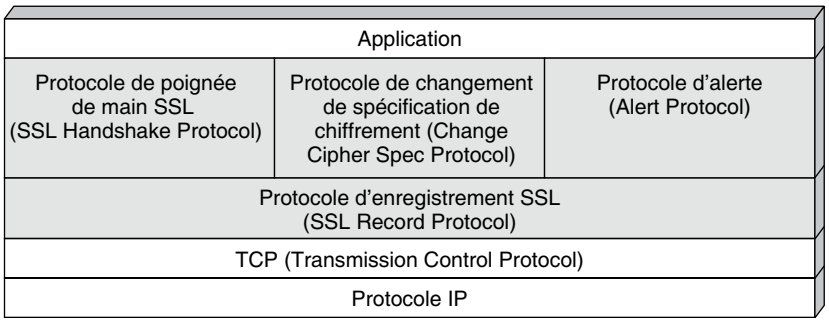


Figure 29.8

Architecture du protocole SSLv3

Le protocole de changement de spécification de chiffrement permet de modifier l'algorithme de chiffrement en cours de communication de sorte à garantir la confidentialité des données transportées. Le protocole d'alerte permet d'envoyer des alertes, accompagnées de leur importance. Ces alertes peuvent être un certificat inconnu, révoqué, expiré, etc. Les alertes de haut niveau entraînent l'arrêt de la communication.

Le protocole Handshake a pour objectif d'authentifier le serveur depuis le client, de négocier la version du protocole, de sélectionner les algorithmes de chiffrement, d'utiliser des techniques de chiffrement à clé publique pour générer et distribuer des clés secrètes et d'établir des connexions SSL chiffrées.

Messages du protocole Handshake

Les messages échangés pour réaliser le protocole Handshake sont les suivants :

- ClientHello : initialisation de la communication par l'envoi d'un hello du client vers le serveur.
- ServerHello : en retour du message précédent, cette réponse peut contenir un certificat et demander une authentification de la part du client.
- ServerKeyExchange : si les certificats ne sont pas pris en charge, ce message permet d'effectuer l'échange de clés publiques.
- ServerHelloDone : permet d'indiquer que la partie serveur du message hello est achevée.
- CertificateRequest : requête envoyée par le serveur au client lui demandant de s'authentifier. Le client répond soit avec un message envoyant le certificat, soit avec une alerte indiquant qu'il ne possède pas de certificat.
- CertificateMessage : message qui envoie le certificat réclamé par le serveur.
- NoCertficate : message d'alerte qui indique que le client ne possède aucun certificat susceptible de correspondre à la demande du serveur.
- ClientKeyExchange : échange de la clé du client avec le serveur.
- Finished : message qui conclut le handshake pour indiquer la fin de la mise en place de la communication.

Le protocole d'enregistrement SRP (SSL Record Protocol) n'est qu'une encapsulation des protocoles situés juste au-dessus, comme le protocole Handshake.

Le protocole SSLv3.0 et son successeur TLS1.0 ne présentent que des différences mineures entre eux mais ne sont cependant pas interopérables. La principale différence entre les deux concerne les méthodes de chiffrement puisque TLS n'impose aucune restriction.

Les protocoles d'authentification

Nous commencerons par introduire le protocole PPP et tous ses dérivés, puis nous examinerons l'extension EAP, qui est devenue le standard de transport des informations d'authentification dans le monde des réseaux IP.

PPP (Point-to-Point Protocol)

PPP a été défini en juillet 1994 dans la RFC 1661. Protocole de niveau trame, il permet de transporter un paquet d'un nœud vers un autre nœud. Bien que conçu initialement pour transporter des paquets IP, il peut prendre en compte d'autres protocoles de contrôle, que nous détaillons également dans ce chapitre.

La structure de la trame PPP est illustrée à la figure 29.9.

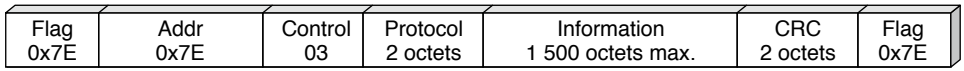


Figure 29.9

Structure de la trame PPP

Le champ Protocol, sur 2 octets, identifie le type de paquet inclus dans la trame PPP. Les valeurs de ce champ sont indiquées au tableau 29.1.

Valeur	Protocole encapsule
0x0021	IP
0xC021	LCP (Link Control Protocol)
0x8021	NCP (Network Control Protocol)
0xC023	PAP (Password Authentication Protocol)
0xC025	LQR (Link Quality Report)
0xC223	CHAP (Challenge Handshake Authentication Protocol)

TABLEAU 29.1 • Valeurs du champ Protocol de la trame PPP

Un diagramme des états du protocole PPP est illustré à la figure 29.10.

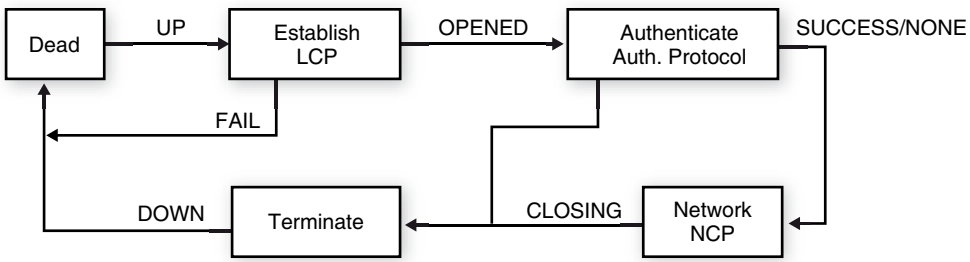


Figure 29.10

Diagramme des états de PPP

La liaison est d'abord mise en place par le protocole LCP (Link Control Protocol). Une fois l'ouverture effectuée, une authentification des extrémités a lieu pour sécuriser la liaison. Les protocoles de la famille CHAP (Challenge Handshake Authentication Protocol) ont été développés dans ce but. Une fois la liaison sécurisée, le protocole de contrôle NCP (Network Control Protocol) prend la suite pour déterminer les protocoles de niveau paquet qui vont utiliser la liaison.

LCP (Link Control Protocol)

Le protocole LCP permet d'ouvrir une liaison PPP et donne les moyens de négocier les options mises en œuvre par PPP, comme la taille des MTU.

Il existe onze types de paquets LCP, identifiés par un code sur 1 octet. Les options sont encodées sous la forme d'un code sur 1 octet, d'un identificateur sur 1 octet et d'une longueur sur 2 octets. Elles sont suivies par les données transportées, dont la longueur est précisée par le champ Length.

Les différents codes qui peuvent être utilisés dans le paquet LCP sont les suivants :

- (1) requête de configuration
- (2) accusé (ACK) de configuration
- (3) non accusé de configuration (NAK)
- (4) requête de terminaison
- (6) accusé de terminaison
- (7) rejet de code
- (8) rejet de protocole
- (9) requête d'écho
- (10) réponse d'écho
- (11) requête d'élimination

L'identificateur du deuxième octet de LCP définit les options suivantes :

- (1) MRU (Maximum Receive Unit)
- (3) protocole d'authentification
- (4) protocole de qualité (mesure de la qualité de la ligne utilisée)

- (5) nombre magique (détection de boucles ; client et serveur sur le même système hôte)
- (7) compression du champ protocole (de 2 octets à 1-PFC)
- (8) compression des champs adresse et contrôle de la trame HDLC (ACFC)

NCP (Network Control Protocol)

Le protocole NCP est défini dans la RFC 1332. Il permet de configurer des types de réseaux différents susceptibles d'utiliser la liaison PPP, par exemple IP ou DECnet. Issu de l'architecture réseau de la société DEC, qui a disparu au cours des années 1990, DECnet n'est plus employé aujourd'hui. Dans le cadre des réseaux IP, le protocole utilisé est IPCP (Internet Protocol Control Protocol).

IPCP utilise seulement les sept premiers types de paquets de LCP. Une option de compression peut être utilisée. Dans ce cas, le code indiqué dans le champ protocole des trames PPP est 0x002D. Une adresse IP peut être attribuée par le serveur au client

PAP (Password Authentication Protocol)

PAP (Password Authentication Protocol) est un protocole d'authentification par mot de passe défini dans la RFC 1334 en 1992.

La demande d'authentification du protocole PAP est indiquée par la présence de la valeur C023 dans le champ Protocol de la trame PPP. Les champs du paquet PAP sont illustrés à la figure 29.11. La longueur de la zone de données transportant le protocole d'authentification est de 4 octets.

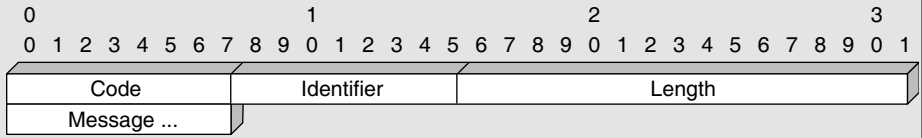


Figure 29.11

Format du paquet PAP

Le champ Code identifie la nature du paquet PAP. Il peut s'agir d'une requête d'authentification (Authentication Request) avec la valeur 1, d'un acquittement positif (Authenticate ACK) avec la valeur 2 ou d'un acquittement négatif de la demande (Authenticate NACK) avec la valeur 3. La structure des paquets correspondants est illustrée aux figures 29.12 et 29.13.

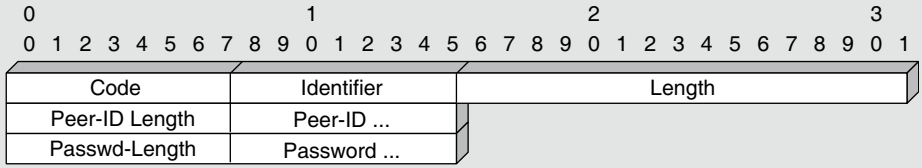


Figure 29.12

Structure du paquet de requête d'authentification

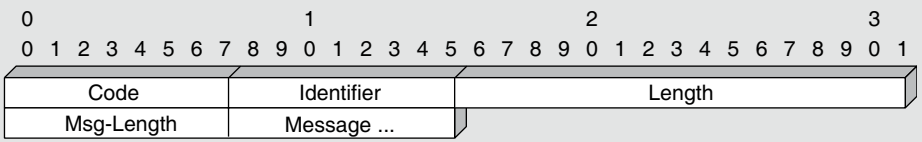


Figure 29.13

Structure du paquet d'authentification et de non-authentification

Le champ Identifier contient le numéro d'une requête et de la réponse associée. Le champ Length détermine la longueur totale du paquet PAP.

CHAP (Challenge Handshake Authentication Protocol)

Le protocole CHAP a été normalisé par la RFC 1334en 1994.

La demande d'authentification CHAP est indiquée par la valeur C223 dans le champ Protocol de la trame PPP. La figure 29.14 illustre le processus d'authentification du protocole CHAP.

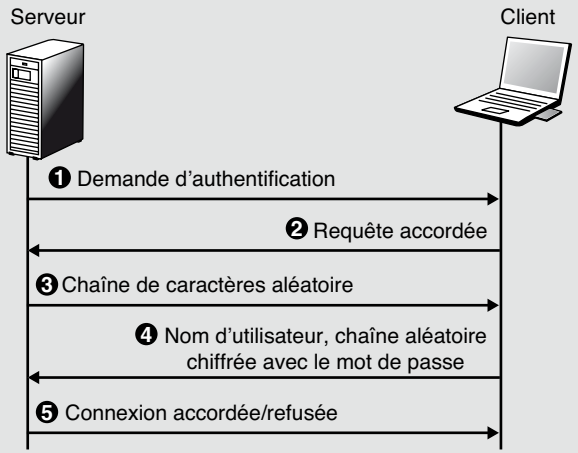


Figure 29.14

Processus d'authentification du protocole CHAP

Le format du paquet CHAP est illustré à la figure 29.15.

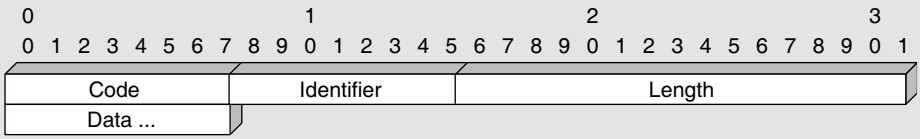


Figure 29.15

Format du paquet CHAP

Lorsque le champ code du paquet CHAP vaut 1-Challenge ou 2-Response, le paquet a la structure illustrée à la figure 29.16. Si le code vaut 3-Success ou 4-Failure, la structure du paquet prend la forme illustrée à la figure 29.17. Dans ces paquets, le champ Identifier indique le numéro d'une requête et de la réponse associée, et le champ *Length* la longueur totale du paquet PAP.

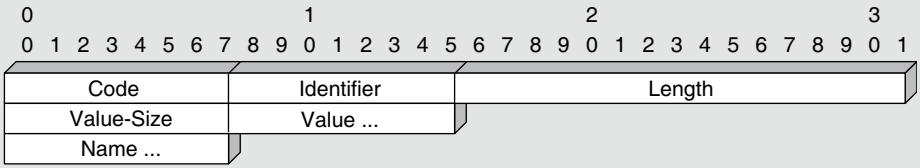


Figure 29.16

Paquet Challenge/Response

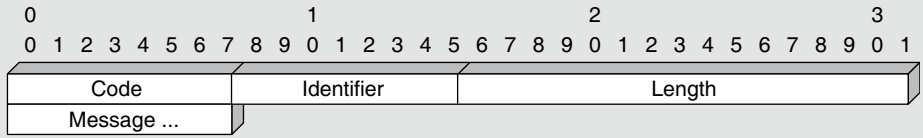


Figure 29.17

Paquet Success/Failure

MS-CHAP-V1

Le protocole MS-CHAP-V1 a été proposé par Microsoft et normalisé par l'IETF sous la RFC 2433 en 1998. Ce protocole est compatible avec la RFC de base datant de 1994.

Dans l'univers Microsoft, la sécurité d'un ordinateur personnel est fortement corrélée au mot de passe de son utilisateur. Ce dernier n'est jamais stocké en clair dans la mémoire de la machine. À partir d'un mot de passe, une empreinte MD4 de 16 octets est calculée puis mémorisée par le système hôte. Cette valeur, parfois nommée clé NT (NtPasswordHash) est complétée par cinq octets nuls. On obtient ainsi 21 octets, interprétés comme une suite de trois clés DES de 56 bits chacune.

La méthode MS-CHAP-V1 est une authentification simple. Le serveur d'authentification produit un nombre aléatoire de 8 octets, et l'authentifié utilise ses trois clés DES pour chiffrer cet aléa, ce qui génère une réponse de 24 octets.

La demande d'authentification MS-CHAP-V1 est indiquée par la valeur C223 dans le champ Protocol de la trame PPP, complétée par un numéro d'algorithme prenant la valeur 0x80. Le format des paquets MS-CHAP-V1 est identique à celui des paquets CHAP. Les formats permettant de transporter les indications Challenge/Response et Success/Failure sont également les mêmes que dans le protocole CHAP. La différence provient de la taille du challenge, qui est de 8 octets. La taille de la réponse est de 25 octets, 24 octets pour les formats LAN manager et Windows NT et 1 octet (Use Windows NT compatible Challenge Response Flag) indiquant la disponibilité du format Windows NT. Le champ Name indique l'identifiant du compte utilisateur, c'est-à-dire nom de domaine plus le nom d'utilisateur.

Les indications 3-Success et 4-Failure comportent toujours une zone Identifier, qui donne le numéro d'une requête et de la réponse associée, et un champ Length, qui précise la longueur totale du paquet PAP.

Les messages portant les valeurs E, C et V indiquent :

- E : Error-Code ;
- R : retry allowed(1/0) ;
- C : new-challenge-value(16 hexadecimal value) ;
- V : decimal-version-code.

Deux nouvelles indications, les valeurs 5 et 6, permettent de modifier un mot de passe. Pour la valeur 5-Change Password Packet (version 1), les champs ont la valeur 5 pour le code et une longueur de 72 octets.

Ces 72 octets se décomposent de la façon suivante :

- 16 octets pour Encrypted LAN Manager Old password Hash ;
- 16 octets pour Encrypted LAN Manager New Password Hash ;
- 16 octets pour Encrypted Windows NT Old Password Hash ;
- 16 octets pour Encrypted Windows NT New Password Hash ;
- 2 octets pour Password Length ;
- 2 octets pour Flags.

Dans la deuxième version du changement de mot de passe, le code 6 est utilisé. La longueur du champ est de 1 114 octets, qui se décomposent de la façon suivante :

- 516 octets pour Password Encrypted with Old NT Hash ;
- 16 octets pour Old NT Hash Encrypted with New NT Hash ;
- 516 octets pour Password Encrypted with Old LM Hash ;
- 16 octets pour Old LM Hash Encrypted With New NT Hash ;
- 24 octets pour LAN Manager compatible challenge response ;
- 24 octets pour Windows NT compatible challenge response ;
- 2 octets pour Flags1.

Les mécanismes d'authentification de Windows NT utilisent un mot de passe. Ce dernier est constitué d'une chaîne Unicode de 256 caractères au plus. Le NTPasswordHash est le résultat d'un Hash MD4 produisant 16 octets (128 bits). Ce NTPasswordHash est complété par 5 octets nuls. On obtient ainsi 21 octets, décomposés en trois clés DES de 7 octets. Le challenge de 8 octets est chiffré par les trois clés DES, qui produisent une réponse de 24 octets : DES1(challenge), DES2(challenge), DES3(challenge).

Le PasswordHash (128 bits) est également utilisé comme clé de chiffrement RC4 dans les messages de modification de mot de passe. Un mot de passe est complété pour atteindre 256 caractères (512 octets) par une suite aléatoire. Cette valeur concaténée à la taille réelle (un entier de 4 octets) est chiffrée par la clé RC4, soit 516 octets.

MS-CHAP-V2

Le protocole MS-CHAP-V2 a été normalisé en 2000 par l'IETF sous la RFC 2759. MS-CHAP-V2 est une extension du protocole précédent, avec lequel il est compatible. L'objectif de cette nouvelle version est d'offrir une sécurité supérieure aux connexions d'accès distant en corrigeant certains problèmes de la précédente, comme la faiblesse des clés de chiffrement.

La demande d'authentification MS-CHAP-V2 est indiquée par la valeur 0x81 du champ Algorithm du protocole CHAP. Le format des paquets de la version 2 est similaire à celui de la version 1.

Le processus d'authentification est le suivant : le serveur d'authentification délivre un nombre aléatoire de 16 octets (AuthenticatorChallenge) ; le client 802.1x calcule un nombre de 8 octets à partir de cette valeur, d'un aléa (Peer-Challenge) qu'il génère et du nom de l'utilisateur (login) ; ce paramètre est chiffré comme dans MS-CHAP-V1 par la clé NT pour obtenir une valeur de 24 octets.

Dans une plate-forme Microsoft, un annuaire stocke le nom des utilisateurs et leur mot de passe. La taille de la réponse est de 49 octets, qui se décomposent de la façon suivante :

- 16 octets pour le Peer-Challenge, qui porte un nombre aléatoire ;
- 8 octets réservés et codés à zéro ;
- 24 octets pour le format de réponse NT (NT-Response)
- 1 octet réservé et codé à zéro.

Le champ Name indique l'identifiant du compte utilisateur (nom-de-domaine\nom-utilisateur). Pour les codes 3-Success et 4-Failure, la longueur du champ Message est de 42 octets.

Le format de ce champ est S=<auth_string> M=<message>, auth_string étant une chaîne de 20 caractères ASCII et message un texte affichable compréhensible.

Lorsqu'un message d'erreur est envoyé en retour, il se présente sous la forme suivante :

E=Error-Code R=retry allowed(1/0) C=new-challenge-value(32 hexadecimal value) V=decimal-version-code

La longueur du code 7, qui indique un changement de mot de passe, est de 586 octets, qui se décomposent de la façon suivante :

- 516 octets pour Encrypted-Password ;
- 16 octets pour Encrypted-Hash ;
- 16 octets pour Peer-Challenge ;
- 8 octets pour Reserved ;
- 24 octets pour NT-Response ;
- 2 octets pour Flags (réservé et codé à zéro).

Comme pour la version précédente, les mécanismes d'authentification que l'on trouve dans NT comprennent le mot de passe, qui est une chaîne Unicode de 256 caractères au plus. Pour la génération de la NT-Response, une procédure (ChallengeHash) fondée sur la fonction SHA-1 produit un nombre (challenge) de 8 octets à partir du nombre aléatoire AuthenticatorChallenge, d'un nombre aléatoire PeerChallenge et du UserName.

Le Password est associé à une empreinte MD4 de 16 octets (NTPasswordHash), étendue à 21 octets, et interprété comme une série de trois clés DES de 7 octets. Le champ Challenge (8 octets) est chiffré par les trois clés DES, DES1(challenge), DES2(challenge) et DES3(challenge). Ces 24 octets constituent la NT-Response. Le Password-Hash (128 bits) est utilisé comme clé RC4 pour le chiffrement d'un nouveau mot de passe. Les deux premières clés DES déduites d'un PasswordHash sont utilisées pour le chiffrement du NtPasswordHash associé au nouveau mot de passe.

EAP (Extensible Authentication Protocol)

Le problème de la gestion de la mobilité des utilisateurs est devenu critique dès lors que les internautes ont massivement utilisé des modems et le protocole PPP pour accéder aux ressources offertes par leurs fournisseurs de services. Les systèmes d'exploitation ont donc intégré les fonctionnalités suivantes afin de renforcer la sécurité des nomades :

- authentification des utilisateurs par des méthodes de défi telles que CHAP, MS-CHAP ou MS-CHAP-V2 ;
- chiffrement des trames PPP, par exemple à l'aide de l'algorithme MPPE (Microsoft Point-To-Point Encryption), défini par la RFC 3078 en mars 2001 ;
- méthodes de calcul des clés de chiffrement (MS-MPPE-Recv-Key et MS-MPPE-Send-Key) ;
- distribution des clés par le protocole RADIUS.

Le besoin de compatibilité avec des infrastructures d'authentification diversifiées et la nécessité de disposer de secrets partagés dans ces environnements multiples ont conduit à la genèse du protocole EAP, capable de transporter des méthodes d'authentification indépendamment de leurs particularités.

Le protocole EAP fournit un cadre peu complexe pour le transport de protocoles d'authentification. Un message comporte un en-tête de 5 octets et des données optionnelles, comme illustré à la figure 29.18.

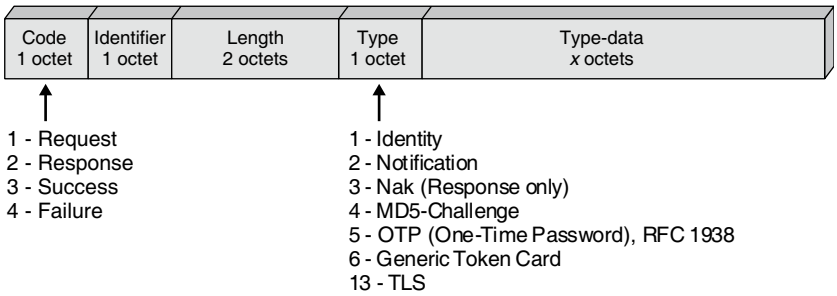


Figure 29.18

Format d'un message EAP

Il existe quatre types de messages, identifiés par un code de 1 octet :

- Request : 1
- Response : 2
- Success : 3
- Failure : 4

Chaque message est étiqueté à l'aide d'un nombre Identifier compris entre 0 et 255. L'étiquette d'une réponse est égale à celle de la requête correspondante. La longueur totale du message, codée sur deux octets, est comprise entre 4 et 65 535.

Le champ Type, compris entre 0 et 255, précise la nature des informations transportées. Les principales d'entre elles sont les suivantes :

- 1 : message relatif à l'identité (Identity).
- 2 : notification. Ce message contient une information affichable, et la réponse à une notification est obligatoirement une notification.
- 3 : notification d'une erreur (NAK).
- 4 : protocole d'authentification à base de défi MD5 (EAP-MD5).
- 6 : OTP (One Time Password).
- 13 : transport de TLS (EAP-TLS).
- 18 : méthode d'authentification fondée sur une carte SIM (EAP-SIM) pour le GSM 11.11, qui est la norme utilisée dans les réseaux GSM.
- 23 : EAP-AKA. Mise en œuvre des cartes USIM définies pour l'UMTS.
- 25 : PEAP. Méthode d'authentification du serveur, fondée sur TLS, et du client variable (MS-CHAP-V2, OTP, TLS, etc.).
- 26 : transport de MS-CHAP-v2.

Dans un réseau sécurisé avec 802.1x, une authentification EAP demande trois éléments : un supplicant que l'on appelle dans le langage courant un client, un authenticator que l'on appelle contrôleur et un serveur d'authentification. Un authenticator est un contrôleur de communication compatible 802.1x. La plupart des contrôleurs de communication dans les réseaux Ethernet sont compatibles 802.11x. Les points d'accès Wi-Fi professionnels sont souvent compatibles 802.1x et jouent le rôle d'authenticator. L'authentification se déroule de la manière suivante :

1. Lorsque la phase d'établissement de la liaison est terminée, le contrôleur envoie une requête d'identité.
2. Le client envoie un paquet EAP RESPONSE, dans lequel il fournit son identité et les méthodes d'authentification qu'il supporte. L'identité de l'utilisateur est indiquée par la valeur EAP-ID associée au message EAP-RESPONSE.IDENTITY.
3. Lorsque ce paramètre est similaire à une adresse de courrier électronique, ou NAI (Network Access Identifier), le contrôleur interprète la partie gauche, avant le caractère @, comme un login utilisateur et la partie droite comme le nom de domaine d'un serveur RADIUS. Une session d'authentification est initiée par le contrôleur grâce au message EAP-REQUEST.IDENTITY.
4. Le serveur d'authentification envoie alors un défi au client.
5. Le client y répond à nouveau par un message EAP RESPONSE.
6. L'authentification se poursuit par une suite de requêtes et de réponses (EAP-REQUEST.TYPE et EAP-RESPONSE.TYPE), relatives à un type, ou scénario d'authentification, particulier et échangés entre le serveur RADIUS et le client 802.1x.
7. Le contrôleur met fin à la phase d'authentification par l'intermédiaire d'un paquet de succès (EAP-SUCCESS) ou d'échec (EAP-FAILURE) qu'il aura reçu du serveur

d'authentification AAA (Authentication, Authorization, Accounting). C'est ce dernier qui prend la décision d'accepter ou de refuser l'accès au réseau.

8. Si la phase d'authentification s'est bien déroulée, le serveur d'authentification peut transmettre une clé de chiffrement au contrôleur, qui l'utilisera pour chiffrer les données envoyées au client.

Cette dernière phase est optionnelle pour le protocole EAP, car elle dépend du protocole d'authentification utilisé.

Ce processus est illustré à la figure 29.19 où un point d'accès Wi-Fi compatible IEEE 802.1x joue le rôle du contrôleur, mais cette solution est évidemment générale et s'applique aussi bien à des réseaux hertziens qu'à des réseaux terrestres.

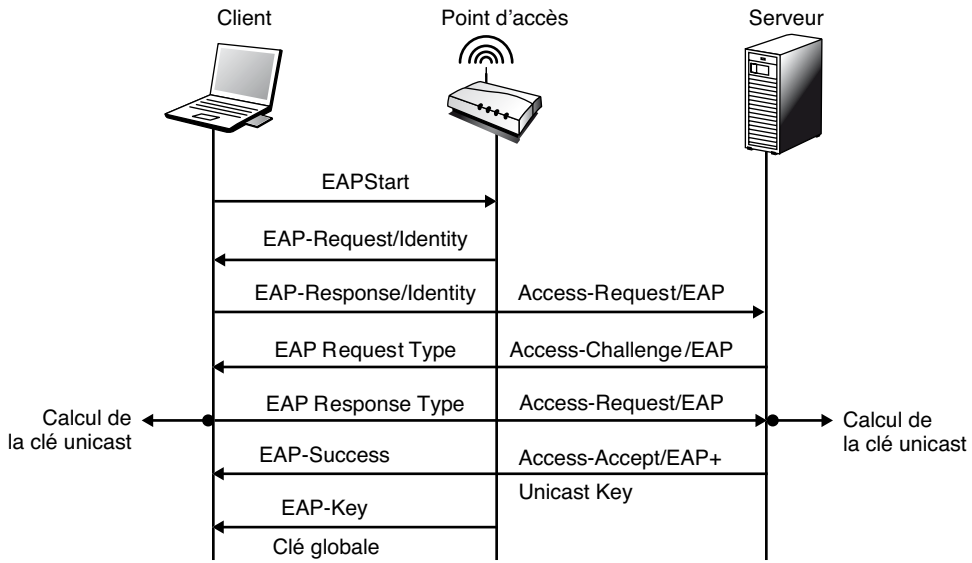


Figure 29.19
Session d'authentification

Un des points faibles du protocole EAP est sa vulnérabilité aux attaques par déni de service. Un pirate peut en effet écouter une session EAP et émettre à l'intention du client 802.1x un message d'échec (EAP-FAILURE). Il ne peut toutefois obtenir la clé globale délivrée par le message EAP-RESPONSE-TYPE car cette dernière est chiffrée et signée par la clé unicast dont il ne connaît pas la valeur.

Les procédures d'authentification liées à EAP

Comme expliqué précédemment, EAP (Extensible Authentication Protocol) est devenu le tunnel standard pour l'authentification. On met en place ce tunnel pour réaliser la procédure d'authentification elle-même. Un vaste choix de mécanismes d'authentification est possible. LEAP (Lightweight Extensible Authentication Protocol) est la solution

choisie par Cisco Systems pour ses premiers équipements de réseau sans fil. FAST-EAP a remplacé LEAP, celui-ci montrant quelques faiblesses dans des cas particuliers comme l'attaque par dictionnaire pour peu que les mots de passe ne soient pas sophistiqués. EAP/SIM et EAP/TLS sont les deux grands standards du moment. Ils correspondent aux choix effectués par les opérateurs de réseaux de mobiles et par de nombreux éditeurs de logiciels, dont Microsoft. Deux solutions supplémentaires, PEAP (Protected EAP) et EAP par carte à puce, sont poussées par Microsoft pour la première et par les équipementiers de la carte à puce pour la seconde. L'annexe U détaille les différentes catégories de protocoles EAP, à l´exception d'EAP-TLS, qui est devenu le standard de base et que nous examinons ci-après.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)

L'authentification EAP-TLS (Transport Layer Security) est devenue la technique d'authentification la mieux reconnue et est considérée comme l'une des plus solides grâce à l'authentification mutuelle qui est exercée. En fait, TLS n'est qu'une extension de la procédure SSLv3, qui est fortement utilisée pour les authentifications de niveau application entre client et serveur Web.

Cette solution EAP-TLS est celle qui a été choisie par de très nombreuses entreprises. Microsoft, par exemple, en possède une version en standard dans son système d'exploitation depuis Windows 2000.

Défini par la RFC 2716 d'octobre 1999, EAP-TLS s'appuie sur une infrastructure de type PKI. Le serveur RADIUS et le client du réseau sont munis de certificats délivrés par une autorité de certification (Certificate Authority) commune.

Le format du paquet EAP-TLS est illustré à la figure 29.20.

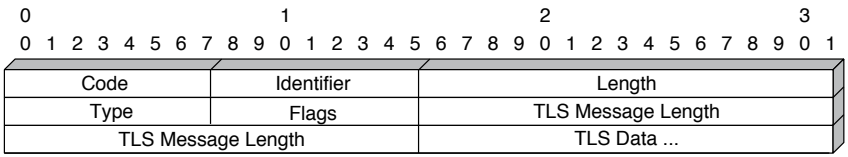


Figure 29.20
Paquet EAP/TLS

EAP-TLS utilise le handshake TLS pour permettre au client et au serveur d'échanger leur certificat numérique, fondement de l'authentification. Le serveur présente un certificat au client, que ce dernier valide. Optionnellement, le client présente son certificat au serveur. Le certificat peut être protégé côté client par un mot de passe ou un code PIN.

Une conversation EAP-TLS entre un client demandant un accès au réseau et le point d'accès se déroule de la façon suivante :

1. Le point d'accès envoie un paquet EAP-REQUEST/IDENTITY.
2. Le client répond par un paquet EAP-RESPONSE/IDENTITY, contenant l'identité de l'utilisateur.

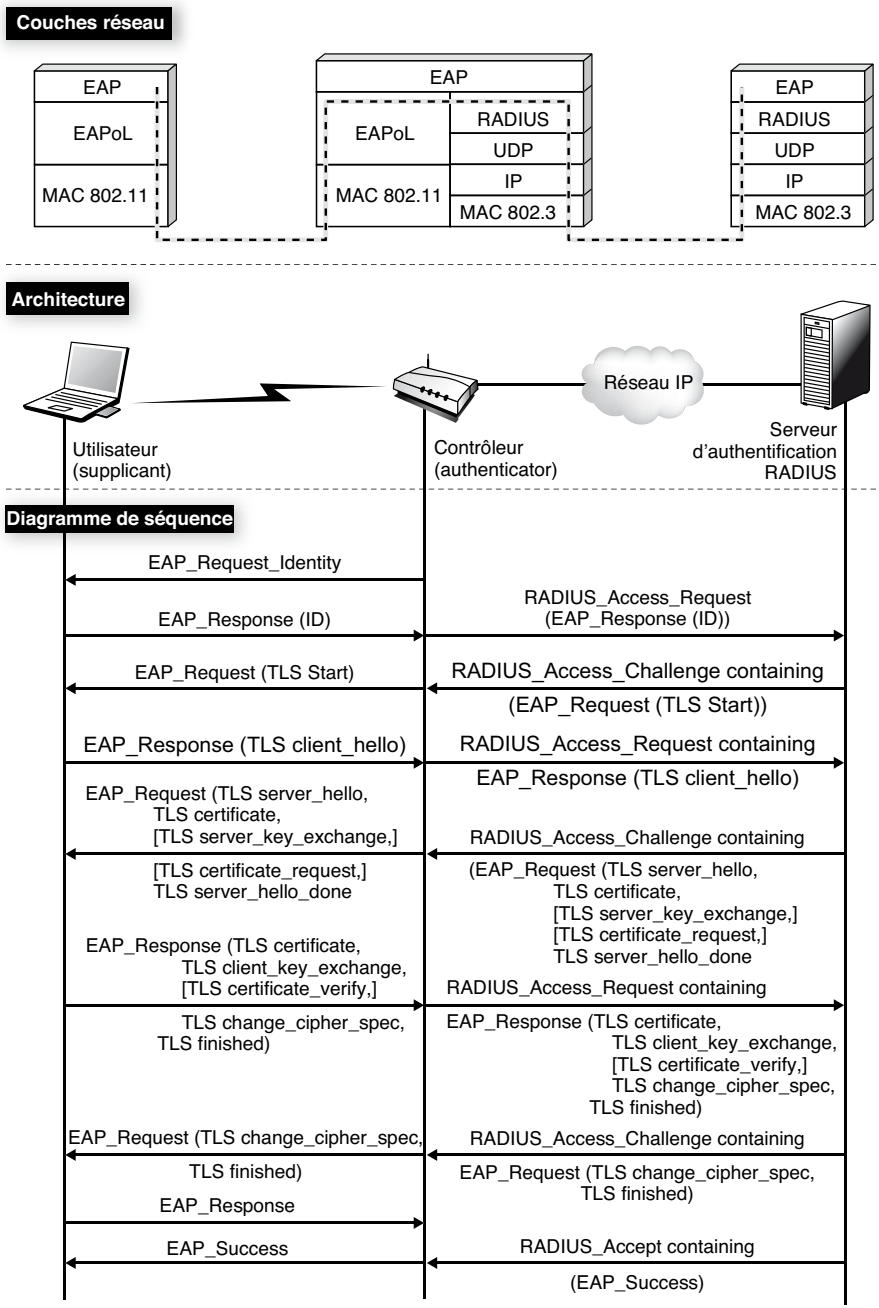


Figure 29.21

Authentification EAP-TLS

3. Le serveur envoie un paquet EAP-TLS/START.
4. La réponse du client est un paquet EAP-RESPONSE contenant un message TLS CLIENT_HELLO HANDSHAKE. Le message CLIENT_HELLO contient la version TLS du client, un nombre aléatoire et une liste d'algorithmes de chiffrement supportés par le client.
5. Le serveur envoie un paquet EAP-REQUEST dont les données contiennent un message SERVER_HELLO HANDSHAKE. Ce message spécifie la version de TLS du serveur, un autre nombre aléatoire, un identifiant de session et un message CIPHERSUITE correspondant à l'algorithme de chiffrement choisi.
6. Le client répond par un paquet EAP-RESPONSE, dont le champ de données encapsule un message TLS_CHANGE_CIPHER_SPEC et un message FINISHED_HANDSHAKE.

La figure 29.21 illustre les différents messages envoyés lors de la phase d'authentification. Ce cas représente une authentification réussie entre l'authentifiant et le client.

Le TLS Master Secret, ou MSK (Master Session Key), est le secret partagé entre le client et le serveur, résultat de la phase de handshake.

Les données suivantes sont dérivées à partir de MSK :

- clé de chiffrement client (MSK(0,31)) ;
- clé de chiffrement serveur (MSK(32,63)) ;
- clé d'authentification client pour le calcul du MAC côté client (MSK(64,95)) ;
- clé d'authentification serveur pour le calcul du MAC côté serveur (MSK(96,127)) ;
- deux vecteurs d'initialisation (IV).

La hiérarchie des clés dérivées est illustrée à la figure 29.22.

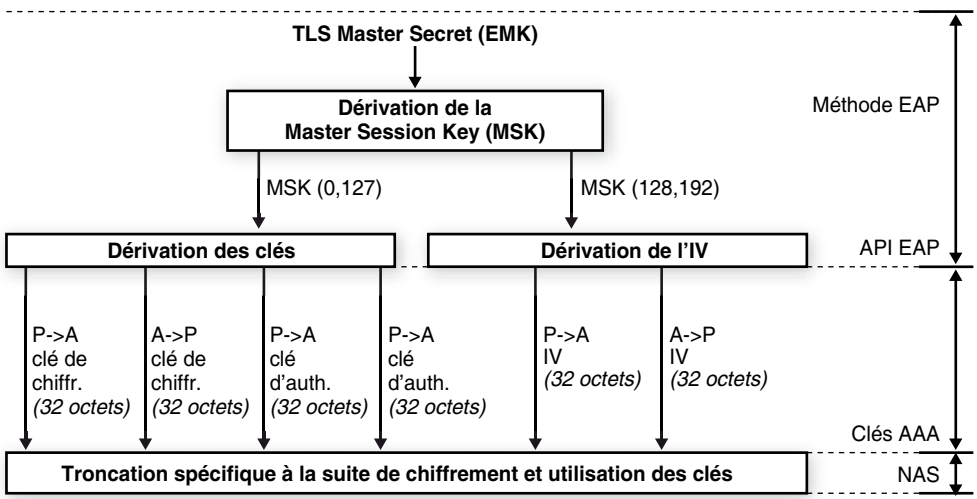


Figure 29.22

Schéma de dérivation des clés dans EAP-TLS

La clé de chiffrement client, aussi appelée PMK (Pairwise Master Key), est transmise au point d'accès *via* l'attribut RADIUS MS-MPPE-RECV-KEY. La clé WEP sera chiffrée avec cette clé puis signée avant d'être remise au client.

Le serveur d'authentification peut vérifier si le certificat d'un client est révoqué. Inversement, le client peut vérifier la validité du certificat du serveur. Cette vérification ne peut toutefois s'effectuer qu'une fois la phase de connexion achevée. En effet, un client en train d'initier une conversation de niveau liaison n'a pas de connectivité.

Le transport de messages TLS pose essentiellement un problème de segmentation. La taille d'un enregistrement TLS est d'au plus 16 384 octets, mais le protocole RADIUS limite sa charge utile à 4 096 octets. De surcroît, la taille des trames 802.11 est limitée à 2 312 octets. EAP-TLS doit donc supporter un mécanisme de segmentation des enregistrements. Contrairement à l'usage courant de TLS, mettant en œuvre une authentification simple du serveur, EAP-TLS utilise une authentification mutuelle entre le serveur RADIUS et le client 802.1x (*voir figure 29.23*).

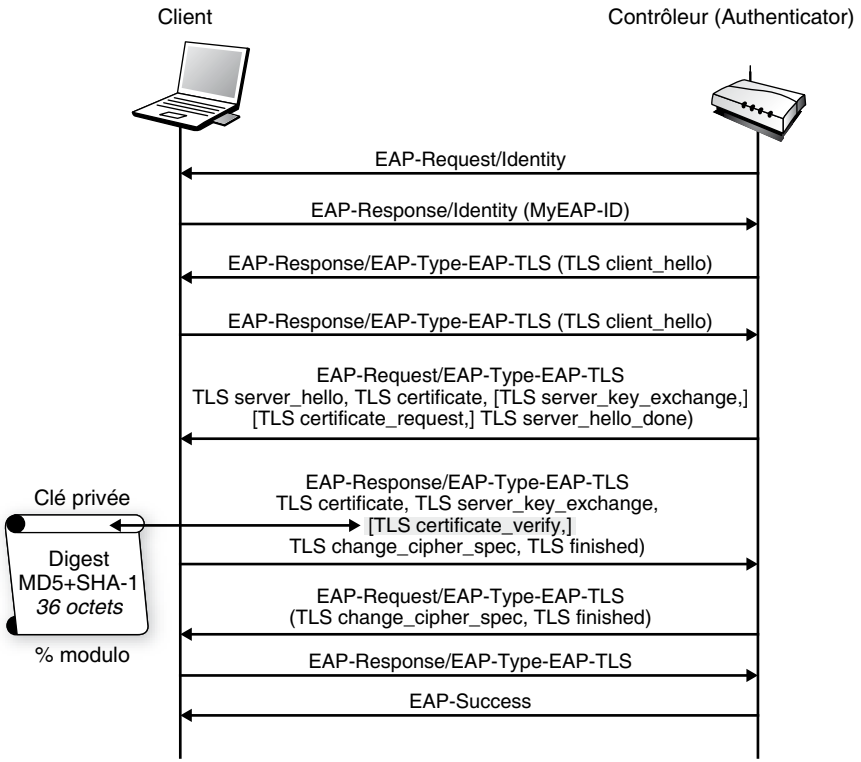


Figure 29.23
Authentification mutuelle EAP-TLS

L'usage d'une clé privé par le client 802.1x soulève le problème critique de la sécurité requise par son stockage ainsi que de la mise en œuvre d'un tel composant. Dans les plates-formes informatiques usuelles, cette sécurité est assurée par des mots de passe permettant de déchiffrer et d'utiliser la clé privée. La carte à puce constitue une solution de rechange plus sécurisée à cette méthode.

L'utilisation de l'authentification à base de certificats numériques oblige à posséder une infrastructure PKI convenable. Si une telle infrastructure n'est pas déployée, les certificats client entraînent un surplus important de gestion. Toutefois, EAP/TLS est nativement supporté sur les plates-formes Windows, où le certificat client peut être stocké dans une carte à puce.

RADIUS (Remote Authentication Dial-In User Server)

Quel que soit le choix du mécanisme d'authentification entre le client et le serveur d'authentification, les paquets EAP sont généralement acheminés grâce au protocole RADIUS. RADIUS est depuis longtemps le protocole AAA (Authentication, Authorization, Accounting) le plus largement adopté. Utilisé par les FAI pour authentifier les utilisateurs, il est principalement conçu pour transporter des données d'authentification, d'autorisation et de facturation entre des NAS (Network Access Server) distribués, qui désirent authentifier leurs utilisateurs et un serveur d'authentification partagé.

RADIUS utilise une architecture client-serveur qui repose sur le protocole UDP. Les NAS, qui jouent le rôle de client, sont responsables du transfert des informations envoyées par l'utilisateur vers les serveurs RADIUS. Ces derniers prennent en charge la réception des demandes d'authentification, l'authentification des utilisateurs et les réponses contenant toutes les informations de configuration nécessaires aux NAS. Les serveurs RADIUS peuvent également agir comme proxy pour d'autres serveurs RADIUS.

Si un équipement mobile a besoin d'accéder au réseau en utilisant RADIUS pour l'authentification, il doit présenter au NAS des crédits d'authentification (identifiant utilisateur, mot de passe, etc.). Ce dernier les transmet au serveur RADIUS en lui envoyant un ACCESS-REQUEST. Le NAS et les proxy RADIUS ne peuvent interpréter ces crédits d'authentification car ces derniers sont chiffrés entre l'utilisateur et le serveur RADIUS destinataire. À réception de cette requête, le serveur RADIUS vérifie l'identifiant du NAS puis les crédits d'authentification de l'utilisateur dans une base de données LDAP (Lightweight Directory Access Protocol) ou autre.

Les données d'autorisation échangées entre le client (le NAS) et le serveur RADIUS sont toujours accompagnées d'un secret partagé. Ce secret est utilisé pour vérifier l'authenticité et l'intégrité de chaque paquet entre le NAS et le serveur.

La figure 29.24 illustre le format type d'un paquet RADIUS. L'authentifiant du message sur 128 bits n'est autre qu'un résumé HMAC-MD5 du paquet échangé, calculé à l'aide du secret partagé.

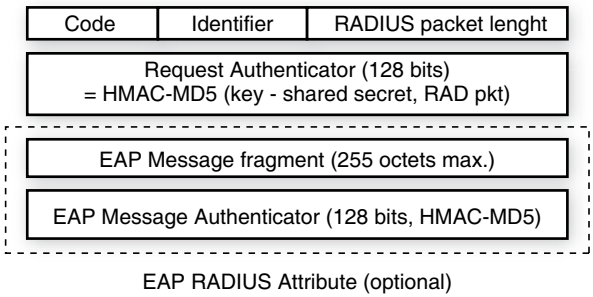


Figure 29.24
Format type d'un paquet RADIUS

RADIUS peut supporter plusieurs mécanismes d'authentification. Il peut utiliser, par exemple, des procédures de défi/réponse (Chap) et des messages ACCEPT-CHALLENGE. L'authentification par mot de passe, ou PAP (Password Authentication Protocol), est aussi prise en charge. Les serveurs RADIUS répondent aux demandes d'authentification par des messages ACCESS-ACCEPT ou ACCESS-REJECT. Les paquets ACCESS-ACCEPT fournissent les informations de configuration nécessaires pour autoriser les clients RADIUS à commencer une connexion sécurisée avec des utilisateurs.

Les pare-feu

Un pare-feu est un équipement de réseau, la plupart du temps de type routeur, placé à l'entrée d'une entreprise afin d'empêcher l'entrée ou la sortie de paquets non autorisés par l'entreprise. La situation géographique d'un pare-feu est illustrée à la figure 29.25.

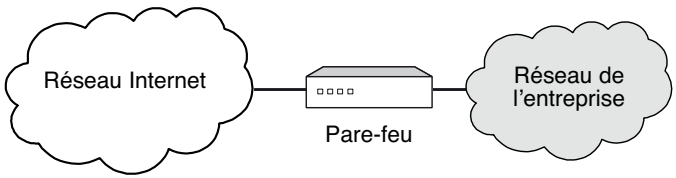


Figure 29.25
Situation d'un pare-feu dans l'entreprise

Toute la question est de savoir comment reconnaître les paquets à accepter et à refuser. Il est possible de travailler de deux façons :

- interdire tous les paquets sauf ceux d'une liste prédéterminée ;
- accepter tous les paquets sauf ceux d'une liste prédéterminée.

En règle générale, un pare-feu utilise la première solution en interdisant tous les paquets, sauf ceux qu'il est possible d'authentifier par rapport à une liste de paquets que l'on souhaite laisser entrer. Cela comporte toutefois un inconvénient : lorsqu'un client de l'entreprise se connecte sur un serveur à l'extérieur, la sortie par le pare-feu est acceptée puisque authentifiée. La réponse est généralement refusée, puisque le port sur lequel elle se présente n'a aucune raison d'accepter ce message s'il est bloqué par mesure de sécurité. Pour que la réponse soit acceptée, il faudrait que le serveur puisse s'authentifier et que le pare-feu lui permette d'accéder au port concerné.

L'autre option est évidemment beaucoup plus dangereuse puisque tous les ports sont ouverts sauf ceux qui ont été bloqués. Une attaque ne se trouve pas bloquée tant qu'elle n'utilise pas les accès interdits.

Quelques ports réservés TCP		
N° de port	**Service**	**Rôle**
1	tcpmux	Multiplexeur de service TCP
3	compressnet	Utilitaire de compression
7	echo	Fonction écho
9	discard	Fonction d'élimination
11	users	Utilisateurs
13	daytime	Jour et heure
15	netstat	État du réseau
20	ftp-data	Données du protocole FTP
21	ftp	Protocole FTP
23	telnet	Protocole Telnet
25	smtp	Protocole SMTP
37	heure	Serveur heure
42	name	Serveur nom d'hôte
43	whols	Nom NIC
53	domain	Serveur DNS
77	rje	Protocole RJE
79	finger	Finger
80	http	Service WWW
87	link	Liaison TTY
103	X400	Messagerie X.400
109	pop	Protocole POP
144	news	Service News
158	tcprepo	Répertoire TCP
Quelques ports réservés UDP		
7	echo	Service écho
9	rejet	Service de rejet
53	dsn	Serveur de nom de domaine
67	dhcp	Serveur de configuration DHCP
68	dhcp	Client de configuration DHCP

TABLEAU 29.2 • Principaux ports TCP et UDP

Avant d'aller plus loin, considérons les moyens d'accepter ou de refuser des flots de paquets. Les filtres permettent de reconnaître un certain nombre de caractéristiques des paquets, comme l'adresse IP d'émission, l'adresse IP de réception, parfois les adresses de niveau trame, le numéro de port et plus généralement tous les éléments disponibles dans l'entête du paquet IP. Pour ce qui concerne la reconnaissance de l'application, les filtres sont essentiellement réalisés sur les numéros de port utilisés par les applications. Nous verrons toutefois un peu plus loin que cette solution n'est pas imparable. Un numéro de port est en fait une partie d'un numéro de socket, ce dernier étant, comme expliqué au chapitre précédent, la concaténation d'une adresse IP et d'un numéro de port. Les numéros de port correspondent à des applications. Les principaux ports sont recensés au tableau 29.2.

Un pare-feu contient donc une table, qui indique les numéros de port acceptés.

Le tableau 29.3 donne la composition d'un pare-feu classique, dans lequel seulement six ports sont ouverts, dont l'un ne l'est que pour une adresse de réseau de classe C spécifique.

Port accepté	Adresse IP
21	*
23	*
25	Adresse réseau C – adresse réseau B
43	*
69	*
79	*

TABLEAU 29.3 • Composition d'un pare-feu classique

Un pare-feu contient donc une table, qui indique les numéros de port acceptés.

Le tableau 29.3 donne la composition d'un pare-feu classique, dans lequel seulement six ports sont ouverts, dont l'un ne l'est que pour une adresse de réseau de classe C spécifique.

Les pare-feu peuvent être de deux types, proxy et applicatif. Dans le premier cas, le pare-feu a pour objectif de couper la communication entre un client et un serveur ou entre un client et un autre client. Ce type de pare-feu ne permet pas à un attaquant d'accéder directement à la machine attaquée, ce qui donne une forte protection supplémentaire. Dans le second cas, le pare-feu détecte les flots applicatifs et les interrompt ou non suivant les éléments filtrés. Dans tous les cas, il faut utiliser des filtres plus ou moins puissants.

Les filtres

Comme expliqué précédemment, les filtres sont essentiellement appliqués sur les numéros de port. La gestion de ces numéros de port n'est toutefois pas simple. En effet, de plus en plus de ports sont dynamiques. Avec ces ports, l'émetteur envoie une demande sur le port standard, mais le récepteur choisit un nouveau port disponible pour effectuer la communication. Par exemple, l'application RPC (Remote Procedure Call) affecte dynamiquement les numéros de port. La plupart des applications P2P (Peer-to-Peer) ou de signalisation de la téléphonie sont également dynamiques.

L'affectation dynamique de port peut être contrôlée par un pare-feu qui se comporte astucieusement. La communication peut ainsi être suivie à la trace, et il est possible de découvrir la nouvelle valeur du port lors du retour de la demande de transmission d'un message TCP. À l'arrivée de la réponse indiquant le nouveau port, il faut détecter le numéro du port qui remplace le port standard. Un cas beaucoup plus complexe est possible, dans lequel l'émetteur et le récepteur se mettent directement d'accord sur un numéro de port. Dans ce cas, le pare-feu ne peut détecter la communication, sauf si tous les ports sont bloqués. C'est la raison essentielle pour laquelle les pare-feu n'acceptent que des communications déterminées à l'avance.

Cette solution de filtrage et de reconnaissance des ports dynamiques n'est toutefois pas suffisante, car il est toujours possible pour un pirate de transporter ses propres données à l'intérieur d'une application standard sur un port ouvert. Par exemple, un tunnel peut être réalisé sur le port 80, qui gère le protocole HTTP. À l'intérieur de l'application HTTP, un flot de paquets d'une autre application peut passer. Le pare-feu voit entrer une application HTTP, qui, en réalité, délivre des paquets d'une autre application.

Une entreprise ne peut pas bloquer tous les ports, sans quoi ses applications ne pourraient plus se dérouler. On peut bien sûr essayer d'ajouter d'autres facteurs de détection, comme l'appartenance à des groupes d'adresses IP connues, c'est-à-dire à des ensembles d'adresses IP qui ont été définies à l'avance. De nouveau, l'emprunt d'une adresse connue est assez facile à mettre en œuvre. De plus, les attaques les plus dangereuses s'effectuent par des ports qu'il est impossible de bloquer, comme le port DNS. Une des attaques les plus dangereuses s'effectue par un tunnel sur le port DNS. Encore faut-il que la machine réseau de l'entreprise qui gère le DNS ait des faiblesses pour que le tunnel puisse se terminer et que l'application pirate s'exprime dans l'entreprise. Nous verrons à la section suivante comment il est possible de renforcer la sécurité des pare-feu.

Pour sécuriser l'accès à un réseau d'entreprise, une solution beaucoup plus puissante consiste à filtrer non plus aux niveaux 3 ou 4 (adresse IP ou adresse de port) mais au niveau applicatif. Cela s'appelle un filtre applicatif. L'idée est de reconnaître directement sur le flot de paquets l'identité de l'application plutôt que de se fier à des numéros de port. Cette solution permet d'identifier une application insérée dans une autre et de reconnaître les applications sur des ports non conformes. La difficulté avec ce type de filtre réside dans la mise à jour des filtres chaque fois qu'une nouvelle application apparaît. Le pare-feu muni d'un tel filtre applicatif peut toutefois interdire toute application non reconnue, ce qui permet de rester à un niveau de sécurité élevé.

La sécurité autour du pare-feu

Comme nous l'avons vu, le pare-feu vise à filtrer les flots de paquets sans empêcher le passage des flots utiles à l'entreprise, flots que peut essayer d'utiliser un pirate. La structure de l'entreprise peut être conçue de différentes façons. Deux solutions générales sont mises en œuvre. La première est illustrée à la figure 29.26, et la seconde à la figure 29.27.

Dans le premier cas, la communication, après avoir traversé le pare-feu, se dirige au travers du réseau d'entreprise vers le poste de travail de l'utilisateur. Dans ce cas, il faut que les postes de travail de l'utilisateur soient des machines sécurisées afin d'empêcher les flots pirates qui auraient réussi à passer le pare-feu d'entrer dans des failles du système de la station. Comme cette solution est très difficile à sécuriser, puisqu'elle dépend de l'ensemble des utilisateurs d'une entreprise, la plupart des architectes réseau préfèrent mettre en entrée de réseau une machine sécurisée, que l'on appelle machine bastion (*voir figure 29.27*).

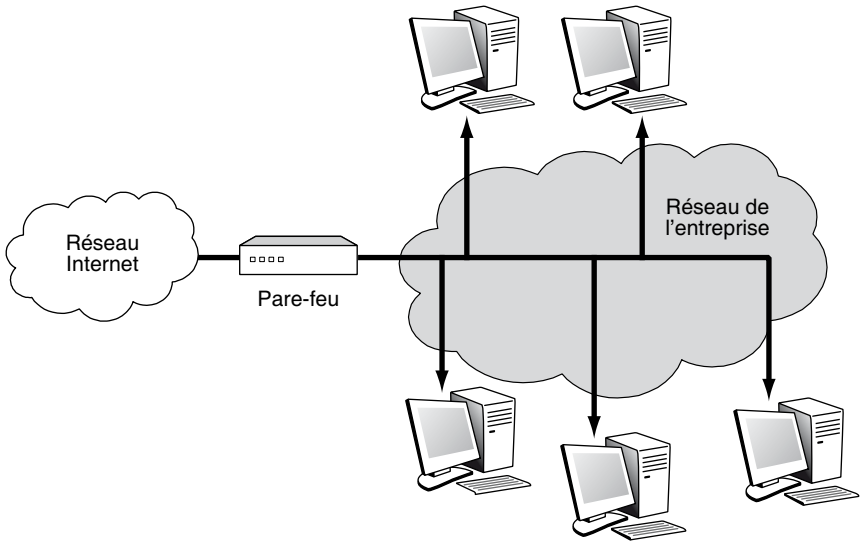


Figure 29.26

Place d'un pare-feu dans l'infrastructure réseau

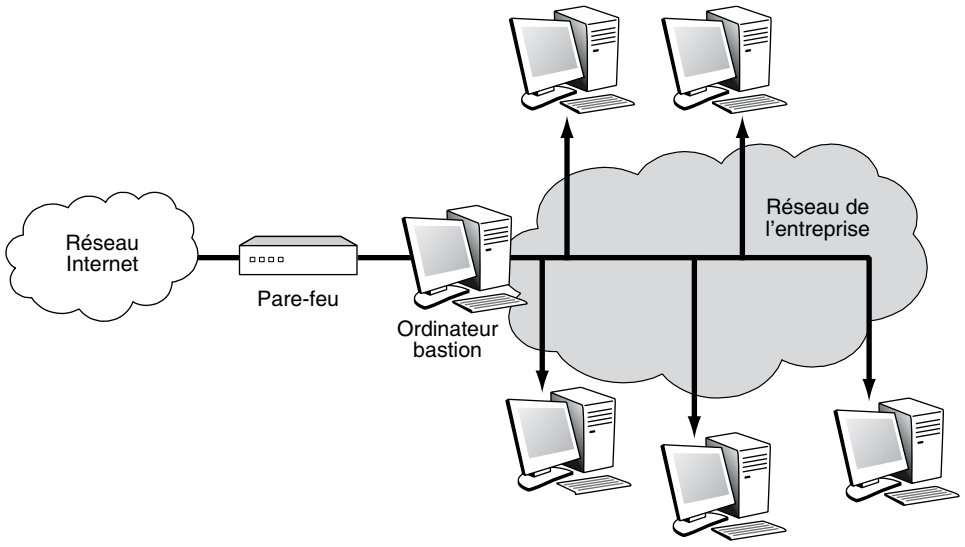


Figure 29.27

Pare-feu associé à une machine bastion

La machine bastion apporte quelques difficultés supplémentaires de gestion. En effet, elle prend en charge l'ouverture et la fermeture des communications d'un utilisateur avec l'extérieur. Par exemple, un client avec son navigateur ne peut plus accéder à un serveur

externe puisque la machine bastion l'arrête automatiquement. Le bastion doit être équipé d'un serveur proxy, et chaque navigateur être configuré pour utiliser le proxy. La communication se fait donc en deux temps. L'utilisateur communique avec son proxy, et celui-ci ouvre une communication avec le serveur distant. Lorsqu'une page parvient au proxy, ce dernier peut la distribuer au client. Le bastion peut d'ailleurs servir de cache pour les pages standards utilisées par une entreprise.

Le défaut de cette dernière architecture provient de sa relative lourdeur, puisqu'il est demandé à une machine spécifique d'effectuer le travail réseau pour toutes les machines de l'entreprise. De plus, la sécurité de toute l'entreprise peut être menacée si l'ordinateur bastion n'est pas parfaitement sécurisé, car un pirate externe peut avoir accès à l'ensemble des ressources de l'entreprise. De fait, l'architecture de sécurité peut s'avérer plus complexe lorsqu'un ordinateur bastion est mis en place.

La figure 29.28 illustre quelques-unes des architectures de sécurité qui peuvent être mises en place.

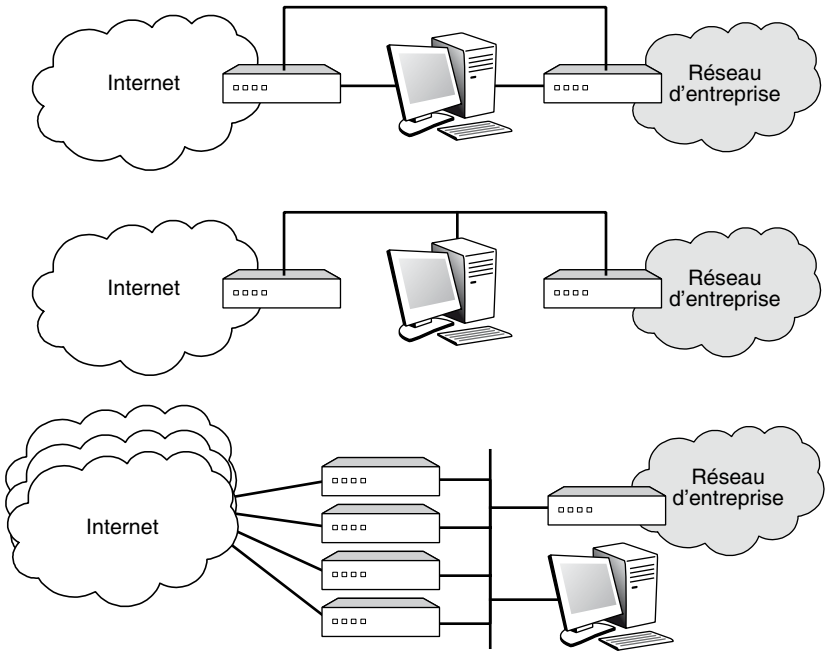


Figure 29.28

Architectures de sécurité avec machine bastion

La partie supérieure de la figure représente une organisation assez classique, dans laquelle l'ordinateur bastion est protégé des deux côtés par des pare-feu, pour filtrer aussi bien ce qui arrive de l'entreprise que ce qui arrive de l'extérieur. Le schéma montre deux pare-feu. Il est possible d'utiliser un seul pare-feu connecté à l'ordinateur bastion. Il est aussi

possible de mettre en place manuellement une connexion directe entre les deux pare-feu pour effectuer des tests et des mises au point.

La deuxième partie de la figure est assez semblable à la précédente. Elle montre toutefois une organisation un peu différente, utilisant un réseau local pour relier les deux pare-feu et l'ordinateur bastion. La troisième partie de la figure montre une architecture encore plus complexe, dans laquelle une entreprise peut accéder à plusieurs opérateurs simultanément. Dans ce cas, un pirate peut entrer dans le réseau d'un opérateur en provenance d'un autre opérateur en passant par la passerelle d'une entreprise. Là, le piratage ne vise pas l'entreprise mais une autre entreprise, située sur le réseau de l'opérateur piraté. Pour sécuriser ce passage, l'ordinateur bastion doit de nouveau jouer le rôle de proxy, empêchant le passage direct.

Conclusion

La sécurité dans Internet est un problème complexe pour la simple raison qu'elle n'a pas été introduite en même temps que les protocoles de base. Pour arriver à vendre des produits rapidement, les équipementiers ont laissé la sécurité de côté en pensant pouvoir facilement l'ajouter par la suite. En réalité, l'effort à faire pour ajouter les éléments de sécurité dans un environnement qui n'a pas été conçu pour cela pose de nombreux problèmes, dont les utilisateurs prennent conscience peu à peu.

Des efforts énormes sont déployés en ce sens depuis une dizaine d'années. Toutefois, même si l'on dispose maintenant de toute une batterie d'outils pour assurer la sécurité d'un réseau IP, ils ne sont généralement pas faciles à utiliser.

Partie VIII

Les nouvelles générations

Sous ce titre général de nouvelles générations, nous souhaitons introduire des applications qui deviennent primordiales et de nouveaux outils pour le contrôle et la gestion des réseaux.

Nous commencerons, au chapitre 30, par les applications en nous focalisant sur deux des plus importantes : la téléphonie et la télévision sous IP. Les autres applications sont détaillées à l'annexe V. Nous examinons au chapitre 31 l'intelligence dans les réseaux, qui apporte des outils très intéressants pour la gestion et le contrôle dans le but d'automatiser ces fonctions.

La virtualisation est devenue primordiale en matière de réseau après avoir conquis le marché des serveurs et des systèmes. Nous introduisons cette technologie au chapitre 32. Ce dernier chapitre fait aussi le point sur le Post-IP, c'est-à-dire l'après IP. Un grand mouvement a été lancé vers 2007 pour tenter de deviner ce que sera le futur des réseaux en repartant de zéro. Enfin, nous aborderons le Cloud, un paradigme fort qui devrait s'étendre dans les années qui viennent.

30

ToIP et IPTV

Les applications de téléphonie et de télévision sont devenues les applications dominantes du monde des réseaux, et elles le resteront pendant de nombreuses années en raison notamment de l'émergence de nouveaux et immenses marchés, comme celui de la Chine. Proportionnellement, le débit de la téléphonie décroît, même si l'ensemble des communications devrait être en VoIP (Voice over IP) en 2015. Au contraire, le débit des applications vidéo, en particulier de la télévision, augmente fortement au point que cette application est devenue prépondérante sur Internet.

La parole téléphonique a été traditionnellement prise en charge par les réseaux à commutation de circuits, mais le passage vers les réseaux à transfert de paquets, essentiellement de type IP, est inéluctable. En 2010, quasiment l'ensemble des communications téléphonique s'effectuent en mode paquet. Le passage au tout-IP permet d'intégrer les services de données et de téléphonie dans un même réseau. Beaucoup d'entreprises intègrent leur environnement téléphonique dans leur réseau à transfert de paquets pour, d'une part, faire baisser les coûts des communications, mais aussi, d'autre part, simplifier la maintenance en passant de deux réseaux à gérer (téléphonie et données) à un seul (données).

La télévision sur IP (IPTV) ne cesse de s'étendre, de même que le nombre de chaînes. Nous examinerons les principes du transport de la télévision sur Internet.

Le chapitre commence par examiner l'évolution de la téléphonie vers les réseaux Internet et intranet puis traite de l'arrivée massive de la télévision et plus généralement de la vidéo sur IP.

L'application téléphonique

La difficulté de faire de la téléphonie par paquet provient de la très forte contrainte temporelle résultant de l'interaction entre individus. Le temps de latence doit être inférieur à 300 ms si l'on veut garder une interaction humaine acceptable. Si l'on souhaite une bonne qualité de la conversation, il ne faut pas que la latence soit supérieure à 150 ms. Un cas encore plus complexe se produit lorsqu'il y a un écho, c'est-à-dire un signal qui revient à l'oreille de l'émetteur. L'écho se produit lorsque le signal rencontre un obstacle, comme l'arrivée sur le combiné téléphonique. L'écho qui repart en sens inverse est numérisé par un codec et traverse sans problème un réseau numérique. La valeur normalisée de la latence de l'écho étant de 56 ms, pour que l'écho ne soit pas gênant à l'oreille, il ne faut pas que le temps aller dépasse 28 ms, en supposant un réseau symétrique qui prend le même temps de réponse à l'aller et au retour. Il faut donc que, dans les équipements terminaux, les logiciels extrémité soient capables de gérer les retards et de resynchroniser les octets qui arrivent. En règle générale, les équipements modernes, comme les terminaux GSM, possèdent des suppresseurs d'écho évitant cette contrainte temporelle forte.

La voix simple en paquet n'est pas aussi contraignante que la parole téléphonique, car elle n'implique aucune contrainte temporelle. Dans le cas d'IP, il ne faut donc pas confondre la téléphonie sur IP (ToIP) et la voix sur IP (VoIP).

L'application de téléphonie est donc complexe à prendre en charge en raison de son caractère interactif et de sa forte synchronisation. Rappelons les trois opérations successives nécessaires à la numérisation de la parole, qu'elle soit téléphonique ou non :

1. **Échantillonnage.** Consiste à prendre des points du signal analogique au fur et à mesure qu'il se déroule. Il est évident que plus la bande passante est importante, plus il faut prendre d'échantillons par seconde. C'est le théorème d'échantillonnage qui donne la solution : il faut échantillonner à une valeur égale à au moins deux fois la bande passante.
2. **Quantification.** Consiste à représenter un échantillon par une valeur numérique au moyen d'une loi de correspondance. Cette phase consiste à trouver la loi de correspondance de telle sorte que la valeur des signaux ait le plus de signification possible.
3. **Codage.** Consiste à donner une valeur numérique aux échantillons. Ce sont ces valeurs qui sont transportées dans le signal numérique.

La largeur de bande de la voix téléphonique analogique est de 3 200 Hz. Pour numériser ce signal correctement sans perte de qualité, puisqu'elle est déjà relativement mauvaise, il faut échantillonner au moins 6 400 fois par seconde. La normalisation a opté pour un échantillonnage de 8 000 fois par seconde. La quantification s'effectue par des lois semi-logarithmiques. L'amplitude maximale permise se trouve divisée en 128 échelons positifs pour la version américaine PCM, auxquels il faut ajouter 128 échelons négatifs dans la version européenne MIC. Le codage s'effectue donc soit sur 128 valeurs, soit sur 256 valeurs, ce qui demande en binaire 7 ou 8 bits de codage. La valeur totale du débit de la numérisation de la parole téléphonique s'obtient en multipliant le nombre d'échantillons par le nombre d'échelons, ce qui donne :

- 8 000 × 7 bit/s = 56 Kbit/s en Amérique du Nord et au Japon ;
- 8 000 × 8 bit/s = 64 Kbit/s en Europe.

Beaucoup d'autres solutions ont été développées par rapport aux qualités et aux défauts de l'oreille :

- AD-PCM (Adaptive Differential-Pulse Code Modulation), ou MIC-DA (Modulation par impulsion et codage-différentiel adaptatif) ;
- SBC (Sub-Band Coding) ;
- LPC (Linear Predictive Coding) ;
- CELP (Code Excited Linear Prediction).

La section suivante fait un tour d'horizon des principaux codeurs audio.

Les codeurs audio

Les codeurs audio associés aux différentes techniques citées précédemment sont nombreux. On trouve notamment les codecs classiques mais aussi de nouveaux codeurs bas débit. La figure 30.1 illustre les vitesses de sortie des différentes normes de codeurs de la voix téléphonique fondées sur un échantillonnage standard à 8 kHz. L'ordonnée représente la qualité du son en réception, qui est évidemment un critère subjectif. Nous avons aussi représenté les codeurs utilisés dans les réseaux de mobiles GSM et les normes régionales.

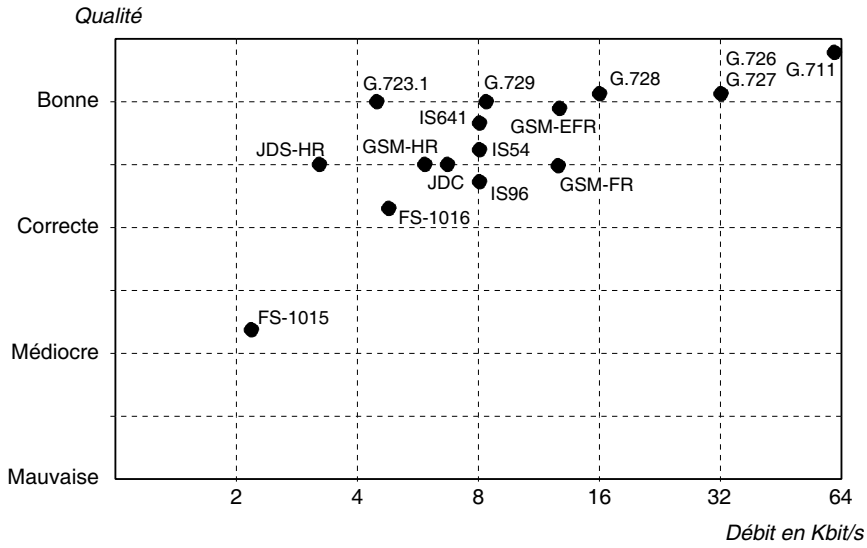


Figure 30.1

Codeurs audio

Pour l'audio haute définition, on considère une bande passante plus importante puisque l'oreille humaine est sensible aux fréquences de 20 à 20 000 Hz. L'échantillonnage s'effectue sur 40 kHz, et c'est la valeur de 44,1 kHz qui a été choisie. Le codage effectué sur un CD tient sur 16 bits par échantillon, ce qui donne 705,6 Kbit/s.

Parmi les nombreux codeurs propriétaires qui existent sur le marché, citons :

- StreamWorks à 8,5 Kbit/s
- VoxWare à 2,4 Kbit/s avec le codeur RT24
- Microsoft à 5,3 Kbit/s avec la norme G.723
- VocalTec à 7,7 Kbit/s

La recommandation G.711 correspond à la numérisation classique à 64 Kbit/s en Europe ou 56 Kbit/s en Amérique du Nord. G.723 est une compression de la parole utilisée par de nombreux industriels, entre autres Microsoft, qui l'utilise dans l'environnement Windows. Le débit descend à presque 5 Kbit/s. G.726 est la norme adoptée pour la compression de la parole en codage différentiel adaptatif en 16, 24, 32 ou 40 Kbit/s. Dans ce cas, au lieu de coder l'échantillon en entier, on n'envoie que la différence avec l'échantillon précédent, ce qui permet un codage sur beaucoup moins d'éléments binaires. G.727 utilise aussi un codage différentiel, qui apporte des compléments au codage précédent. Cette recommandation indique comment changer, en cours de numérisation, le nombre de bits utilisés pour coder les échantillons. Elle est particulièrement utile dans le cadre des réseaux qui demandent à l'application de s'adapter en fonction de la charge du réseau. G.728 est une compression à 16 Kbit/s utilisant une technique de prédiction, qui consiste à coder la différence entre la valeur réelle et une valeur estimée de l'échantillon à partir des échantillons précédents. On comprend que cette différence peut être encore plus petite que dans la technique différentielle. Si l'estimation est bonne, la valeur à transporter avoisine toujours 0. Très peu de bits sont alors nécessaires pour acheminer cette différence. Les standards FS proviennent du ministère américain de la Défense.

Les codeurs les plus récents sont G.723.1, G.729 et G.729.A. Le codeur G.723.1 permet un débit compris entre 5,3 et 6,4 Kbit/s. Les deux codeurs G.729 donnent un débit de 8 Kbit/s, mais la qualité de la communication est meilleure. Ce codec a été choisi pour compresser la voix dans l'UMTS.

La parole téléphonique est une application très contraignante, comme nous l'avons vu à plusieurs reprises dans cet ouvrage. La première contrainte provient de l'interactivité entre les deux utilisateurs, qui limite le temps aller-retour à une valeur de 600 ms au maximum. Les normes de l'UIT-T portent cette valeur à 800 ms. Cependant, pour avoir une bonne qualité de la communication, il faut descendre à 300 ms aller-retour. Suivant les protocoles sous-jacents, plusieurs méthodes permettant de satisfaire à ces contraintes ont été développées à la fin des années 1990, que nous allons examiner.

La téléphonie sur IP

La problématique du transport de la parole téléphonique dans des environnements IP est assez différente suivant que l'on est sur un réseau IP non contrôlé, comme Internet, ou sur un réseau permettant l'introduction d'un contrôle, comme le réseau privé d'une compagnie, de type intranet, ou celui d'un FAI.

Sur l'Internet de première génération, il faut que le réseau soit peu chargé pour que la contrainte de 300 ms soit respectée. Sur les réseaux intranet et ceux des fournisseurs

d'accès à Internet, mais aussi ceux des opérateurs, le passage de la parole est possible à condition de contrôler le réseau pour que le temps total de transport, y compris la paquétisation et la dépaquétisation, soit limité.

De nombreuses solutions ont été proposées, comme VoIP (Voice over IP) de l'IMTC (International Multimedia Teleconferencing Consortium). Dans ces solutions, il a d'abord fallu définir un codeur normalisé. Le choix s'est généralement porté sur G.723, mais d'autres solutions sont opérationnelles, comme le codeur G.711. Le paquet IP doit être le plus court possible, et il faut multiplexer plusieurs voies de parole dans un même paquet, de façon à raccourcir le temps de remplissage et à limiter les temps de transfert dans le réseau. Si les routeurs peuvent gérer des priorités, ce qui est possible en utilisant des services de type DiffServ, la parole téléphonique est acheminée beaucoup plus facilement dans le laps de temps demandé.

Plusieurs organismes de normalisation, de droit ou de fait, ont fortement travaillé sur ce sujet. Dans les organismes de droit, l'ETSI, l'organisme de normalisation européen, a mis sur pied le groupe TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks). Ce groupe a défini la parole et le fax entre utilisateurs connectés, en particulier sur des réseaux IP. Le cas où un utilisateur travaille sur un réseau IP et un autre sur un réseau à commutation de circuits, qu'il soit téléphonique, RNIS, GSM ou UMTS, entre également dans le cadre des études de TIPHON. Les activités de TIPHON concernent en outre la validation de solutions pour transporter la parole téléphonique par le biais de démonstrateurs.

L'UIT-T travaille de son côté activement sur le problème de la téléphonie sur IP dans trois groupes du SG 16 : le WP1 pour les modems (série V), le WP2 pour les codecs (série G) et le WP3 pour les terminaux (série H). L'objectif de l'UIT-T est de finaliser un environnement complet et non pas simplement un terminal ou un protocole.

Au sein de l'IETF, de nombreux groupes de travail se sont attaqués à cette problématique, parmi lesquels :

- AVT (Audio Video Transport), qui utilise le protocole RTP (RFC 1889 et 1890) pour effectuer la communication en temps réel.
- MMUSIC (Multiparty Multimedia Session Control), qui utilise le protocole SIP.
- IPTel (IP Telephony), qui définit un protocole de localisation des passerelles et un langage permettant de mettre en communication des circuits et des flots IP.
- PINT (PSTN IP Internetworking), qui utilise également le protocole SIP.
- FAX (Fax over IP), qui stocke et émet des fax par l'intermédiaire de messages électroniques.
- MEGACO (Media Gateway Control), qui détermine un protocole entre une passerelle et son contrôleur.
- SIGTRAN (Signal Translation), qui propose l'utilisation du passage des commandes de la signalisation CCITT n° 7 dans des paquets IP.
- ENUM (E.164/IP translations), qui gère les translations d'adresses E.164 vers des adresses IP.

Respecter la contrainte temporelle est une première priorité pour le transport de la parole téléphonique. Une seconde priorité concerne la mise en place d'une signalisation pour mettre en connexion les deux utilisateurs qui veulent se parler.

Les protocoles de signalisation utilisés pour le transport et la gestion de la parole sous forme de paquets IP regroupent essentiellement H.323 et SIP (Session Initiation Protocol). La signalisation H.323 a été définie dans un environnement de télécommunications, à la différence de SIP, qui provient de l'informatique et plus spécifiquement du Web. SIP peut utiliser le code HTTP ainsi que la sécurité qui y est liée. Il peut en outre s'accommoder des pare-feu de protection. SIP met en place des sessions, qui ne sont que des appels téléphoniques entre un client et un serveur. Comme nous l'avons vu, six primitives HTTP sont utilisées pour cela : INVITE, BYE, OPTIONS, ACK, REGISTER et CANCEL.

La VoIP est devenue une application classique grâce aux possibilités de numérisation et à la puissance des PC, qui permettent d'annuler les échos. L'élément le plus contraignant reste le délai, surtout lorsqu'il faut traverser des terminaux de type PC, des modems, des réseaux d'accès, des passerelles, des routeurs, etc.

On peut considérer que le PC demande un temps de traversée d'une centaine de millisecondes, le modem de quelques dizaines de millisecondes, la passerelle également d'une centaine de millisecondes et le réseau IP de quelques dizaines de millisecondes. Le total montre que la limite des 300 ms pour avoir une interactivité est rapidement atteinte. Si l'on dépasse les 150 ms de transit et que l'on s'approche des 300 ms, la qualité de la communication s'en ressent, comme lors d'une conversation par satellite.

Détaillons la mise en place de la communication. Il faut utiliser une signalisation pour mettre en place la session. Premier élément, la localisation du récepteur (User Location) s'effectue par une mise en correspondance de l'adresse du destinataire (adresse IP ou téléphonique classique) en une adresse IP. Le protocole DHCP et les passerelles spécialisées sont des éléments de solution pour déterminer les adresses des récepteurs. L'établissement de la communication passe par une acceptation du terminal destinataire, que ce soit un téléphone, une boîte vocale ou un serveur Web. Comme nous l'avons vu, plusieurs protocoles de signalisation peuvent être utilisés, comme SIP, de l'IETF, ou H.323, de l'UIT-T.

Les protocoles de signalisation

Nous avons déjà examiné en détail le protocole SIP au chapitre 27. Rappelons quelques éléments de ce protocole avant d'aborder SDP et surtout RTP-RTCP.

Comme son nom l'indique, SIP (Session Initiation Protocol) est utilisé pour initialiser la session. Une requête SIP contient un ensemble d'en-têtes qui décrivent l'appel, suivis du corps du message, contenant la description de la demande de session. SIP est un protocole client-serveur, qui utilise la syntaxe et la sémantique de HTTP. Le serveur gère la demande et fournit une réponse au client.

Trois types de serveurs gèrent différents éléments : un serveur d'enregistrement (Registration Server), un serveur relais (Proxy Server) et un serveur de redirection (Redirect Server). Ces serveurs travaillent à trouver la route. Le serveur proxy détermine le prochain serveur (Next-Hop Server), qui, lui-même, trouve le suivant, et ainsi de suite. Des

champs supplémentaires de l'en-tête précisent les options, comme le transfert d'appel ou la gestion de conférence téléphonique.

Le protocole SDP (Session Description Protocol) est utilisé pour décrire les sessions multimédias pour la partie téléphonique mais aussi pour d'autres applications distribuées, comme la radio sur Internet.

SDP permet le transfert de nombreuses informations, notamment les suivantes :

- flots correspondant aux médias de l'application ;
- pour chaque flot, adresse de destination, unicast ou multicast ;
- pour chaque flot, numéro de port UDP ;
- type de charge transportée ;
- instants de synchronisation (par exemple, l'instant de début d'un programme de télévision diffusée) ;
- origine de la demande de communication.

Le protocole RTP (Real-time Transport Protocol) prend le relais pour le transport de l'information proprement dite. Son rôle est d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie pour reformer le flot avec ses caractéristiques (synchronisme, perte, etc.). C'est un protocole qui travaille au niveau transport et essaye de corriger les défauts apportés par le réseau.

Les fonctions de RTP sont les suivantes :

- Le séquencement des paquets par une numérotation permettant de détecter les paquets perdus, ce qui est essentiel pour la recomposition de la parole. La perte d'un paquet n'est pas en soi un problème, s'il n'y en a pas trop de perdus. En revanche, repérer qu'un paquet a été perdu est impératif car il faut en tenir compte et éventuellement le remplacer par une synthèse déterminée en fonction des paquets précédant et suivant.
- L'identification de ce qui est transporté dans le message pour permettre, par exemple, une compensation en cas de perte.
- La synchronisation entre médias, grâce à des estampilles.
- L'indication de tramage. Les applications audio et vidéo sont transportées dans des trames dont la dimension dépend des codecs effectuant la numérisation. Ces trames sont incluses dans les paquets pour être transportées et doivent être récupérées facilement au moment de la dépaquétisation afin que l'application soit décodée simplement.
- L'identification de la source. Dans les applications en multicast, l'identité de la source doit être déterminée.

RTP utilise le protocole RTCP (Real-Time Control Protocol) pour transporter les informations supplémentaires suivantes pour la gestion de la session :

- Retour de la qualité de service lors de la demande de session. Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs des rapports sur la QoS. Ces rapports comprennent le nombre de paquets perdus, la gigue et le délai aller-retour. Ces informations permettent à la source de s'adapter, c'est-à-dire, par exemple, de modifier le degré de compression pour maintenir la QoS.

- Synchronisation supplémentaire entre médias. Les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la voix et l'image, ou même une application numérisée sur plusieurs niveaux hiérarchiques, peuvent voir les flots générés suivre des chemins distincts.
- Identification. Les paquets RTCP contiennent des informations d'adresse, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- Contrôle de la session. RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement une indication de leur comportement.

Le protocole RTCP demande aux participants de la session d'envoyer périodiquement ces informations. La périodicité est calculée en fonction du nombre de participants à l'application.

Un autre protocole utilisable est RTSP (Real-Time Streaming Protocol), dont le rôle est de contrôler une communication entre deux serveurs où sont stockées des informations multimédias audio et vidéo. RTSP offre des commandes assez semblables à celles d'un magnétoscope, telles qu'avance, avance rapide, retour, pause, etc. Ce protocole peut être très utile dans le cadre de la téléphonie sur IP en permettant l'enregistrement d'une téléconférence pour la réentendre ultérieurement, la vision d'une séquence vidéo, l'enregistrement de message téléphonique, etc.

Un autre point important pour réaliser la communication de l'émetteur vers le récepteur concerne les fonctionnalités de la passerelle permettant de passer d'un réseau à transfert de paquets à un réseau à commutation de circuits, avec les problèmes d'adressage, de signalisation et de transcodage que cela pose. Ces passerelles se démultiplient entre FAI et opérateurs télécoms.

Pour finaliser l'ouverture d'un appel, le protocole SIP envoie une requête à la passerelle. Le premier problème est de déterminer quelle passerelle est capable de réaliser la liaison circuit pour atteindre le destinataire. En théorie, chaque passerelle peut appeler n'importe quel numéro de téléphone. Cependant, pour réduire les coûts, il vaut mieux choisir une passerelle locale.

Les réseaux de téléphonie IP d'entreprise

Les réseaux de téléphonie d'entreprise utilisant le protocole IP sont disponibles sur le marché depuis le début des années 2000. L'objectif de ces réseaux est d'intégrer le réseau de données et le réseau téléphonique en un seul et même réseau. La norme IP est bien sûr à la base de cette intégration.

La parole téléphonique est numérisée, et les octets sont mis dans des paquets IP les plus courts possibles afin qu'il n'y ait pas trop de perte de bande passante. La compression de la parole avec G.729, par exemple, qui est très utilisé, donne naissance à des trames de 16 octets toutes les 16 ms. Si l'on veut de la qualité, il faut s'arrêter à cette valeur de 16 octets par paquet IP. Les paquets IP sont transportés avec la contrainte de 150 ms de délai jusqu'au poste du destinataire.

Dans l'entreprise, on utilise des trames Ethernet pour effectuer le transport. On place donc le paquet IP dans une trame Ethernet, qui possède une longueur de 64 octets. Au débit de 8 Kbit/s du codec G.729 correspond un débit de 32 Kbit/s sur le réseau Ethernet. Si l'on utilise un réseau Gigabit Ethernet, la trame minimale est de 512 octets, et le débit d'une seule parole téléphonique devient de 256 Kbit/s.

Pour la contrainte temporelle à respecter, il ne faut perdre aucun temps. Le premier point où des pertes de temps sont possibles provient potentiellement du traitement du son, effectué par une carte son dans un PC si le PC est utilisé comme téléphone. Ces cartes son ont généralement un temps de réaction très lent, de l'ordre d'une quarantaine de millisecondes, ce qui est inacceptable. Il faut donc utiliser des téléphones spécifiques, que l'on appelle téléphones IP. Un téléphone IP est un routeur qui encapsule directement les octets dans un paquet IP. Ce routeur possède des sorties Ethernet de façon que le téléphone puisse se connecter directement sur le réseau de l'entreprise. La figure 30.4 illustre un téléphone IP.

Figure 30.2
Téléphone IP

Toujours pour perdre le moins de temps possible dans le transport, le réseau ne doit posséder aucun réseau Ethernet partagé, le partage engendrant une perte de temps importante. Il faut donc utiliser uniquement des réseaux Ethernet commutés, si possible au débit de 100 Mbit/s, pour être sûr que le débit des paroles superposées ne pose pas de problème. Enfin, il faut que les paquets IP ou les trames portant les paquets IP de parole soient prioritaires partout dans le réseau d'entreprise. Pour cela, il faut se servir, par exemple, des priorités de type DiffServ au niveau paquet et des priorités de niveau trame dans Ethernet. Les priorités de niveau 2 correspondent à la norme IEEE 802.1p, qui définit un champ de 3 bits pour gérer jusqu'à huit classes de priorités.

Mise en œuvre de la téléphonie sur IP

Après avoir évoqué les caractéristiques principales des protocoles supportant la téléphonie sur IP, nous décrivons dans cette section le processus à suivre pour installer une téléphonie sur IP, ou ToIP (Telephony over IP), dans une entreprise possédant plusieurs sites. Les éléments à prendre en compte doivent suivre une architecture à quatre niveaux, comme illustré à la figure 30.3.

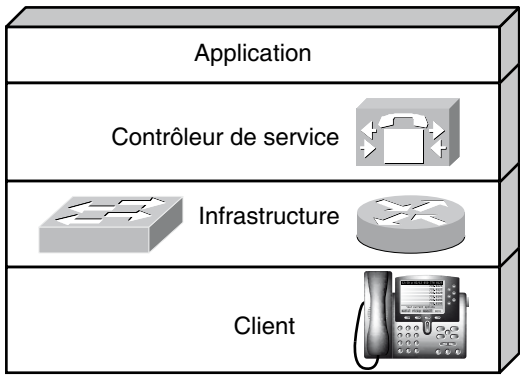


Figure 30.3
Architecture d'un réseau de téléphonie sur IP

Un réseau d'entreprise assez standard est décrit à la figure 30.4. Il contient deux sites, l'un principal et l'autre secondaire. Le réseau est composé d'un réseau local dans chaque site. Les deux réseaux locaux sont reliés par un réseau WAN, qui peut-être, par exemple, un réseau privé virtuel. Ce réseau est composé de commutateurs Ethernet formant un réseau local Ethernet commuté. Sur ce réseau local, on trouve aussi bien des téléphones IP que des stations de travail. Les stations de travail peuvent être connectées aux téléphones IP ou directement au commutateur Ethernet. Les deux réseaux locaux Ethernet commutés sont connectés à des routeurs d'entrée-sortie de l'entreprise, et les deux routeurs sont reliés entre eux par un réseau étendu, par exemple un réseau privé virtuel d'opérateur.

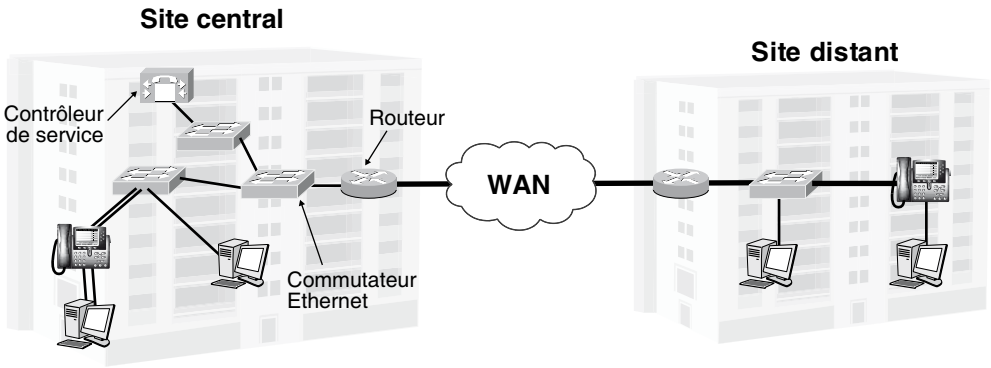


Figure 30.4
Réseau intégrant la téléphonie sur IP

En remontant l'architecture par le bas, nous trouvons tout d'abord les téléphones IP. Ce sont des routeurs de niveau paquet capables d'encapsuler des octets de téléphonie. Les postes de travail peuvent également être utilisés comme téléphones, mais il faut faire attention à ce que la carte son soit de bonne qualité pour ne pas trop retarder la mise en paquet des octets téléphoniques. Ces postes de travail un peu spécifiques sont connectés par Ethernet, généralement à 100 Mbit/s, avec la priorité disponible la plus haute.

La zone DSCP du paquet IP est positionnée sur la classe de service EF (Expedited Forwarding), et le paquet est encapsulé dans une trame Ethernet de priorité la plus haute, cette priorité étant indiquée par la zone IEEE 802.1p. Les autres machines, qui ne produisent pas de la parole, ou plus précisément les autres applications positionnent le DSCP à une valeur AF ou BE moins forte que celle utilisée pour la téléphonie sur IP. L'entreprise doit donc se munir de routeurs DiffServ capables de traiter la priorité au niveau IP et de commutateurs Ethernet capables de gérer les classes de priorités IEEE 802.1p.

Si la valeur du DSCP est normalisée, celle du champ IEEE 802.1p l'est beaucoup moins. Tout d'abord, ce champ ne contient que 3 bits de priorité, ce qui donne naissance à 8 classes de priorités, alors que DiffServ en comporte 14. Ensuite, il faut vérifier que les équipementiers suivent les mêmes règles pour déterminer la valeur du champ IEEE 802.1p. Toujours au niveau du transport, il faut faire une évaluation du temps maximal de transit dans chaque site afin d'en déduire le temps maximal de traversée du réseau WAN. Une fois cette valeur connue, il est possible de déduire le temps maximal de transit dans le réseau. L'entreprise doit alors négocier un SLA avec son opérateur et lui demander que cette contrainte soit satisfaite dans la partie technique, c'est-à-dire le SLS. La valeur maximale du temps de transit se situe généralement autour de 50 ms.

En passant à la couche supérieure, il faut introduire un contrôleur de service capable de déclencher les processus de recherche du correspondant et d'initialiser la signalisation permettant l'ouverture de la session. Le contrôleur de service peut être centralisé sur un seul site, même si les deux sites sont assez distants. Ce contrôleur de service peut gérer un grand nombre de services, tels que la téléphonie, les passerelles, les ports TAPI (Telephony API) et JTAPI (Java TAPI), la messagerie, les conférences, etc. Ce contrôleur de communication peut éventuellement prendre en charge des terminaux analogiques de générations précédentes ou des lignes de sortie plus classiques allant vers un opérateur de téléphonie fixe.

Les applications de téléphonie sur IP grand public

Une première application de téléphonie sur IP grand public est proposée par les opérateurs de téléphonie pour offrir des communications internationales à tarif local. Elle consiste à rassembler un grand nombre de voies téléphoniques classiques et à les encapsuler dans un même paquet IP, qui peut devenir assez long. L'utilisateur se connecte en local sur un point de présence d'un opérateur IP, lequel multiplexe toutes les voies téléphoniques sur une même liaison IP, transatlantique par exemple. À la sortie de la liaison IP transatlantique, la parole recouvre sa composition normale et est envoyée de façon classique au destinataire.

Des applications grand public telles que Skype ou MNS (Microsoft Network Service) proposent de la téléphonie sur IP de bout en bout. Pour cela, il faut généralement passer par un modem ADSL aux deux extrémités de la communication afin que le débit soit accepté sur la boucle locale. Skype fait appel à une technique P2P pour rester le plus simple possible et ne pas avoir de contrôle centralisé. La signalisation de MNS est quant à elle gérée par une base de données centralisée mais qui peut être distribuée sur plusieurs sites.

Skype

Avec plus de 100 millions d'utilisateurs dans le monde, Skype, leader mondial de la téléphonie sur Internet et pionnier des offres de téléphonie grand public sur Internet, bouleverse l'industrie des télécommunications en modifiant en profondeur les habitudes des consommateurs.

Chaque jour, 150 000 nouveaux utilisateurs téléchargent cette solution de téléphonie sur Internet qui utilise la technologie peer-to-peer (P2P) qui propose deux services différents : une offre gratuite entre utilisateurs équipés du logiciel pour une exploitation purement Internet et une offre payante, qui permet de joindre et d'être joint *via* Internet tandis que les correspondants utilisent la téléphonie traditionnelle RTC.

Skype est l'un des premiers logiciels grand public à avoir permis la jonction entre la téléphonie du monde Internet et celle du monde RTC. C'est sans doute là la clé de son succès. Grâce à une qualité d'écoute excellente, une facilité d'utilisation ne nécessitant généralement aucune configuration (y compris dans les infrastructures réseau déployant des pare-feu), une mobilité accrue, une gamme de services complémentaires et un prix incomparablement moins cher que la téléphonie traditionnelle, Skype s'est répandu de manière virale.

Skype a été lancé le 29 août 2003 à l'initiative de Niklas Zennström, un Suédois de 36 ans, et Janus Friis, une Danois de 26 ans, tous deux experts en technologies de peer-to-peer puisqu'ils avaient fait frémir l'industrie des loisirs au début des années 2000, avec le logiciel KaZaA qu'ils avaient conçu.

Microsoft et Google d'abord, puis Yahoo! et News Corporation (la société de Rupert Murdoch), s'intéressent à Skype, mais, en 2005, ses deux fondateurs créent la surprise en vendant la société à eBay, un acteur pour le moins inattendu dans le domaine des télécoms.

Architecture de Skype

Comme expliqué précédemment, Skype fonctionne selon un mode décentralisé et une architecture peer-to-peer (P2P), c'est-à-dire de poste à poste, ou point à point, ou encore de pair en pair ou d'égal à égal, dans lequel chaque poste intermédiaire est susceptible de jouer le rôle de relais et de participer de manière dynamique au processus d'acheminement des paquets.

Le client logiciel n'est pas seulement utilisé par le possesseur du logiciel. Il est mis à contribution pour les besoins d'autres utilisateurs et sert de support de transmission aux flux de ces derniers. Chaque élément du réseau (on parle de nœuds) constitue à la fois un client, qui peut demander un service, et un serveur, qui peut agir pour le compte d'un

autre client. Ce modèle distribue ainsi totalement ses traitements, à l'opposé du traditionnel modèle client-serveur, dans lequel chaque entité joue exclusivement le rôle de serveur ou de client, ce qui nécessite de centraliser les flux vers des centres de contrôles.

Le terme peer-to-peer est parfois utilisé pour désigner toute communication directe entre un poste et un autre, indépendamment du mode de routage des données utilisé. C'est là un abus de langage, puisque le routage caractérise la technologie P2P et définit un moyen de transporter des informations faisant intervenir des terminaux intermédiaires de proche en proche jusqu'au véritable destinataire. Skype est d'ailleurs le seul softphone parmi ceux que nous présentons dans les chapitres suivants qui puisse utiliser un mode de routage de type peer-to-peer.

Limiter les ressources

Le modèle décentralisé peer-to-peer proposé par Skype fait reposer l'intelligence de son réseau sur les utilisateurs eux-mêmes, et non sur des serveurs centraux. Dès lors, le passage à l'échelle est permis à moindres frais, puisque chaque nouvel utilisateur est potentiellement une source de traitement pour l'ensemble du réseau. Skype a ainsi pu s'étendre sur toute la planète sans avoir à s'intéresser directement aux ressources de traitement de la montée en charge. C'est l'un des secrets de sa réussite.

Traverser les pare-feu

Une condition essentielle de la réussite de ToIP est la possibilité de traverser les pare-feu. Les communications de ce type exploitent des ports dynamiques qui ne sont généralement pas ouverts par ces pare-feu. Par ailleurs, le réseau sur lequel se trouve l'utilisateur peut mettre en œuvre un mécanisme de NAT (Network Address Translation), ou translation d'adresse réseau, qui donne à l'utilisateur une adresse IP non routable sur Internet. Pour ces deux raisons, la communication directe entre correspondants est impossible.

Skype a trouvé la parade en exploitant différentes techniques. L'une d'elle consiste en l'utilisation de ports standards, qui sont étrangers à la téléphonie sur IP, mais qui présentent l'avantage d'être le plus souvent ouverts par les pare-feu. C'est le cas du port 80, associé généralement au Web pour le protocole HTTP.

Skype permet en outre d'utiliser des ressources situées à l'extérieur de la zone protégée par le pare-feu. Cette ressource peut être un utilisateur parmi d'autres, choisi pour accomplir cette tâche selon un algorithme propriétaire. Les flux IP de Skype suivent ainsi un chemin détourné lorsque le chemin direct est impossible. Ce sont de tels chemins qu'empruntent les communications entre utilisateurs de Skype, lesquels se prêtent à la fonctionnalité de routage sans en avoir conscience et pour les besoins d'autres clients.

Ce type de connexion s'effectue aux dépens des utilisateurs intermédiaires, mais à un débit faible, de 0,5 kg-octet par seconde, qui ne perturbe que très peu ces derniers. Ceux-ci sont en outre sélectionnés en fonction de la bande passante dont ils disposent afin d'assumer la charge supplémentaire induite par ces communications. L'idée du transfert relayé est d'avoir une communication, fût-elle de qualité médiocre, plutôt que pas de communication du tout.

Si l'architecture de Skype est globalement décentralisée, il existe cependant des serveurs centralisés, qui assurent un ensemble de fonctionnalités annexes indispensables à la communication. Par exemple, pour savoir si un utilisateur est connecté ou non, le logiciel se connecte à l'un de ces serveurs, qui informe de la disponibilité de tous les contacts.

Skype et la sécurité

Si aucune attaque ou vulnérabilité critique concernant le logiciel n'a encore été recensée, de nombreux spécialistes déplorent la facilité avec laquelle le logiciel parvient à traverser et se jouer des pare-feu censés bloquer les flux non autorisés. De ce fait, ces experts recommandent d'interdire l'utilisation du logiciel dans un cadre professionnel.

De leur côté, les autorités s'inquiètent du manque de transparence du logiciel, qui se comporte comme une boîte noire. Il n'est donc pas possible de savoir s'il contient une porte dérobée, accessible à partir d'Internet, pas plus qu'il n'est possible de savoir si des données sensibles sur les utilisateurs ne sont pas envoyées à leur insu.

Quant au fondement même du logiciel, le peer-to-peer, puisque les communications peuvent être acheminées *via* des ordinateurs intermédiaires, elles peuvent faire l'objet d'écoutes clandestines par ces mêmes intermédiaires.

De même, les pièces jointes transmises par l'outil de transfert de fichiers de Skype ne sont pas soumises à des contrôles d'antivirus. Même si l'on peut supposer que les interlocuteurs sont dignes de confiance, il n'est va pas forcément de même des fichiers qu'ils transfèrent qui peuvent avoir été corrompus.

Selon un raisonnement paranoïaque, on pourrait imaginer que toutes les communications soient relayées vers des serveurs centraux qui les enregistreraient, agissant comme un système automatisé de profiling des utilisateurs. Techniquement, ce serait parfaitement réalisable. Dans le doute, et dans la mesure où Skype refuse d'ouvrir les spécifications de son protocole, on comprend la méfiance de certains.

Chez Skype, on garantit que le logiciel est parfaitement sécurisé et ne présente aucun risque pour l'internaute. Le cryptage se fait de bout en bout, au moyen de l'algorithme de chiffrement symétrique AES (Advanced Encryption Standard), le standard utilisé par les organisations gouvernementales aux États-Unis. AES utilise un cryptage sur 256 bits. La négociation des clés symétriques AES s'effectue par un RSA de 1 536 à 2 048 bits.

Si les spécifications générales du protocole ne sont pas rendues publiques, explique-t-on chez Skype, c'est uniquement pour offrir au logiciel une protection supplémentaire et éviter de donner aux pirates l'occasion d'y chercher des failles.

En entreprise, même si des administrateurs souhaitent bloquer l'utilisation de Skype chez les utilisateurs de leur réseau, dans la pratique il est très difficile de mettre en place une politique de sécurité qui prenne en compte les spécificités du logiciel. Le cryptage rendant impossible le filtrage, il n'est même pas possible de protéger le logiciel d'attaques malicieuses ou de le rendre compatible avec un système de détection d'intrusion IDS (Intrusion Detection System) puisque les échanges ne sont pas analysables.

Plusieurs sociétés proposent des logiciels qui détectent et bloquent les flux de Skype. Appelés SkypeKiller, ces logiciels poussent la reconnaissance de l'analyse protocolaire

jusqu'au niveau applicatif, et pas uniquement en se fondant sur les protocoles de transport ou les ports, afin d'empêcher les flux Skype de traverser le réseau.

IPTV

Cette section est dévolue à la télévision sur Internet, ou IPTV. Le décollage de cette application à tarder principalement par manque de débit des infrastructures. Avec le déploiement de la fibre optique et des composants haute capacité associés, la télévision et plus généralement la vidéo, l'IPTV devient une application standard. Nous allons regarder dans un premier temps les caractéristiques de cette application.

Trois grandes catégories d'IPTV ont été définies :

- la télévision classique ;
- la télévision en temps différé ;
- la vidéo à la demande ou VoD (Video on Demand).

Contrairement à la télévision des diffuseurs, qui utilisent les voies hertziennes ou le CATV (Community Antenna TeleVision), l'IPTV arrive par la boucle locale que ce soit terrestre ou hertzienne. L'ADSL ou le modem câble pour la partie terrestre et la 3G/4G pour la partie hertzienne.

Deux architectures sont acceptables : centralisée ou distribuée. Dans le cas centralisé, le serveur de distribution des programmes est comme le nom l'indique centralisé. Cette solution est assez simple à mettre en œuvre mais elle ne passe pas l'échelle. Le cas distribué demande un service de distribution des contenus adapté aux grands réseaux.

La distribution chez l'utilisateur s'effectue via la Home Gateway. Cependant, la partie traitement est repoussée vers l'utilisateur dans la set-top-box. Dans l'ordre à partir de l'accès opérateur il y a la Home Gateway, la set-top-box et le téléviseur. La direction, poussée en particulier par DLNA (cf. chapitre 12), est d'intégrer la set-top-box dans le téléviseur avec la terminaison de réseau. Les paquets IP transportant le canal de télévision vont jusqu'au terminal.

Le codage des flots TV s'effectue en MPEG-2 et surtout MPEG-4. Les protocoles utilisés sont :

- IGMP version 2 ou IGMP version 3, pour prendre en charge un flot multimédia en multicast, c'est-à-dire une diffusion du canal de télévision vers l'ensemble des utilisateurs voulant regarder la même chaîne.
- RTSP (Real Time Streaming Protocol) pour la vidéo à la demande.
- NPVR (Network-based Personal Video Recorder).

Une des particularités, comme dans la téléphonie, concerne le temps réel de l'application de télévision en direct et de streaming en général. L'application de streaming est plus ou moins facile en fonction des qualités de service du réseau.

Conclusion

Ce chapitre a effectué un bref tour d'horizon de la téléphonie en paquet et plus particulièrement de la téléphonie sur IP ainsi qu'une introduction à la télévision sur IP : IPTV.

L'hégémonie de la téléphonie sur IP est inéluctable étant donné le gain financier procuré en quelques années par l'intégration des réseaux de données et de paroles téléphoniques. La téléphonie est cependant une application particulièrement difficile à mettre en œuvre du fait de son temps réel et de son flux continu.

Pour le moment, les solutions consistent surtout à surdimensionner les équipements et les liaisons en ne tenant compte que des clients effectuant de la téléphonie sur IP.

La télévision sur IP est en pleine maturation et devrait devenir le standard de la distribution de la télévision dans quelques années.

31

Les réseaux autonomiques

L'intelligence est un terme classique en informatique, qui désigne simplement la capacité de communiquer, de raisonner et de décider. Jusqu'au début des années 2000, l'intelligence dans les réseaux était très faible. Les concepts de réseaux intelligents, qui datent du début des années 1990, introduisent une intelligence primaire, dont le rôle est d'adapter automatiquement des composants du réseau aux demandes des utilisateurs, mais sans raisonnement et uniquement en suivant des règles définies à l'avance. Ce chapitre est dévolu à cette vision de l'intelligence dans les réseaux. Il introduit en outre les réseaux autonomiques, qui ont tendance à remplacer les réseaux programmables ou les réseaux actifs. Un réseau autonomique est un réseau qui est capable de s'autoconfigurer et dont les nœuds peuvent devenir autonomes en cas de panne ou de coupure des communications.

Depuis le début des années 2000, l'intelligence réelle, c'est-à-dire à base de raisonnement, apparaît dans certains composants du réseau pour prendre des décisions de contrôle ou de gestion. Les organes qui prennent les décisions proviennent du domaine de l'intelligence artificielle et des objets intelligents. En particulier, les systèmes multiagents commencent à faire leur apparition pour gérer la sécurité ou les pannes.

Les agents intelligents

Les agents intelligents constituent une première catégorie d'outils dont l'introduction à grande échelle pourrait modifier les environnements de gestion et de contrôle en les rendant plus autonomes et plus réactifs.

Nous allons examiner les raisons de cette puissance puis la façon de construire des systèmes multiagents.

Gestion d'un environnement complexe

Les réseaux étant de plus en plus complexes, la gestion de ces environnements est devenue nécessaire pour de multiples raisons, que nous allons examiner. Les environnements réseau sont aujourd'hui dynamiques. Des applications nombreuses et variées se superposent et rendent le contrôle des ressources difficile. Le gain statistique, c'est-à-dire ce que l'on gagne en traitant les paquets de façon statistique, dans les réseaux à transfert de paquets est indéniable, mais, si les flux dépassent trop fortement les capacités du réseau, un effondrement des performances est inévitable.

Les environnements réseau sont par nature distribués, ce qui complique leur contrôle et leur gestion. De plus, le gigantisme impose un contrôle encore plus fin. Le dimensionnement est un problème complexe à appréhender, et l'on peut affirmer qu'il n'existe pas d'outil véritablement efficace dans ce domaine, dans la mesure où les paramètres à prendre en compte dans un environnement de réseau complexe sont difficiles à apprécier. On a le choix entre débit, temps de réponse, taux d'utilisation des coupleurs de ligne et des unités centrales, taux d'erreur bit, taux d'erreur paquet, taux de reprise et taux de panne. En outre, les valeurs de la moyenne, de la variance et parfois des moments d'ordre supérieur doivent être prises en considération pour avoir une idée réelle des performances.

L'ingénierie de la conception du réseau présente deux grands aspects, le qualitatif et le quantitatif. Le qualitatif correspond souvent à une sécurité de fonctionnement, dans le sens où il est possible de prouver que le système est stable ou qu'il n'existe pas d'état dans lequel le réseau se bloque. L'aspect quantitatif fait référence aux valeurs des paramètres indiqués au paragraphe précédent, le but d'une analyse quantitative étant de montrer que ces valeurs sont raisonnables pour un bon fonctionnement du réseau.

La sécurité est une fonction importante pour laquelle peut intervenir de l'intelligence. Aujourd'hui, une certaine normalisation permet de mieux cerner les problèmes, et quelques grandes classes de sécurité ont été définies, correspondant à des besoins bien exprimés par les utilisateurs. On peut facilement imaginer l'apport d'outils intelligents dans le monde de la sécurité pour reconnaître les anomalies, les analyser, donner un diagnostic, proposer une solution et résoudre le problème.

La gestion est également un domaine où les agents intelligents peuvent jouer un rôle moteur. Lorsqu'un réseau est en état de marche, il faut l'administrer, c'est-à-dire être en mesure de contrôler toutes les opérations qui se déroulent dans le réseau, depuis les pannes jusqu'à la comptabilité en passant par la sécurité, la gestion des performances et la gestion des noms des utilisateurs.

Plusieurs domaines d'administration spécifiques utilisent déjà des composants intelligents, notamment les suivants :

- configuration (configuration management) ;
- sécurité (security management) ;
- pannes (fault management) ;
- audit des performances (performance management) ;
- comptabilité (accounting management).

L'intelligence des agents peut provenir de différents horizons. Le schéma le plus classique émane de l'intelligence artificielle distribuée, ou IAD.

L'intelligence artificielle signifie que l'on se met à la place d'un être humain pour réaliser une tâche. L'IAD équivaut à une société d'agents autonomes travaillant en commun pour aboutir à un objectif global. Il existe de nombreuses raisons pour se diriger vers l'utilisation de l'IAD, notamment les suivantes :

- Prise en compte de points de vue différents. Lorsque les données deviennent de plus en plus précises, des incohérences peuvent survenir dans la base de règles. Les façons d'exprimer les connaissances sont différentes selon qu'on s'adresse à l'utilisateur, au développeur ou au technicien. De plus, deux experts possédant la même expertise n'arrivent pas toujours au même résultat. Les points de vue sont également souvent contradictoires : l'un veut privilégier les coûts, et donc un système moins cher, alors que l'autre choisit de développer la publicité, et donc un système plus cher. L'utilisation de l'IAD permet, par négociation, d'aboutir à un compromis entre différentes options.
- Adéquation au monde réel. D'une manière générale, c'est toujours un groupe d'experts, avec des qualifications et des spécialités différentes, qui parvient, par collaboration, à réaliser un objectif fixé. De plus, s'il semble aisé de comprendre et donc de modéliser le comportement des individus (l'ensemble de leurs échanges) grâce aux nombreuses études sociologiques disponibles, en revanche le fonctionnement du cerveau et le raisonnement sont moins connus.

Pour ces raisons, l'application de l'intelligence artificielle distribuée s'impose peu à peu dans le cadre de la maîtrise des réseaux.

Les systèmes multiagents

Un agent est une entité autonome, capable de communiquer avec d'autres agents, ainsi que de percevoir et de représenter son environnement. L'ensemble de ces agents en interaction forme les systèmes multiagents. On classe ces derniers selon de nombreux critères, tels que la taille des agents, leur nombre en interaction, les mécanismes et les types de communication, le comportement, l'organisation et le contrôle de chaque agent, la représentation de l'environnement, etc.

À partir de ces critères, on distingue deux grandes catégories de système multiagent :

- les systèmes d'agents cognitifs ;
- les systèmes d'agents réactifs.

Les agents cognitifs ont une représentation explicite de l'environnement et des autres agents. Ils savent tenir compte de leur passé et fonctionnent selon un mode social d'organisation. Les systèmes dotés de ce type d'agent ne possèdent qu'un petit nombre d'agents. Plusieurs niveaux de complexité peuvent être envisagés :

- Les processus dans lesquels les acteurs mettent en œuvre des primitives de communication.
- Les modules communicants, qui utilisent des protocoles de communication spécialisés (requêtes, commandes).

- Les agents coopératifs, qui font intervenir des notions de compétence, de représentation mutuelle et d'allocation de tâches.
- Les agents intentionnels, qui utilisent des notions d'intention, d'engagement et de plans partiels.
- Les agents négociants, qui mettent en œuvre la résolution de conflit par négociation.
- Les agents organisés, qui agissent selon une réglementation et des lois sociales.

Les agents communiquent entre eux à l'aide d'un langage et utilisent des protocoles de communication. C'est une communication intentionnelle, qui comporte essentiellement deux types, la communication par partage d'information et la communication par envoi de messages.

La communication entre agents est réalisée par partage d'information lorsque la solution courante du problème est centralisée dans une structure de données globale, partagée par tous les agents. Cette structure contient initialement les données du problème et est enrichie au cours de la résolution jusqu'à obtention de la solution. Elle constitue le seul moyen de communication entre les agents.

Ce type de communication est souvent désigné par le modèle du tableau noir, ou blackboard, développé dans de nombreuses publications. Les agents déposent et lisent une information dans une zone de données commune, le tableau noir, comme illustré à la figure 31.1.

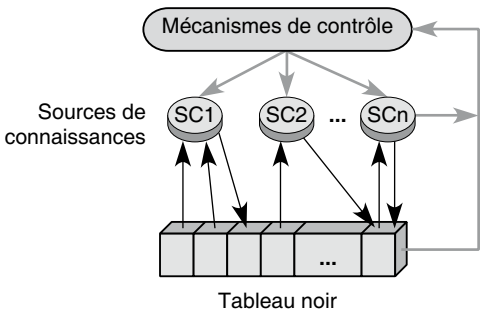


Figure 31.1

Fonctionnement du tableau noir

Un système de tableau noir comporte les trois éléments de base suivants :

- Le tableau noir, dans lequel tous les éléments engendrés durant la résolution sont stockés. Cette structure de données est partagée par les agents et est organisée de manière hiérarchique, ce qui permet de considérer la solution en plusieurs niveaux de détails.
- Les agents, qui engendrent et stockent leurs hypothèses dans le tableau noir. Ce sont des modules indépendants, appelés sources de connaissances. Leur rôle est de coopérer pour résoudre un problème donné. Les sources de connaissances sont indépendantes, puisqu'elles s'ignorent mutuellement et ne réagissent qu'aux événements de changement du tableau noir.

- Un dispositif de contrôle, qui assure le fonctionnement du système en fonction d'une certaine stratégie. Son rôle est, entre autres, de résoudre les conflits d'accès au tableau noir entre les agents, ceux-ci intervenant sans être déclenchés. En l'absence de contrôle centralisé, en effet, les sources de connaissance réagissent de manière opportuniste, c'est-à-dire du mieux qu'elles peuvent. Ce dispositif de contrôle fonctionne lui-même selon le modèle du tableau noir.

Les tableaux noirs ont l'avantage d'offrir une structuration et une méthode automatique (découpages et hiérarchie) dans la manière d'aborder un domaine de connaissance. Ils présentent aussi l'intérêt d'organiser des ensembles de règles dans les systèmes à règles de production. Cependant, leur manque de mémoire locale ne leur autorise pas un véritable fonctionnement multiagent. En règle générale, les systèmes multiagents utilisent un tableau noir pour chaque agent.

Les systèmes multiagents fondés sur la communication par message sont caractérisés par la distribution totale à la fois des connaissances, des résultats partiels et des méthodes utilisées pour aboutir à un résultat (*voir figure 31.2*). Certains langages d'acteurs incarnent bien ce type de système. La communication peut se faire en point-à-point ou par diffusion.

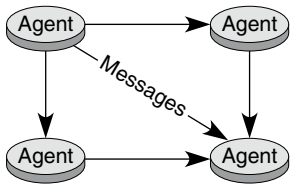


Figure 31.2

Fonctionnement d'un système multiagent

Un tel système s'articule autour de deux composantes :

- Traitement local. À l'inverse des systèmes fondés sur le tableau noir, les connaissances ne sont plus concentrées dans un même espace mais réparties entre les différents agents. Un agent ne peut manipuler que sa base de connaissance locale, envoyer des messages aux autres agents qu'il connaît, que l'on appelle ses accointances, et créer de nouveaux agents. À un instant donné, les agents n'ont pas une vision globale du système et ne possèdent qu'un point de vue local sur les éléments.
- Envoi de messages avec continuation. Quand un agent envoie un message, il précise à quel agent la réponse au message doit être adressée. Il peut s'agir de l'agent émetteur du message mais aussi d'un autre agent, spécialement créé pour la circonstance.

Les agents ont une connaissance plus ou moins précise des autres agents du système. Ils doivent connaître et représenter les compétences de ces agents, ainsi que les tâches qui se réalisent à un instant donné, les intentions et les engagements des agents. Cet aspect des choses pose le problème de la représentation de ce type de connaissance ainsi que celui de sa mise à jour.

Le principe de l'allocation de tâches constitue l'un des points essentiels des systèmes multiagents cognitifs. Un problème se compose d'un certain nombre de tâches réalisées par des agents qui regroupent l'ensemble des solutions partielles pour obtenir la solution globale (*voir figure 31.3*).

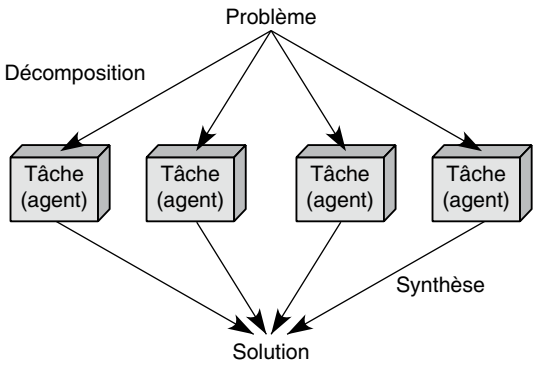


Figure 31.3
Résolution de problèmes

Pour réussir l'allocation de tâches, il faut connaître les compétences de chacun des agents, décomposer un problème en sous-problèmes, répartir les activités de résolution en fonction des agents et, au besoin, répartir à nouveau ces activités de façon dynamique.

Les modèles d'allocation de tâches peuvent être regroupés en deux catégories :

- Allocation centralisée. Dans cette approche modulaire, un agent décompose un problème en sous-problèmes et distribue ceux-ci aux autres agents, qui se retrouvent sous son autorité. Dans ce cas, les actions sont cohérentes, mais il y a un problème de fiabilité et d'extensibilité. De plus, un agent est entièrement dédié à la répartition de tâches. Le système n'est donc pas utilisé au maximum de ses capacités.
- Allocation décentralisée, ou distribuée. Chaque agent est capable de décomposer son problème en sous-problèmes et de répartir ainsi les tâches associées. Tous les agents ont le même poids dans la prise de décision. Ce type d'allocation convient à des applications ayant déjà une structure distribuée. La fiabilité et les possibilités d'extension sont meilleures que dans le modèle précédent, mais le maintien de la cohérence est plus difficile à réaliser.

Les méthodes pour décomposer un problème peuvent être de trois sortes :

- Statiques : chaque agent connaissant les compétences des autres agents, les sous-problèmes peuvent être attribués aux agents les plus qualifiés.
- Dynamiques : les agents se concertent afin de répartir les sous-problèmes de manière plus efficace.
- Mixtes : chaque agent connaît les compétences des autres agents, mais cette connaissance est remise à jour de manière périodique.

L'autonomie des agents repose sur la notion d'intentionnalité. On peut différencier l'intention dans l'action de l'intention d'accomplir une action dans le futur. Dans ce dernier cas, il s'agit d'un but persistant. Pour qu'un agent ait l'intention d'accomplir une action, il faut qu'il estime que l'action est possible, qu'il envisage de s'engager à la réaliser, qu'il estime que si certaines conditions sont remplies il peut accomplir l'action et enfin qu'il ne cherche pas à en réaliser toutes les conséquences. On peut toutefois se demander ce qui se passe lorsque l'action a été accomplie par un autre agent, lorsqu'un agent possède deux intentions ou dans quelles conditions un agent peut abandonner son intention.

Approches pour la coopération entre agents

Il existe actuellement deux approches pour la coopération entre agents :

- Volontaire : les agents interagissent de façon non conflictuelle, qu'ils aient le même but ou non.
- Conflictuelle : les agents peuvent avoir des buts identiques mais des vues divergentes, voire opposés.

C'est la coopération volontaire qui nous intéresse ici, puisqu'elle reflète une interaction des agents pour la résolution distribuée de problèmes. On peut réaliser une planification pour agents multiples ou une planification distribuée. Dans le premier cas, il existe un agent coordinateur qui constitue et réalise les plans et gère les conflits. En ce qui concerne la planification distribuée, chaque agent est capable de produire ses propres plans, qui seront fusionnés pour un résultat global. On peut également envisager la résolution distribuée de problèmes comme une assistance mutuelle. Un agent résout le problème, et un autre critique la solution obtenue.

Dans le domaine de la résolution distribuée, quatre modes de coopération sont envisageables lorsque la notion de hiérarchie est présente :

- Commande : un agent décompose un problème en sous-problèmes, qu'il répartit entre les autres agents selon leurs compétences. Ces derniers résolvent leur sous-problème et renvoient les solutions partielles à l'agent centralisateur (*voir figure 31.4*).

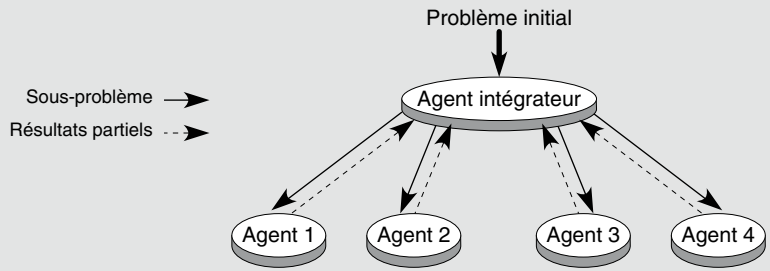


Figure 31.4

Fonctionnement du mode commande

- Diffusion : un agent décompose encore le problème, mais les agents intéressés par la résolution des sous-problèmes décident s'ils passent ou non à l'action. Les résultats sont envoyés ensuite à tous les agents du système.
- Appel d'offres : un agent décompose le problème en sous-problèmes, dont il diffuse la liste. Les agents intéressés par une tâche envoient une offre à l'agent qui a engendré cette tâche. Ce dernier choisit une offre parmi celles à sa disposition. Il distribue ensuite les sous-problèmes aux agents qu'il a choisis (*voir figure 31.5*). Les résultats partiels sont ensuite retournés, comme dans le mode commande.

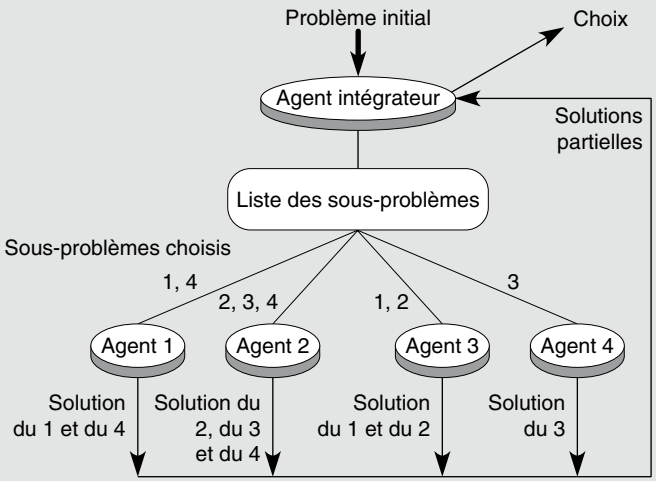


Figure 31.5

Fonctionnement du mode appel d'offres

- Compétition : comme dans les autres modes, le problème est décomposé en sous-problèmes par un agent central. Les agents choisissent la ou les tâches qu'ils vont réaliser. Les résultats partiels sont envoyés à l'agent centralisateur, qui décide de la solution parmi tous les résultats engendrés (*voir figure 31.6*).

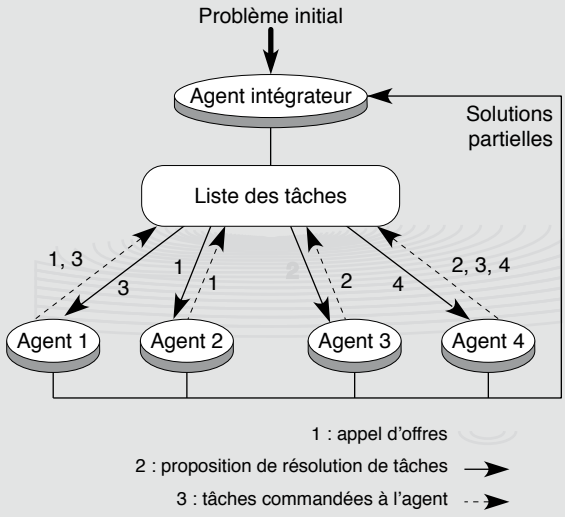


Figure 31.6

Fonctionnement du mode compétition

Lorsque la notion de hiérarchie n'est pas présente, les agents peuvent fonctionner selon un mode de partage des tâches, par négociation, par exemple, ou échanger des résultats partiels.

Parler de négociation dans le cas du partage des tâches revient à évoquer un concept et une structure d'interactions (le réseau contractuel) relevant fortement de l'intelligence artificielle distribuée. Le réseau contractuel est composé d'un ensemble d'agents, qui peuvent passer des contrats selon un protocole fixe. Les agents doivent effectuer des tâches qu'ils peuvent décomposer. S'ils ne sont pas en mesure d'effectuer ces sous-tâches, faute de compétences, de temps ou de moyens, ils peuvent tenter de les sous-traiter en lançant un appel d'offres. Les agents intéressés envoient une offre à l'agent demandeur, appelé manager, qui choisit l'agent auquel il attribue la tâche. Un contrat est alors établi. Ce modèle est calqué sur les protocoles d'appel d'offres des contrats publics.

Le réseau contractuel représente une allocation de tâches dynamique et distribuée par appel d'offres. Ce système présente de nombreux avantages (distribution des décisions, extensibilité, etc.) mais reste entaché de nombreux problèmes (conception hiérarchique, coût élevé de communication, rigidité de la procédure, etc.).

Les conflits peuvent être de plusieurs ordres : accès à une ressource, solutions différentes à un problème donné, conflits d'intérêt et de buts, etc. Pour tenter de remédier à ces conflits, on peut :

- Établir un contrôle centralisé et donc mettre en place un agent avec un poids supérieur.
- Nommer un agent capable d'établir un arbitrage entre différents points de vue.
- Établir une négociation entre les différents agents en conflit afin d'aboutir à une situation qui les satisfasse par une série d'échanges, de tractations et de compromis.

Les systèmes d'agents réactifs

Un agent réactif n'a pas une représentation explicite de son environnement et ne peut tenir compte de son passé. Son mode de fonctionnement est simple et suit un ensemble de décisions préprogrammées, de type stimulus-réponse. L'organisation s'effectue selon un mode biologique, et le nombre d'agents présents dans un tel système est très élevé. La communication est non intentionnelle. Les agents laissent, par exemple, des traces de leur présence, ou signaux, qui peuvent être perçus par d'autres agents. On parle alors de communication par environnement.

Ce type d'agent résulte du postulat suivant : de l'interaction d'un grand nombre d'agents simples peuvent émerger des organisations complexes.

On peut considérer plusieurs niveaux de complexité pour un agent réactif :

- stimulus-réponse : simples réactions à l'environnement ;
- coordination d'actions élémentaires : mécanismes d'inhibition, relations entre actions élémentaires ;
- coopération réactive : mécanismes de recrutement entre agents, agrégation d'agents élémentaires ;
- reproduction : mécanismes de reproduction d'agents réactifs ;
- organisation d'agents réactifs.

L'écorésolution est une technique de résolution de problèmes fondée sur l'utilisation d'agents réactifs. La résolution de problèmes est ici considérée comme le résultat d'un

ensemble d'interactions. Cette conception s'oppose aux approches classiques en résolution de problèmes, telles que l'exploration d'espaces d'états, qui pose des problèmes d'explosion combinatoire.

L'approche de la résolution distribuée de problèmes repose sur une conception radicalement différente : celle de l'apparition de configurations comme états stables ou stationnaires d'un système dynamique, dont l'évolution est due à des interactions provenant des comportements de petits agents assez simples.

Dans les systèmes classiques, toutes les données se trouvent dans l'énoncé, le système se bornant à trouver comment passer de la configuration initiale à l'état final. Au contraire, dans le phénomène de l'écorésolution, la détermination est seulement locale. Les agents sont caractérisés par des comportements de satisfaction, d'agression et de fuite. Le problème lui-même est défini par une population d'agents autonomes, qui cherchent à se satisfaire. Le résultat final est la conséquence d'une interaction non déterministe. Le modèle définit la combinaison des comportements.

Comportement des agents

D'une façon quasi générale, on peut caractériser le comportement des agents par un ensemble d'éléments :

- Une condition de satisfaction locale, qui décrit un état stable pour l'agent, compte tenu des informations dont il dispose. Cette condition ne repose pas sur des critères objectifs mais sur les croyances et les caractéristiques locales des agents.
- Une condition locale de rejet, c'est-à-dire un ensemble de contraintes décrivant les situations que rejette temporairement un agent (celles qu'il cherche à fuir).
- Une réaction de survie, c'est-à-dire un ensemble d'actions (satisfaction, agression, fuite) qui sont accomplies pour que l'agent puisse s'approcher de sa condition de satisfaction en évitant les situations néfastes.
- Une fonction de coût énergétique, qui permet de choisir l'action de moindre coût à réaliser.
- Une information.

Cette méthode évite l'explosion combinatoire classique lors de la résolution de problèmes, mais, en contrepartie, la solution trouvée n'est pas forcément la meilleure. L'écorésolution de problèmes peut être utilisée de façon privilégiée pour des problèmes structurellement distribués ou dans le cadre d'un univers évolutif.

En conclusion de cette section, on peut avancer que l'étude de l'apprentissage, du temps réel ou de la distribution correspond à une nécessité dans le domaine de la gestion réseau. C'est toutefois le dernier point qui semble le plus intéressant, dans la mesure où les systèmes multiagents constituent en quelque sorte une généralisation des techniques des systèmes experts. De ce fait, ils apportent une valeur ajoutée aux systèmes conventionnels de l'intelligence artificielle en proposant un nouveau type d'architecture, faisant intervenir aussi bien la communication que le raisonnement interne. Les aspects d'ouverture et de distribution les rendent intéressants pour un système de gestion réseau.

En ce qui concerne l'aspect temps réel, l'approche adoptée par l'intelligence artificielle semble moins claire. Pourtant, c'est une étape indispensable dans la conception d'un système d'administration des réseaux. En effet, les temps de réponse à une panne, par exemple, doivent être minimaux, même si cela ne revêt pas la même importance que dans les systèmes d'aide à la décision ou au commandement.

L'apprentissage constitue encore le talon d'Achille des systèmes à base de connaissances. Tant que ceux-ci ne pourront améliorer, augmenter et affiner leurs connaissances grâce à leur propre expérience, ils dépendront de la bonne volonté et de la disponibilité des experts et de la qualité d'une mise à jour manuelle.

Les agents réseau

Un agent réseau est un composant logiciel qui utilise soit un service lié au réseau (courrier électronique, transfert de fichiers, Web, etc.), soit le réseau lui-même, comme dans le cas des agents mobiles que nous examinons à la section suivante.

Un agent réseau peut être défini de multiples façons. Nous avons choisi de le définir comme un composant logiciel qui agit au nom de son utilisateur. Il est évident que cette définition est beaucoup plus réductrice que celle donnée par les chercheurs en intelligence artificielle, qui envisagent l'agent comme un composant logiciel capable de rendre un service, avec une certaine possibilité de raisonnement et de communication.

Les agents réseau assurent généralement des tâches simples. Par exemple, ils filtrent des messages électroniques en utilisant un ensemble de mots-clés. Ainsi, l'agent peut être confondu avec un programme classique. Certains agents sont beaucoup plus élaborés. L'utilisateur peut demander à un agent de lui organiser une réunion, par exemple. Pour ce faire, l'agent doit décomposer cette tâche en sous-tâches et coopérer avec les agents des différents participants.

Il existe trois catégories principales d'agents réseau :

- les agents Internet ;
- les agents intranet ;
- les agents assistants, ou bureautiques.

Nous allons examiner ces trois catégories d'agents, qui peuvent elles-mêmes être décomposées en sous-catégories.

Les agents Internet

Les agents Internet proviennent essentiellement des applications développées pour ce réseau. On y trouve les agents suivants :

- Agents de recherche du Web : fournissent à un utilisateur des services de recherche sur le Web.
- Agents serveur du Web : résident sur un site Web spécifique pour fournir des services.

- Agents de filtrage d'information : filtrent des informations selon des critères spécifiés par l'utilisateur.
- Agents de recherche documentaire : retournent un ensemble personnalisé d'informations correspondant à la demande de l'utilisateur.
- Agents de notification : indiquent à un utilisateur des événements susceptibles de l'intéresser.
- Agents de service : fournissent des services spécialisés à des utilisateurs.
- Agents mobiles : se déplacent d'un lieu à un autre afin d'exécuter les tâches spécifiques d'un utilisateur.

Les agents intranet

Les agents intranet proviennent également des applications Internet mais sont personnalisés pour un environnement privé. Quatre types d'agents sont reconnus :

- Agents de personnalisation coopérative : permettent l'automatisation du workflow à l'intérieur d'une entreprise.
- Agents d'automatisation : automatisent le workflow d'une entreprise.
- Agents de base de données : fournissent des services agent à l'utilisateur de bases de données.
- Agents courtiers de ressources : réalisent l'allocation de ressources dans les architectures client-serveur.

Les agents assistants ou bureautiques

Les agents assistants sont, comme leur nom l'indique, des composants logiciels capables d'apporter une aide à un utilisateur dans l'utilisation d'un produit. Ces agents assistants sont souvent appelés agents bureautiques car on les rencontre essentiellement comme agents d'interface dans les suites bureautiques commercialisées pour le grand public.

Les trois grandes catégories d'agents assistants sont les suivantes :

- Agents système : fournissent une aide à l'utilisateur pour qu'il puisse se servir du système d'exploitation.
- Agents d'application : fournissent une aide à l'utilisateur pour qu'il emploie correctement une application particulière.
- Agents de suite logicielle : fournissent une aide à l'utilisateur pour que celui-ci puisse travailler avec des applications corrélées.

Les agents mobiles

Un agent mobile est un agent logiciel qui peut se déplacer entre plusieurs points. Cette définition implique qu'un agent mobile est aussi caractérisé par un modèle d'agent de base. En plus du modèle de base, chaque agent logiciel définit un modèle de cycle de vie, un modèle

de calcul, un modèle de sécurité et un modèle de communication. Un agent mobile est de surcroît caractérisé par un modèle de navigation. L'agent mobile peut être implémenté en utilisant les codes mobiles ou les objets distants. Des exemples de la première catégorie proviennent des agents de TCL (Tool Command Language), un langage agent, et de Telescript. La deuxième catégorie est représentée par les aglets (*voir ci-après*).

Pour utiliser les agents mobiles, un système doit incorporer une plate-forme agent. Cette plate-forme doit permettre toutes les fonctionnalités dont les agents ont besoin, en particulier le modèle de navigation. Pour le cycle de vie, il faut définir les services de création, de destruction, de démarrage, de suspension, d'arrêt, etc. Le modèle de calcul indique les moyens de calcul de l'agent. Le modèle de sécurité décrit la façon dont les agents ont le droit d'accéder aux ressources du réseau et aux terminaux. Le modèle de communication définit les modes de communication entre agents et entre un agent et une autre entité, comme le réseau. Le modèle de navigation se charge de tous les transports de l'agent entre deux entités du réseau.

L'intégration du code par une machine Java est déjà très puissante, mais des chips Java pourraient renforcer encore l'intégration des agents dans les systèmes actuels. De nouveaux progiciels, comme Jini, pourraient encore accentuer la puissance des agents mobiles. La taille de ces agents dépend de leurs fonctions. Par exemple, les agents mobiles de contrôle de la sécurité peuvent être très gros et contenir plusieurs milliers de lignes de code. Il faut noter que ces agents mobiles peuvent augmenter leurs fonctions en chargeant du code *via* le réseau.

Pour que les codes mobiles puissent s'imposer, ils doivent être normalisés. L'OMG a déjà proposé un premier standard indépendant de la plate-forme utilisant fortement CORBA.

Une autre façon d'introduire les agents mobiles consiste à les définir comme des processus logiciels qui se substituent à l'utilisateur pour interagir en toute liberté dans le réseau avec des serveurs. L'autonomie fonctionnelle des agents mobiles, qui est un de leurs points forts, sollicite le minimum de ressources de communication. Le langage Telescript, de General Magic, constitue l'un des premiers outils de développement d'agents mobiles, aux côtés du langage Java.

Les agents mobiles Telescript intègrent les instructions de l'utilisateur concernant une tâche spécifique et se déplacent aux endroits nécessaires à l'exécution de leur tâche, par exemple l'achat de billets. Les sites qui réceptionnent ces agents mobiles agissent comme des hôtes et assurent la sécurité de l'exécution des programmes de l'agent.

De nombreux autres exemples de conception et d'utilisation d'agents mobiles dans les environnements de télécommunications sont mentionnés dans diverses publications. En particulier, les virus peuvent être considérés comme de tels agents. Trois cibles se retrouvent dans ces travaux :

- les caractéristiques du langage pour fournir les besoins des agents mobiles ;
- l'implémentation de ces besoins à partir d'extensions du système d'exploitation pour bénéficier des avantages des agents mobiles ;
- le système d'agents mobiles, considéré comme une application spécialisée, fonctionnant au-dessus du système d'exploitation.

En résumé, les systèmes d'agents mobiles existants s'appuient soit sur des classes Java, soit sur des langages de script interprétés, soit sur des services existants du système d'exploitation. Il existe des contraintes pour limiter les possibilités et pour contrôler les agents mobiles. Ces contraintes proviennent des points suivants : sécurité, identification, portabilité, mobilité, communication, gestion des ressources, contrôle et gestion des données.

Pour comparer l'approche agent avec l'approche client-serveur, il faut rappeler que, dans l'architecture client-serveur, des programmes spécialisés sont implémentés en vue de satisfaire le plus de clients possible. Le processus client s'exécute le plus souvent sur une machine distante et communique avec le serveur pour accomplir une tâche. Cette approche peut générer une forte hausse du trafic sur le réseau, laquelle, suivant le type de réseau, peut arriver à congestionner le réseau. Le concept d'agent mobile propose de rapprocher le client de la source et de réduire le trafic engendré en déplaçant les requêtes des clients au niveau des serveurs.

Les réseaux actifs

Les réseaux actifs sont similaires aux autres réseaux à transfert de paquets et de trames. L'unité de base transférée dans ce réseau est le paquet. Les nœuds ont pour mission d'examiner les différents champs du paquet, qui ont un emplacement parfaitement déterminé. En particulier, le champ d'adresse permet de déterminer le port de sortie. C'est une machine virtuelle qui interprète les différents champs du paquet. On peut considérer que cette machine virtuelle est une interface paquet, ce que l'on appelle classiquement une API réseau, ou NAPI (Network Application Programming Interface). Pour un réseau IP, l'API IP est le langage défini par la syntaxe et la sémantique de l'en-tête IP. Dans les réseaux que nous connaissons, la machine virtuelle est fixe, et le langage utilisé primaire.

On peut dire des réseaux actifs que les nœuds fournissent une API réseau programmable. Si l'on considère que, dans un réseau IP, l'en-tête du paquet fournit les entrées de la machine virtuelle, on peut définir un réseau actif comme un réseau dans lequel les nœuds possèdent une machine virtuelle qui exécute le code contenu dans l'en-tête des paquets.

De nombreuses catégories de réseaux actifs peuvent être définies à partir des attributs suivants :

- Puissance d'expression du langage, qui détermine le degré avec lequel le réseau va pouvoir être programmé. Le langage peut aller d'ordres simples à des langages très évolués. Plus le langage est simple, plus le temps de traitement est court. À l'inverse, plus le langage est puissant, plus du sur-mesure peut être mis en œuvre.
- Possibilité de définir un état stable à partir des précédents messages du même flot, de façon que la rapidité d'exécution puisse être augmentée sans qu'il soit nécessaire de redéfinir un état de la machine virtuelle.
- Granularité du contrôle, qui permet de modifier le comportement d'un nœud pour tous les paquets qui le traversent, quel que soit le flot auquel il appartient, ou, à l'autre extrême, de ne modifier le comportement du nœud que pour le seul paquet en cours de traitement. Tous les cas intermédiaires sont possibles, en particulier le comportement commun sur un même flot ou sur un même ensemble de flots.

- Moyen de donner les ordres de programmation : il est possible de considérer que les ordres aux nœuds actifs sont donnés par des paquets spécifiques, par exemple des paquets de signalisation, et non plus par un ordre indiqué par un langage plus ou moins évolué contenu dans l'en-tête des paquets.
- Architecture des nœuds, pour regarder à quel niveau de cette architecture interviennent les commandes ou, en d'autres termes, à quel niveau se trouve l'interface de programmation. L'architecture peut influer sur les choix du logiciel et du matériel. En particulier, elle peut utiliser des processeurs reconfigurables, à des niveaux conceptuels plus ou moins élevés.

Les fonctionnalités des nœuds des réseaux actifs sont partagées entre l'environnement d'exécution et le système d'exploitation du nœud. La figure 31.7 illustre une telle architecture de réseau actif.

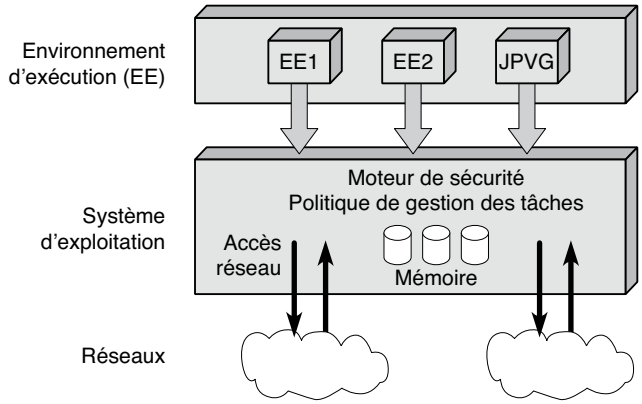


Figure 31.7

Architecture des réseaux actifs

Il est possible d'envoyer des commandes sur l'environnement d'exécution par le biais d'un protocole d'encapsulation, appelé ANEP (Active Network Encapsulation Protocol). L'en-tête d'un paquet ANEP contient un champ d'identification du type de paquet. Plusieurs environnements d'exécution pouvant être présents dans un nœud actif, l'adresse du nœud nécessite une adresse complémentaire.

Les interfaces existantes incluent :

- l'interface d'accès à l'environnement d'exécution ;
- l'interface entre l'environnement d'exécution et le système d'exploitation du nœud ;
- l'interface d'accès au système d'exploitation du nœud.

Les réseaux programmables

Les réseaux programmables forment une partie des réseaux actifs, dont le rôle est de développer un ensemble d'abstractions logicielles des ressources du réseau permettant d'accéder à ces ressources par leur abstraction.

L'objectif de ces réseaux est de rendre les nœuds programmables pour les adapter aux demandes des utilisateurs et des services. Les commandes de programmation, qui peuvent être effectuées tant par un réseau de signalisation que par des paquets utilisateur contenant des programmes de contrôle, peuvent attaquer les nœuds à différents niveaux d'abstraction. L'IEEE a lancé un groupe de travail destiné à normaliser ces interfaces.

Le modèle de référence P.1520

La figure 31.8 illustre les différentes couches du modèle de référence P.1520, qui est l'une des propositions de l'ISO pour définir les niveaux des interfaces programmables. En d'autres termes, l'architecture P.1520 propose une programmation des nœuds actifs au niveau de quatre interfaces, nommées V, U, L et CCM.

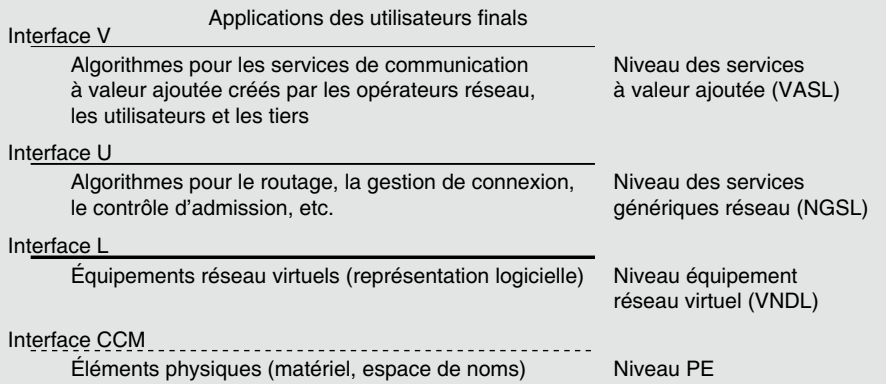


Figure 31.8

Le modèle de référence P.1520

En haut de l'architecture, nous trouvons le niveau VASL (Value-Added Services Level), dont les entités sont les algorithmes de bout en bout qui confèrent de la valeur ajoutée aux services exécutés par les couches inférieures. Ces services peuvent être de type gestion des flots en temps réel, synchronisation des flots de différents médias, etc.

Le niveau sous-jacent, NGSL (Network Generic Services Level), comporte des entités qui sont les algorithmes travaillant sur les fonctions de la couche réseau, comme les algorithmes de mise en place de circuits ou de chemins virtuels dans un réseau ATM ou d'ouverture d'un flot dans un environnement IP. Cette couche doit également avoir une connaissance des sous-réseaux. Dans le même ordre d'idée, la structuration en VPN fait partie de cette couche.

Le niveau VNDL (Virtual Network Device Level) possède des entités qui sont des représentations logiques des ressources matérielles et logicielles des composants du réseau.

La dernière couche est composée des éléments physiques du réseau. Cette couche PE (Physical Element) gère le matériel et l'espace d'adresse physique pour atteindre ces éléments physiques. On y trouve les commutateurs ATM et les routeurs IP.

Associés à ces différentes couches, quatre types d'interfaces ont été définis :

- L'interface V, qui permet à une application d'accéder à la couche VASL. Elle fournit un grand ensemble d'API pour écrire des logiciels de haut niveau permettant d'ajouter une plus-value aux applications.

- L'interface U (Upper Interface), qui se trouve entre les couches VASL et NGSL et qui présente les fonctionnalités de la couche NGSL à la couche VASL. L'interface U travaille sur les services génériques des réseaux et sur les propriétés des ouvertures des connexions entre applications ou entre clients et serveurs.
- L'interface L (Lower Interface), qui permet d'utiliser les ressources de la couche VNDL par la couche NGSL. L'interface L permet de traiter les états des ressources réseau, comme une table de commutation ATM ou une table de routage IP.
- L'interface CCM (Connection Control and Management), qui permet d'accéder aux ressources physiques. Cette interface n'est pas une interface programmable, à la différence des précédentes, mais un ensemble de protocoles permettant l'échange et le contrôle des informations à un niveau bas de l'architecture.

La figure 31.9 illustre cette architecture pour un environnement IP.

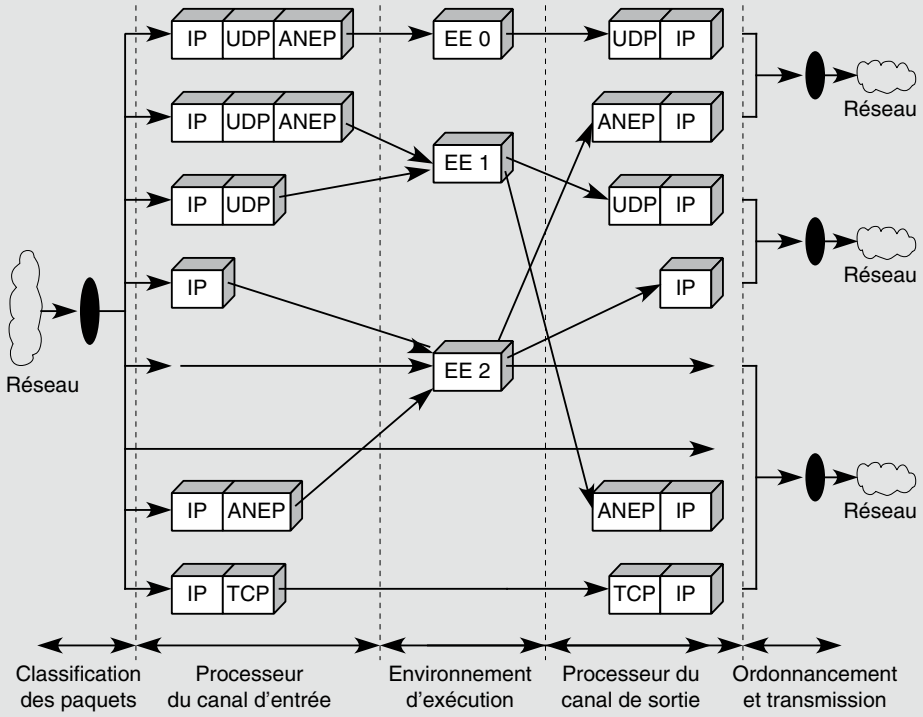


Figure 31.9

Application du modèle P.1520 à un réseau IP

Les réseaux autonomes

Le concept de réseau actif et programmable est en train d'être remplacé par le concept de réseau autonome. Un réseau autonome est un réseau qui n'a pas besoin de centre de gestion ou de centre de contrôle pour prendre ses décisions. Un réseau autonome est donc un réseau qui peut décider par lui-même la façon dont il se comporte. C'est un concept qui a été introduit pour les réseaux NGN (Next Generation Network), dont l'objectif est de remplacer tous les réseaux existants en intégrant tous les médias de communication.

Un réseau autonome doit être capable de s'autogérer, de détecter les problèmes, de réparer lui-même les pannes et de s'autocontrôler lorsque aucune communication n'est pas possible.

Les éléments de réseau doivent participer eux-mêmes à la construction d'un réseau autonome avec des propriétés diverses, comme l'optimisation des ressources, la reconnaissance automatique de l'environnement (*context aware*) et l'organisation automatique de la sécurité. L'objectif est de comprendre comment apprendre les bonnes décisions, quelle influence ont les différents éléments de réseau et, plus globalement, comment optimiser le comportement du réseau. Les outils pour arriver à ce type de système autonome proviennent des systèmes multiagents que nous avons détaillés précédemment.

L'auto-organisation d'un réseau IP passe d'abord par le besoin d'avoir une vue globale du réseau et de comprendre les conséquences d'un événement quelconque qui se produit dans le réseau. Ensuite, le réseau doit être capable de réagir à l'événement.

Les réseaux autonomes peuvent se concevoir sur d'autres réseaux qu'IP pour des objectifs très particuliers, comme des réseaux avec des missions critiques ou des réseaux interplanétaires où le centre de contrôle met tellement de temps à communiquer avec les sondes qu'il est impossible de prendre des décisions en temps réel.

Les réseaux autonomiques

Nous en arrivons aux réseaux autonomiques, qui sont, par définition, des réseaux autonomes et spontanés. Ce sont les réseaux que nous avons défini précédemment, mais en y ajoutant la propriété de spontanéité, c'est-à-dire de temps réel : le processus est capable de réagir de façon autonome et dans un laps de temps acceptable pour le processus.

Une première définition des réseaux autonomiques est illustrée à la figure 31.10.

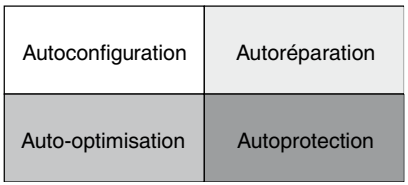


Figure 31.10
Définition d'un réseau autonomique

Les réseaux autonomiques sont capables de s'autoconfigurer pour s'adapter dynamiquement aux modifications de l'environnement, de s'auto-optimiser pour lui donner une efficacité opérationnelle toujours optimisée, de s'autoréparer pour lui permettre d'avoir une fiabilité importante et de s'autoprotéger pour sécuriser les ressources et les informations qui transitent.

Pour réaliser ces différentes fonctions, les réseaux autonomiques doivent posséder un certain nombre d'attributs :

- connaître leur état interne (self aware) ;
- connaître leur environnement (environment aware) ;
- être capables de comprendre les caractéristiques de leurs performances (self monitoring) ;
- être capables de changer leur état interne (self adjusting).

Pour atteindre ces objectifs, il faut changer l'architecture des réseaux. Les réseaux autonomiques proposent donc une nouvelle architecture à quatre plans, qui ajoute un plan de connaissance aux trois plans habituels que sont le plan de données, le plan de contrôle et le plan de gestion.

La figure 31.11 illustre la nouvelle architecture des réseaux autonomiques. L'objectif du plan de connaissance est de rassembler les connaissances du réseau et d'obtenir pour chaque point du réseau une vision plus ou moins globale.

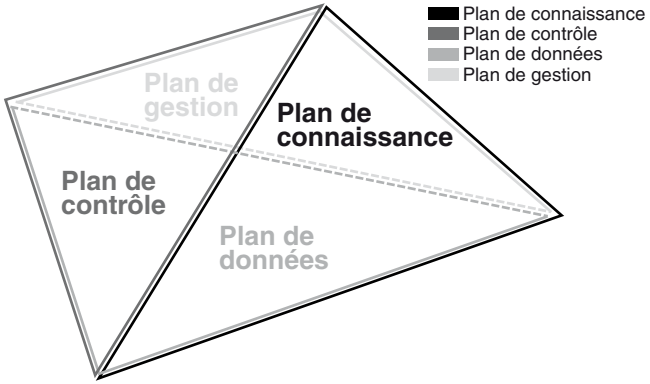


Figure 31.11
L'architecture des réseaux autonomiques

Le plan de connaissance (Knowledge Plane) a pour objectif de piloter les algorithmes de contrôle qui se trouvent dans le plan de contrôle (Control Plane), lequel contrôle le plan de données (Data Plane), qui correspond aux quatre premières couches de l'architecture classique des réseaux. Le plan de gestion (Management Plane) a pour charge d'administrer les trois autres couches.

L'objectif du plan de connaissance est de rendre le réseau plus intelligent en lui permettant de comprendre son comportement, ce qui a donné lieu à une nouvelle génération de protocoles. Jusqu'à présent, chaque algorithme de contrôle (routage, qualité de service, sécurité, fiabilité, etc.) devait aller rechercher par lui-même les éléments dont il avait besoin. Par exemple, un algorithme de routage tel qu'OSPF recherche les états des liens en amont et en aval jusqu'aux entrées et sorties du réseau. Ces informations sont

exploitables par d'autres algorithmes, comme un algorithme de contrôle de la qualité de service ou de la congestion ou encore de l'admission dans le réseau. En utilisant un plan de connaissance, cette information se trouve dans ce plan, et chaque algorithme de contrôle peut aller la chercher à l'instant où il en a besoin.

À terme, les protocoles normalisés devraient être modifiés pour tenir compte de ce plan de connaissance. Un autre avantage du plan de connaissance est la possibilité d'utiliser dans un algorithme de contrôle des informations qui n'auraient pas pu être prises en compte dans l'algorithme normal.

Vue située

Il est évidemment important de ne pas rendre le réseau trop lourd à force de transporter des connaissances en tout genre et en quantité importantes. Pour cela, il est possible d'utiliser des « vues situées ». Ces dernières proviennent du monde de l'intelligence artificielle et indiquent la prise en compte de connaissances qui sont situées dans une vue à déterminer. On peut ainsi définir une vue située par le nombre de sauts nécessaires pour aller chercher l'information, par exemple à un ou deux sauts, etc.

La figure 31.12 illustre une vue située à un saut.

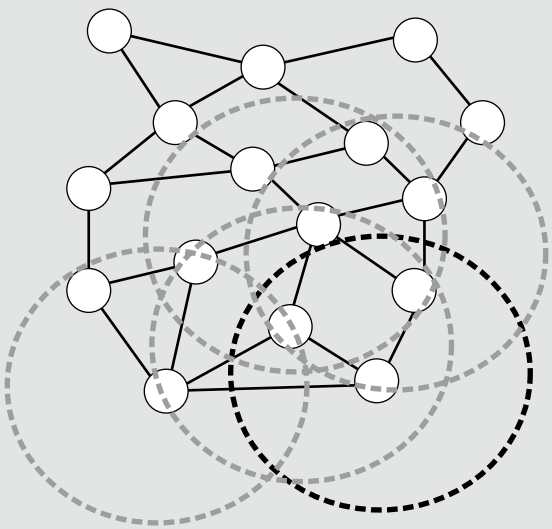


Figure 31.12

Vue située à un saut

La vue située à un saut présente l'avantage de très bien passer à l'échelle puisque le transport des connaissances est limité. Cela n'empêche pas les connaissances de se diffuser dans le réseau puisqu'un point recevant une connaissance l'intègre dans ses propres connaissances et la diffuse à ses voisins. Cette connaissance est cependant moins fraîche que si la vue située était un peu plus grande.

Une optimisation de la vue située doit donc être réalisée en fonction des connaissances dont ont besoin les algorithmes de contrôle. Il faut pour cela répondre aux questions lesquelles ? où ? et quand ? « Lesquelles » référence les connaissances nécessaires à l'optimisation d'un algorithme ; « où » concerne la portée de la vue située ; « quand » indique les rafraîchissements nécessaires pour que la connaissance soit exploitable. En partant de ces différents paramètres, il est possible de générer des vues situées un peu plus complexes que la seule définition à un saut, les informations de liens et toutes les secondes.

Les réseaux autopilotés

Jusqu'en 2008, les réseaux ont été remarquablement statiques, et un ingénieur réseau devait souvent être présent pour prendre les choses en main dès qu'un problème survenait. Pour les très grands réseaux, plusieurs dizaines d'ingénieurs réseau pouvaient être nécessaires pour assurer la maintenance et gérer les problèmes divers et variés qui survenaient.

L'objectif des réseaux autopilotés est de garantir un pilotage automatique du réseau par le biais d'un logiciel capable de gérer les algorithmes de contrôle d'une façon coordonnée et d'optimiser de ce fait le fonctionnement du réseau.

Au début des années 2000, une première tentative a consisté à utiliser des réseaux programmables et des réseaux actifs. Les recherches n'ont pas été totalement concluantes pour des raisons de sécurité et de coût. Une nouvelle génération a été lancée à partir de 2005 avec les réseaux autonomiques que nous venons de présenter.

Conclusion

Doucement, mais sûrement, l'intelligence arrive dans les réseaux. Cette intelligence englobe la communication, le raisonnement et la décision. Les systèmes multiagents fournissent le socle principal de cette intelligence, qui permet de prendre des décisions de contrôle ou de gestion lorsqu'il en est temps. Nous n'en sommes encore qu'aux prémices, et pourtant l'intelligence est omniprésente depuis le début des années 2010.

La sécurité est un des premiers bénéficiaires de cette intelligence. Par exemple, un composant intelligent, de type réseau de neurones, est capable d'analyser la saisie d'une personne sur un clavier et d'arrêter la communication en cas de saisie non reconnue.

L'intelligence dans les réseaux est donc un vaste champ de recherche, qui devrait déboucher sur l'implémentation de beaucoup plus d'intelligence dans les équipements de réseau tels que routeurs, pare-feu et boîtiers intermédiaires.

32

Virtualisation, Post-IP et Cloud

Dans ce dernier chapitre, nous examinons la virtualisation de réseau, qui tend à se généraliser après la virtualisation des serveurs, le Post-IP, l'architecture qui pourrait être mise en place pour succéder au monde IP, et enfin le Cloud, qui est également une lame de fond dans le domaine applicatif.

Les raisons de la révolution en cours vers le Post-IP proviennent des faiblesses du monde IP à plusieurs égards, notamment la sécurité, la consommation énergétique et les communications avec les mobiles. La virtualisation est certainement le premier atout de cette nouvelle génération. C'est pourquoi nous l'examinerons en premier.

La virtualisation de réseau

La virtualisation n'est pas une technique neuve, puisqu'elle avait été introduite sur les premiers gros ordinateurs, qui utilisaient une mémoire virtuelle, c'est-à-dire une mémoire qui, au lieu d'être en RAM, se trouvait sur un disque dur. Toute l'astuce était de ramener les pages de mémoire du disque dur sur la mémoire RAM juste avant que l'unité centrale en ait besoin. Par la suite, un certain nombre de mécanismes ont été implémentés avec cette solution afin que l'utilisateur ait l'impression que les services dont il a besoin sont situés sur une machine à proximité, alors qu'ils se trouvent en réalité sur une machine lointaine.

La virtualisation de serveurs a connu un formidable succès en permettant de regrouper plusieurs serveurs sur une machine unique, l'utilisateur ayant pourtant l'impression de ne disposer que d'un seul serveur. La virtualisation de réseau tient du même principe : plusieurs réseaux virtuels se partagent une même infrastructure physique.

La virtualisation de réseau a été lancée par un projet américain appelé GENI (Global Environment for Network Innovations), dans lequel Intel proposait de construire un routeur uniquement constitué de sa partie matérielle, sans aucun système d'exploitation réseau. Les éditeurs de logiciels n'avaient plus qu'à implémenter leur système sur la machine. L'avantage de la virtualisation réside précisément dans la possibilité d'implémenter plusieurs systèmes d'exploitation réseau sur une même machine à l'aide d'un « hyperviseur ». Un routeur virtuel se présente comme illustré à la figure 32.1.

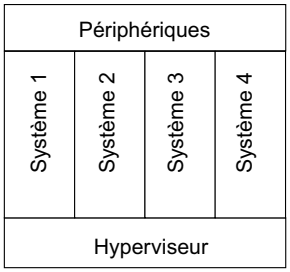


Figure 32.1
Un routeur virtuel

Un routeur virtuel n'est donc qu'une instance d'un routeur physique, et plusieurs routeurs virtuels peuvent s'exécuter en même temps sur un même routeur physique. On obtient alors la possibilité de déployer plusieurs réseaux, que l'on peut appeler des réseaux virtuels, sur le même réseau physique.

Un tel environnement est illustré à la figure 32.2, dans laquelle les réseaux A, B, C et D coexistent sur les mêmes routeurs et les mêmes lignes physiques.

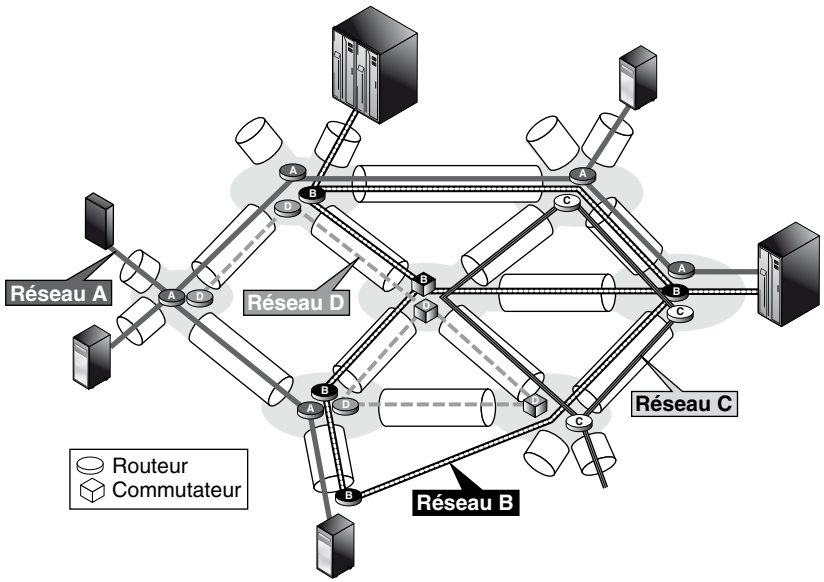


Figure 32.2
Virtualisation des routeurs

Le réseau virtuel A est réalisé à partir des routeurs virtuels avec le système d'exploitation A. De même, le réseau virtuels B est réalisé avec les instances B et ainsi de suite. Chaque instance d'un même routeur physique pouvant employer des protocoles complètement différents, les réseaux sont également totalement différents. Chacun peut utiliser les protocoles liés à une application données.

Les avantages de cette technique de virtualisation sont nombreux. Le premier est de pouvoir faire tourner sur le même réseau physique, des réseaux virtuels utilisant des technologies totalement différentes. On peut, par exemple, obtenir un premier réseau utilisant le système d'exploitation réseau IOS de Cisco, un deuxième utilisant JUNOS de Juniper, un troisième et un quatrième utilisant les systèmes d'Alcatel-Lucent et de Ericsson, etc. Il est également possible de faire tourner plusieurs *releases* différentes d'un même système d'exploitation réseau. Il est évident que les exemples précédents n'ont guère de chance d'être réalisés, car les équipementiers ne souhaitent pas forcément commercialiser leur logiciel sans leur matériel. Le découplage matériel/logiciel ne sera disponible que pour des systèmes ouverts parvenus à maturité.

Un second avantage de la virtualisation concerne l'utilisation des ressources. Il est évident que les ressources peuvent être beaucoup mieux utilisées en mettant en marche et en arrêtant des routeurs virtuels ou encore en les déplaçant : si un routeur est trop chargé, il est ainsi possible de déplacer un ou plusieurs routeurs virtuels vers d'autres routeurs physiques.

Dans tous les cas, les ressources doivent être totalement isolées. Cela implique une excellente sécurité entre les réseaux. Si l'un des routeurs virtuels tombe en panne, cela ne doit pas affecter les autres. Si, bien sûr, un routeur physique tombe en panne, tous les routeurs virtuels seront eux aussi en panne. L'isolation des réseaux protège également contre les attaques globales.

Utilisation

Deux types d'utilisation peuvent être faits de la virtualisation de réseaux :

- Plusieurs réseaux virtuels à l'intérieur d'une même entreprise. Cette solution permet de créer un réseau virtuel pour la téléphonie, un autre pour la télésurveillance, un autre encore pour les vidéoconférences dans l'entreprise, etc.
- Plusieurs réseaux virtuels d'opérateurs différents peuvent se partager les mêmes ressources physiques et permettre ainsi une baisse des coûts. Il s'agit alors d'une sorte de VPN à l'échelle d'un opérateur primaire qui ouvre des réseaux pour des opérateurs. Lorsqu'un opérateur virtuel veut augmenter sa capacité, il va demander à l'opérateur primaire d'augmenter ses ressources.

Une autre utilisation de la virtualisation qui ne fait que croître concerne les applications de type « Cloud ». En termes simples, le principe du Cloud consiste à mettre les ressources d'une entreprise quelque part dans le réseau afin de les partager avec d'autres utilisateurs. Le Cloud propose des ressources de type serveur, capacité de calcul, capacité de stockage, logiciels divers et variés, etc. L'utilisateur peut partager ces ressources avec

d'autres utilisateurs en tenant compte bien sûr de la sécurité des informations. Les ressources virtuelles peuvent migrer pour optimiser les ressources physiques. De même, le client peut se déplacer sur l'Internet et avoir accès à ses ressources de n'importe où. Pour relier les ressources à l'utilisateur, il faut créer des réseaux, et ces réseaux ne peuvent être que virtuels puisqu'il serait impossible de créer un nouveau réseau à chaque déplacement ou demande de ressources supplémentaires d'un utilisateur.

La virtualisation est enfin une technologie idéale pour tester de nouveaux protocoles et de nouvelles architectures sans arrêter le réseau opérationnel. Il suffit de construire un nouveau réseau virtuel avec les nouvelles générations de protocoles ou d'architecture. L'isolation est dans ce cas une propriété essentielle pour que le test des nouvelles architectures ne vienne pas gêner les réseaux opérationnels.

On peut en conclure que la virtualisation présente de nombreux avantages. Elle est aujourd'hui considérée comme une opportunité pour apporter de la souplesse aux réseaux. De plus, elle permet de passer d'une technologie à une autre sans se compliquer trop la vie.

Les désavantages de la virtualisation sont liés à la surcharge apportée par l'hyperviseur et aux besoins de mémoire et de puissance de calcul, surtout si l'on veut séparer totalement les différents domaines.

Isolation

L'isolation est un principe fondamental de la virtualisation de réseaux. Il ne faut pas qu'un réseau puisse avoir un impact sur les autres réseaux.

Une première solution simple, mais peu efficace, serait de partitionner les ressources entre les différents réseaux. Dans ce cas, il n'y aurait pas grand-chose à gagner, car les ressources d'un réseau non utilisées à un instant t ne peuvent être utilisées par d'autres réseaux virtuels. Il faut donc trouver une solution pour à la fois partitionner les ressources et faire en sorte que les ressources non utilisées puissent profiter aux autres.

On peut obtenir cette propriété par des ordonnanceurs. Le plus simple est d'avoir dans un nœud autant de files d'attente que de réseaux virtuels. À chaque file d'attente, on octroie des crédits en fonction des ressources qui ont été allouées au nœud. Chaque réseau utilise un crédit pour envoyer un paquet. Lorsqu'une station n'a plus de crédit, elle ne peut plus émettre. Tant qu'il y a d'autres files actives, elle est arrêtée. Si, à un moment donné, toutes les files sont vides, une réallocation de crédits est attribuée à toutes les files. Cela peut toutefois conduire à un blocage, à la fois des files d'attente n'ayant plus de crédit et de celles ayant des crédits mais pas de paquet à servir. Pour éviter ce problème, les files d'attente bloquées peuvent créer des crédits négatifs et continuer à transmettre. Lorsque la somme des crédits positifs et négatifs devient égale à zéro, on réinitialise le système en accordant des crédits positifs à l'ensemble des nœuds.

On peut, à partir de cet exemple repris de Xen (*http://www.xen.org*), modifier des paramètres ou en ajouter d'autres, comme permettre à une file d'attente de servir plusieurs paquets, c'est-à-dire d'utiliser plusieurs jetons sans interruption. On utilise ainsi moins d'énergie, une même machine virtuelle étant à l'œuvre sans interruption.

Virtualisation de réseau étendue

La technologie de virtualisation que nous avons décrite est la première à être apparue en matière de réseau et est sûrement l'une des plus intéressantes. Il est cependant possible de virtualiser bien d'autres équipements et logiciels que les seuls routeurs. La virtualisation d'un contrôleur Wi-Fi, le contrôleur Ucopia par exemple, permet de gérer des points d'accès associés à chaque contrôleur virtuel. Les points d'accès associés peuvent avoir leur propre pile protocolaire.

Les points d'accès eux-mêmes peuvent être virtualisés. Il suffit pour cela d'introduire un hyperviseur soutenant plusieurs systèmes d'exploitation. Chaque point d'accès virtuel possède ses propres logiciels de gestion et de contrôle et est indépendant : il peut donc représenter un opérateur. De même, il est possible de virtualiser les antennes 2G et 3G (BTS et NodeB) et de partager les antennes virtuelles entre différents opérateurs.

Globalement, toute ressource peut être virtualisée, à partir du moment où elle peut être réalisée en logiciel. L'avenir est donc à la virtualisation de l'ensemble des logiciels et des matériels.

Il est également possible de virtualiser des couches protocolaires, comme l'illustre la figure 32.3.

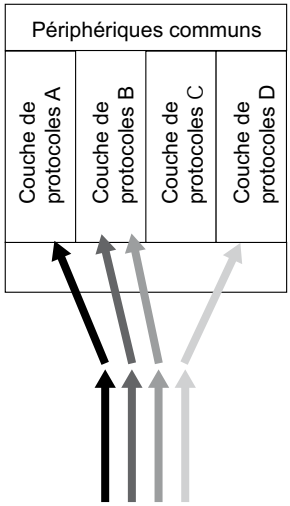


Figure 32.3
Virtualisation de protocoles

Dans cette figure, le système d'exploitation supporte toute une série de piles protocolaires adaptées à différents problèmes, comme le manque d'énergie, la sécurité, la qualité de service, l'augmentation de la disponibilité, etc. Chaque sous-réseau virtuel peut utiliser sa propre pile protocolaire (A, B, C ou D) et en changer en cas de découverte d'un problème, tel qu'une batterie presque vide ou une attaque DDOS.

Il est également possible de virtualiser des liens physiques ou hertziens. Pour un lien physique, il est possible de faire croire à des utilisateurs qu'ils ont leur propre lien physique,

comme s'il n'était pas partagé alors qu'il l'est. Il est de même possible de virtualiser des liens hertziens en faisant croire à un utilisateur qu'il a son propre point d'accès Wi-Fi.

En conclusion, la virtualisation est une technique importante, qui permet d'introduire de nouvelles technologies sans douleur sous forme de réseaux virtuels particuliers. Il est ainsi possible de tester sur un réseau opérationnel de nouvelles architectures sans prendre de risque. Cette solution permet également de penser au long terme puisque la solution transitoire est déjà inventée avec la virtualisation. Lorsque l'architecture du futur sera trouvée, elle pourra entrer petit à petit dans le monde des réseaux grâce à la virtualisation.

Le Post-IP

Cette dernière section s'oriente vers la conclusion du livre. Avant cela, nous allons examiner les différentes voies qui s'ouvrent pour se diriger vers la future génération de réseaux, ou Post-IP. Le monde IP montrant ses limites de plus en plus clairement, le Post-IP est la génération qui doit succéder à IP. Le Post-IP peut être compatible IP ou non. Il serait dans une certaine mesure meilleur de recommencer à zéro plutôt que de poser des rustines un peu partout.

Pourquoi une nouvelle génération ?

Avant de se poser les questions sur le Post-IP, résumons les étapes déjà traversée pour essayer de deviner le futur.

Par un premier pas essentiel, Internet a introduit la notion de paquet d'informations. Grâce à la numérisation en des suites de bits 0 et 1, l'information à véhiculer est regroupée en paquets de quelques milliers de bits pouvant être transmis sur les lignes de télécommunications. Les utilisateurs envoient leurs paquets plus ou moins simultanément sur les portes d'entrée du réseau. Des lignes de communication internes prennent en charge les paquets pour les acheminer vers leurs destinataires respectifs. Lorsqu'un utilisateur ne parle pas ou n'émet rien, aucune ressource n'est monopolisée à son intention, contrairement au bon vieux réseau téléphonique, qui, dans ce cas, laisse le circuit inutilisé.

La bataille s'engage alors entre une intelligence dans le poste de travail et une intelligence dans le réseau, autrement dit entre l'informatique, qui veut vendre des PC de plus en plus gourmands, et les télécommunications, qui souhaitent imposer un cœur de réseau puissant, capable d'offrir une panoplie de services réseau. La première solution fournit un réseau bon marché, avec des terminaux relativement chers à la périphérie. La seconde accepte des terminaux bas de gamme, mais le coût de l'accès au réseau devient important. Aucun des deux combattants ne peut gagner, puisque, de toute évidence, la solution consiste à partager l'intelligence entre le terminal et le réseau. Pour compliquer cette première étape, les câblo-opérateurs perturbent le jeu avec leurs accès haut débit vers l'utilisateur et la mainmise sur l'interface avec le téléviseur.

La deuxième génération d'Internet, l'Internet 2, a explosé au début des années 2000. Les prototypes se sont succédé : vBNS, Abilene, ou VTHD (vraiment très haut débit), construit par France Télécom. La différence avec la première génération est nette.

L'intelligence gérant le transport dans le réseau se partage entre le terminal et les équipements réseau. L'intelligence consiste ici à noter en clair dans le paquet la sémantique des informations transportées. Grâce à cette connaissance, les nœuds traversés peuvent privilégier le traitement de certains flux au détriment d'autres. Par exemple, un paquet contenant de la parole téléphonique devient hautement prioritaire afin de réduire le temps de traversée du réseau et de rejouer la parole correctement à l'oreille du destinataire.

Une deuxième révolution concerne un domaine connexe, celui du codage de l'information. Des progrès fulgurants permettent d'atteindre des compressions considérables. Pour transporter un canal de télévision couleur au début des années 1980, le débit nécessaire se comptait en une centaine de mégabits par seconde. Pour avoir la même qualité d'image aujourd'hui, 1 Mbit/s est suffisant, et demain 100 Kbit/s. La compression atteint un facteur de 1 000. Ces valeurs s'obtiennent en temps réel, tous les calculs nécessaires étant effectués en quelques millisecondes. Ces progrès s'expliquent, bien sûr, par l'augmentation de la puissance des processeurs, mais aussi par le perfectionnement des algorithmes de compression.

Dans le même temps, la parole téléphonique se contente de 8 000 bits par seconde. Quant aux informations des serveurs Web, elles sont compressées dans des proportions moindres. Dans un certain sens, les progrès accomplis pour compresser les flots d'information sont plus importants que ceux qui concernent le débit des utilisateurs et des applications. Un débit de 10 Mbit/s par utilisateur représente un excellent compromis pour l'interface avec le réseau. Un calcul à partir de cette valeur pour un pays de la taille de la France montre que si 60 millions d'habitants transmettent à pleine charge en même temps, un débit de 600 000 Gbit/s s'exerce sur le réseau. En comparaison, les câbles posés dans la première décennie du XXI^{e} siècle acceptent des capacités de 40 Gbit/s. Pour un pays comme la France, 12 500 longueurs d'onde de ce type seraient suffisantes pour tout transporter, ce qui représente douze ou treize câbles à 1 000 longueurs d'onde. En 2005, une dizaine de câbles étaient suffisants pour supporter à eux seuls tout le trafic, les plus hautes capacités pour une seule fibre optique atteignant 128 Tbit/s. En 2010 les câbles transportent dix fois plus de débit ; les débits ayant été multipliés par 100, il faut donc dix fois plus de câbles.

Cependant, ce raisonnement comporte quelques faiblesses, car un utilisateur peut envoyer de l'information vers plusieurs points en même temps, ce qui démultiplie les débits, et des applications autres que la parole, comme la télévision, la vidéo à la demande ou l'accès à de grandes masses de données, pourraient accentuer encore la demande. Néanmoins, on peut considérer que le problème du débit est presque résolu dans les cœurs de réseau.

La troisième révolution en cours concerne l'accès de l'utilisateur au réseau et *vice versa*. La fibre optique FTTH (Fiber to the Home) est une première réponse, avec des débits de 100 Mbit/s et plus. Plus étonnant, le téléphone portable, le fameux GSM, qui se transforme en Wi-Fi/UMTS, puis en LTE et LTE Advanced propose également des débits se dirigeant vers les 100 Mbit/s. Entre fixe et mobile, les débits s'équilibrent, et la convergence vers un seul réseau s'établit.

En résumé, l'Internet 2 offre le multimédia à tous et de n'importe où. Que reste-t-il à modifier pour atteindre le Post-IP ? La rupture technologique du Post-IP, résidera dans

la maîtrise de la complexité du réseau et de ses services, qui reste cachée et restera peu visible de l'utilisateur final. Depuis des années, un maître mot se retrouve sans arrêt dans les discours des scientifiques : faire simple. La simplicité est cependant tout le contraire de la réalité, puisque les composants, matériels ou logiciels, se compliquent à la vitesse du progrès et que leur maîtrise complète n'est plus exercée que par des ingénieurs chercheurs extrêmement qualifiés. Imaginer que simplification puisse rimer avec progrès est irréaliste dans le contexte actuel d'une explosion tous azimuts de la recherche et des développements.

Sans maîtrise, le Post-IP pourrait s'effondrer sous l'effet d'un virus, de la défaillance d'un nœud ou d'une liaison, d'une panne électrique, de l'incendie d'une salle de contrôle, d'une application qui diverge ou d'une surcharge passagère. La maîtrise doit donc prévenir, mais aussi secourir. Les difficultés à surmonter pour y parvenir sont nombreuses. En particulier, la nature distribuée des environnements réseau complique le contrôle et la gestion. De plus, le gigantisme devient une donnée du problème, impliquant un contrôle encore plus fin.

La direction à privilégier est l'intelligence. Le débat sur l'intelligence en informatique n'est pas nouveau, mais il prend ici une signification inédite, qui réside dans la capacité à s'adapter à une situation nouvelle, à contrôler le bon fonctionnement du réseau et à gérer les services dans des conditions non prévues. L'intelligence recoupe en fait plusieurs actions distinctes : apprendre, communiquer et raisonner.

Plusieurs voies peuvent être envisagées, dont nous voyons déjà les prémices : les réseaux intelligents et les réseaux autonomiques. Les réseaux intelligents forment un concept architectural déjà ancien, où le mot « intelligent » renvoie à l'adaptation. Le réseau doit pouvoir s'adapter à la demande des utilisateurs. Même si les retombées sont très nettes dans les réseaux de télécommunications, nous n'en sommes qu'aux premiers balbutiements.

Dans cette direction, l'informatique comble son retard à pas de géant, avec des langages tels que Java, capables de disperser en tous points du réseau, voire chez l'utilisateur, des fragments de logiciel à même de s'exécuter pour réaliser une tâche définie. Ces fragments de logiciel peuvent éventuellement se déplacer par eux-mêmes. Lutter contre la complexité par la complexité est-elle pour autant une solution acceptable ? La complexité pour prévenir et secourir progressera-t-elle plus rapidement que la complexité du réseau ? La réponse semble positive, mais la course-poursuite ne fait que commencer.

La deuxième direction s'attaque au processus de l'autonomique : les nœuds du réseau doivent pouvoir s'autoconfigurer et prendre des décisions par eux-mêmes à partir de la valeur de leurs paramètres de fonctionnement, et ce en temp réel. En cas de panne, ou simplement de surcharge, les nœuds doivent être capables instantanément de prendre les dispositions nécessaires pour continuer à rendre les services demandés, parfois de façon dégradée.

Une autre forte direction provient de la virtualisation, qui permet, comme on l'a vu, à plusieurs systèmes et plusieurs piles protocolaires de cohabiter. Suivant l'état du système, une architecture de communication peut être meilleure qu'une autre. Associée à l'autonomique, la virtualisation permet de trouver la meilleure pile protocolaire pour un sous-réseau particulier.

Dans le Post-IP, l'évolution vers le pilotage automatique des réseaux n'a pas pour objectif d'augmenter les performances, mais de permettre de mieux les gérer. Cette génération n'est plus très loin, puisqu'il suffira de stabiliser les techniques apportant de l'intelligence dans les réseaux et de les mettre en œuvre dans l'infrastructure.

Le Post-IP devra faire beaucoup plus attention aux clients. En particulier, il devra caractériser la qualité de service qui leur est offert : comment un opérateur peut-il prouver à l'un de ces clients qu'il lui a bien offert la qualité de service que celui-ci a négociée au travers d'un SLA ?

Pour atteindre ces objectifs, les opérateurs vont devoir se munir d'équipements de mesure et de contrôle. La métrologie devrait donc devenir un domaine important des réseaux. Aujourd'hui, si la station terminale ne reçoit pas la page Web demandée dans un laps de temps acceptable, qui était de 8 s avant 2002 et qui est passé ensuite à 4 s puis à 2 s, il est difficile de diagnostiquer en temps réel les raisons entre le slow-start, l'occupation du serveur, une surcharge ou un problème de la station de travail, de la boucle locale, de la machine d'accès de l'opérateur, du réseau de l'ISP auquel le client est abonné, du réseau d'un ISP traversé, du serveur distant, etc.

Les services rendus par les opérateurs sont donc assez différents les uns des autres, ce qui perturbe fortement les interconnexions des opérateurs pour obtenir une qualité de service de bout en bout.

Les deux schémas de la figure 32.4 illustrent la problématique de l'hétérogénéité et de l'homogénéité des réseaux. Dans la partie supérieure, une communication doit traverser les réseaux de quatre opérateurs distincts, qui semblent offrir la même qualité de service. En fait, les qualités sont différentes, et la communication a globalement une qualité de service égale à la moins bonne des qualités de service.

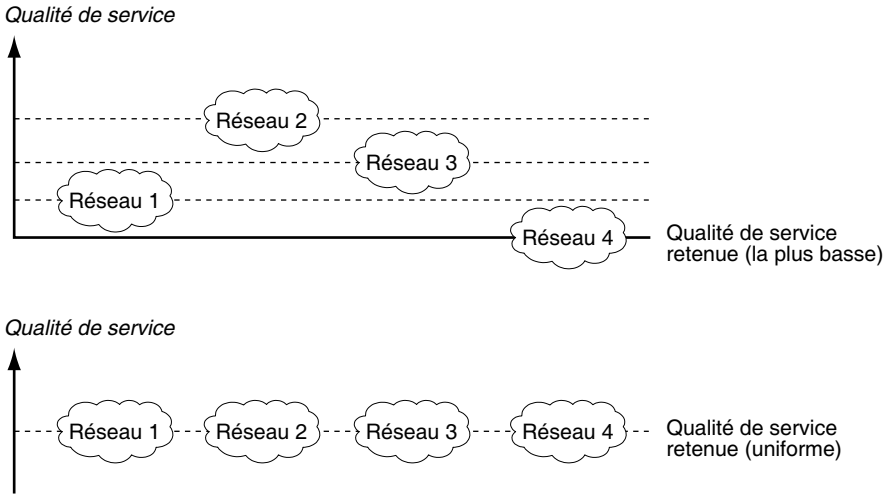


Figure 32.4

Comparaison des qualités de service retenues pour une interconnexion de réseaux

Si les ISP arrivent à s'entendre, les réseaux devraient offrir des services de même niveau, comme illustré au bas de la figure 32.4, et la qualité de bout en bout sera homogène. Pour cela, il faut que les opérateurs obéissent aux mêmes règles et configurent leurs nœuds de la même façon. C'est la raison pour laquelle les techniques de contrôle par politique (*voir l'annexe S*), dans lesquelles l'ensemble des grands opérateurs suivraient les mêmes politiques, devraient faciliter les communications de bout en bout.

La sécurité est un problème de fond pour les réseaux de communication mondiale. Une authentification forte et une gestion des identités, telles que celles que nous avons introduites au chapitre 29, sont indispensables. De même, le respect de la vie privée passera par de nouvelles techniques de traçabilité fermée.

On peut enfin se poser la question de l'arrivée d'une génération Post-IP. Sa perspective est encore lointaine, mais les spécialistes s'accordent à dire qu'au début de 2011 nous sommes encore dans l'âge de pierre des réseaux. Entre la pierre, le bronze et l'or, beaucoup de découvertes sont encore à effectuer. Nombreux sont ceux qui pensent que le monde IP devra être remplacé par un autre environnement, qui marquera le début de l'âge de bronze. Ce remplacement pourrait intervenir d'ici à une dizaine d'années, au travers des progrès de la virtualisation, des réseaux autonomiques, des réseaux hyper-sécurisés et certainement d'une technologie de transport qui n'a pas encore été inventée.

Les raisons de ce changement à long terme sont multiples : forte dépense énergétique de la pile protocolaire IP, mauvaise adaptation dans beaucoup de circonstances au monde des mobiles et du hertzien, difficulté à sécuriser cette architecture, etc. Les recherches se dirigent aujourd'hui vers des protocoles reconfigurables par eux-mêmes et capables de s'adapter à leur environnement.

D'autres pistes totalement différentes sont également à l'étude, avec les communications dites quantiques et l'introduction de communications biotechnologiques.

Les tendances 2015

Penchons-nous d'abord sur les deux grandes familles de réseaux toujours représentées schématiquement par l'informatique et les télécommunications : les réseaux sans signalisation et les réseaux avec signalisation.

La figure 32.5 illustre les principaux réseaux de ces deux catégories.

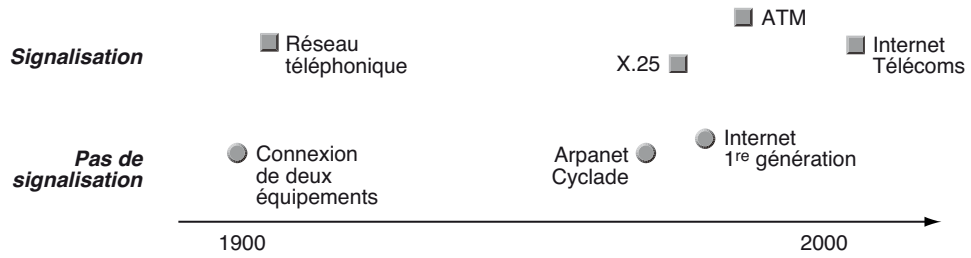


Figure 32.5

Les deux grandes familles de réseaux, avec et sans signalisation

Les réseaux sans signalisation permettent une communication simple entre un émetteur et un récepteur. L'information est véhiculée dans des paquets, qui portent l'adresse complète du destinataire, de telle sorte que ces paquets se suffisent à eux-mêmes pour atteindre ce dernier. Au contraire, dans un réseau avec signalisation, aucune information ne peut transiter d'un émetteur vers un récepteur tant que la communication n'a pas été signalée au récepteur. Dans pratiquement tous les cas, on profite de la signalisation pour mettre en place dans le réseau un chemin, sur lequel des ressources peuvent être réservées.

Les réseaux avec signalisation sont nombreux dans le monde des télécommunications. Le premier d'entre eux a dû être le réseau téléphonique, la gestion de la signalisation par des opératrices ayant été remplacée par une signalisation automatique par la suite, utilisant le protocole CCITT n° 7. Les réseaux à commutation de type X.25 puis relais de trames, ATM et Ethernet proviennent d'idées émanant du secteur des télécommunications. Comme il faut une signalisation provenant également du monde IP, l'IRTF (Internet Research Task Force) a décidé de monter le groupe de travail NSIS (Next Step In Signaling). Ce groupe de travail a été repris par l'IETF pour aller vers une normalisation de fait.

Une fois le domaine des réseaux séparé en deux grandes familles, on peut rechercher les différentes directions que peuvent prendre les réseaux de demain. Dans chacune de ces familles, deux grandes possibilités s'offrent aux architectes réseau, ce qui donne quatre architectures. Dans le domaine du routage, le réseau peut être surdimensionné dans le seul but de permettre une certaine qualité de service. Cette solution est souvent inacceptable pour des raisons de coût. Une seconde solution est de surdimensionner uniquement les classes les plus prioritaires, c'est-à-dire la classe EF (Expedited Forwarding). En ce qui concerne la commutation, la direction forte reste MPLS et à plus long terme le NGN.

Le Cloud

Le Cloud est un paradigme né vers 2005 qui propose de positionner les équipements et les logiciels d'une entreprise à l'extérieur de l'entreprise elle-même, c'est-à-dire dans le Cloud.

Les avantages de cette solution sont nombreux pour l'entreprise : elle peut augmenter ou diminuer les ressources à volonté. L'entreprise n'est pas obligée de surdimensionner son système puisqu'elle peut ajouter de nouvelles ressources dès que nécessaire. De plus, l'utilisateur ne paie que pour ce qu'il consomme. L'entreprise n'a pas à gérer du personnel pour prendre en charge la gestion des équipements, ce qui est un avantage indéniable pour les solutions de type Cloud. Du côté du fournisseur de service Cloud, les avantages sont également nombreux : partage des ressources entre tous les clients et, de façon sous-jacente, virtualisation de serveurs, de systèmes, de logiciels, de réseaux, etc. Le multiplexage statistique de ressources est d'autant meilleur que le nombre de clients est élevé.

Le Cloud peut être assez bien représenté par l'environnement Internet, qui est capable de prendre en charge des serveurs de différents types susceptibles d'exécuter les demandes

des entreprises. Cette solution représente un déport de l'environnement informatique de l'entreprise vers Internet. Les ressources du Cloud peuvent être extrêmement diverses : ressources de calcul, stockage des informations, logiciel, service de mail, etc. En fonction des éléments virtualisés dans le Cloud, plusieurs types de Clouds ont été définis :

- IaaS (Infrastructure as a Service) : toute première approche, avec une partie de la virtualisation prise en charge par le Cloud, telle que serveurs réseau, serveurs de stockage, réseau lui-même. On déporte dans le réseau Internet PABX, pare-feu, serveurs de stockage, etc., et plus généralement les serveurs liés à l'infrastructure réseau.
- PaaS (Platform as a Service) : second modèle de Cloud, avec, en plus de l'infrastructure, le logiciel intermédiaire correspondant à la plate-forme Internet. Les serveurs de l'entreprise ne prennent en compte que les applications.
- SaaS (Software as a Service) : permet au fournisseur de Cloud de proposer, en plus de l'infrastructure et de la plate-forme, les applications elles-mêmes. Globalement, il ne reste plus rien dans l'entreprise, si ce n'est des terminaux d'accès à Internet. Cette solution, également appelée Cloud Computing, extériorise quasiment l'ensemble de l'informatique et des réseaux de l'entreprise.

Ces solutions devraient énormément se développer dans les années 2010. Il est cependant assez difficile pour un fournisseur de Cloud d'optimiser ses infrastructures et surtout le placement des ressources à la disposition des utilisateurs. En effet, l'optimisation dépend fortement de ce que l'on recherche, côté opérateur comme utilisateur. Si l'on cherche à optimiser le Cloud, le critère de performance est important : optimisation des performances et de la consommation d'énergie, meilleurs équilibrage de charge, etc.

L'emplacement des ressources doit varier dans le temps pour réaliser des économies : mieux vaut les placer sur des serveurs situés dans une zone où il fait nuit sur terre. Cependant le déplacement des ressources peut être coûteux. Si l'optimisation concerne l'énergie dépensée, il est évident que les ressources doivent être rassemblées sur une même machine, le plus près possible de l'entreprise. On peut trouver des dizaines de solutions différentes en fonction du critère de performance à optimiser.

La virtualisation joue un rôle essentiel puisque toutes les ressources sont virtualisées (serveurs, stockages, équipements de réseau, etc.). En particulier, la connexion de l'entreprise à ses serveurs dans le Cloud doit s'effectuer par le biais d'un réseau virtuel mis en place dans ce but et où les routeurs virtuels se déplacent en fonction des emplacements des ressources de l'entreprise.

L'une des difficultés qui se pose à une entreprise est de trouver le meilleur fournisseur de Cloud par rapport à ses besoins. Malheureusement, trouver un fournisseur de messagerie, de temps calcul, de mémoire, d'un logiciel particulier, etc., est impossible. Il faut faire appel à plusieurs fournisseurs de Cloud, ce qui complique la décision de l'entreprise. Pour résoudre ce problème, des fournisseurs intermédiaires apparaissent, que l'on pourrait appeler des fournisseurs de Sky, capables de sélectionner les Clouds nécessaires à une entreprise.

Un fournisseur de Sky peut être vu comme le fournisseur d'un ensemble de Clouds adaptés à une entreprise. Un autre nom pour un fournisseur de Sky est un fournisseur de Clouds

virtuels. Le client (l'entreprise), au lieu de rechercher lui-même l'ensemble des Clouds qui vont lui offrir le service dont il a besoin, s'adresse au fournisseur de Sky capable de gérer lui-même tous les accès aux différents Clouds nécessaires à l'entreprise.

Les plus grandes entreprises de la fin des années 2010 devraient être des fournisseurs de Sky.

Conclusion

Sans être exhaustif, loin s'en faut, cet ouvrage a cherché à fournir un panorama des principales techniques mises en œuvre pour réaliser une communication entre des processus distants. Il est évident qu'il devra être à nouveau mis à jour dans quelque temps pour permettre au lecteur d'avoir une vue aussi précise que possible de l'état d'avancement des architectures de réseau.

Comme nous l'esquissions dans ce dernier chapitre, la grande direction que devraient prendre les réseaux dans les années à venir concerne la fourniture de service de types Cloud ou Sky. On peut y rajouter la virtualisation, la sécurité et le pilotage automatique, c'est-à-dire la mise en œuvre de mécanismes capables de configurer automatiquement et en temps réel les équipements de réseau afin qu'ils rendent le meilleur service possible par rapport à ce qui leur est demandé.

Il faut ajouter la potentielle arrivée d'un Post-IP. Si aucune découverte de rupture n'est effectuée, le Post-IP sera compatible avec IP et constituera une nouvelle génération du monde Internet. Dans le cas contraire, les architectures de réseau seront bouleversées.

Les Réseaux, 7e édition

Annexes

Annexe A

1. Introduction aux réseaux

Le RNIS, en anglais ISDN (Integrated Services Digital Network), a été le premier réseau à transporter simultanément la parole téléphonique sous forme circuit et les données sous forme paquet. Bien que ce type de réseau soit en bout de course, il est intéressant de comprendre le chemin parcouru en quelques années par les réseaux multimédias.

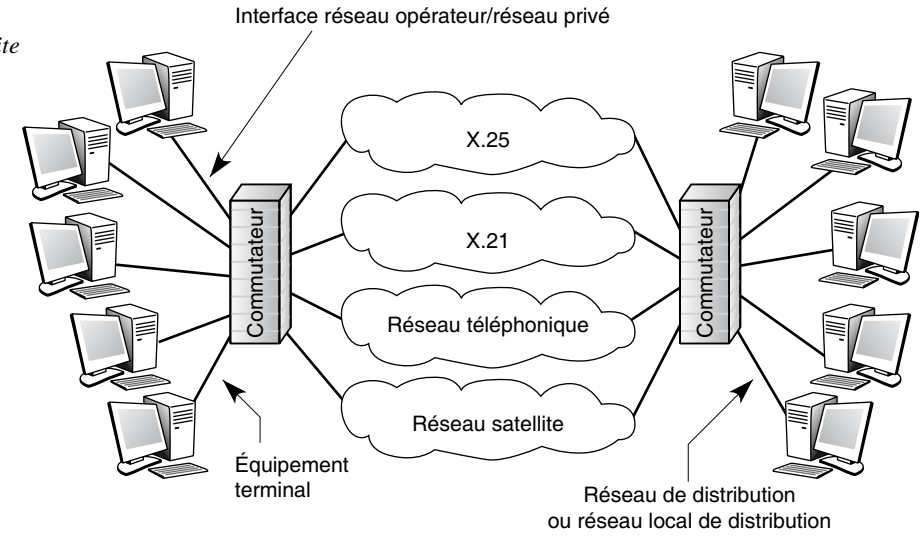
Le RNIS (réseau numérique à intégration de services)

Les figures A.1 à A.3 illustrent l'évolution des réseaux à intégration de services. La première étape a consisté à cacher les différents réseaux existants par une interface utilisateur unique, l'interface S, permettant aux équipements terminaux d'accéder à ces réseaux. Pour l'utilisateur, la vue était unique, et les réseaux étaient transparents. Les données devaient être transportées par le meilleur chemin possible, avec une qualité de service déterminée. Ce premier réseau RNIS, dit RNIS bande étroite, est illustré à la figure A.2.

Le RNIS a été étendu par l'introduction d'un réseau de signalisation, encore appelé réseau sémaphore, ayant pour fonction de transporter les commandes. Pour comprendre le rôle de la signalisation, prenons l'exemple simple de l'application téléphonique. Lorsque l'abonné numérote, sa signalisation part par l'interface S et arrive dans le réseau sémaphore, qui véhicule ces quelques octets jusqu'à l'appareil du correspondant en un temps inférieur à 100 ms. Si celui-ci est déjà en train de téléphoner, une signalisation repart vers l'émetteur et produit une tonalité d'occupation. Les circuits du réseau téléphonique ne sont donc pas utilisés. Si le poste du correspondant est libre, la signalisation déclenche la sonnerie. Si l'utilisateur distant est absent, une nouvelle signalisation part de l'émetteur, toujours acheminée par le réseau sémaphore, pour arrêter la sonnerie.

Le réseau téléphonique n'est pas non plus utilisé dans ce cas. Si l'abonné destinataire décroche, une signalisation part pour mettre en place un circuit. Ce circuit a été prévu par la commande initiale, qui, lors de son acheminement, a consulté les nœuds de commutation du réseau téléphonique pour s'assurer de sa mise en place en cas de succès de la communication.

Figure A.1
RNIS bande étroite



Le réseau sémaphore permettait un gain d'utilisation de 10 à 20 % du réseau téléphonique. Ce réseau de signalisation est connu et normalisé depuis de longues années sous le sigle CCITT n° 7, ou, en anglais, SS7. C'est un réseau à transfert de paquets, qui suit l'architecture du modèle de référence. La figure A.2 présente cette extension du RNIS.

L'étape suivante a vu arriver un nouveau réseau, le RNIS large bande, qui permettait de prendre en charge les très hauts débits. La première technique choisie pour ce réseau a été le transfert ATM. Ce réseau supplémentaire s'ajoutait en fait aux réseaux bande étroite, comme l'illustre la figure A.3.

Figure A.2
RNIS avec réseau sémaphore

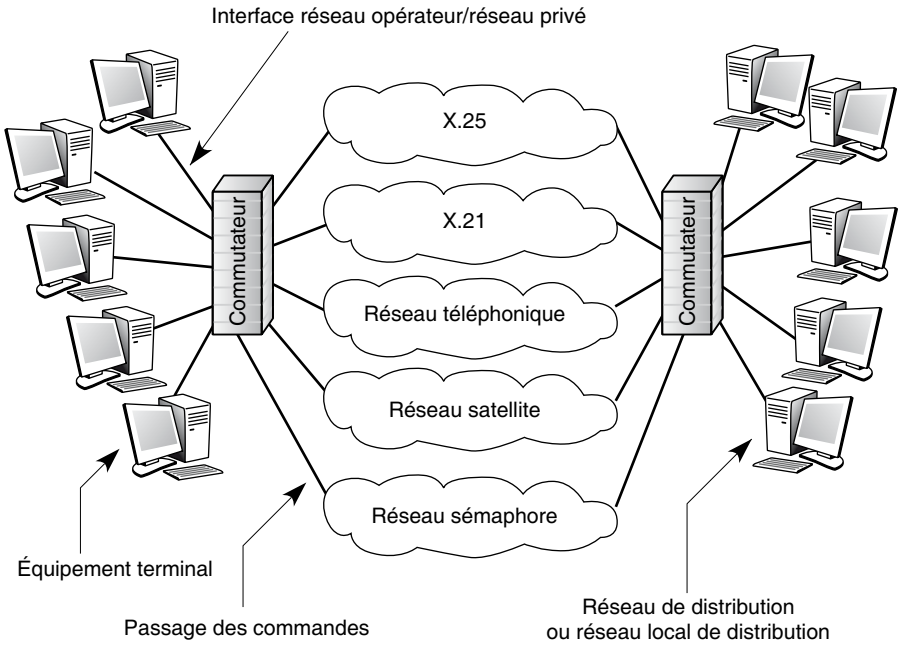
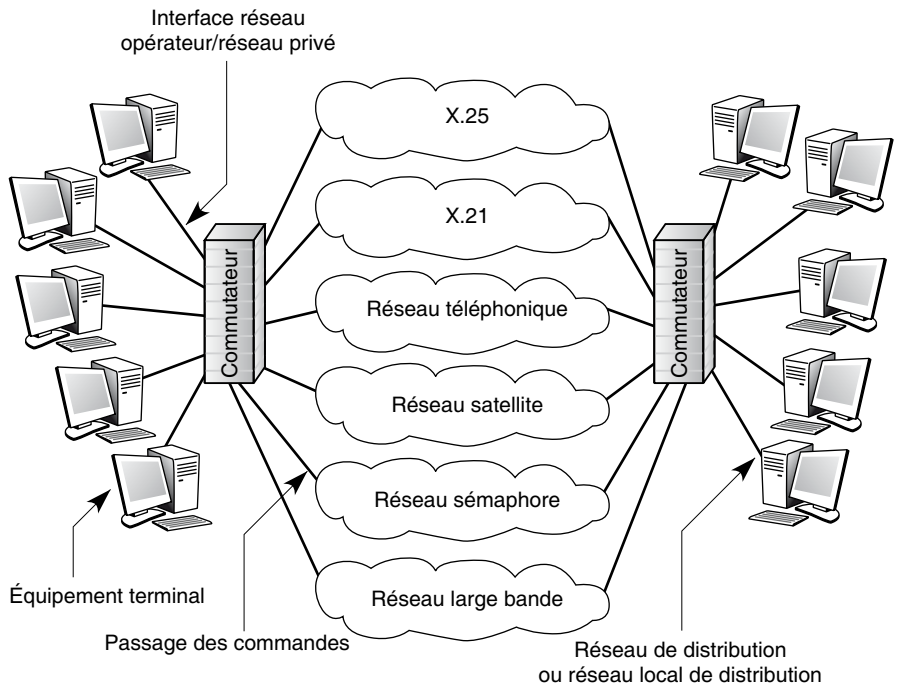


Figure A.3
Extension du RNIS avec un réseau large bande

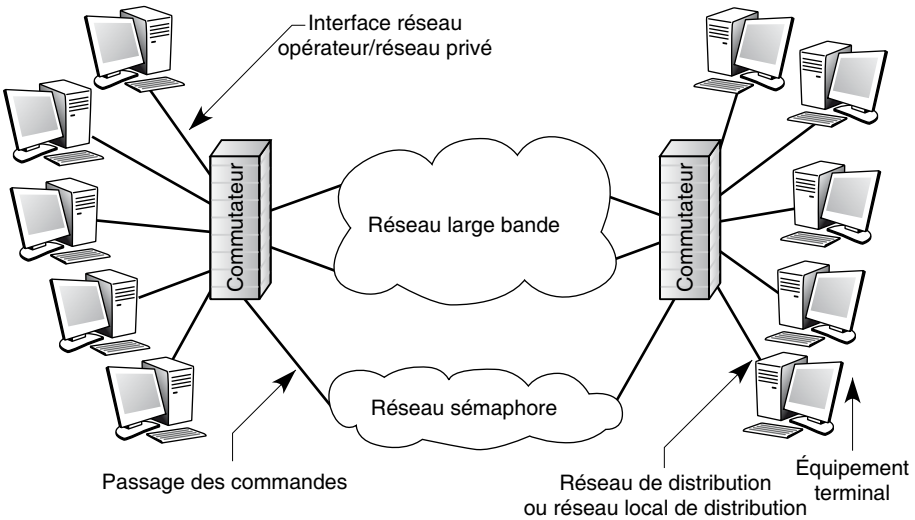


L'étape ultime a visé l'intégration de tous les réseaux en un seul et même réseau, le réseau large bande. Le réseau sémaphore était lui-même intégré au réseau large bande. Les équipements terminaux comportaient des organes permettant de produire et de recevoir directement des paquets IP.

Ce réseau est illustré à la figure A.4. Il s'agit du réseau large bande intégré, ou IBCN (Integrated Broadband Communication Network). Ce réseau forme les prémices du réseau qui porte le nom de NGN (Next Generation Network), parce que l'IBCN a été introduit en pensant que le cœur du réseau serait ATM, alors que les choix se sont portés vers d'autres solutions.

Le réseau de signalisation, qui était spécifique, s'est transformé en un réseau IP. Les réseaux de ce type sont aujourd'hui des réseaux MPLS (MultiProtocol Label Switching) ou GMPLS (Generalized MPLS).

Figure A.4
Réseau large bande intégré



Annexe B

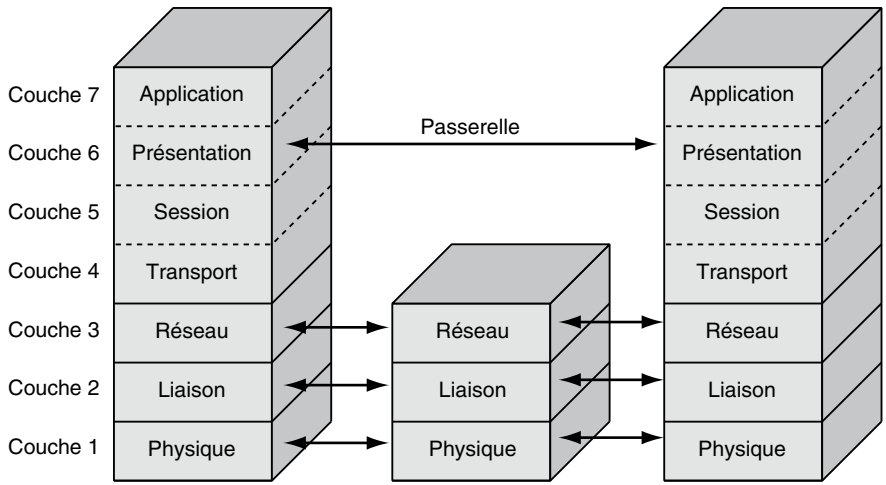
2. Architecture des réseaux

Cette annexe détaille le modèle de référence, puis l'architecture ISO qui en est dérivée et les architectures multipoints qui sont de plus en plus utilisées.

Le modèle de référence

La figure B.1 illustre l'architecture en sept couches du modèle de référence.

Figure B.1
L'architecture OSI



Le concept d'architecture en couches consiste à attribuer trois objets à chaque couche. Pour une couche de niveau N, ces objets sont les suivants :

- **Service N.** Désigne le service qui doit être rendu par la couche N de l'architecture à la couche supérieure (N + 1). Ce service correspond à un ensemble d'actions devant être effectuées par cette couche, incluant événements et primitives, pour rendre ce service au niveau supérieur.
- **Protocole N.** Désigne l'ensemble des règles nécessaires à la réalisation du service N. Ces règles définissent les mécanismes permettant de transporter les informations d'un même service N d'une couche N à une autre couche N. En particulier, le protocole N propose les règles de contrôle de l'envoi des données.
- **Points d'accès au service N, ou N-SAP (Service Access Point).** Les points d'accès à un service N sont situés à la frontière entre les couches N + 1 et N. Les services N sont fournis par une entité N à une entité N + 1 par le biais de ces points d'accès. Les différents paramètres nécessaires à la réalisation du service N s'échangent sur cette frontière. Un N-SAP (Service Access Point) permet donc d'identifier une entité de la couche N + 1, et chaque N-SAP peut être mis en correspondance avec une adresse.

Chaque service, protocole ou N-SAP d'une couche N comporte les attributs suivants :

- sémantique d'association ;
- sémantique de fonctionnalité ;
- syntaxe de codage.

La sémantique d'association désigne la façon de dialoguer de deux entités communicantes. Elle peut être de deux types : avec ou sans connexion. Dans un dialogue avec connexion, trois phases se succèdent dans le temps :

1. Établissement de la connexion entre les deux entités communicantes.
2. Transfert des données.
3. Fermeture de la connexion.

Ces phases sont longuement décrites dans ce chapitre.

La figure B.2 illustre les concepts de base du modèle de référence.

Les différentes phases de la communication sont caractérisées par l'échange de primitives de service et d'unités de donnée de protocole, ou PDU (Protocol Data Unit). Nous revenons plus en détail sur ces primitives et unités de donnée un peu plus loin dans ce chapitre.

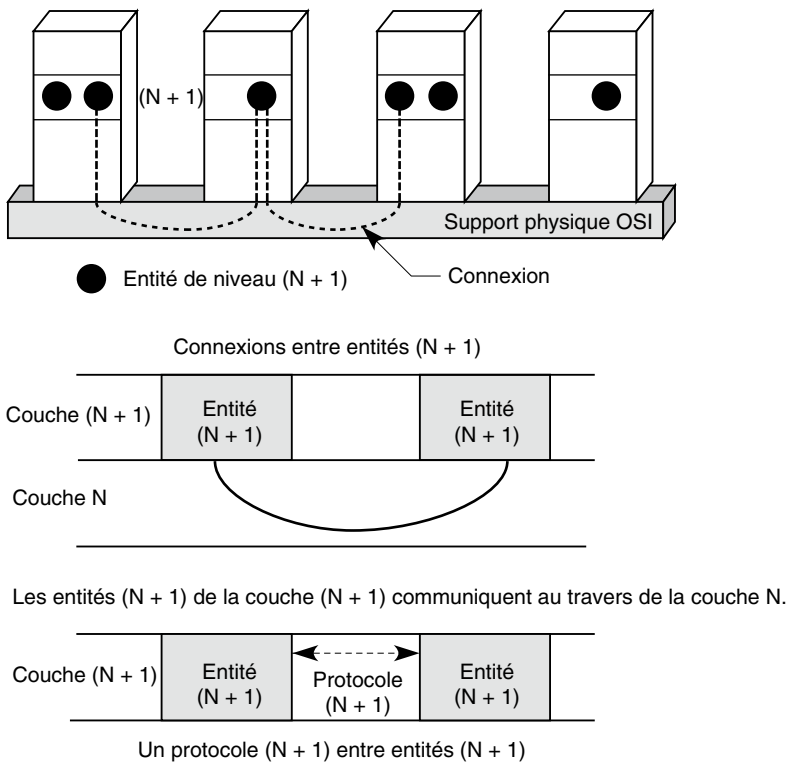
Comme expliqué précédemment, le deuxième attribut des objets d'une couche est la sémantique de fonctionnalité. Ce concept désigne l'ensemble des procédures qui sont utilisées pendant la phase de transfert des données. Pour une association avec connexion, par exemple, ces procédures sont les suivantes :

- fragmentation-réassemblage
- concaténation-séparation
- données expresses

- remise en séquence
- réinitialisation
- contrôle de flux
- contrôle d'erreur

Le troisième attribut d'un service, protocole ou N-SAP d'une couche N est la syntaxe de codage. Il s'applique au codage des primitives de service et des PDU utilisées par la sémantique d'association. Ces syntaxes de codage permettent de décrire les entités rencontrées dans un réseau. La syntaxe la plus utilisée est ASN.1 (Abstract Syntax Notation 1), que nous introduisons dans ce chapitre en même temps que la couche 6 du modèle de référence.

Figure B.2
Concepts de base du modèle de référence



La sémantique d'association

La sémantique d'association propose deux types de dialogue entre les entités communicantes : le mode avec connexion (connection oriented) et le mode sans connexion (connectionless oriented).

La norme de base du modèle de référence opte pour le mode avec connexion, tandis que l'additif n° 1 à la norme retient le mode sans connexion. Dans ce dernier mode, les entités homologues ont une connaissance *a priori* des possibilités de communication communes. Les discussions actuelles pourraient aboutir à une intégration des deux modes dans les futures architectures NGN (Next Generation Network).

Le mode avec connexion

La norme de base ISO 7498 définit explicitement la mise en place d'une connexion pour les communications entre des entités de même niveau. Elle indique qu'une entité de niveau N ne peut émettre de bloc d'information qu'après avoir demandé à l'homologue avec lequel elle souhaite communiquer la permission de le faire.

Pour mettre en place une connexion, le protocole de niveau N émet donc un bloc d'information contenant une demande de connexion de niveau N. Le récepteur a le choix d'accepter ou de refuser la connexion par l'émission d'un bloc de données indiquant sa décision. Dans certains cas, la demande de connexion peut être arrêtée par le gestionnaire du service, qui peut refuser de propager la demande de connexion jusqu'au récepteur, par exemple par manque de ressources internes. Une demande d'ouverture de circuit virtuel de niveau 3, qui n'est rien d'autre qu'une connexion réseau, peut ainsi être stoppée dans un nœud intermédiaire si la mémoire est insuffisante ou si la capacité d'émission est dépassée.

La mise en place du mode avec connexion, permettant la communication entre entités homologues, se déroule en trois phases distinctes :

1. Établissement de la connexion.
2. Transfert des données de l'utilisateur d'une entité à l'autre.
3. Libération de la connexion.

L'avantage du mode avec connexion est évident pour la sécurisation du transport de l'information. Puisque les émetteurs et les récepteurs se mettent d'accord, l'ensemble de l'activité du réseau est facilement contrôlable, tout au moins au niveau des nœuds extrémité. Au moment de l'ouverture d'une connexion, des paramètres peuvent de surcroît être passés entre l'émetteur et le récepteur pour équilibrer la transmission dans des limites admissibles par les deux extrémités. On parle en ce cas de négociation de la qualité de service, ou QoS (Quality of Service), laquelle s'effectue au moment de l'ouverture de la connexion. Pendant toute la durée de vie de la connexion, des paramètres peuvent être échangés entre les participants à la communication.

Le mode avec connexion présente cependant plusieurs difficultés, engendrées notamment par la lourdeur de la mise en place d'une connexion. Même pour n'envoyer que quelques octets, il faut mettre en place la connexion et discuter des valeurs des paramètres de service et, le cas échéant, de la qualité de service. S'il faut ouvrir une connexion à chaque niveau de l'architecture OSI, le temps d'émission de quelques octets est considérablement plus long que dans le mode sans connexion.

L'accès à des applications multipoint est par ailleurs délicat dans ce mode, puisqu'il faut ouvrir autant de connexions que de points à atteindre. Si, par exemple, on veut diffuser un fichier vers 1 000 utilisateurs distants, il est nécessaire d'ouvrir 1 000 connexions,

c'est-à-dire d'émettre 1 000 demandes de connexion, et ce à tous les niveaux de l'architecture.

Le mode sans connexion

Dans le mode sans connexion, les blocs de données sont émis sans qu'il soit nécessaire de s'assurer au préalable que l'entité distante est présente. L'existence d'une connexion à l'un quelconque des niveaux de l'architecture est cependant nécessaire pour s'assurer que le service rendu n'est pas complètement inutile. Pour mettre en place une telle connexion, il faut utiliser les services des couches inférieures, ce qui implique nécessairement leur activité.

La principale difficulté d'une communication en mode sans connexion réside dans le contrôle de la communication, puisqu'il n'y a pas de négociation entre l'émetteur et le récepteur. Une station peut ainsi recevoir des données venant simultanément d'un grand nombre de stations émettrices, alors que, dans le mode avec connexion, la station réceptrice n'accepterait pas d'ouvrir autant de connexions. En raison de la difficulté à contrôler la communication, le gestionnaire du réseau doit souvent prendre plus de précautions dans une communication sans connexion que dans le mode avec connexion.

Le mode sans connexion est intéressant pour le transport de messages courts, tandis que celui avec connexion est plus adapté aux messages longs, à condition que les temps de mise en place et de libération des connexions soient négligeables par rapport à la durée de la communication. Comme expliqué précédemment, le mode avec connexion est privilégié dans la norme de base.

Si une connexion est réalisée à un niveau N, les niveaux supérieurs peuvent utiliser un mode sans connexion. Parmi les nombreuses applications qui peuvent utiliser le mode sans connexion, citons la messagerie électronique dans sa définition la plus large. La messagerie est le moyen d'émettre de l'information vers un utilisateur lointain dont on ne sait s'il est présent ou non. Lorsque le client n'est pas actif, il est remplacé par une boîte aux lettres. La connexion de session s'effectue avec la machine qui gère cette boîte aux lettres.

Quantité d'autres applications fonctionnent dans le mode sans connexion, notamment les suivantes :

- **Transfert de fichiers.** Il suffit de s'assurer que le représentant de l'utilisateur final est capable de mémoriser l'ensemble des données contenues dans le fichier.
- **Conférence répartie.** Différents clients mettent en commun des informations dans une boîte aux lettres spécialisée, accessible à l'ensemble des éléments du groupe. Cette application se satisfait très bien du mode messagerie.
- **Accès à une base de données distribuée.** Un utilisateur à la recherche d'informations d'un type non complètement spécifié émet sa demande en messagerie et obtient une réponse quelques heures plus tard.
- **Transactionnel.** Par essence, cette application fonctionne en mode avec connexion, mais elle peut aussi, dans le cas où le temps réel n'est pas nécessaire, se contenter d'un temps de réponse de quelques secondes au lieu d'une fraction de seconde. L'utilisation d'un mode sans connexion n'est alors pas contre-indiquée.

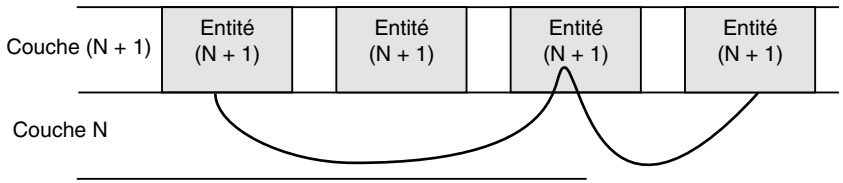
Dans une communication en mode sans connexion, les caractéristiques des unités de donnée doivent être connues à l'avance. À chaque émission, il faut spécifier toutes les informations de contrôle nécessaires pour que l'unité de donnée arrive à destination. En particulier, l'adresse complète de l'entité à joindre ainsi que celle de l'émetteur sont exigées dans le corps de l'unité de donnée. L'ensemble de ces informations peut représenter une longueur non négligeable par rapport à celle des informations à transmettre.

Pour que la communication puisse s'effectuer, il faut en outre une association préalable, provenant d'une connexion à un niveau supérieur de l'architecture, et une connaissance réciproque des deux entités homologues. Cette connaissance concerne les quatre éléments suivants :

- adresses des entités homologues ;
- nature du protocole accepté par les entités homologues ;
- disponibilité des entités homologues ;
- qualité de service offerte par le service N.

Comme dans le mode avec connexion, la communication entre deux entités d'une couche N peut s'effectuer par l'intermédiaire d'un relais de la couche N + 1, laquelle prend en charge les fonctionnalités nécessaires pour que le service N – 1 soit rendu entre les deux entités communicantes. La figure B.3 illustre ce relais.

Figure B.3
Relais en mode sans connexion



Les entités (N + 1) communiquent en mode sans connexion par un relais.

Choix d'un mode

Dans les couches de communication de l'architecture du modèle de référence autres que le niveau application, les deux modes sont possibles, le choix de l'un ou de l'autre dépendant des contraintes imposées par les protocoles considérés. En voici quelques exemples choisis aux différents niveaux de l'architecture :

- **Niveau 2.** La norme de base du niveau 2, HDLC (High-level Data Link Control) est en mode avec connexion. Au moment de l'ouverture, on définit les options de fonctionnement et la valeur des paramètres. Le protocole HDLC travaille en bipoint. Le cas particulier du sous-ensemble LAP-B du protocole HDLC, qui a été normalisé par le CCITT (Consultative Committee for International Telegraph and Telephone), est aussi en mode avec connexion. Les protocoles ATM et relais de trames sont de même en mode avec connexion. En revanche, pour les réseaux locaux dans lesquels la distance est faible entre les utilisateurs et où ces derniers sont tous connectés sur un même câble, le mode de base est sans connexion. On suppose en ce cas qu'il y a connexion à un niveau supérieur pour assurer l'activité des récepteurs. Le protocole

LLC 1 (Logical Link Control 1), ISO 8802.2, qui est utilisé dans la plupart des réseaux commercialisés, est en mode sans connexion.

- **Niveau 3.** Le protocole IP (Internet Protocol) est sans connexion. On envoie les paquets IP sans demander son avis au récepteur. À l'inverse, le protocole X.25 du CCITT est en mode avec connexion. La raison de ce choix est compréhensible. Cette norme a surtout été mise en place pour les réseaux des opérateurs et des organismes publics de télécommunications. Dans un environnement national, il faut pouvoir assurer une qualité de service définie, et le mode avec connexion est beaucoup plus apte à satisfaire cette contrainte. En revanche, pour des environnements privés de réseaux locaux, le mode sans connexion est suffisant.
- **Niveau 4.** Le protocole TCP demande une connexion, tandis qu'UDP est sans connexion. La recommandation X.224, ou ISO 8073, utilise aussi un mode avec connexion. En règle générale, au niveau 4, il faut pouvoir assurer une qualité de service, laquelle doit être discutée au préalable entre l'émetteur et le récepteur. Autant donc se mettre en mode avec connexion. Si l'on sait que l'interlocuteur distant est toujours présent, on peut se satisfaire d'un mode sans connexion.

Au niveau de la session, le mode avec connexion est fortement recommandé dans la mesure où il faut s'assurer qu'une entité distante est bien présente pour récupérer l'information. Il existe bien une norme de session en mode sans connexion, mais les applications qui en bénéficient, comme la télévision diffusée, sont peu nombreuses.

Les deux modes sont comparés et discutés dans l'additif n° 1 à la norme ISO 7498.

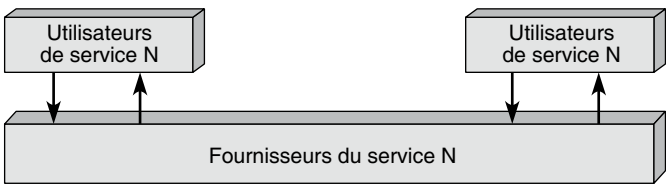
La sémantique de fonctionnalité

La sémantique de fonctionnalité fait référence aux propriétés qui doivent être mises en œuvre pour réaliser une communication. Nous allons commencer par examiner les propriétés d'une connexion point-à-point avant de nous pencher sur les différentes fonctionnalités que l'on peut y associer.

Propriétés d'une connexion point-à-point

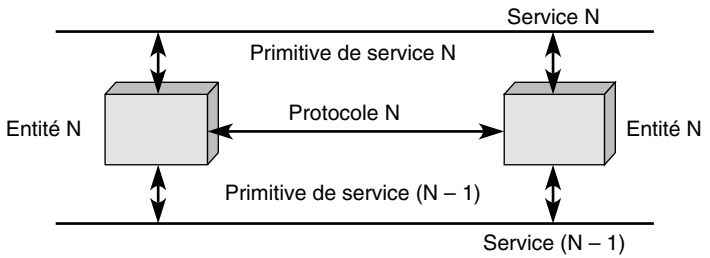
Un réseau en couches est défini par des utilisateurs d'un service N et par des fournisseurs du même service N, comme l'illustre la figure B.4.

Figure B.4
Modèle de service d'un réseau en couches



La figure B.5 illustre les différentes relations entre l'entité N (le logiciel ou le matériel qui gère le protocole de niveau N) et les services N et N – 1. Les entités N communiquent par le biais d'un protocole N.

Figure B.5
Interactions entre entités



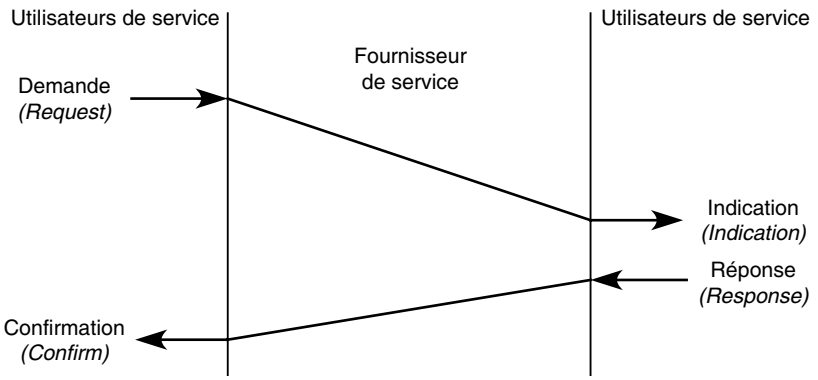
Quatre primitives de service sont définies pour permettre à un utilisateur de service de s'adresser à une entité ou à une entité de répondre à un utilisateur de service (*comme indiqué par les flèches verticales à la figure B.5*) :

- Les primitives de demande, par lesquelles un utilisateur de service appelle une procédure.
- Les primitives d'indication, par lesquelles l'entité destinataire est avertie qu'une procédure a été mise en route par l'entité émettrice sur son point d'accès au service ou que le fournisseur de service indique qu'il appelle une procédure.
- Les primitives de réponse, par lesquelles l'utilisateur distant du service N accepte ou refuse le service demandé.
- Les primitives de confirmation, qui indiquent l'acceptation ou le refus du service demandé qui a été fait au point d'accès au service N.

Les services N peuvent être obligatoires. Dans ce cas, le logiciel ou le matériel réalisant ces services doit être présent. Ils peuvent aussi être optionnels. L'implémentation physique de ces services par le fournisseur de service N n'est alors pas obligatoire. Enfin, les services peuvent être confirmés ou non, c'est-à-dire demander une confirmation explicite ou non du fournisseur de service vers l'utilisateur du service.

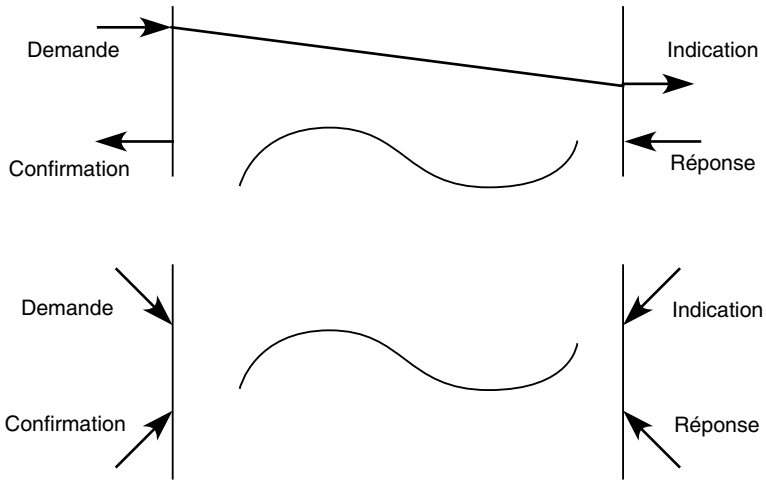
On peut représenter les quatre primitives de service sous la forme illustrée à la figure B.6.

Figure B.6
Primitives de service



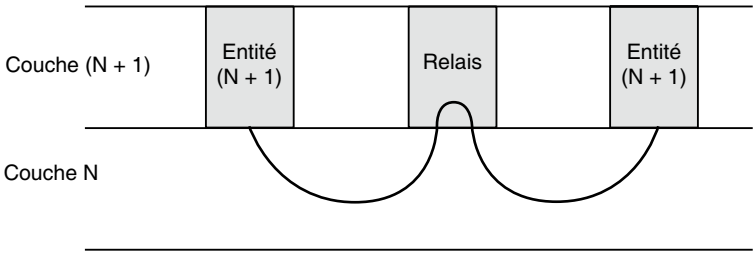
L'ordre temporel dans lequel les interactions aux deux points d'accès au service sont effectuées n'est pas obligatoirement la réponse avant la confirmation. Le fournisseur de service peut envoyer une confirmation de non-exécution avant la réponse définie, par exemple. On représente le chronogramme des ordres d'exécution temporels des primitives de l'une ou l'autre des façons illustrées à la figure B.7. Lorsqu'il n'y a pas de relation temporelle, un tilde est dessiné entre les utilisateurs de service.

Figure B.7
Chronogrammes de primitives de service



Pour échanger des informations entre deux entités du niveau N + 1, il faut établir entre elles une association dans la couche N en suivant un protocole N. Cette association définit une connexion N. Dans certains cas, la communication n'est pas directe et nécessite un relais, comme illustré à la figure B.8.

Figure B.8
Relais de niveau N + 1



Pour déterminer où se trouvent les entités avec lesquelles on souhaite communiquer et comment y arriver, les fonctions suivantes ont été ajoutées à la norme :

- Appellation, pour identifier une entité de façon permanente.
- Adresse N, pour indiquer où se trouve un point d'accès à des services N.
- Répertoire N, pour traduire l'appellation d'une entité N en l'adresse N – 1 du point d'accès aux services N – 1 auxquels elle est reliée.

La figure B.9 illustre ces fonctions ainsi que les correspondances possibles entre entités et points d'accès au service. L'identificateur d'extrémité de connexion N doit être unique dans le contexte d'un point d'accès à des services N. La mise en correspondance des adresses pour aller d'une entité d'application à une autre en passant par l'ensemble des couches peut se faire soit par un adressage hiérarchique, comme illustré à la figure B.10, soit par une gestion de tables.

Figure B.9
Correspondances entre entités et N-SAP

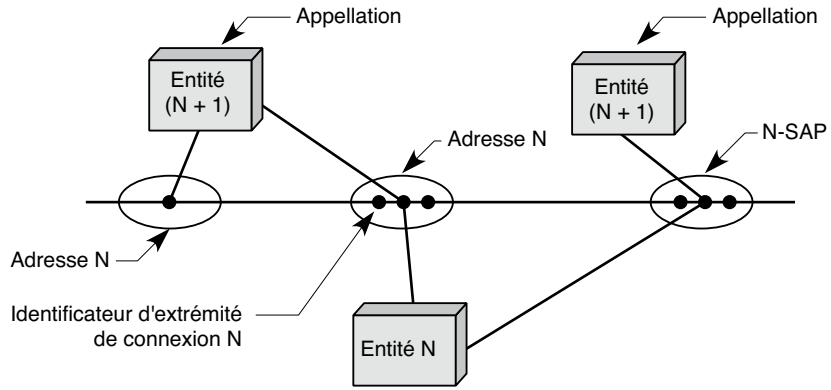
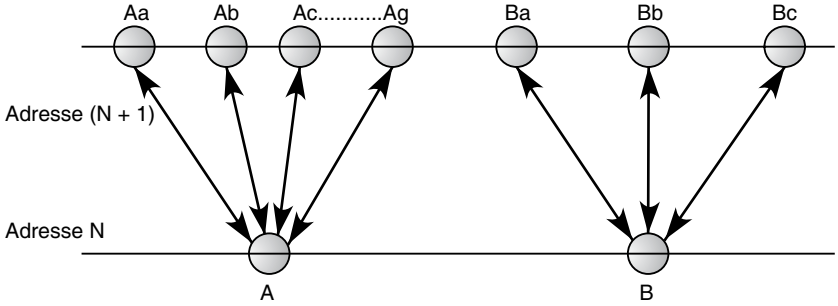
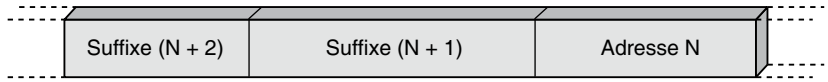


Figure B.10
Adressage hiérarchique



Dans le cas d'un adressage hiérarchique, l'adresse est composée de plusieurs parties, comme illustré à la figure B.11.

Figure B.11
Adresses hiérarchiques



À partir d'une adresse de niveau supérieur à N, il est possible de retrouver l'adresse N en enlevant les suffixes N + 1, N + 2, etc., qui sont des éléments d'adresse unique dans le contexte d'un point d'accès à des services N + 1, N + 2, etc.

L'adressage hiérarchique simplifie considérablement le routage des unités de donnée dans un réseau. Il est simple à mettre en œuvre, quoique le nombre d'octet à transporter soit généralement important et implique une surcharge pour les lignes de communication.

Les adresses de niveau 3 et de niveau 7 sont particulièrement importantes. L'adresse portée par la couche 3, que l'on appelle également adresse de niveau paquet, est située dans l'en-tête du paquet. Elle permet d'acheminer les paquets d'une extrémité à une autre du réseau. L'adresse utilisée dans la couche 7, ou adresse de niveau application, est située dans la zone de contrôle associée au niveau application. Elle permet de retrouver le processus qui, à l'intérieur du niveau application, a procédé à l'émission ou qui doit recevoir les données. L'adresse de niveau 3 peut être remplacée par une adresse de niveau 2 dans les réseaux qui ont adopté un transfert de niveau trame. L'adresse importante reste de niveau 3 si un paquet est transporté dans la trame mais devient de niveau 2 si la couche paquet est supprimée.

Une seconde méthode de mise en correspondance des adresses consiste à utiliser des tables d'adressage pour traduire les adresses N en adresses N – 1. La structure des adresses aux différents niveaux peut en effet se présenter de manière très différente. Certaines peuvent revêtir une forme hiérarchique, d'autres une forme géographique et d'autres encore une forme plate. La taille de ces tables peut rendre leur gestion délicate. Plus le nombre d'entrées dans une table est important, plus la surcharge de travail des nœuds de routage augmente.

L'adressage géographique

L'adressage géographique est un cas particulier de l'adressage hiérarchique dans lequel les parties de l'adresse sont dictées par la situation géographique de l'interface utilisateur. Autrefois, le réseau téléphonique utilisait un adressage totalement géographique, de telle sorte que l'adresse permettait de situer l'emplacement de l'utilisateur.

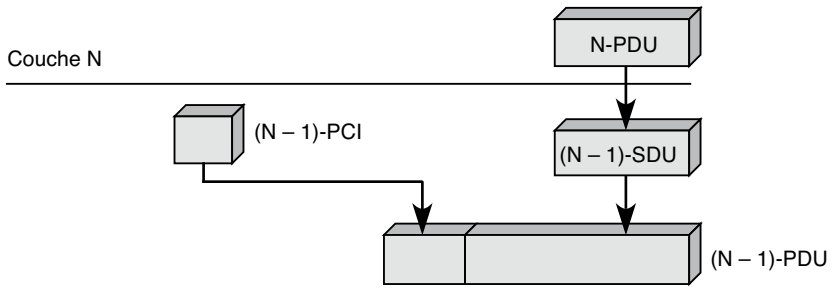
Aujourd'hui, même si la plupart des adresses téléphoniques sont encore hiérarchiques, le fait de garder son adresse téléphonique en déménageant détruit le contexte géographique. Les adresses Internet sont hiérarchiques mais non géographiques. Le nombre de niveaux hiérarchiques est de deux pour la première génération d'Internet, dite IPv4, et de huit pour la deuxième, IPv6.

Les unités de donnée

Une unité de donnée d'un service N, ou N-SDU (Service Data Unit), est un ensemble de données provenant de l'interface avec la couche N et devant être transportées sur une connexion N. Les informations de contrôle du protocole N, dites N-PCI (Protocol Control Information), proviennent d'entités N. Elles sont ajoutées, le cas échéant, à des SDU sur une connexion N – 1.

Les principales unités de donnée sont illustrées à la figure B.12.

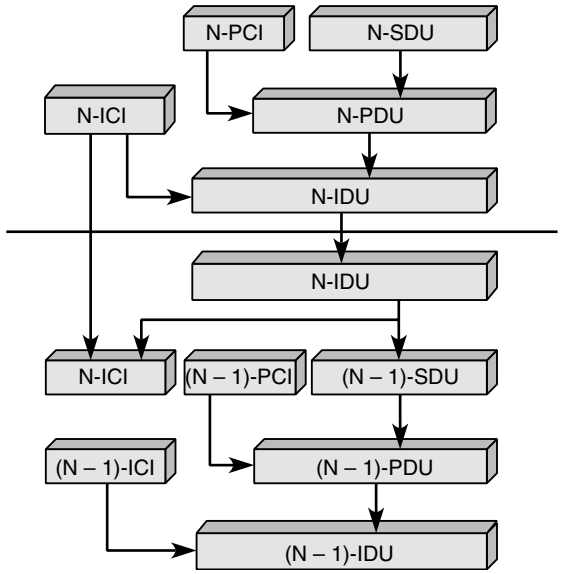
Figure B.12
Unités de donnée



Les unités de donnée du protocole N, ou N-PDU (Protocol Data Unit), sont spécifiées par un protocole N. Elles consistent en informations de contrôle du niveau N et en informations provenant de une ou plusieurs unités de donnée de service. Pour coordonner le travail au même niveau, nous avons déjà rencontré les unités de donnée PCI. Pour contrôler la communication entre entités de niveau N + 1 et entités de niveau N, les informations nécessaires sont transportées dans des N-ICI (Interface Control Information). Ces informations de gestion peuvent être ajoutées aux données à transporter au travers de l'interface N, autrement dit aux N-PDU, pour donner naissance à des N-IDU (Interface Data Unit).

La figure B.13 illustre la structure d'ensemble des entités de transport de données et de contrôle.

Figure B.13
Structure d'ensemble des entités de transport de données et de contrôle

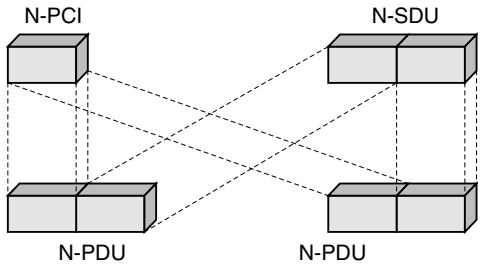


Les données utilisateur qui traversent l'interface de couche N peuvent être appelées données de l'interface N, ou N-IDU. Elles proviennent des données utilisateur N ou N-UD.

Dans le cas le plus simple, lorsqu'il n'y a ni segmentation ni groupage, à une N-SDU correspond une seule N-PDU. En règle générale, les unités de donnée ont des longueurs déterminées par une valeur maximale et une valeur minimale, pouvant être 0 octet, et ce pour chaque protocole et chaque service. Le réseau doit découvrir la meilleure longueur possible des unités de donnée pour fonctionner de manière optimale, en coupant ou, au contraire, en recollant des morceaux. Nous examinons dans la suite de ce chapitre les diverses possibilités de découpage et de regroupage proposées par la normalisation.

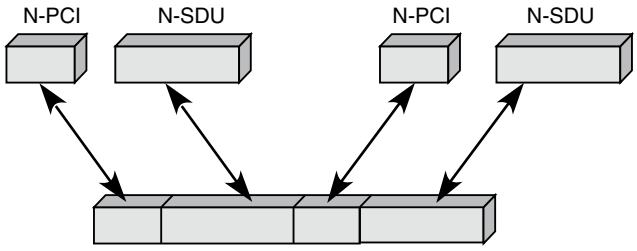
La fonction de segmentation-réassemblage est illustrée à la figure B.14. C'est la fonction accomplie par une entité N pour mettre en correspondance une unité de donnée du service N avec plusieurs unités de donnée du protocole N. Cette figure ne présente que le cas où une N-SDU est segmentée en deux parties. Dans la réalité, il peut y avoir un nombre de fragments beaucoup plus important. Le réassemblage est la fonction inverse de la segmentation.

Figure B.14
Segmentation-réassemblage



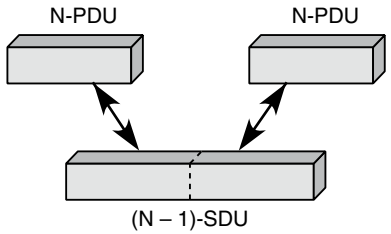
Le groupage-dégroupage est illustré à la figure B.15. Le groupage est la fonction accomplie par une entité N pour mettre en correspondance plusieurs unités de donnée du service N avec une unité de donnée du protocole N. Le dégroupage est la fonction inverse du groupage.

Figure B.15
Groupage-dégroupage



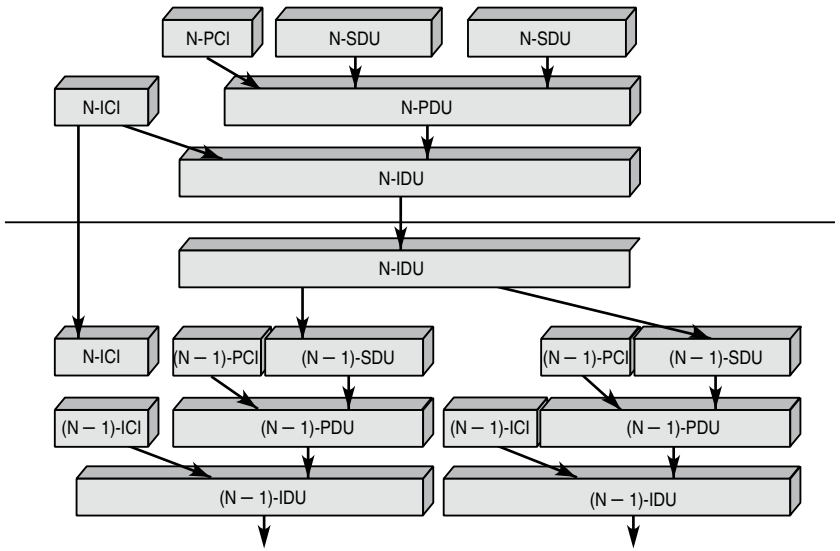
La concaténation-séparation est illustrée à la figure B.16. La concaténation est la fonction accomplie par une entité N pour mettre en correspondance plusieurs unités de donnée du protocole N avec une unité de donnée du service N – 1. La séparation est l'opération inverse. Au travers de l'interface, il n'est possible, entre deux couches, que d'effectuer une concaténation dans un sens et une séparation dans l'autre sens. Il n'est pas possible de couper une N-PDU en plusieurs morceaux, lesquels deviendraient des (N – 1)-SDU.

Figure B.16
Concaténation-séparation



La figure B.17 illustre la transmission de la figure B.13, mais en ajoutant une segmentation et une concaténation.

Figure B.17
Concaténation de niveau N suivie d'une segmentation de niveau N – 1



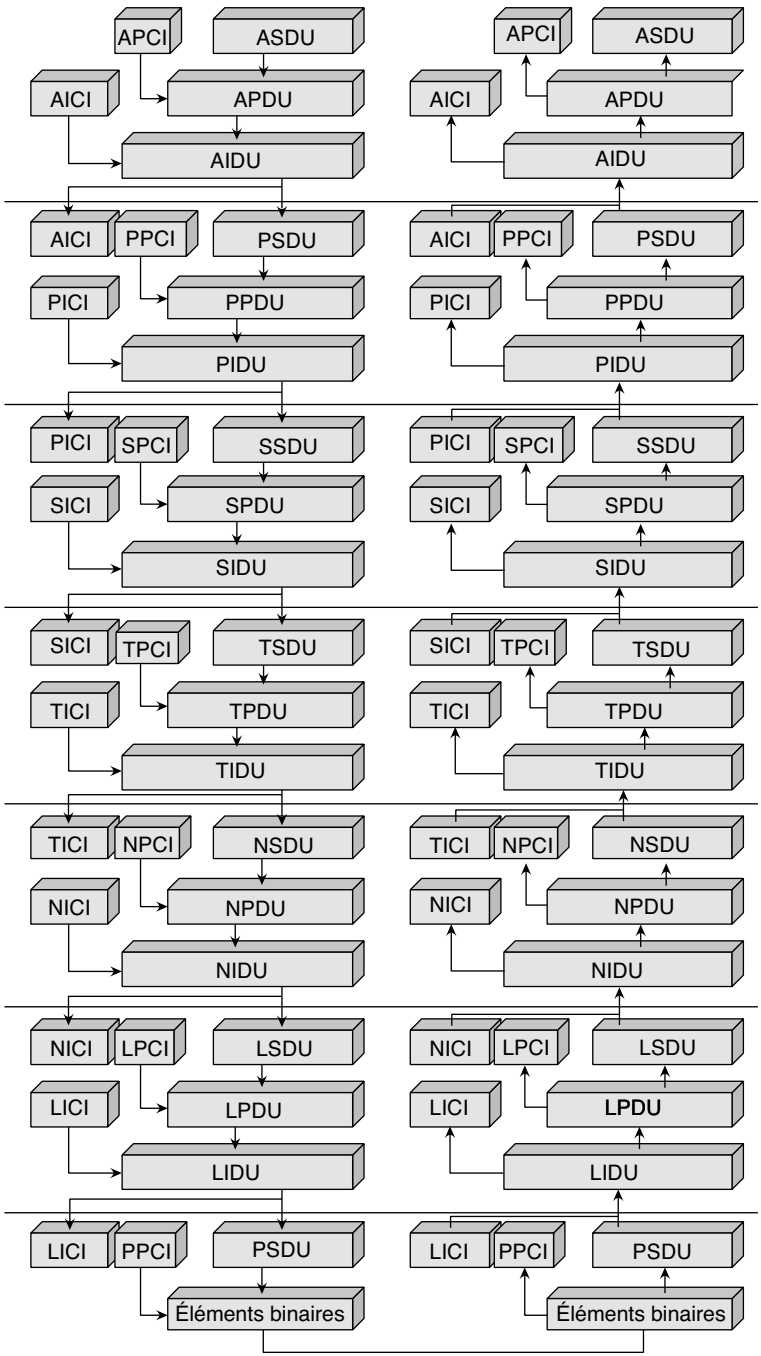
Nous avons employé jusqu'ici le numéro de la couche N pour indiquer la énième couche. Dans la réalité, on utilise une lettre pour désigner ce niveau. Pour chaque niveau du modèle de référence ces lettres sont les suivantes :

- P – Physique
- L – Liaison : LSDU, LPDU, LSAP
- N – Réseau : NSDU, NPDU, NSAP
- T – Transport : TSDU, TPDU, TSAP
- S – Session : SSDU, SPDU, SSAP
- P – Présentation : PSDU, PPDU, PSAP
- A – Application : ASDU, APDU, ASAP

La figure B.18 illustre les unités de donnée de l'ensemble de l'architecture en partant du principe qu'à chaque SDU correspond une PDU et *vice versa*. Dans cette

représentation simplifiée, il n'y a ni segmentation-réassemblage, ni groupage-dégroupage, ni concaténation-séparation.

Figure B.18
Unités de donnée de l'architecture OSI



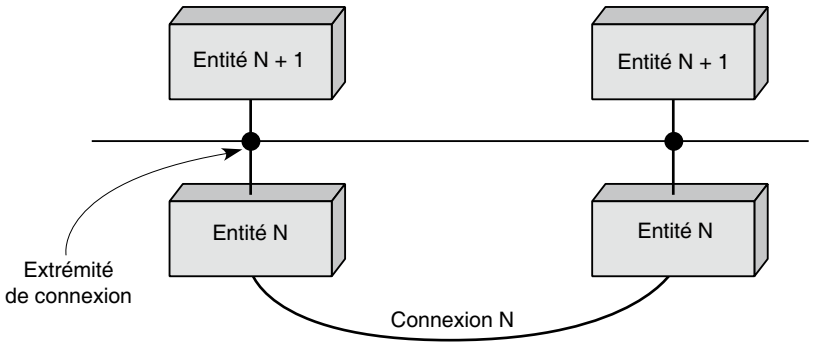
Les connexions

Chaque niveau de l'architecture du modèle de référence possède des fonctionnalités qui lui permettent d'appliquer le traitement approprié aux entités qui la traversent. Les plus importantes de ces fonctionnalités sont les connexions, qui mettent en relation les entités distantes, le contrôle de flux et le contrôle d'erreur.

Une connexion N est une association établie pour permettre la communication entre au moins deux entités N + 1 identifiées par leur adresse N. Une connexion N est donc un service offert par la couche N pour permettre l'échange d'informations entre des entités N + 1. Une connexion multipoint lie au moins trois entités N + 1.

Une connexion N possède au moins deux extrémités de connexion N, qui associent deux entités, comme l'illustre la figure B.19 (une extrémité de connexion est indiquée par un rond noir).

Figure B.19
Extrémités de connexion



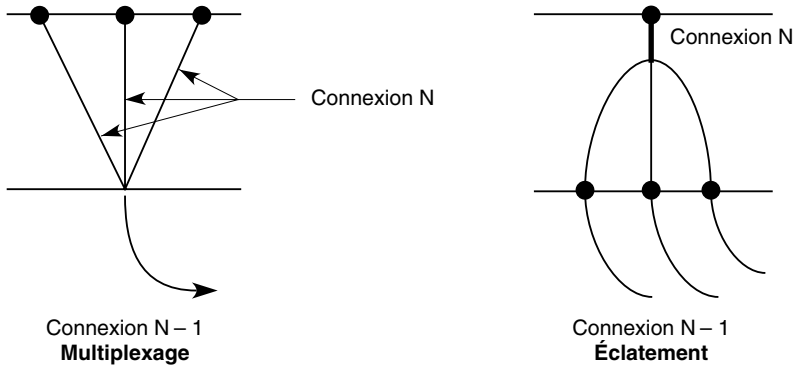
À une extrémité de connexion N correspond une adresse N. Pour qu'une connexion s'établisse, il faut que les deux entités qui veulent communiquer disposent des mêmes éléments de protocole et d'une connexion N – 1. Une fois les données utilisateur N transférées, il faut libérer la connexion. Il existe pour cela deux possibilités :

- Libération immédiate de la connexion, indépendamment du fait que toutes les données utilisateur sont ou non parvenues à destination.
- Libération négociée, qui laisse le temps de s'assurer que les données ont bien été transportées. Dans ce cas, les accusés de réception doivent être parvenus avant la véritable libération de la connexion.

Pour optimiser l'utilisation des connexions, il est possible de multiplexer plusieurs connexions N sur une même connexion N – 1 ou, inversement, d'éclater une connexion N sur plusieurs connexions N – 1, comme illustré à la figure B.20.

Pour mettre en place un multiplexage, une identification de la connexion N est nécessaire. Elle est multiplexée sur la connexion N – 1, de façon que chaque connexion N destination puisse retrouver les N-PDU des différentes connexions N émettrices. Cette identification est bien sûr différente des identificateurs d'extrémité de connexion N, qui sont liés au N-SAP. L'éclatement demande la remise en séquence des PDU, qui doivent être redonnées dans le bon ordre à l'extrémité de la connexion N.

Figure B.20
Multiplexage et éclatement



Contrôle de flux et contrôle d'erreur

Une autre fonctionnalité, que l'on rencontre dans la plupart des niveaux du modèle de référence, est le contrôle de flux. Son rôle est de cadencer l'envoi des PDU sur la connexion, de telle sorte que l'entité homologue puisse récupérer les informations à une vitesse lui convenant, sans perte d'information ni de temps. Un autre contrôle de flux a lieu sur l'interface entre deux couches. Ce contrôle est généralement d'autant plus facile à effectuer que les entités correspondantes sont plus rapprochées.

Sur une connexion N, il faut aussi être capable de prendre en charge les erreurs, tant celles en ligne, c'est-à-dire sur la connexion, que celles dues aux protocoles traversés, ou encore les pertes d'information par écrasement dans des mémoires intermédiaires. On utilise pour cela des accusés de réception,, qui font partie des informations de contrôle du protocole N-PCI. Le cas échéant, une notification d'erreur peut être envoyée à l'entité communicante pour lui signaler la perte d'information et la cause de cette perte. Une réinitialisation peut être demandée par une entité N pour que les deux entités N homologues repartent sur des bases connues.

L'architecture OSI

L'ISO (International Standardization Organization) a normalisé sa propre architecture sous le nom d'OSI (Open Systems Interconnection). L'architecture ISO est la première à avoir été définie, et ce de façon relativement parallèle à celle d'Internet. La distinction entre les deux est que l'architecture ISO définit formellement les différentes couches, tandis que l'architecture Internet s'applique à réaliser un environnement pragmatique.

La couche physique est complexe. De nombreuses normes décrivent la façon de coder et d'émettre les signaux physiques sur une ligne de communication. La couche trame fournit les moyens fonctionnels et procéduraux nécessaires à l'établissement, au maintien et à la libération des connexions entre entités de réseau, ainsi qu'au transfert des unités de donnée du service de liaison. C'est la norme ISO 8886, ou CCITT X.212, qui définit le service procuré par la couche 2.

Les autres normes importantes de l'architecture ISO sont les suivantes :

- ISO 3309 et 4335 pour la normalisation du protocole de liaison HDLC (High-level Data Link Control) ;
- ISO 3309, pour la structure des trames ou LPDU ;
- ISO 4335 et 7809, pour les éléments de procédure ;
- ISO 8471, pour la description de la classe en mode équilibré de HDLC ;
- ISO 7776, pour la description de la norme CCITT LAP-B dans un contexte ISO.

Le rôle de la couche paquet (niveau transfert) est, d'une part, de fournir les moyens d'établir, de maintenir et de libérer des connexions réseau entre systèmes ouverts et, d'autre part, de fournir les moyens fonctionnels et les procédures nécessaires pour échanger, entre entités de transport, des unités du service de réseau.

La normalisation de la couche 3 comporte les normes suivantes :

- ISO 8348, ou CCITT X.213, qui définit le service réseau.
- ISO 8208, ou CCITT X.25, qui définit le protocole réseau en mode avec connexion. Ce protocole est le plus souvent appelé X.25, et tous les grands réseaux publics du monde suivent cette recommandation.
- ISO 8473, qui définit le protocole de réseau en mode sans connexion, connu sous le nom d'Internet ISO. C'est une normalisation du protocole développé par le département de la Défense américain sous le nom d'IP (Internet Protocol).
- ISO 8878, ou CCITT X.223, qui décrit l'utilisation de X.25 pour obtenir le service réseau orienté connexion.
- ISO 8648, qui définit l'organisation interne de la couche réseau.
- ISO 8880, en quatre parties, qui définit les différentes combinaisons possibles de protocoles pour rendre un service de niveau 3 conforme à la normalisation.
- ISO 8881, qui permet l'adaptation du niveau 3 de X.25 sur un réseau local possédant un protocole de liaison de type LLC 1.

La couche message (niveau transport) doit assurer un transfert de données entre les entités de session. Ce transport doit être transparent, c'est-à-dire indépendant de la succession des caractères et même des éléments binaires transportés. La normalisation internationale provenant de l'ISO prévoit cinq classes de protocoles capables de satisfaire aux exigences de l'utilisateur.

Les différentes classes du niveau 4 vont de logiciels très simples, qui ne font que formater les données provenant du niveau supérieur et les déformater à l'arrivée, à des logiciels de communication complexes, qui reprennent l'ensemble des fonctionnalités des trois niveaux inférieurs. On peut y trouver une zone de détection d'erreur et des algorithmes de reprise sur erreur. Des redémarrages sur perte de message ou de paquet signalée par la couche inférieure font également partie des outils disponibles dans ces logiciels.

Les principales normes de cette couche sont les suivantes :

- ISO 8072, ou CCITT X.214, qui définit le service transport.

- ISO 8073, ou CCITT X.224, qui définit le protocole de transport orienté connexion et qui possède, comme nous l'avons vu, cinq classes sous-jacentes.
- ISO 8602, qui définit un protocole de transport en mode sans connexion.

Les trois couches supérieures correspondent exactement à celles décrites dans l'architecture du modèle de référence.

Les architectures multipoint

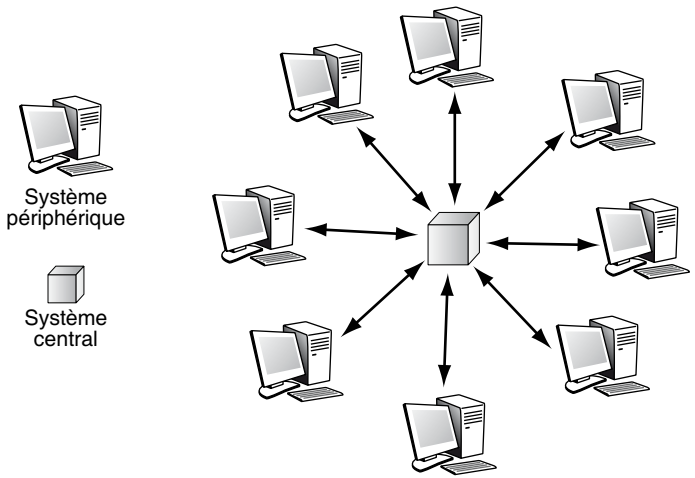
Les applications que l'on utilise classiquement sur un équipement terminal mettent en œuvre une communication point-à-point, c'est-à-dire que la communication part du micro pour aller rechercher l'information vers un seul autre point. Beaucoup d'autres applications font appel à la coopération de plusieurs processus. Par exemple, une recherche dans une base de données distribuée, dans laquelle les informations sont réparties sur plusieurs sites, fait appel à une demande simultanée d'informations vers plusieurs centres. Pour faire cette demande, l'application et toutes les couches de protocoles associées doivent gérer des multipoint. Cette façon de communiquer est plus performante que celle qui consiste à faire la demande à un premier site puis, une fois la réponse obtenue, à un deuxième, et ainsi de suite.

La mise en place d'une communication multipoint est évidemment plus complexe que celle d'une communication point-à-point simple. Avant de décrire ce que les normalisateurs ont retenu dans l'additif n° 2 à la norme ISO 7498-1, il est important de comprendre les deux possibilités extrêmes d'une communication multipoint.

Dans le cas le plus simple, il existe un système central et des systèmes périphériques. Seul le système central peut communiquer avec l'ensemble des sites périphériques, les systèmes périphériques ne pouvant communiquer qu'avec le site central. L'avantage de cette méthode est la grande simplicité des communications. La gestion de l'ensemble peut s'effectuer par le centre. Ce cas est illustré à la figure B.21.

Figure B.21

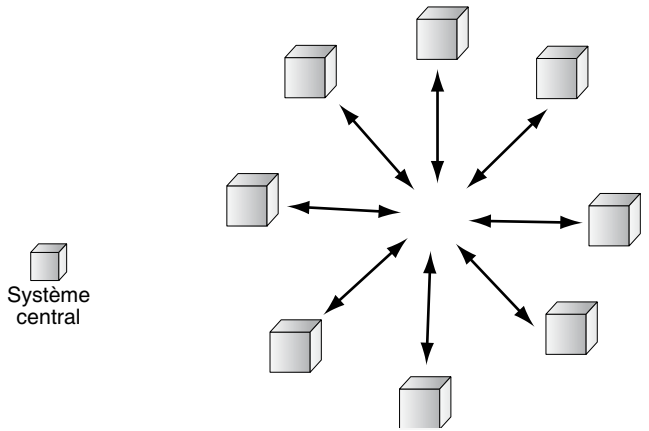
Système multipoint le plus simple



À l'opposé, le multipoint le plus complexe est celui dans lequel tout système est un système central, c'est-à-dire où chaque site peut communiquer directement avec tout autre site. On voit bien la complexité globale de cette configuration, puisque la gestion des échanges est totalement distribuée et que la coordination des systèmes est difficile à prendre en charge. Ce cas est illustré à la figure B.22.

Figure B.22

Système multipoint le plus complexe



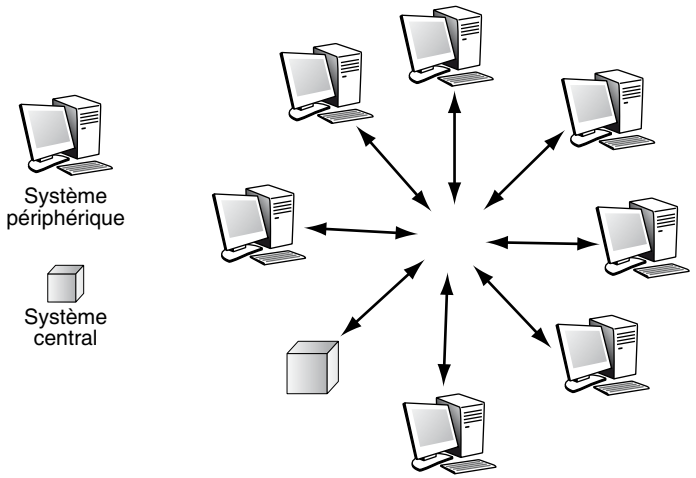
Entre ces deux configurations extrêmes, il existe toute une hiérarchie de possibilités. Les normalisateurs en ont retenu deux, la communication multipoint à centre mobile et la communication multicentre.

La communication multipoint à centre mobile est une légère amélioration du multipoint le plus simple : à un instant donné, il n'y a qu'un seul système central, mais ce site primaire peut varier dans le temps. Un système multipoint complexe est toujours équivalent à une succession de communications multipoint à centre mobile.

Cette configuration est illustrée à la figure B.23. Son inconvénient peut être sa relative lenteur lorsque le système multipoint veut faire du parallélisme.

Figure B.23

Communication multipoint à centre mobile

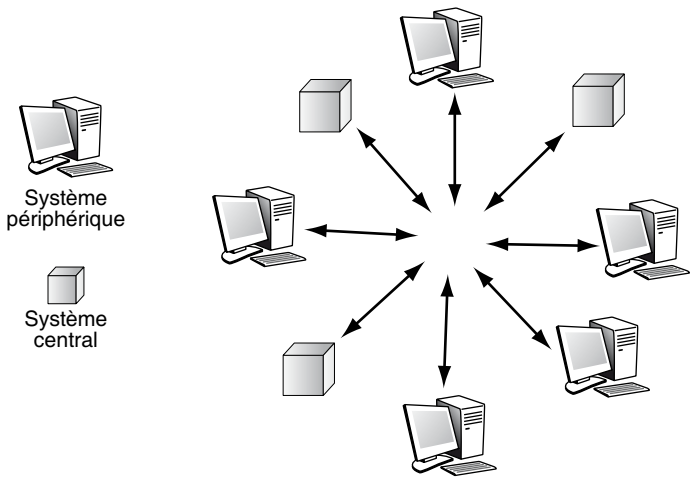


Dans la communication multicentre, si N sites participent à la réalisation de la communication multipoint, seulement M. sites au maximum peuvent se comporter comme un système central, M. étant généralement très inférieur à N.

Cette configuration est illustrée à la figure B.24, dans laquelle, sur les 8 sites du réseau, 3 sont des systèmes centraux et 5 des systèmes périphériques.

Figure B.24

Communication multicentre



Annexe C

3. Le médium de transport

Cette annexe fait le point sur les contraintes d'installation du câblage et des systèmes de distribution. En particulier, elle détaille les environnements banalisés.

Contraintes d'installation du câblage

Le choix de la distribution du câble est délicat. Les chemins que les câbles empruntent sont des supports généralement métalliques. Cela implique de nombreuses contraintes d'installation, parmi lesquelles la distance entre les équipements, la séparation entre les réseaux courant fort, tel le secteur électrique, et courant faible, comme l'informatique ou le téléphone.

Les chemins de câbles du réseau courant faible doivent être éloignés des sources de perturbation du réseau courant fort et éviter la proximité d'ascenseurs, de tubes fluorescents, de machines à café, etc.

De nombreux procédés existent pour la pose des câbles :

- Les plinthes, très utilisées dans l'environnement domestique pour les fils électriques, offrent une grande souplesse d'utilisation et d'installation des prises.
- Les faux plafonds, disposés à quelques dizaines de centimètres du plafond réel, permettent le passage des câbles et de la ventilation. Les câbles arrivent du faux plafond au poste de travail par des conduits verticaux, appelés potelets.
- Les faux planchers, ou planchers techniques, disposés à quelques dizaines de centimètres du sol, ont la même fonction que les faux plafonds.
- Les cloisons, etc.

Faux plafonds et faux planchers sont aussi appelés plénums. On peut utiliser le câblage sous-moquette avec des câbles plats. Des colonnes montantes sont utilisées pour faire passer les câbles d'un étage à un autre.

Les locaux techniques regroupant les concentrateurs, les passerelles et les autres matériels de transmission informatique peuvent, selon leur encombrement, contenir l'autocommutateur, si les réseaux téléphoniques et informatiques sont encore séparés. S'il y a lieu, ce regroupement doit être contrôlé afin d'éviter toute confusion possible.

Les locaux techniques peuvent être regroupés avec ceux destinés à recevoir les équipements de brassage et les sous-répartiteurs. La disposition de ces locaux doit être bien choisie. Ils doivent être faciles d'accès et suffisamment spacieux pour rendre aisée l'installation et la maintenance des liaisons et des équipements. Il faut y prévoir des dispositifs pour la climatisation, la ventilation, la sécurité et l'alimentation électrique de façon autonome et fiabilisée ainsi que la mise en place d'un téléphone de service. Leur emplacement doit également être judicieusement choisi, en fonction de la disposition des lieux à desservir.

Même si les locaux techniques peuvent être regroupés, il faut prévoir, pour des raisons de sécurité, des gaines différentes pour les réseaux courant faible et courant fort. Les chemins de câbles doivent aussi être protégés contre l'eau et le feu. Dans un souci de maintenance et d'évolution, un système d'étiquetage doit permettre une reconnaissance aisée des différents câbles.

Le câblage banalisé, ou structuré

Les problèmes de conception, de mise en œuvre et d'exploitation n'étant pas identiques suivant la taille des installations, on peut distinguer plusieurs types d'installations :

- **Grande entreprise.** Caractérisée par plusieurs centaines de postes de travail, des réseaux multiples et complexes et une structuration en zones desservies chacune par un sous-répartiteur.
- **Entreprise moyenne.** Comporte au maximum une centaine de postes de travail connectés à un répartiteur unique.
- **SOHO et résidentiel.** Marché globalement considérable mais diffus.

Les règles, normes de transmission, types de terminaux, ainsi que les composants de câblage, par exemple les prises RJ-45, les câbles en paires torsadées ou le brassage des équipements actifs, sont quasiment identiques pour les trois types d'installations. Les différences considérables entre elles viennent des systèmes de distribution, qui sont illustrés plus loin dans cette section.

Si le câblage des sites d'entreprise est désormais entré dans une phase de banalisation du fait de l'application des normes indiquées à la section suivante, celui des locaux d'habitation et des petits bureaux, ou SOHO, est encore relativement nouveau. Sa normalisation n'a été finalisée qu'en 2003 par le guide UTE C 90 483 et la nouvelle norme NF C 15-100. Il s'agit d'un marché considérable, deux fois plus important que celui des entreprises. En revanche, il est techniquement plus difficile, en raison de l'obligation de transmettre la TV en grade 3 sur des paires torsadées sur une bande de fréquences allant jusqu'à 862 MHz.

Ce nouveau marché est généré par l'avènement des réseaux haut débit et multimédias chez les usagers, et en particulier de l'ADSL, qui permet de distribuer simultanément le téléphone, l'accès Internet et les chaînes TV. Le problème reste de distribuer tous ces services là où ils sont utilisés, au salon, dans les chambres ou au bureau, voire d'y associer d'autres services, comme la hi-fi, la télésurveillance, les automatismes du logement, etc.

La normalisation

Avant l'avènement et la généralisation des normes ISO 11801, EN 50173, EIA/TIA 2002, IEEE 802.3, IEEE 802.11, etc., le marché était occupé par une multitude d'offres de câblage propriétaires. Les matériels d'un constructeur informatique ne pouvaient être supportés ou simplement garantis qu'avec le système de câblage de ce même constructeur. On trouvait donc une trentaine de câbles en paires torsadées, d'impédances 100, 110, 120 ou 150 Ω, à une, deux, quatre ou six paires, sans compter les câbles coaxiaux 50 Ω différents des câbles CATV 75 Ω.

L'époque des câblages exotiques est désormais révolue. Le câblage généré par les normes est devenu universel et international. Il permet d'interconnecter :

- tous les réseaux du marché ;
- tous les équipements actifs ou terminaux, en toute topologie (point-à-point, étoile, bus, arbre, etc.) ;
- tous les débits de transmission selon des modèles normalisés.

Fonctionnement du câblage banalisé

Le câblage banalisé consiste à disposer, partout où elles sont potentiellement utilisables, des prises RJ-45 (ISO 8877), elles-mêmes interconnectées à des répartiteurs ou sous-répartiteurs intégrant les équipements actifs de réseau, comme illustré aux figures C.1 et C.2.

Figure C.1

Bandeau de prises RJ-45, montable en rack 19 pouces, permettant la connexion des postes de travail

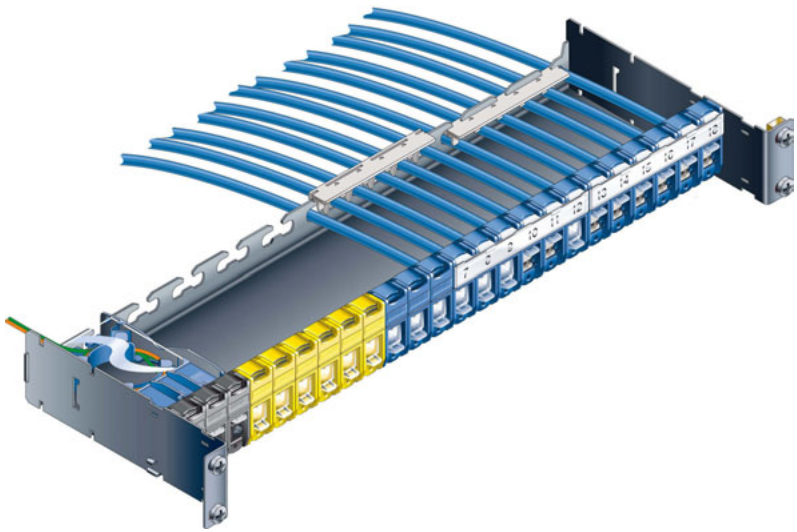


Figure C.2

Cordon de brassage RJ-45 interconnectant les équipements

Ce câblage est réalisé une fois pour toutes et devient une partie structurelle du bâtiment. Il permet de supporter tous les réseaux, tous les logiciels, tous les terminaux, sans qu'il soit nécessaire de repasser un seul câble.

Les liaisons quatre paires horizontales

Les liaisons quatre paires horizontales, aussi appelées capillaires, constituent l'essentiel du câblage banalisé puisqu'elles interconnectent tous les terminaux aux équipements de réseau actifs (*voir figure C.3*). Toutes les prises RJ-45 sont câblées de manière identique et répétitive aux deux extrémités du câble quatre paires, au niveau à la fois des postes de travail et des sous-répartiteurs. Une convention de raccordement immuable — 568 B est la plus courante — permet d'attribuer chaque fil du câble quatre paires à une borne définie des connecteurs RJ-45, comme l'illustre la figure C.4.

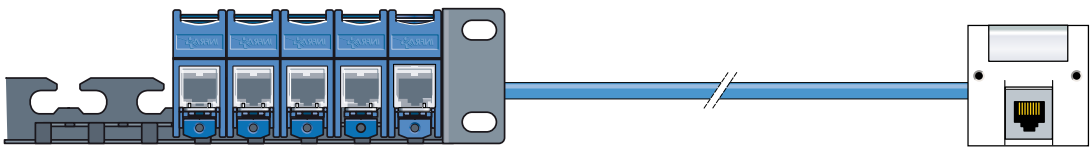
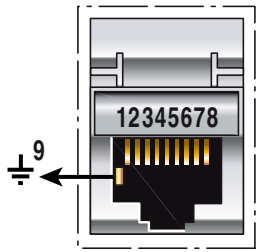


Figure C.3

Constitution d'une liaison quatre paires

Figure C.4

Vue en face avant d'un connecteur RJ-45 avec repérage de ses bornes



Le tableau C.1 donne la correspondance entre les paires et les bornes des connecteurs RJ-45 associés.

Tableau C.1 • Correspondance entre paires et bornes des connecteurs RJ-45

Nombre de bornes RJ-45 aux sous-repartiteurs	Couleur des fils des quatre paires	Nombre de bornes RJ-45 aux postes de travail
4 5	*Paire 1* Bleu Bleu/blanc	4 5
1 2	*Paire 2* Blanc/orange Orange	1 2
3 6	*Paire 3* Blanc/vert Vert	3 6
7 8	*Paire 4* Blanc/marron Marron	7 8

Critères de qualification des liaisons horizontales

Les normes laissent le choix entre plusieurs types de composants, qui diffèrent par leurs performances de transmission et leur immunité à l'environnement électromagnétique. Le tableau C.2 récapitule les performances et domaines d'application des principaux composants des liaisons horizontales.

Tableau C.2 • Performances des principaux composants des liaisons horizontales

Composant	Performance de transmission	Domaine d'application
Lien classe D Composant catégorie 5	100 MHz	- Téléphonie - LAN Ethernet 10BaseT
Lien classe E Composant catégorie 6	250 MHz	- Téléphonie - LAN Ethernet 100BaseT et 1000BaseT
UTP (Unshielded Twisted Pair), câble non blindé	Immunité moyenne aux perturbations électromagnétiques	- Environnement peu pollué, bâtiment incorporant des structures métalliques - Séparation courant fort-courant faible obligatoire (risque de foudre) - Pas de TV (5-862 MHz)
FTP (Foiled Twisted Pair), avec écran blindant l'ensemble du câble	Immunité forte aux perturbations électromagnétiques	- Environnement pollué, bâtiment incorporant des structures métalliques - Séparation courant fort-courant faible facultative

Il existe d'autres types de câbles, comme les câbles de catégories 7 et 8 ou les câbles SFTP (Shielded Foiled Twisted Pair), mais ils sont très marginaux.

Sans entrer dans le détail de la technologie des câbles, il est possible de se protéger des perturbations électromagnétiques de deux manières :

- En torsadant les paires de câbles UTP et FTP. En ce cas, à chaque demi-spire, le champ induit s'inverse et s'annule. C'est pour cette raison que l'on recommande d'éviter de détorsader les paires.
- En blindant les câbles et les connecteurs. Un écran mis à la terre est une protection peu coûteuse et très efficace.

Pour mémoire, les câbles SFTP comportent, comme les FTP, un écran général, voire une tresse, mais les paires sont écrantées individuellement. L'intérêt de ce câble réside surtout dans le blindage entre les paires, et non dans la protection électromagnétique par rapport à l'environnement. C'est là une des deux manières efficaces d'éviter que les paires ne se perturbent entre elles (diaphonie), l'autre étant, sur les UTP et les FTP, de fabriquer des paires à des pas de torsades différents.

Il est recommandé de choisir les câbles en paires torsadées les plus optimisés suivants :

- **Entreprise.** Catégorie 5 ou 6 FTP, écranté globalement.
- **Résidentiel.** Grade 3 SFTP, écranté globalement mais aussi paire par paire. La paire dédiée à la TV doit impérativement être écrantée.

Les rocades

Les rocades servent à interconnecter les sous-répartiteurs, ou SR, desservant chacun une zone du bâtiment, généralement un étage, avec un maximum de 200 prises RJ-45. Elles ne concernent que les grandes installations et sont généralement dédiées aux applications qu'elles supportent, telles que LAN, téléphonie, gestion technique du bâtiment, etc.

La figure C.5 illustre l'organisation d'une installation avec deux sous-répartiteurs. Une installation de 2 000 prises comporte au moins une dizaine de sous-répartiteurs. Sur la figure, des liaisons horizontales raccordent les terminaux des utilisateurs, et les équipements actifs sont de simples hubs.

On distingue plusieurs types de rocades en fonction des applications qui y circulent :

- **Rocade téléphonique.** Étoile de câbles multipaires reliant tous les SR à un répartiteur général téléphonique, ou RG, lui-même raccordé directement à l'autocommutateur téléphonique. Cette organisation peut être différente pour les très grands sites, dans lesquels des autocommutateurs avec satellite peuvent être répartis sur plusieurs bâtiments, ou pour la téléphonie sur IP.
- **Rocade informatique.** Leur rôle est d'interconnecter le réseau d'entreprise. Elles peuvent être constituées par de simples câbles quatre paires raccordés suivant les mêmes conventions que le câblage horizontal.

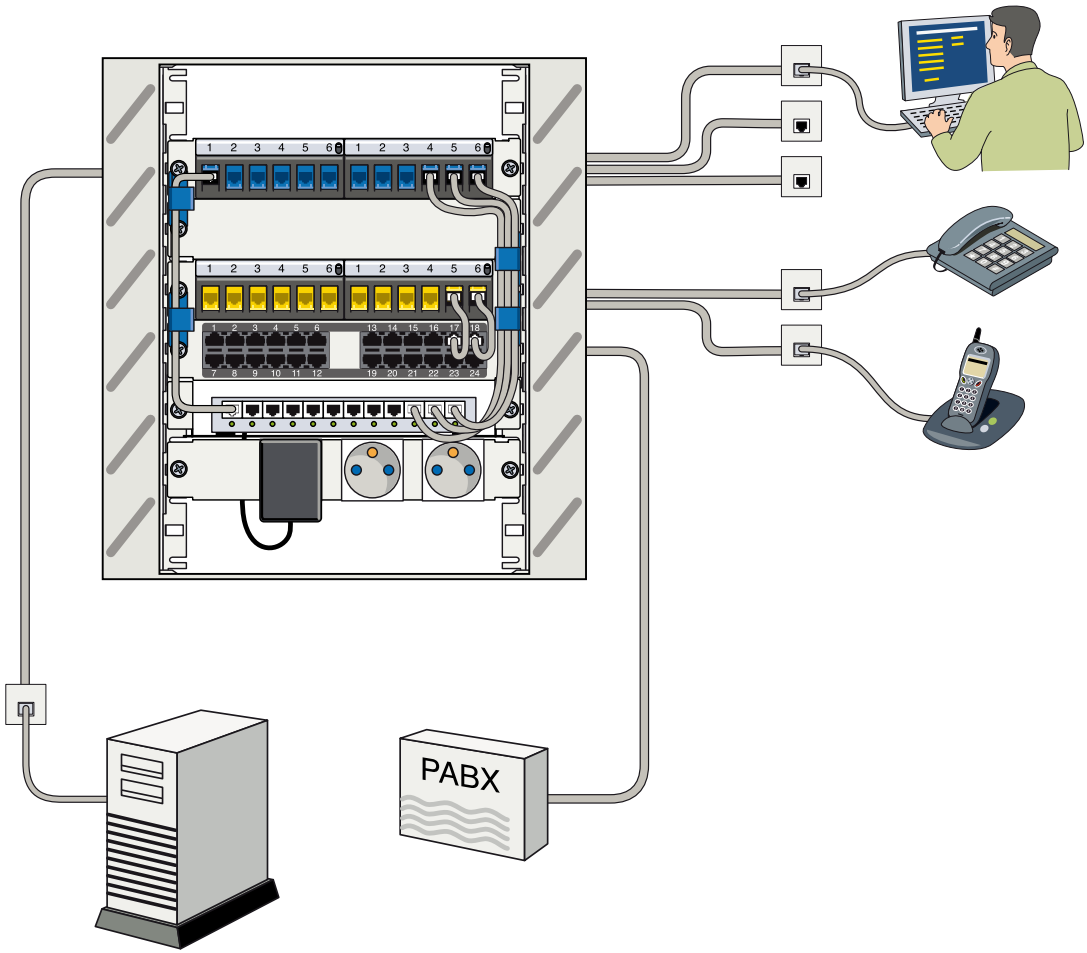


Figure C.5

Exemple d'organisation de deux sous-répartiteurs

- **Rocade optique.** Utilisées pour la connexion entre les bâtiments pour compenser la non-équipotentialité de leurs terres respectives, principalement pour les liaisons informatiques.
- **Rocade TV.** Constituées par un simple câble coaxial 75 Ω partant de la tête de réseau TV ou des sources audiovisuelles et aboutissant à chaque sous-répartiteur sur un distributeur actif TV. Il s'agit d'une sorte de hub destiné à transformer le signal coaxial entrant en signaux transportables sur les paires torsadées et brassables vers toutes les prises RJ-45. On peut donc, à partir des distributeurs TV, amener le signal TV analogique ou numérique sur toutes les prises RJ-45 de n'importe quel poste de travail, sans avoir besoin d'ajouter de câble CATV.

Raccordement des terminaux et des réseaux

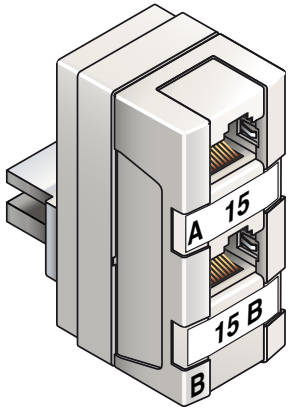
Les normes et les usages déterminent sur quelles bornes du RJ-45 doivent se connecter les principaux équipements et réseaux du marché. Ces bornes sont récapitulées au tableau C.3.

Tableau C.3 • Bornes de raccordement des équipements et réseaux

Équipement et réseau	Borne
Téléphonie une paire Téléphonie quatre paires	4-5 4-5 et 7-8
Ethernet 10 ou 100BaseT, micro-informatique, ADSL	1-2/3-6
Réseau fédérateur (backbone) 1000BaseT	Toutes les paires
TV/audiovisuel (5-862 MHz)	7-8
Terminaux écrans, hi-fi, enceintes actives, caméras, bus de terrain, etc.	Non défini

Il est possible de faire passer plusieurs réseaux sur des paires distinctes, par exemple le téléphone sur la paire 5-5 et Ethernet sur les paires 1-2 et 3-6. Dans ce cas, on utilise des duplicateurs à chaque extrémité de la liaison, comme illustré à la figure C.6.

Figure C.6
Exemple de duplicateur RJ-45



Les systèmes de distribution

Les systèmes de distribution déterminent les qualités organisationnelles des câblages banalisés. Ils reçoivent, outre les extrémités des câblages horizontaux et des rocades, les équipements actifs de réseau, tels que modems, hubs, routeurs, répéteurs, etc.

Les exemples suivants montrent les différences entre les systèmes de distribution spécifiques des trois types d'installations mentionnés précédemment :

- **Grande entreprise.** Comprend plusieurs centaines ou milliers de prises RJ-45, de nombreuses rocades et des équipements actifs divers (*voir figure C.7*).

Figure C.7

Armoire 19 pouces 42 U (Infra+)

- **Entreprise moyenne.** Comprend au maximum 200 prises RJ-45, aucune rocade, peu d'équipements actifs au format 19 pouces, voire aucun dans le cas d'une connexion à un ordinateur central de type AS400 (*voir figure C.8*).

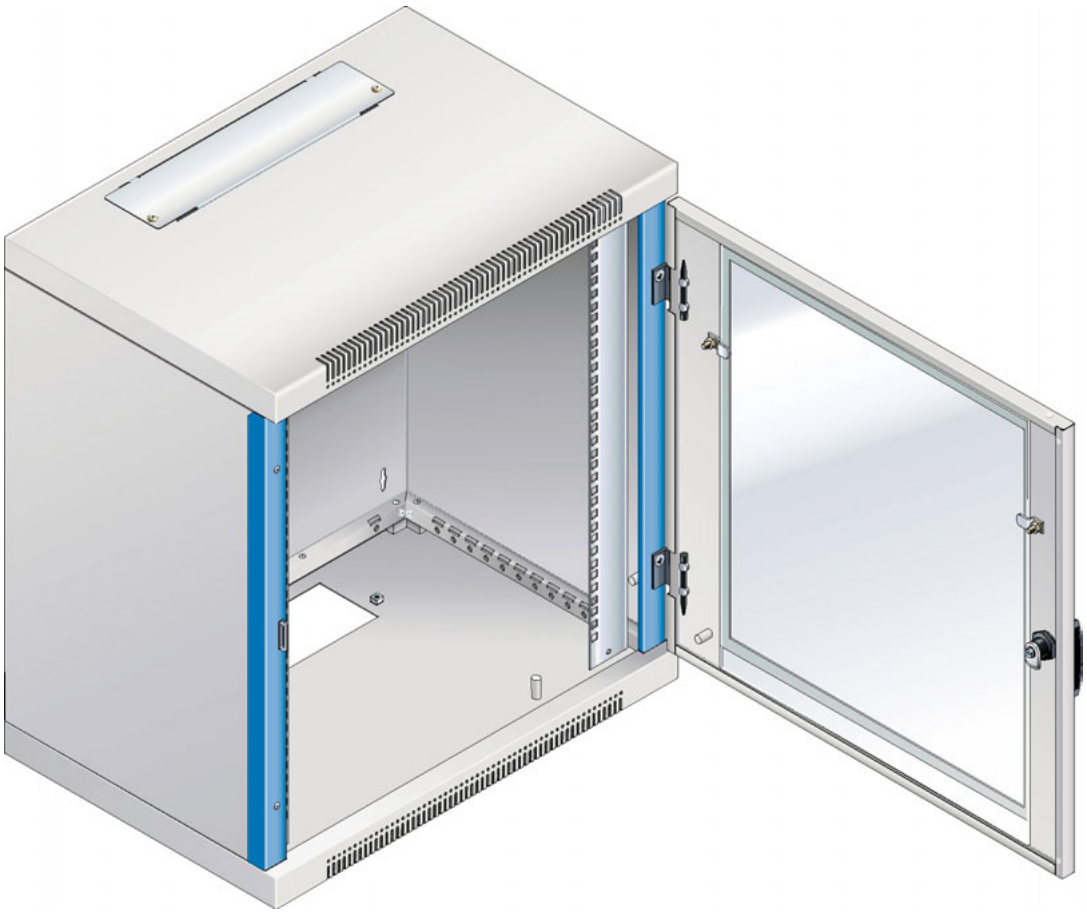


Figure C.8

Répartiteur pour petit site de 8 à 42 U (Infra+)

- **SOHO et résidentiel.** Comprend environ 8 à 24 prises RJ-45. Les équipements actifs sont de petit format (*voir figures C.9 et C.10*).

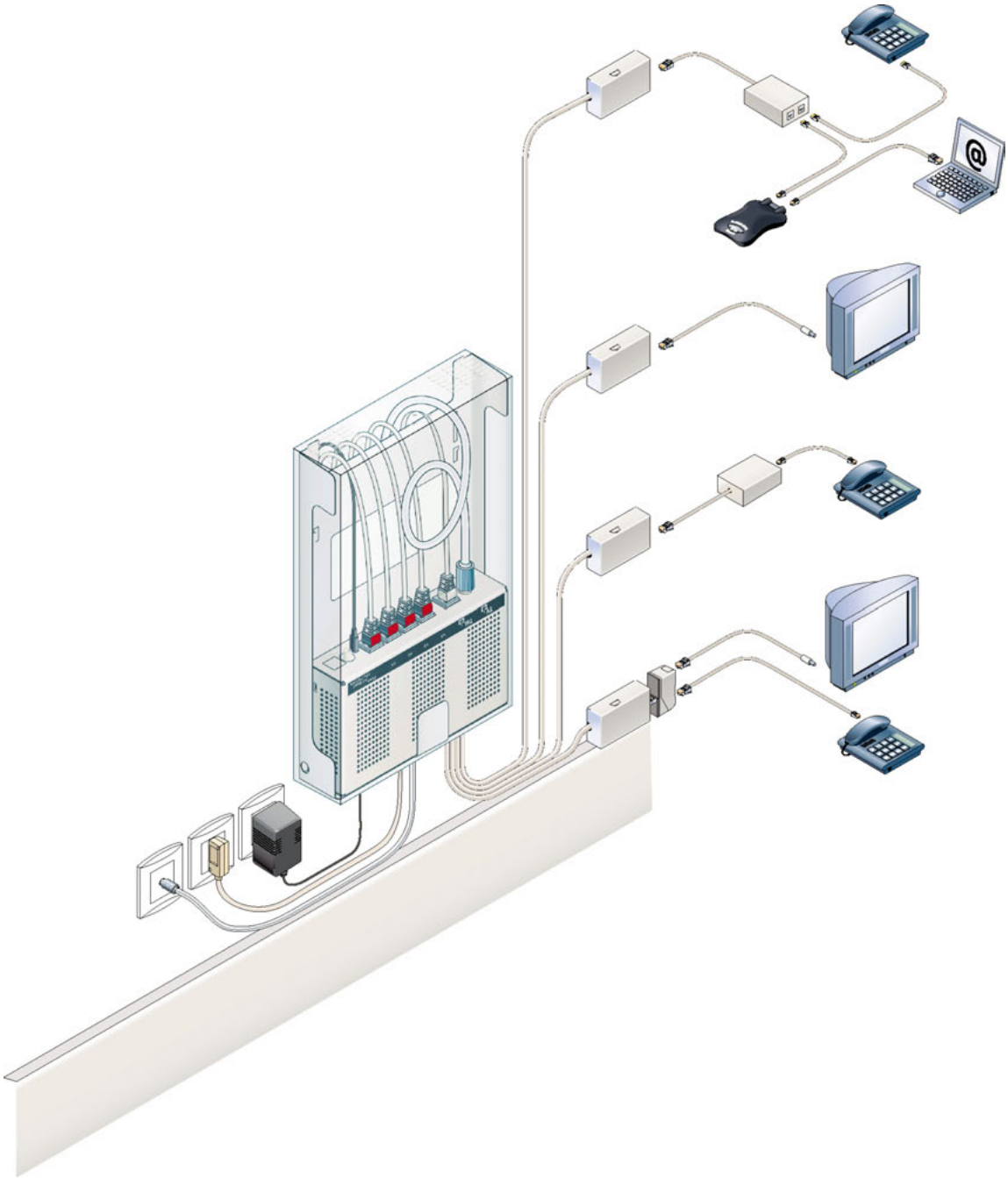


Figure C.9

Kit résidentiel SOLO (Casanova-sas) distribuant deux lignes téléphoniques, la TV et l'ADSL sur 8 prises RJ-45

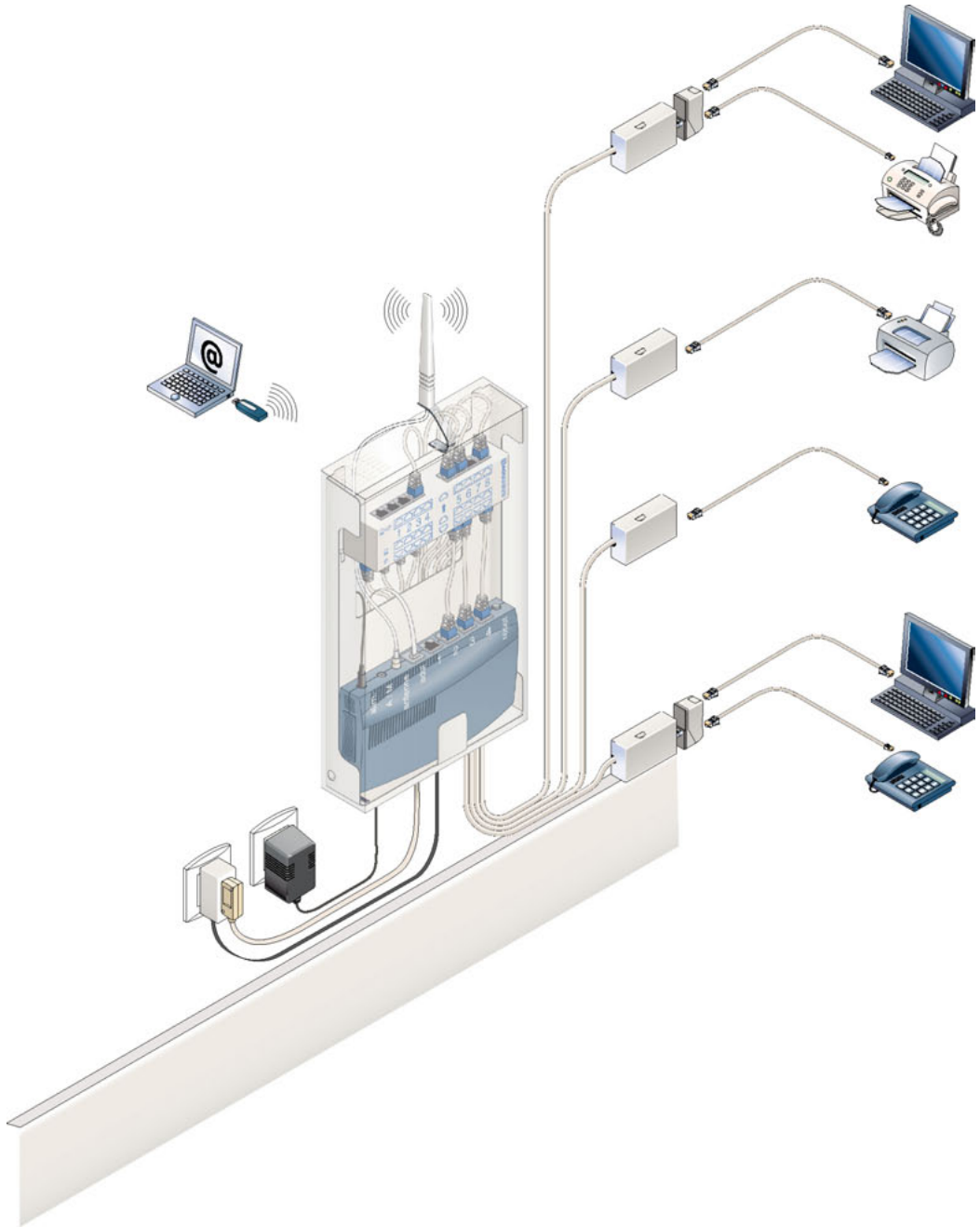


Figure C.10

Kit de bureau MINI OFFICE (Casanova-sas) distribuant deux lignes téléphoniques ou un micro-commutateur téléphonique, un réseau local 10-100BaseT, huit prises RJ-45, plus une option Wi-Fi

Recommandations pour réussir un câblage banalisé

Quelques règles sont nécessaires pour réussir un câblage banalisé, ou VDI (voix, données, images). Elles résultent de l'application des usages, du bon sens et des normes.

Les normes qui régissent le câblage actuel sont les suivantes :

- NF C15 -100 (électrique) ;
- NF C15 – 900 (cohabitation des réseaux) ;
- EN 50 173 ou ISO 11801 (câblage structuré) ;
- EN 90125 (TV/audiovisuel).

Dimensionnement

- Prévoir 30 à 50 % de prises en plus du besoin. Les prises en attente favoriseront la flexibilité des postes de travail.
- Densité des postes de travail : environ 1 pour 10 m^2.
- Poste de travail type : 2 prises RJ-45 et 3 à 4 prises 230 V.
- Nombre de prises RJ-45 par répartiteur : 200 au maximum. Au-delà, l'infrastructure devient ingérable (cordons de brassages trop longs et trop nombreux).
- Longueur du câblage horizontal : 90 m maximum (modèle de la norme). La longueur moyenne pour un câblage bien conçu doit être inférieure à 30 m. Mieux vaut prévoir 2 SR de 100 prises qu'un seul de 200 prises centralisé. Il en résulte un gain de main-d'œuvre et de câble de 35 % et un gain de performance de 50 %

CEM (compatibilité électromagnétique)

- Séparation courant fort/faible : obligatoire en UTP (30 cm entre les chemins de câbles, 5 cm pour les plinthes et chemins de câbles impérativement métalliques) et facultative en FTP pour des cheminements parallèles inférieurs à 5 m.
- Mise à la terre équipotentielle des SR, RG par tresse ou feuillard de section inférieure à 25 mm^2. Entre bâtiments ayant des terres différentes, la fibre optique est recommandée.

L'environnement électromagnétique est difficilement contrôlable. Il peut de plus se dégrader dans le temps du fait d'équipements radio de plus en plus nombreux, de matériels électriques défectueux, etc. Il est judicieux de privilégier les câbles FTP et les prises RJ-45 blindées.

Gestion

Il est important d'aérer les répartiteurs en intercalant des bandeaux passe-câbles entre les bandeaux de connexion ou actifs.

Au-delà de 200 postes de travail, il est nécessaire d'utiliser un système de gestion informatisé courant fort/faible. Un tel système permet la mémorisation des liaisons, des équipements actifs de réseau, des meilleurs cheminements et des disponibilités et fournit des statistiques, ainsi qu'une validation sous SNMP.

Le logiciel BMC de la société ARC offre, par exemple, les fonctionnalités suivantes :

- intégration directe des informations des testeurs dans la base de données du site ;
- ingénierie des réseaux (vision fédératrice des systèmes de communication) ;
- inventaire des liaisons, des réseaux et des équipements actifs raccordés ;
- gestion du câblage et des équipements actifs sous SNMP (bons de travaux, meilleur cheminement, etc.).

Contrôle et test du câblage

Le contrôle et le test sont indispensables car le câblage, une fois validé, ne doit jamais être suspecté en cas de dysfonctionnement éventuel de l'installation. Le contrôle dynamique n'est pas indispensable pour le résidentiel.

Contrôle électrique

Le contrôle électrique est réalisé systématiquement par l'installateur au moyen d'un testeur économique afin de vérifier que le câblage des paires sur les connecteurs est effectué correctement et que la continuité de la terre est assurée. Il s'effectue sur les RJ-45 depuis les SR. Des bouchons sont introduits à l'autre extrémité des câbles pour boucler les paires.

Un autre test permet de vérifier qu'il n'y a pas de court-circuit entre les paires et la terre (les bouchons doivent alors être retirés).

Test dynamique

Un test dynamique simule le fonctionnement des réseaux informatiques normalisés et mesure les paramètres fondamentaux de transmission, en fonction de la classe de câblage choisie :

- Classe E 250 MHz : composants catégorie 6 ;
- Classe D 100 MHz : composants catégorie 5.

Les testeurs de chantier sont des appareils sophistiqués, dont l'usage nécessite une formation spécifique. Ils permettent d'interpréter les résultats de test en fonction des valeurs mesurées suivantes :

- **Affaiblissement ou atténuation.** Cette valeur dépend de la longueur et de la qualité du câble. Elle doit être la plus faible possible.
- **Next.** Mesure la perturbation provoquée par le couplage d'une paire sur une autre. Cette valeur doit être la plus élevée possible.
- **ACR.** Résulte du calcul Next moins Atténuation. Cette valeur doit être la plus élevée possible.
- **Return Loss, ou affaiblissement de réflexion.** C'est la différence entre la puissance du signal émis et celle du signal réfléchi en raison des variations d'impédance du lien (connecteurs, mauvaise connexion, câble endommagé, etc.). Cette valeur doit être la plus élevée possible.

Annexe D

4. Les équipements réseau

Cette annexe décrit en détail les commutateurs Banyan, Knock-out, Lambdanet et ShuffleNet. Elle passe ensuite en revue différentes solutions de commutateurs ATM, dont l'objectif est de transférer des trames de longueur constante. Ces architectures sont à la base des commutateurs d'aujourd'hui.

Les commutateurs de base

Au moins trois possibilités sont utilisées comme éléments de base pour les commutateurs que l'on trouve dans le commerce :

- plusieurs commutateurs Banyan en série ;
- commutateur Batcher Banyan ;
- commutateur Knock-out.

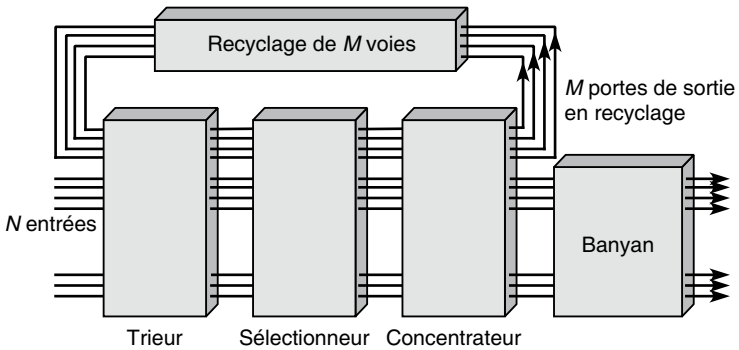
Commutateurs Banyan en série

Pour deux commutateurs en série, il y a m façons d'aller de l'émetteur au récepteur, si m est le nombre d'entrées et de sorties. Si k commutateurs sont en série, mk^{-1} chemins peuvent être envisagés. Néanmoins, cela ne résout pas directement les problèmes de collisions en sortie et rallonge le délai de transit.

Commutateur Batcher Banyan

Dans un commutateur Batcher Banyan, les trames qui entrent en collision en sortie sont recyclées suivant le principe illustré à la figure D.1. Le premier commutateur Banyan (trieur) permet de changer de ligne, et le deuxième (sélectionneur) d'opérer une sélection parmi les trames qui ont la même direction et qui entreraient en collision sur la ligne de sortie. Ensuite, le concentrateur permet de diriger la trame soit vers le dernier commutateur Banyan, et donc d'atteindre la ligne de sortie, soit de l'envoyer vers l'une des entrées d'un commutateur de recyclage de type MxM permettant de réintroduire la trame en début de cycle. Le choix de recycler une trame est pris dès que la ligne de sortie sur laquelle doit se rendre la trame est saturée. Une trame peut donc tourner dans le commutateur tant que la ligne de sortie est saturée.

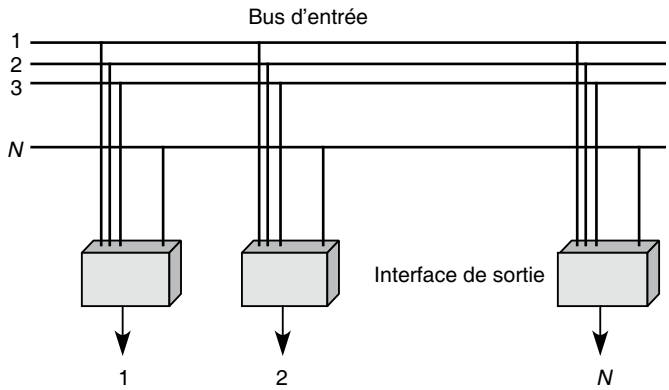
Figure D.1
Fonctionnement du commutateur Batcher Banyan



Commutateur Knock-out

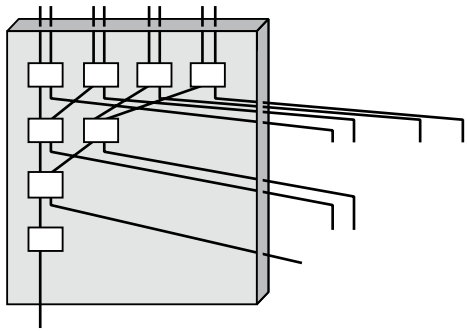
Dans le commutateur Knock-out illustré à la figure D.2, à partir d'une ligne d'entrée, les trames sont diffusées vers l'ensemble des interfaces de sortie. Dans l'interface de sortie, un Banyan à *n* entrées permet de faire converger les trames qui se dirigent vers la sortie *n*.

Figure D.2
Fonctionnement du commutateur Knock-out



Si plusieurs trames se présentent sur le même commutateur élémentaire, l'une d'elles est mise en attente de telle sorte qu'une seule trame sorte vers *n*. Le commutateur interne à l'interface de sortie est illustré à la figure D.3.

Figure D.3
Commutateur d'interface d'un Knock-out



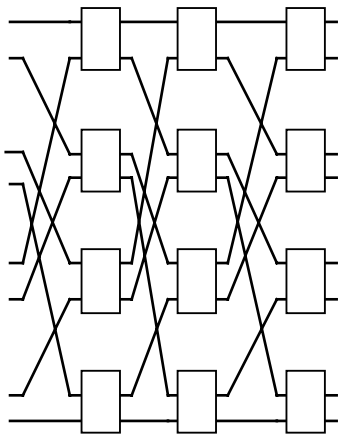
Autres commutateurs

Pour compléter la description des commutateurs actuels, on peut noter que, dans un réseau Banyan, si huit trames arrivent aux huit entrées simultanément, il n'y a qu'une seule possibilité de sortie pour que le parallélisme soit complet. Dans le réseau Banyan, cette possibilité est la suivante :

1 1 ; 2 5 ; 3 3 ; 4 7 ; 5 2 ; 6 6 ; 7 4 ; 8 8.

On peut imaginer d'autres commutateurs, avec des parallélismes différents (commutateurs Δ, Ω, etc.), dans lesquels les chemins suivis par les huit trames arrivant sur les huit entrées sont différents de ceux qui existent dans le commutateur Banyan. Le commutateur Ω permet l'identité, c'est-à-dire que la trame qui se présente sur l'entrée numéro 1 sort par la sortie numéro 1, la trame qui arrive en même temps sur l'entrée numéro 2 sort par la sortie numéro 2, et ainsi de suite. Le commutateur Ω est illustré à la figure D.4.

Figure D.4
Fonctionnement d'un commutateur Ω



En prenant, par exemple, la troisième entrée à partir du haut et en suivant toujours tout droit dans les commutateurs élémentaires, on se retrouve sur la troisième ligne de sortie. À la énième ligne d'entrée correspond la énième ligne de sortie.

Ce commutateur Ω présente toutefois l'inconvénient de ne plus permettre un routage aussi simple que le Banyan, où l'adresse de sortie autorise, lorsqu'elle est codée en binaire, le routage de la trame : avec un 0, on va vers le haut, et avec un 1 on va vers le bas. L'adresse de sortie 010 est atteinte si la trame est routée vers le haut puis vers le bas puis vers le haut pour terminer, et ce quelle que soit l'entrée. L'avantage global de ce système est de permettre le parallélisme des flux de trames à travers le commutateur.

Aujourd'hui, un regain d'intérêt se fait jour pour les techniques de commutation utilisant un bus partagé, car les progrès technologiques permettent de concevoir des bus atteignant des capacités de transport de plusieurs centaines de gigabits par seconde.

Le tableau D.1 recense les caractéristiques des différents commutateurs provenant de la source Banyan en fonction des cinq critères que nous avons retenus pour la définition d'un commutateur au début de ce chapitre.

Tableau D.1 • Caractéristiques des commutateurs de type Banyan

	Architecture interne	Liaison interne	Commutation interne	Contrôle du commutateur	Mémoire et blocage
Banyan élémentaire	1 étape	Liaisons dédiées	Répartition dans l'espace	Autoroutage	Pas de blocage interne
Banyan avec mémoire	*m* étapes	Liaisons dédiées	Répartition dans l'espace	Autoroutage dynamique	Pas de blocage résolu par des mémoire
Batcher Banyan	1 étape (*n* étapes si *n* rebouclages)	Liaisons statistiques	Répartition dans l'espace	Routage spécifique	Blocage interne résolu par le routage
Knock-out	1 étape	Liaisons dédiées	Répartition dans l'espace	Autoroutage	Blocage interne résolu par des mémoires internes

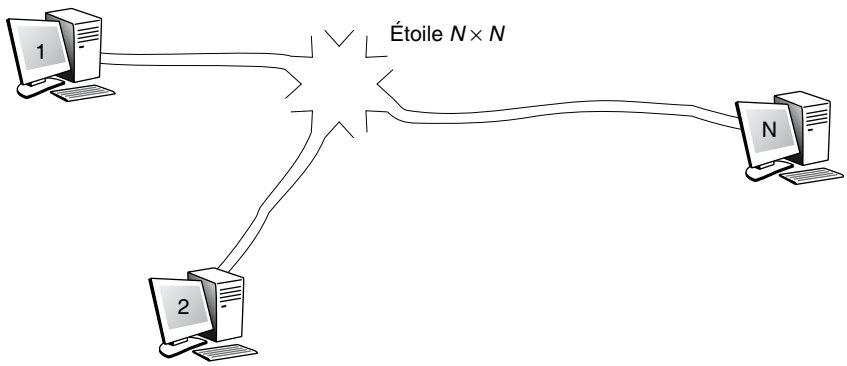
D'autres types de commutateurs de trames sont incarnés par le Lambdanet et le ShuffleNet. Ces deux commutateurs utilisent de la fibre optique avec du multiplexage en longueur d'onde, plusieurs faisceaux lumineux étant véhiculés en parallèle dans le cœur de la fibre optique.

Le Lambdanet

La figure D.5 illustre le fonctionnement d'un commutateur Lambdanet. À partir d'un émetteur, on envoie sur un sous-canal des trames diffusées par une étoile passive centrale vers des sous-canaux correspondant aux nœuds connectés. Pour 16 nœuds au total, il y a une voie aller et 16 voies de retour entre un nœud et l'étoile optique. Toutes ces voies sont

multiplexées en longueur d'onde dans une fibre optique monomode. Chaque voie atteint un débit de 10 Gbit/s si nécessaire. Cette technique facilite la diffusion et le multipoint, mais elle est coûteuse. En particulier, les machines terminales doivent avoir 16 récepteurs distincts pour recevoir sur les 16 longueurs d'onde en même temps.

Figure D.5
Fonctionnement du commutateur Lambdanet

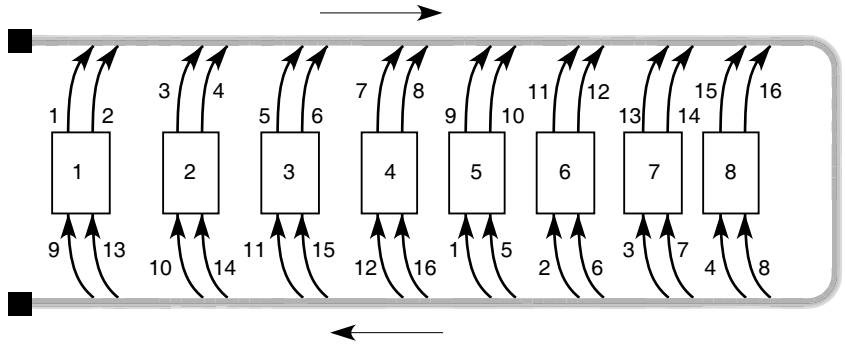


Le commutateur Lambdanet se caractérise par une étape, une liaison dédiée, une commutation spatiale, pas de contrôle *a priori*, des mémoires en sortie et pas de blocage.

Le ShuffleNet

Le commutateur ShuffleNet essaie de concilier les méthodes précédentes par des nœuds intermédiaires de commutation. Pour aller d'un point à un autre point, il faut généralement passer par un ou plusieurs nœuds intermédiaires, comme illustré à la figure D.6.

Figure D.6
Structure physique du ShuffleNet



L'avantage de cette technique est d'avoir plusieurs chemins utiles en cas de panne. Ces chemins ont une longueur variable. S'il y a trop d'embouteillage, on peut toujours prendre un autre chemin, certes plus long, pour atteindre le destinataire. Le support est une fibre qui prend en charge 16 canaux multiplexés en longueur d'onde. Sur la figure, pour aller

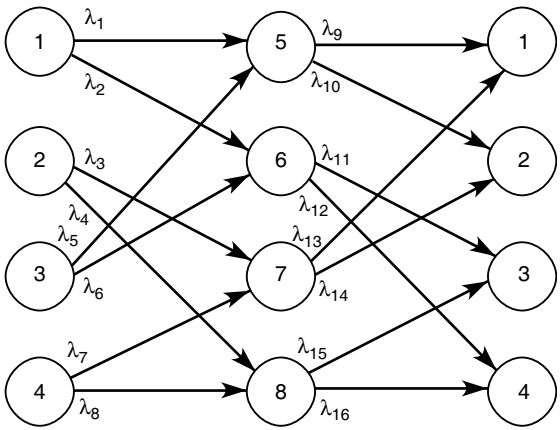
d'un nœud quelconque à un autre nœud, il faut passer au maximum par 3 nœuds intermédiaires. Par exemple, pour aller du nœud 1 au nœud 3, le nœud 1 émet sa trame vers la sortie 2 ; celle-ci arrive au nœud 6, qui l'envoie vers la sortie 11, ce qui permet au nœud 3 de recevoir l'information. L'avantage de cette technique est de n'avoir à chaque nœud que deux émetteurs et deux récepteurs et de disposer de plusieurs chemins pour aller d'un nœud à un autre.

Le commutateur ShuffleNet se caractérise par plusieurs étapes, une liaison statistique, une commutation spatiale, un contrôle à l'entrée pour optimiser le chemin et des mémoires dans les nœuds intermédiaires pour éviter les blocages.

Un commutateur ShuffleNet peut aussi être réalisé par le maillage illustré à la figure D.7. Une trame entrant par le nœud 1 et sortant par le nœud 3 doit être émise par le nœud 1 sur la longueur d'onde 2(λ_2) jusqu'à la porte 6, qui retransmet la trame sur la longueur d'onde 11(λ_{11}) jusqu'à la porte 3. Nous pouvons vérifier sur la figure que, partant du nœud 1, la trame arrive bien au nœud 3 après avoir suivi le chemin que nous venons d'indiquer. Il est bien sûr possible de trouver d'autres chemins pour aller du nœud 1 au nœud 3. Par exemple, en partant du nœud 1 sur la longueur d'onde 1, la trame arrive sur le nœud 5, qui envoie la trame sur la longueur d'onde 10, ce qui lui permet d'arriver au nœud 2. À partir de ce nœud, en se replaçant à droite de la figure, nous pouvons envoyer la trame sur la longueur d'onde 4, ce qui lui permet d'arriver au nœud 8, et, enfin, en utilisant la longueur d'onde 15, l'envoyer au nœud 3. Le chemin suivi comporte quatre étapes au lieu de deux dans le choix précédent. Ce deuxième choix n'est cependant pas inutile si le nœud 6 tombe en panne.

Figure D.7

Structure logique du ShuffleNet



Les techniques que nous venons de décrire sont à la base d'un grand nombre d'architectures de commutateurs actuellement commercialisées. Elles sont fondées sur une répartition dans l'espace. Une génération de commutateurs totalement différente, fondée sur la répartition dans le temps, est analysée à la section suivante.

Les commutateurs à répartition dans le temps

Les architectures à base de Crossbar ou de Banyan utilisent une répartition dans l'espace, qui privilégie l'affectation de voies parallèles pour effectuer le transport des trames entre les portes d'entrée et de sortie. Une autre grande solution consiste à travailler avec une répartition dans le temps, ce que l'on appelle encore répartition statistique, puisque la répartition des trames dans les tranches de temps se fait de façon statistique. C'est la raison pour laquelle on appelle ces commutateurs à répartition dans le temps des commutateurs temporels statistiques.

Dans ces commutateurs, le support physique est commun à l'ensemble des chemins, un découpage dans le temps permettant d'affecter les communications à tour de rôle. Bien évidemment, des solutions mixtes se sont développées, dans lesquelles un commutateur à répartition dans l'espace commence par proposer de multiples chemins entre une entrée et une sortie. Sur chaque chemin, un multiplexage temporel statistique permet ensuite à plusieurs communications de passer simultanément.

L'inconvénient majeur des techniques de répartition dans le temps est l'obligation d'utiliser un bus commun d'une capacité de transport égale à la somme des vitesses des voies d'accès, ce qui représente un coût important. Les commutateurs ATM temporels statistiques commercialisés par de grands équipementiers incarnent toutefois des solutions acceptables du point de vue du coût.

Commutateurs ATM temporels statistiques

Comme expliqué précédemment, les commutateurs temporels statistiques doivent posséder un bus par lequel transitent toutes les trames. Cette contrainte est très forte : pour 64 entrées avec une interface T_B à 155,52 Mbit/s, qui est l'interface de base normalisée pour les réseaux large bande, le débit du bus doit être de 10 Gbit/s. Le commutateur ATM que nous décrivons ci-après utilise un bus de très grande largeur, d'exactement 424 fils pour les données, une valeur qui correspond à la taille d'une cellule (424 bits). Si le débit de chaque fil est de 100 Mbit/s, on obtient une capacité de transport de 42,4 Gbit/s pour le commutateur. Les deux architectures que nous décrivons reposent, pour la première, sur un support en boucle et, pour la seconde, sur un support en bus.

Architecture en boucle

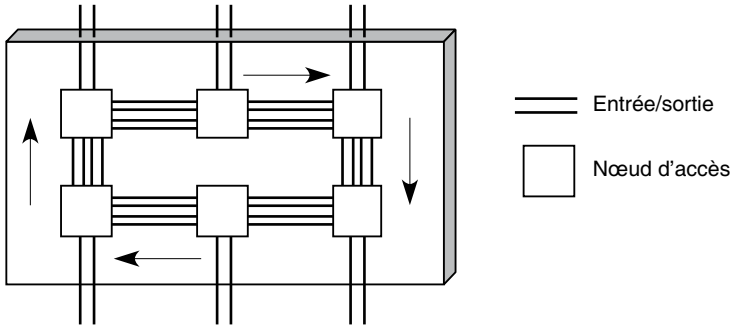
La boucle possède 424 lignes, ce qui permet de transporter les cellules en parallèle. Deux lignes supplémentaires sont réservées à la synchronisation et à la supervision. La vitesse de chaque ligne détermine une unité de temps. Si nous supposons une vitesse de 100 Mbit/s, l'unité de temps qui représente la durée d'une transmission est $y = 10$ ns. Pour entrer sur la boucle, un arbitrage est nécessaire. Nous proposons ici d'utiliser une insertion en parallèle, qui peut être considérée comme un arbitrage distribué. Cette solution est implémentée dans de nombreux commutateurs temporels statistiques sous des formes parfois légèrement différentes.

La cellule est introduite et retirée du support par l'émetteur. Cette solution permet de prendre en charge le multipoint ou la diffusion d'une cellule, les nœuds intermédiaires n'ayant qu'à réaliser une copie de la cellule lors de son passage.

Le support physique illustré à la figure D.8 est constitué de 6 portes d'entrée-sortie, qui donnent naissance à 6 nœuds internes sur la boucle. Entre ces nœuds, une boucle comportant 424 fils est constituée pour transporter les cellules en parallèle. Dans un nœud, un processus de sérialisation-parallélisation a lieu pour transmettre la cellule en série sur la porte d'entrée-sortie et en parallèle sur le bus interne. Cette partie du commutateur est décrite plus en détail dans l'encadré « L'architecture en bus ». Nous nous intéressons ici au transport de la cellule d'une porte d'entrée à une porte de sortie, en supposant que la parallélisation a été effectuée.

Figure D.8

Support physique du commutateur ATM temporel statistique



La cellule est transmise en parallèle, la synchronisation s'effectuant par un signal spécifique sur le fil supplémentaire. Comme la distance est particulièrement petite entre les nœuds d'accès au support, qui se trouvent tous soit sur la même carte physique, soit sur le même circuit imprimé, la synchronisation ne pose aucun problème. Le temps de transmission de la cellule sur le support physique est très court, puisque la transmission s'effectue en parallèle. De plus, dans chaque nœud du support physique, le signal n'a que deux registres à traverser.

L'accès au support physique est détaillé à la figure D.9. Il utilise deux registres parallèles dont les temps de remplacement sont variables et s'adaptent aux contraintes. Ces deux registres garantissent l'absence de collision sur le support.

Soit T_e = 10 ns le temps de remplacement maximal du registre correspondant au temps de transmission d'une cellule. Ce temps de remplacement pouvant en fait être variable, nous supposons ici que les valeurs 2, 4... à 10 ns sont possibles. Ce temps de remplacement dépend de l'activité du nœud, comme nous le verrons plus loin.

Le signal SYO (SYnchronization Out) est transformé en signal SYI (SYnchronization In) sur le fil de synchronisation. Ce signal permet de lire le contenu du registre d'entrée. Il faut noter qu'il n'y a pas d'horloge synchronisée entre les nœuds du support physique.

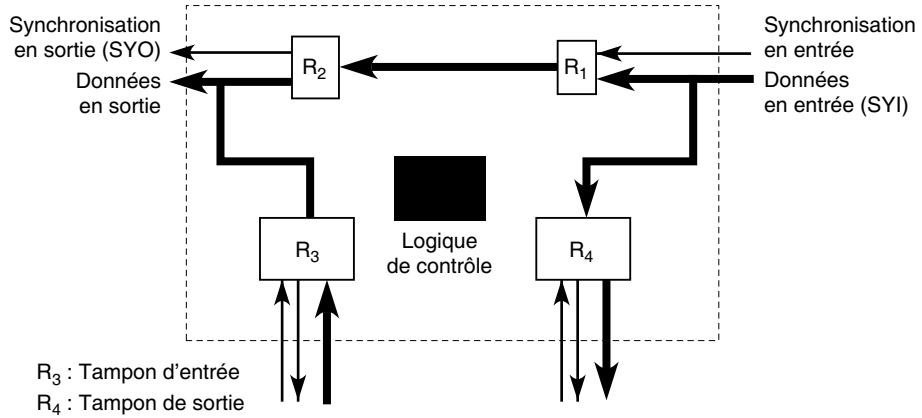


Figure D.9

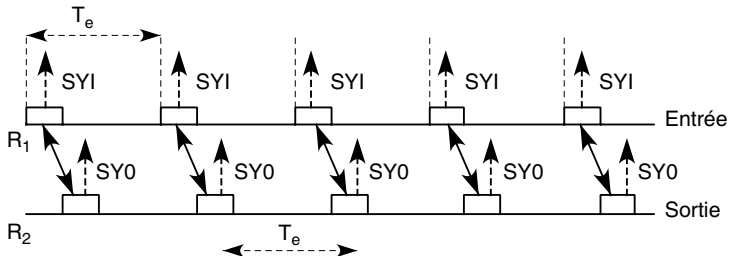
Architecture du nœud d'accès au support physique

Transit d'une cellule

Différents cas de figure peuvent se produire dans le nœud d'accès. Une cellule peut transiter dans un nœud sans que celui-ci soit concerné par l'émission ou la réception. Ce passage est illustré à la figure D.10. La cellule est stockée dans chaque registre pendant un temps minimal, soit 10 ns dans notre exemple, si le nœud n'est pas dans un état d'insertion. Si le temps de remplacement des registres est supérieur à cette valeur, il faut réduire le plus possible le temps pendant lequel la cellule reste dans les deux registres.

Figure D.10

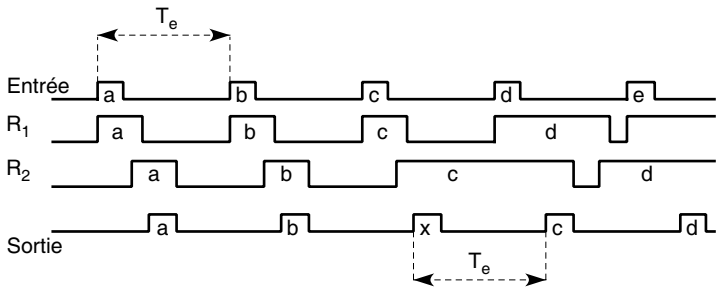
Transit dans un nœud



Insertion d'une cellule

Lorsque le registre R_3 d'émission est plein, la cellule contenue au sommet est insérée sur la boucle juste après la transmission. Si une cellule arrive de la boucle, elle est retardée dans le registre R_1 car la plus petite valeur possible du temps de remplacement est utilisée, mais sans qu'il y ait collision avec la cellule qui vient d'être insérée. Comme illustré à la figure D.11, la cellule *x* est insérée, ce qui retarde la cellule c, qui doit rester un temps de 50 ns dans les registres R_1 et R_2 avant d'être émise.

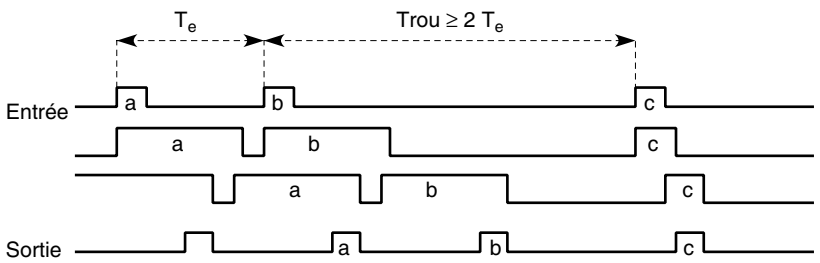
Figure D.11
Insertion d'une cellule



Une fois qu'une cellule est émise, il n'est pas possible d'en transmettre une nouvelle tant que les registres R_1 et R_2 ne retrouvent pas leur état (illustré à la figure D.12). Pour atteindre cette position, deux possibilités se présentent :

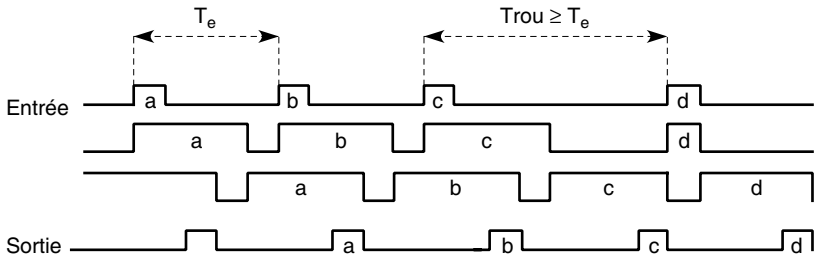
- Attendre un trou suffisamment grand entre deux cellules qui se présentent dans le nœud. Ce cas est illustré à la figure A.50.
- Attendre qu'une cellule insérée par ce même nœud revienne après un tour de boucle. Lors de son prélèvement du support, le nœud revient à son état de base.

Figure D.12
Retour en position de base



Grâce aux registres dont les temps de remplacement sont variables, il est possible de récupérer facilement des trous, qui, sinon, resteraient inemployés. Cette récupération est illustrée à la figure D.13.

Figure D.13
Récupération d'un trou sur le support



Les performances de ce commutateur à répartition dans le temps sont bien adaptées aux contraintes des flux ATM grâce à une très grande flexibilité de l'arbitrage distribué du

support physique. Tout d'abord, chaque porte du commutateur possède un débit minimal garanti, que nous appelons débit synchrone. Au minimum, une cellule peut être émise durant tous les intervalles de temps égaux au délai de propagation sur la boucle. Dans notre exemple, le temps maximal pour traverser un nœud est de 100 ns. En supposant le délai de propagation négligeable et 64 portes d'entrée-sortie, le temps de propagation maximal sur la boucle est de 6,4 µs. On en déduit que toutes les 6,4 µs, 48 octets d'informations peuvent être pris en charge, ce qui donne un débit minimal de 60 Mbit/s par porte. Le total des débits minimaux est de 3,84 Gbit/s. Cela représente exactement la moitié de la capacité utile du support. Les autres 3,84 Gbit/s peuvent être distribués de façon asynchrone aux différentes portes du commutateur.

Au moins deux possibilités de gestion de la bande asynchrone peuvent être définies :

- Outre son accès synchrone, une porte peut émettre dans les trous du support. Une fois qu'une cellule a pu être émise sur le support, la porte peut conserver le débit supplémentaire qui lui est donné par cette cellule. Il faut dans ce cas qu'à chaque retard de la cellule supplémentaire une nouvelle cellule soit émise immédiatement pour ne pas perdre le trou qui a été conquis.
- Interdire au nœud qui a conquis un trou supplémentaire de le réutiliser immédiatement.

Dans le premier cas, la porte possède un débit complètement garanti et synchrone, tandis que, dans le second, la bande supplémentaire est équitablement répartie entre les nœuds actifs.

D'après les simulations effectuées pour comprendre le comportement d'un tel commutateur ATM, la seconde solution est satisfaisante et s'adapte bien au trafic par à-coups que l'on rencontre dans les réseaux ATM. Nous avons également noté que les bandes passantes synchrones non utilisées sont récupérées par les autres portes en cas de nécessité. Cela se comprend très bien eu égard au temps de transit sur la boucle. Si nous supposons que 32 stations sur 64 sont inactives, le temps de transit d'une cellule sur la boucle est de 3,84 µs — les temps de passage sont de 20 ns dans les stations inactives. Le débit synchrone des stations actives devient donc de 100 Mbit/s.

Architecture en bus

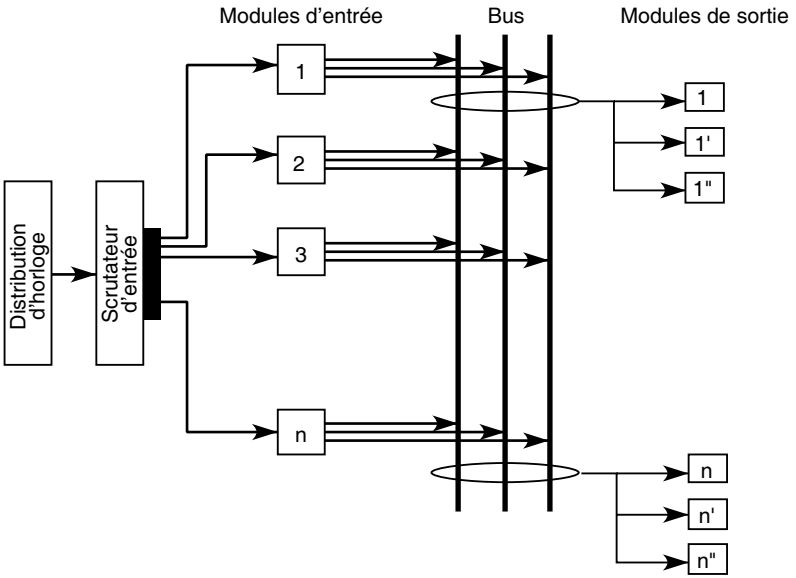
L'idée de cette architecture est de remplacer le support physique en boucle par une architecture en bus. La topologie en bus présente l'avantage de ne pas se préoccuper du prélèvement des informations qui transitent sur le support physique.

Dans ce nouveau commutateur, un scrutateur d'entrée dispose séquentiellement l'information provenant des *n* portes d'entrée sur le bus. En fonction de l'adresse des destinataires, la cellule est véhiculée ou non vers les portes de sortie. Le système est conçu de façon que, à chaque changement d'information sur le bus, une mémoire soit toujours disponible sur chaque sortie pour recevoir la cellule. Une mémoire de sortie doit impérativement être libérée entre deux pas successifs de scrutation en entrée, ce qui suppose un nombre de mémoires suffisant en sortie et un contrôle entre les entrées et les sorties.

La figure D.14 illustre le scrutateur d'entrée, les modules d'entrée et de sortie et un distributeur d'horloge.

Figure D.14

Schéma de fonctionnement d'un commutateur temporel statistique en bus



Le scrutateur d'entrée a pour fonction de prendre l'information contenue dans la porte d'entrée et de la déposer sur le bus, en synchronisation avec un signal d'horloge. Lors du top d'horloge suivant, une nouvelle entrée est scrutée, et sa cellule est insérée sur le bus.

Le rôle du module de sortie est d'extraire l'information qui lui est destinée et de la charger en parallèle dans le registre de sortie. Celui-ci est composé de 424 bits plus un bit PI (Presence Information). Tous les registres de sortie reçoivent le contenu du bus, mais seuls sont sélectionnés ceux qui correspondent au décodage d'adresse. Chaque sortie dispose d'un distributeur d'adresses, de telle sorte que, dès qu'une mémoire de sortie est chargée, une nouvelle mémoire libre est connectée.

Annexe E

6. Le niveau trame

Cette annexe détaille le protocole HDLC, qui a été des années durant le modèle des protocoles de liaison. Aujourd'hui, il n'est quasiment plus utilisé directement, mais reste un modèle de référence. Nous examinons ensuite les divers protocoles de liaison des réseaux Ethernet LLC (Link Logical Control).

HDLC (High-level Data Link Control)

En 1976, l'ISO normalise une procédure de communication entre deux ordinateurs sous le nom de HDLC (High-level Data Link Control). C'est la naissance du premier protocole standardisé de niveau liaison. D'autres protocoles moins puissants étaient jusqu'alors utilisés. Ils étaient du type « envoyer et attendre », l'émission d'une trame étant suivie d'une période d'attente de l'acquittement de la part du récepteur. La génération HDLC procède par anticipation : l'attente de l'acquittement n'empêche pas la transmission des trames suivantes.

Pour les besoins de transmission sur les liaisons des réseaux des opérateurs, l'UIT-T a repris un sous-ensemble de la norme HDLC, la partie concernant le mode équilibré. Cette procédure a pris au départ le nom de LAP (Link Access Protocol) et comportait des options particulières. Après des mises à jour en 1980 et en 1984, la procédure a été appelée LAP-B (Link Access Protocol-Balanced). La lettre B peut aussi indiquer le canal B du RNIS. C'est la procédure adaptée au niveau 2 du RNIS pour les canaux en mode circuit de type B. Cette norme a été complétée par le LAP-D (Link Access Procedure for the D-channel), associé au canal D du RNIS. Avant d'examiner plus en détail le protocole LAP-B, indiquons qu'il existe une possibilité normalisée de travailler en mode multi-liaison grâce au multiplexage de plusieurs protocoles LAP-B en mode équilibré sur une seule liaison.

Nous allons analyser le fonctionnement du protocole LAP-B, qui est aussi le protocole le plus courant dans le monde HDLC. Les deux autres protocoles décrits dans HDLC travaillent en mode maître-esclave, ce qui veut dire qu'une extrémité de la liaison dirige l'autre côté. La structure de la trame LAP-B est illustrée à la figure E.1.

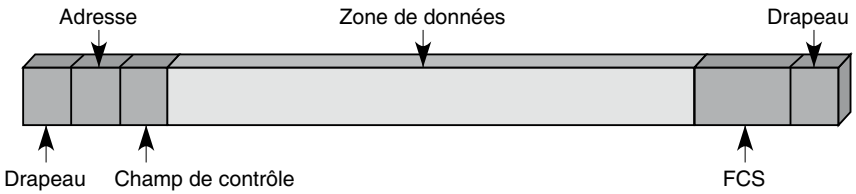


Figure E.1
Trame LAP-B

La trame LAP-B est composée d'une suite d'éléments binaires et d'un drapeau en début et en fin de trame de la forme 01111110.

Pour être certain qu'il n'existe pas de suite identique dans les données transportées, une technique, appelée insertion de 0, a été normalisée. Elle consiste à insérer automatiquement un 0 après cinq 1. Au niveau du récepteur, le 0 est supprimé dès que la valeur binaire 1 est reçue cinq fois de suite et que ces cinq bits sont suivis de la valeur 0. Cette démarche est illustrée dans les quatre transformations suivantes, très faciles à mettre en œuvre :

- 0111110 devient 01111100
- 01111110 devient 111111010
- 01111111 devient 011111011
- 011111110 devient 0111110110

La trame LAP-B comporte également un champ de contrôle et un champ d'adresse.

Les trois types de trames suivants ont été définis :

- trame I (Information) ;
- trame S (Supervision) ;
- trame U (Unumbered, ou non numérotée, ou encore trame de gestion).

Les trames U permettent de mettre en place les mécanismes nécessaires au bon fonctionnement du protocole. Les trames I portent les données provenant de la couche supérieure. Au nombre de trois, les trames S permettent le transport des commandes : la trame RR (Receive Ready) porte les acquittements qui ne sont pas émis dans une trame I, la trame RNR (Receive Not Ready) donne un contrôle de flux de niveau trame en demandant à l'émetteur de stopper les envois jusqu'à réception d'une nouvelle trame RR spécifiant le même numéro et la trame REJ (Reject) correspond à une reprise sur erreur en cas

de détection d'anomalie. La norme HDLC de base offre une quatrième possibilité, la trame SREJ (Selective Reject), qui ne demande la retransmission que de la seule trame en erreur.

Le champ de contrôle du protocole HDLC

Trois structures ont été définies pour le champ de contrôle (*voir tableau E.1*). Elles sont utilisées pour effectuer le transfert de trames d'information, numérotées ou non, de trames de supervision numérotées et de trames de commande non numérotées :

- **Structure de transfert de l'information (trame I).** La trame I permet d'effectuer le transfert de l'information. Les fonctions de N(S) et P/F sont indépendantes, chaque trame I contenant un numéro d'ordre N(S), un numéro d'ordre N(R), qui peut ou non accuser réception d'autres trames I à la station réceptrice, et un élément binaire P/F, qui peut être mis à 1 ou à 0.
- **Structure de supervision (trame S).** La trame S sert à réaliser les fonctions de commande de supervision de la liaison, comme l'accusé de réception, la demande de retransmission ou la demande de suspension temporaire de transmission. Les fonctions de N(R) et P/F sont indépendantes, chaque trame de structure S contenant un numéro d'ordre N(R), qui peut ou non accuser réception d'autres trames I à la station réceptrice, et un élément binaire P/F, qui peut être mis à 1 ou à 0.
- **Structure non numérotée (trame U).** La trame U est utilisée pour effectuer les fonctions de commande de la liaison et pour le transfert d'informations non numérotées. Cette structure ne doit pas contenir de numéro d'ordre mais comprendre un élément binaire P/F, qui peut être mis à 1 ou à 0. Cinq positions d'élément binaire modificateur sont disponibles, ce qui permet de définir jusqu'à 32 fonctions de commande et 32 fonctions de réponse supplémentaires.

Tableau E.1 • Formats du champ de contrôle (les numéros sont exprimés modulo 8)

Format du champ de contrôle	Élément binaire du champ de contrôle							
	1	2	3	4	5	6	7	8
Format I	0	N(S)			P	N(R)		
Format S	1	0	S	S	P/F	N(R)		
Format U	1	1	M	M	P/F	M	M	M

N(S)	numéro de séquence en émission (l'élément binaire 2 = élément binaire de poids faible).
N(R)	numéro de séquence en réception (l'élément binaire 6 = élément binaire de poids faible).
S	élément binaire de la fonction de supervision
M	élément binaire de la fonction de modification
P/F	élément binaire d'invitation à émettre lorsqu'il provient d'une commande ; élément binaire final lorsqu'il provient d'une réponse (1 = invitation à émettre/fin).
P	élément binaire d'invitation à émettre (1 = invitation à émettre)

Paramètres du champ de contrôle de HDLC

Les numéros, ainsi que les autres valeurs transportées dans les champs de contrôle, sont limités par la longueur du champ dans lequel ils sont notés. Si le champ est de 8 bits, la valeur varie de 0 à $2^8 - 1$, c'est-à-dire 255. Plus le champ est grand, plus la numérotation sans repasser par la valeur 0 est longue. La longueur du champ donne le modulo de comptage.

Modulo

Si *a* est un entier quelconque et *n* un entier strictement positif, nous écrivons *a* mod *n* pour représenter le reste dans {0,... , *n* – 1} obtenu en effectuant une division de *a* par *n*. Par exemple, 28 mod 12 = 4. Dans cet exemple, 12 est le modulo de comptage.

Numérotation

Chaque trame I doit recevoir un numéro d'ordre, qui peut prendre des valeurs allant de 0 à modulo – 1, correspondant au modulo de congruence des numéros d'ordre. Le modulo est égal à 8 ou à 128. La numérotation parcourt le cycle complet. Les formats du champ de commandes et réponses de modulo 8 sont indiqués au tableau E.2. Les formats du champ de commande de modulo 128 sont simplement une extension sur 2 octets du champ de contrôle.

Tableau E.2 • Formats du champ de commandes et réponses de modulo 8

Format	Commande	Réponse	Codage								
			1	2	3	4	5	6	7	8
Transfert d'information	I (information)		0	N(S)			P	N(R)		
Contrôle	RR (prêt à recevoir) RNR (non prêt à recevoir) REJ (rejet)	RR (prêt à recevoir) RNR (non prêt à recevoir) REJ (rejet)	1 1 1	0 0 0	0 1 0	0 0 1	P/F P/F P/F	N(R) N(R) N(R)		
Non numéroté	SABM (mise en mode asynchrone équilibré)		1	1	1	1	P	1	0	0
	DISC (déconnexion)		1	1	0	0	P	0	1	0
		UA (accusé de réception non numéroté)	1	1	0	0	P	1	1	0
		DM (mode déconnecté)	1	1	1	1	F	0	0	0
		FRMR (rejet de trame)	1	1	1	0	F	0	0	1

Le nombre maximal de trames I numérotées en séquence dans la station primaire ou secondaire en attente d'acquittement, c'est-à-dire pour lesquelles il n'y a pas eu d'accusé

de réception, ne doit jamais excéder le modulo des numéros d'ordre moins un. Cette restriction empêche toute ambiguïté dans l'association des trames I transmises avec les numéros d'ordre pendant le fonctionnement normal ou pendant les reprises en cas d'erreur.

Le nombre de trames I en attente d'acquittement peut être également limité par la capacité de stockage de la station de données, c'est-à-dire par le nombre de trames I qui peuvent être stockées pour la transmission ou la retransmission en cas d'erreur. Toutefois, le rendement optimal de la liaison ne peut être obtenu que si la capacité minimale de stockage de trames de la station de données est égale ou supérieure au délai de transmission aller-retour.

Variables d'état et numéros d'ordre

Chaque station de données doit maintenir de façon indépendante une variable d'état lors de l'émission V(S) et de la réception V(R) des trames I qu'elle transmet et reçoit :

- **Variable d'état à l'émission V(S).** Désigne le numéro d'ordre de la trame I suivante à transmettre en séquence. Cette variable peut prendre des valeurs comprises entre 0 et modulo – 1, correspondant au modulo de congruence des numéros d'ordre des trames, la numérotation parcourant le cycle complet. La valeur de la variable d'état à l'émission doit être augmentée d'une unité pour chaque trame I consécutive transmise mais ne doit pas dépasser la valeur de N(R) de la dernière trame reçue de plus de modulo moins un.
- **Numéro d'ordre à l'émission N(S).** Seules les trames I contiennent la valeur N(S), qui est le numéro d'ordre à l'émission des trames transmises.
- **Variable d'état à la réception V(R).** Désigne le numéro d'ordre de la prochaine trame I à recevoir en séquence. Cette variable d'état à la réception peut prendre des valeurs comprises entre 0 et le modulo – 1, qui correspond au modulo de congruence des numéros d'ordre des trames, la numérotation parcourant le cycle complet. La valeur de la variable d'état à la réception doit être augmentée d'une unité pour chacune des trames I reçues sans erreur et en séquence, le numéro d'ordre à l'émission N(S) devant être égal à la variable d'état à la réception.
- **Numéro d'ordre à la réception N(R).** Toutes les trames I et S doivent contenir la valeur N(R), qui indique le numéro d'ordre N(S) de la prochaine trame I attendue, à l'exception de la trame de supervision de rejet sélectif (SREJ), l'élément binaire P/F étant dans ce cas à 0. Avant de transmettre une trame I ou S, le N(R) doit être rendu égal à la valeur courante de la variable d'état à la réception. Le N(R) indique que la station transmettant le N(R) a reçu correctement toutes les trames I numérotées jusqu'à N(R) – 1.

Les figures E.2 à E.4 illustrent quelques exemples de fonctionnement du protocole et de la numérotation des trames.

Figure E.2
Transfert des données

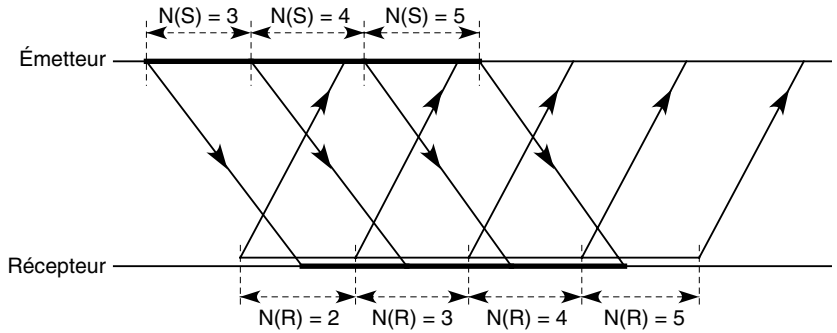


Figure E.3
Acquittements regroupés

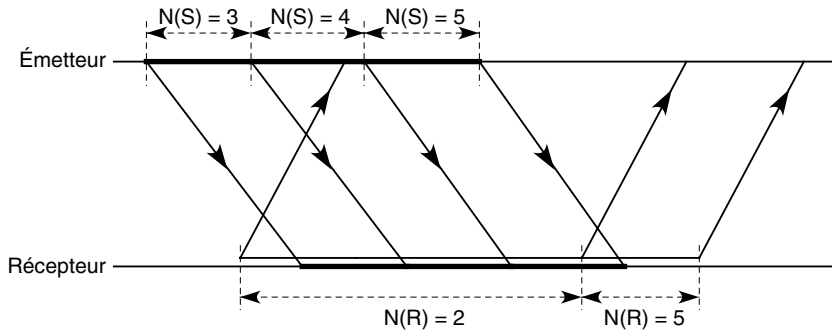
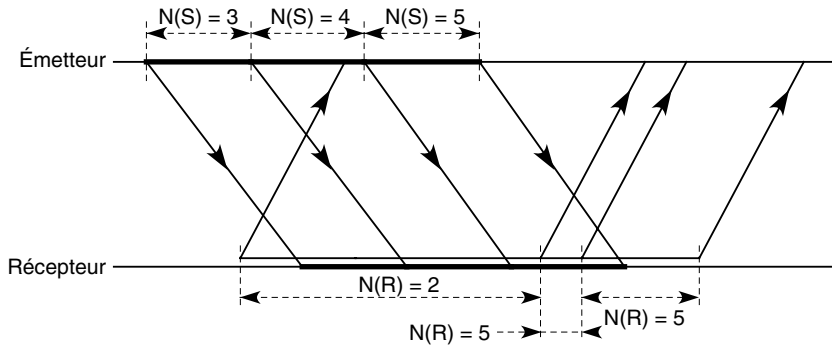


Figure E.4
Acquittements multiples



Commandes du champ de contrôle

Pour fonctionner correctement, le protocole doit émettre et recevoir des ordres de l'autre extrémité. Ces ordres s'exercent par le biais de valeurs, qui sont transportées dans le champ de contrôle. Regardons dans un premier temps les commandes disponibles dans HDLC.

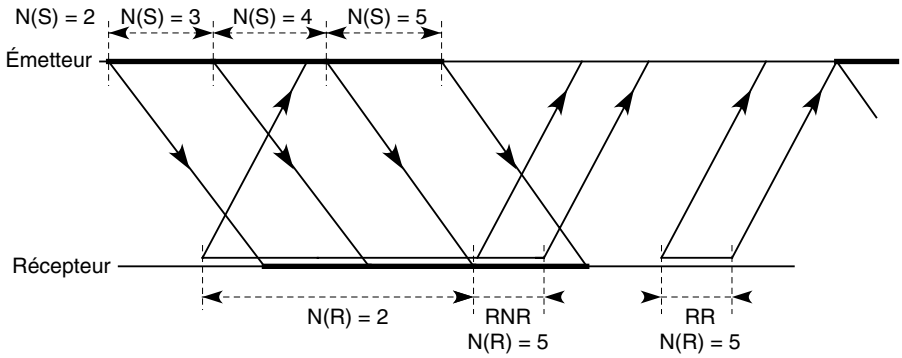
Commande et réponse RR

La trame de supervision RR, ou prêt à recevoir, doit être utilisée par l'émetteur pour indiquer qu'il est prêt à recevoir une trame I ou accuser réception des trames I reçues précédemment et dont le numéro de séquence est inférieur ou égal à N(R) – 1. Une trame RR peut être utilisée pour indiquer la fin d'un état d'occupation qui a été signalé auparavant par l'émission d'une trame RNR par cette même station (émetteur ou récepteur distant). Outre l'indication de l'état de l'émetteur, la commande RR, avec l'élément binaire P positionné à la valeur 1, peut être utilisée par l'émetteur pour demander l'état du récepteur distant.

Commande et réponse RNR

La trame de supervision RNR, ou non prêt à recevoir, est utilisée par l'ETTD (équipement terminal de transmission de données) pour indiquer un état d'occupation, c'est-à-dire une incapacité momentanée à accepter des trames I supplémentaires. La trame RNR accuse réception des trames I dont le numéro de séquence est inférieur ou égal à N(R) – 1. Elle ne doit pas accuser réception de la trame I numérotée N(R), ni d'aucune autre trame I qui pourrait éventuellement être reçue à sa suite, les acceptations de ces trames I étant indiquées dans des échanges ultérieurs. Le fonctionnement de la trame RNR est illustré à la figure E.5. Outre l'indication de l'état de l'émetteur, la commande RNR, avec l'élément binaire P positionné à 1, peut être utilisée par l'émetteur pour demander l'état du récepteur distant.

Figure E.5
Utilisation de la trame RNR



Commande et réponse REJ

La trame de supervision REJ, ou de rejet, doit être utilisée par l'émetteur pour demander la retransmission de trames I numérotées à partir de N(R). La trame REJ accuse réception des trames I dont le numéro de séquence est inférieur ou égal à N(R) – 1. Les trames I suivantes, en attente de transmission initiale, peuvent être transmises à la suite de la ou des trames I retransmise. Pour une liaison donnée, une seule trame REJ peut être émise à la fois. La commande REJ doit être annulée à la réception d'une trame I dont le numéro de séquence N(S) est égal au numéro N(R) spécifié dans la trame REJ.

Une trame REJ peut être utilisée par une station pour indiquer sa sortie d'un état d'occupation qu'elle avait signalé par la transmission antérieure d'une trame RNR. Outre

l'indication de l'état de l'émetteur, la commande REJ, dont l'élément binaire P a la valeur 1, peut être employée par l'émetteur pour demander l'état du récepteur distant.

Erreur sur le numéro de séquence N(S)

Le champ d'information de toutes les trames I reçues par le récepteur dont le numéro N(S) n'est pas égal à la variable d'état en réception V(R) doit être ignoré. Une condition d'exception apparaît lorsqu'une trame I reçue contient un numéro N(S) qui n'est pas égal à la variable d'état en réception. Le récepteur n'accuse pas réception, autrement dit n'incrémente pas sa variable d'état en réception, de la trame I qui a causé l'erreur de séquence, ni d'aucune autre trame I qui pourrait la suivre, avant d'avoir reçu une trame I comportant le numéro N(S) correct.

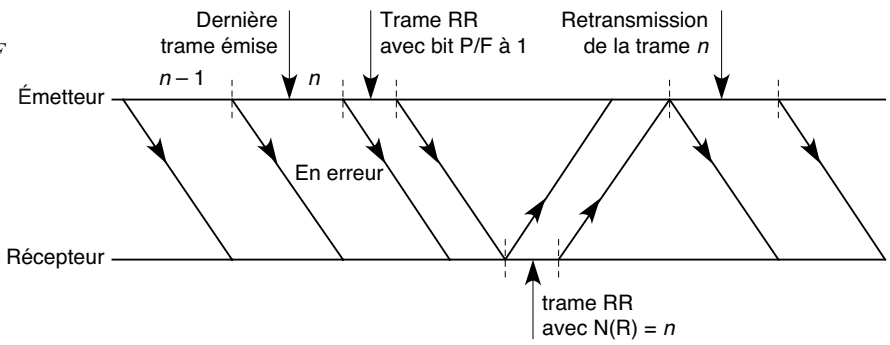
Un récepteur qui reçoit une ou plusieurs trames I comportant des erreurs de séquence ou des trames de supervision RR, RNR et REJ doit accepter l'information de commande contenue dans le champ N(R) et l'élément binaire P ou F afin d'exécuter les fonctions de commande de la liaison. Il doit, par exemple, accepter de recevoir des accusés de réception de trames I précédemment émises par l'émetteur et répondre, l'élément binaire P étant positionné à 1. Les moyens spécifiés ci-après doivent être disponibles pour déclencher la retransmission de trames I perdues ou erronées, suite à l'apparition d'une condition d'erreur sur le numéro de séquence N(S).

Reprise par le bit P/F

La reprise par le bit P/F se fonde sur un cycle de point de reprise. Pour l'ETTD, un cycle de point de reprise commence au moment de la transmission d'une trame de commande, avec l'élément binaire P positionné à 1. Elle prend fin soit lors de la réception d'une trame de réponse avec un élément binaire F positionné à 1, soit lorsque la fonction de temporisation de réponse s'achève, le temporisateur T1 ayant été déclenché au moment de l'émission de la trame comportant le bit P = 1.

Par la transmission d'une trame I, RR, RNR ou REJ avec l'élément binaire P positionné à 1, l'émetteur réclame une réponse sous la forme d'une trame de supervision avec l'élément binaire F positionné à 1. Au moment de la réception de cette trame, il commence la retransmission de toutes les trames I non acquittées et possédant un numéro de séquence inférieur à la valeur qu'avait la variable d'état en émission V(S) au moment où la trame de commande avec l'élément binaire P positionné à 1 a été transmise (*voir figure E.6*).

Figure E.6
Reprise par le bit P/F

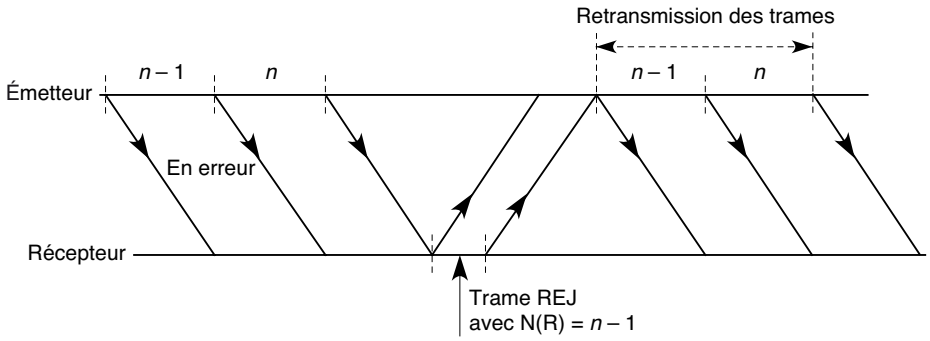


Reprise par REJ

La trame REJ doit être utilisée par un récepteur pour déclencher une reprise, ou retransmission, à la suite de la détection d'une erreur de séquence N(S).

On ne doit établir qu'une seule condition d'exception « REJ envoyée », issue du récepteur à un instant donné. Il faut annuler les conditions d'exception « REJ envoyée » lors de la réception de la trame I requise. Une trame REJ peut être retransmise un nombre de fois déterminé par le protocole, si la condition d'exception de REJ n'est pas annulée par le temporisateur T1 suite à la transmission d'une trame REJ (*voir figure E.7*).

Figure E.7
Reprise par REJ



L'émetteur recevant une trame REJ en provenance d'un récepteur distant déclenche la retransmission séquentielle de trames I, en commençant par celle comprenant le même numéro N(R) que celui contenu dans la trame REJ. Les trames retransmises peuvent comprendre un numéro N(R) et un élément binaire P mis à jour, par conséquent différents de ceux contenus dans les trames I transmises à l'origine. L'ETTD commence la retransmission avant ou pendant la transmission de la nouvelle tranche de commande, avec l'élément binaire P positionné à 1.

La retransmission suite à une trame REJ doit être interdite par l'émetteur dans les deux cas suivants :

- La retransmission de l'ETTD commençant par une trame particulière se produit par l'intermédiaire du point de reprise (*voir plus haut*).
- Une trame REJ est reçue de l'ETCD avant la fin du cycle de point de reprise suivant, cycle qui amorcerait également la retransmission de cette même trame (telle qu'elle est identifiée par le numéro N(R) dans la trame REJ).

Nous décrivons dans la suite du chapitre quelques trames de gestion (trame U) utilisées en mode LAP-B.

Commandes de mise en mode asynchrone équilibré (SABM) et équilibré étendu (SABME)

La commande non numérotée SABM (Set Asynchronous Balanced Mode) est utilisée pour placer l'ETCD ou l'ETTD appelé dans l'état de transfert de l'information en mode

asynchrone équilibré (LAP-B). Dans ce mode, tous les champs de commandes et de commandes-réponses doivent s'étendre sur une longueur d'un octet.

La commande non numérotée SABME (Set Asynchronous Balanced Mode Extended) a les mêmes fonctions que la commande SABM, mais les champs de commandes et de commandes-réponses numérotées doivent maintenant avoir une longueur de 2 octets, et les réponses non numérotées une longueur de 1 octet.

Commande de déconnexion (DISC)

La commande non numérotée DISC (Disconnect Command) est utilisée par l'ETTD pour demander que prenne fin le mode préalablement établi. Elle sert à informer l'ETCD-ETTD distant, récepteur de la commande DISC, que l'ETTD émetteur de la commande DISC suspend son fonctionnement. Il n'est pas permis d'inclure un champ d'information dans la commande DISC. Avant d'exécuter la commande, l'ETCD-ETTD distant, récepteur de la commande DISC, exprime l'acceptation de la commande DISC en envoyant un accusé de réception non numéroté (UA). L'ETTD émetteur de la commande DISC passe à la phase de déconnexion lorsqu'il reçoit l'accusé de réception UA.

Réponse d'accusé de réception non numérotée (UA)

La réponse non numérotée UA (Unnumbered Acknowledgement) est utilisée par l'ETTD pour accuser réception des commandes non numérotées SABM-SABME et DISC et les accepter. Il n'est pas permis d'inclure un champ d'information dans la réponse UA. L'émission d'une réponse UA doit indiquer la sortie d'un état d'occupation qui avait été signalé auparavant par la même station par l'émission d'une trame RNR.

Réponse en mode déconnecté (DM)

La réponse en mode déconnecté, DM, est utilisée par l'ETTD pour signaler un état dans lequel l'ETTD est logiquement déconnecté de la liaison et se trouve dans la phase de déconnexion. La réponse DM peut être émise dans cette phase pour demander une commande de mise en mode. Si elle est déjà émise, elle peut répondre à la réception d'une commande de mise en mode informant l'ETCD-ETTD distant que l'ETTD se trouve toujours en phase de déconnexion et ne peut exécuter la commande de mise en mode. Il n'est pas permis d'inclure un champ d'information dans la réponse DM.

Réponse de rejet de trame (FRMR)

La réponse FRMR (Frame Reject) est utilisée par l'ETTD pour indiquer une condition d'erreur ne pouvant être récupérée par la retransmission de la trame identique par l'ETCD-ETTD distant. Cela revient à dire que l'une au moins des conditions suivantes qui résultent de la réception d'une trame valide doit être satisfaite :

- Réception d'un champ de commande ou de commande-réponse non défini ou non mis en œuvre.
- Réception d'une trame I dont le champ d'information dépasse la longueur maximale déterminée.

- Réception d'un N(R) non valide.
- Réception d'une trame comprenant un champ d'information qui n'est pas permis ou la réception d'une trame de supervision de longueur incorrecte (comprenant de 32 à 39 éléments binaires inclusivement).

Un N(R) non valide est défini comme un N(R) qui pointe vers une trame I émise auparavant et acquittée ou vers une trame I non encore émise, qui n'est pas la trame I suivante en séquence ou en attente de transmission. Un N(R) valide doit être contenu dans l'intervalle compris entre le numéro de séquence en émission le plus faible N(S) de la ou des trame non encore acquittée et la valeur en cours de la variable d'état en émission de l'ETTD.

Un champ d'information doit être joint à cette réponse et fournir la raison de l'émission de la réponse FRMR. Ce champ suit immédiatement le champ de commande et consiste en 3 octets (fonctionnement de base modulo 8) ou en 5 octets (fonctionnement étendu modulo 128).

LAP-F

Le protocole LAP-F (Link Access Protocol-Frame) est né avec le relais de trames, conçu pour améliorer les performances des réseaux issus de la recommandation X.25 de l'UIT-T. Cette dernière s'étant révélée trop lourde et donc incapable d'accroître les débits, il a fallu en rechercher une simplification.

L'idée mise en œuvre a consisté à supprimer le niveau paquet et à faire redescendre les fonctionnalités de ce niveau dans le niveau trame. Le protocole LAP-B a évolué pour devenir le protocole LAP-F, caractérisée par le remplacement de la zone d'adresse par une zone destinée à accueillir une référence de commutation, le DLCI (Data Link Connection Identifier).

Le champ DLCI de base a été étendu par l'adjonction d'un deuxième octet puis d'un troisième, dans lesquels 6 et 7 bits sont dévolus à l'allongement du champ DLCI. La structure de la trame LAP-F est illustrée à la figure E.8.

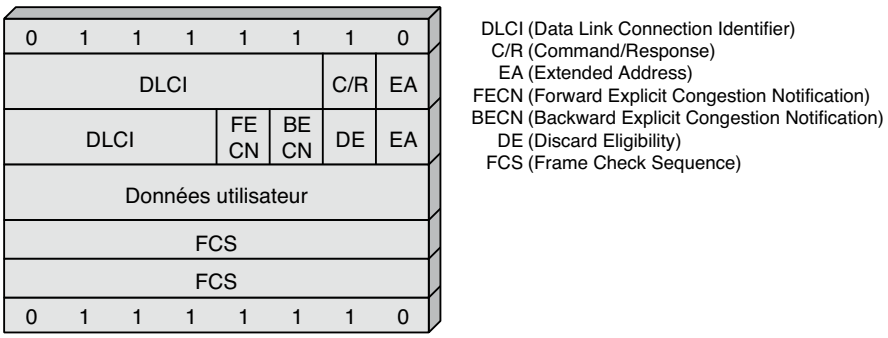


Figure E.8

Structure de la trame LAP-F

Les trames LLC

Les réseaux locaux (LAN) ont des particularités assez différentes des réseaux étendus (WAN). Ils sont d'abord multipoint. Cela revient à dire que toutes les stations peuvent être atteintes à partir d'un coupleur. La prise en compte du multipoint a poussé l'ISO à normaliser un protocole de niveau trame spécifique pour les réseaux locaux. Le travail a été effectué en grande partie par le groupe 802.2 de l'IEEE. La norme correspondante reprise par l'ISO porte la valeur ISO 8802.2 et est appelée LLC (Logical Link Control).

En réalité, il n'y a pas une norme LLC mais trois : LLC 1, LLC 2 et LLC 3, chacune adaptée à un mode de fonctionnement spécifique. Lors de l'élaboration de la norme de base LLC 1, souvent appelée LLC pour des raisons historiques, le faible taux d'erreur résiduelle au sommet de la couche 1 a été pris en compte. Puisqu'il était inutile de mettre en œuvre une technique de reprise sur erreur, la norme LLC 1 n'en possède pas. Enfin, pour prendre en compte plus facilement le multipoint, le protocole est exploité dans un mode sans connexion.

Le protocole LLC 1 est assez simple et comporte peu de fonctionnalités. Une zone de contrôle d'erreur a été introduite dans la trame afin de vérifier que les erreurs sont en nombre négligeable. Lorsqu'une trame en erreur est détectée, elle est détruite, de façon à éviter que des informations erronées soient utilisées. Le taux d'erreur résiduelle peut ne plus être négligeable après ces destructions. Puisque le niveau liaison n'a pas la possibilité d'effectuer les reprises nécessaires, un niveau supérieur de l'architecture doit s'en occuper. C'est le niveau message qui effectue la reprise, et plus spécifiquement le protocole TCP.

La norme LLC 2 est issue d'une constatation simple : si le nombre d'erreur en ligne n'est pas négligeable, plutôt que de repousser le problème de la correction au niveau message (couche 4), il est préférable d'effectuer directement la reprise sur erreur au niveau trame (couche 2). Pour sécuriser l'acheminement des données, la norme LLC 2 spécifie un protocole de niveau trame en mode avec connexion. Avec la reprise sur erreur et le mode avec connexion, LLC 2 dispose de toutes les fonctionnalités de la norme HDLC.

La norme LLC 3 provient d'un constat particulier du monde industriel. Si une trame est erronée et doit être renvoyée, on peut se poser la question de sa validité et de son utilité, surtout si elle est renvoyée après un temps assez long. La procédure LLC 3 est une norme sans connexion, mais avec une possibilité de reprise sur erreur laissée à l'initiative de l'émetteur, qui peut ainsi récupérer les trames dont les temps critiques ne sont pas dépassés.

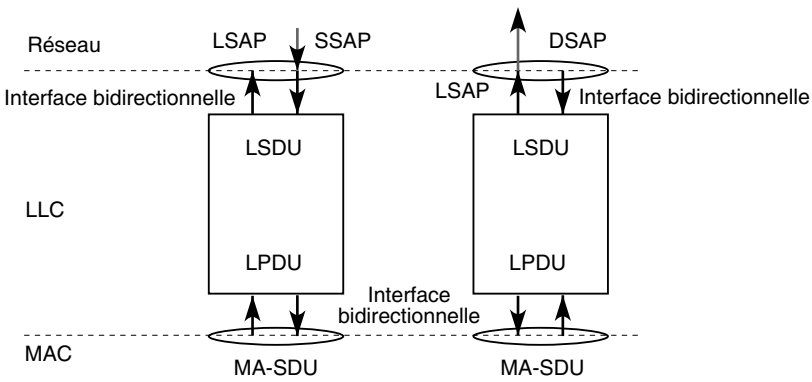
La couche LLC offre un service de niveau paquet, ou couche 3 (ISO 8802.2). Des primitives de service permettent de demander ce service au travers de LSAP (Link Service Access Point).

En mode sans connexion, les extrémités d'une connexion, ou portes d'accès au service, sont désignées de la façon suivante :

- DSAP (Destination Service Access Point), ou point d'accès au service destination.
- SSAP (Source Service Access Point), ou point d'accès au service source, qu'il ne faut pas confondre avec le point d'accès au service de session.

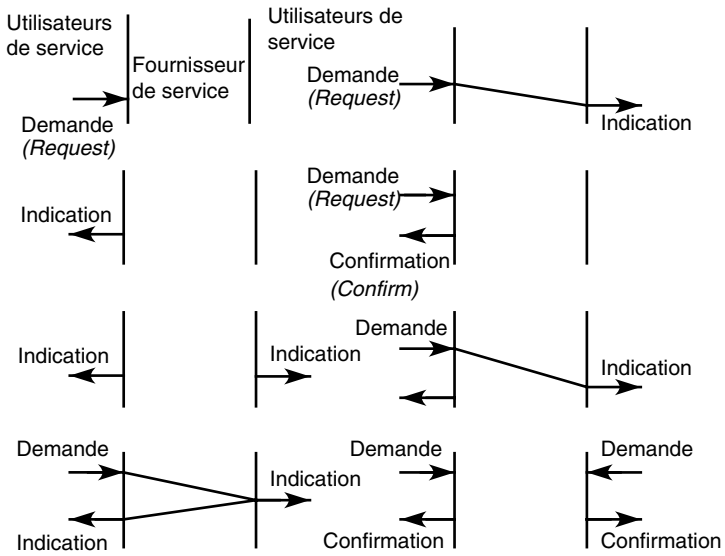
Les interfaces des couches réseau et MAC avec la couche LLC sont illustrées à la figure E.9.

Figure E.9
Interfaces de la couche LLC



Les primitives de contrôle des interactions entre la couche réseau et la couche LLC sont représentées à la figure E.10.

Figure E.10
Primitives de contrôle LLC



Différences entre les normes LLC et HDLC

Les protocoles LLC et HDLC comportent globalement les mêmes normes et les mêmes formats de trame, mais avec les six différences fondamentales suivantes :

- Comme la trame HDLC dans son mode étendu, la trame LLC comporte deux champs d'adresse sur 7 bits (*voir figure E.11*). Le bit supplémentaire du premier octet indique une adresse multipoint ou de diffusion :

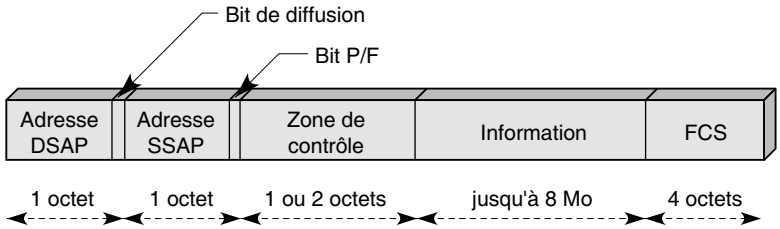
  1 : adresse multipoint. Si le champ d'adresse porte la valeur 7, c'est une diffusion.

  0 : adresse individuelle. La valeur 0 dans le champ d'adresse indique le service de gestion du niveau MAC.
- Le dernier bit du deuxième octet indique une commande ou une réponse. Il travaille à peu près comme le bit P/F de HDLC :

  1 : indique une réponse.

  0 : indique une commande.

Figure E.11
Format de la trame LLC



- La zone de contrôle est généralement sur deux octets, avec une numérotation des trames sur 7 bits, ce qui permet une anticipation de 127 trames. La numérotation sur 3 bits n'est pas interdite.
- LLC n'utilise que le mode ABM (Asynchronous Balanced Mode), ou mode équilibré. Les trames de gestion SABM et DISC sont utilisées pour établir et libérer la connexion dans le protocole LLC 2. Le mode sans connexion de LLC 1 et LLC 3 supporte la trame de gestion UI.
- Les protocoles LLC se servent d'un multiplexage sur les points d'accès au service MAC.
- Deux trames de gestion spécifiques de LLC 3 ont été définies pour prendre en charge le service avec acquittement, mais sans connexion.

Annexe F

7. Le niveau paquet

Cette annexe détaille l'adressage ISO, qui n'est plus utilisé mais qui sert toujours de modèle pour de nombreuses solutions d'adressage. Elle passe également en revue le protocole X.25, qui a été très important durant les années 1980 et 1990. Les plus grands réseaux du monde ont utilisé ce standard, comme le réseau français Transpac.

L'adressage ISO

Donnons tout d'abord quelques définitions de la norme d'adressage ISO de base :

- Une appellation est un identificateur permanent d'une entité.
- Le domaine d'appellation est le sous-ensemble de l'espace d'appellation de l'environnement OSI.
- Le nom de domaine est un sous-ensemble de l'espace d'appellation dans l'environnement OSI. Les couches OSI sont des domaines d'appellation.
- Une appellation locale est une appellation unique à l'intérieur d'un domaine d'application.
- Une appellation globale est une appellation unique à l'intérieur de l'environnement OSI. Elle comprend deux parties : un nom de domaine et une appellation locale.
- Une adresse N est un identificateur indiquant où se trouve un point d'accès à des services N.

Un suffixe N est un élément d'adresse N unique dans le contexte d'un point d'accès à des services N. Pour que le système d'adressage fonctionne correctement, il faut que chaque utilisateur et chaque application puissent connaître de façon naturelle l'identité des objets à joindre. À cet effet, les entités de niveau réseau et de niveau application

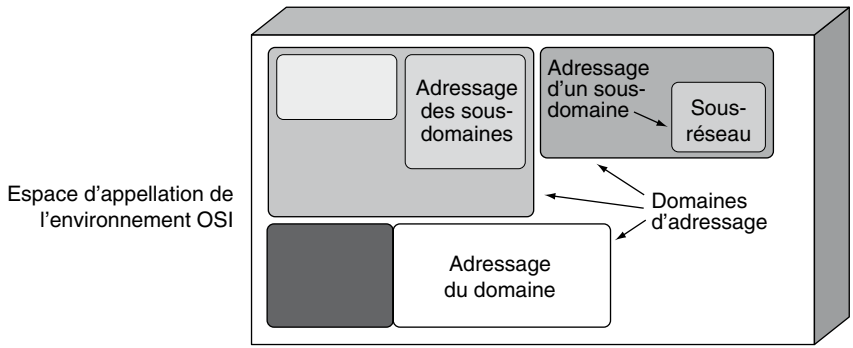
peuvent posséder un ou plusieurs nom (appelé titre par les organismes de normalisation). Des correspondances permettent de passer du nom d'une entité au point d'accès qui y mène. Pour obtenir une adresse de niveau N, il faut ajouter un sélecteur ou un suffixe à l'adresse du (N – 1)-SAP sous-jacent (*voir l'annexe B*).

Pour arriver à une concordance de tous ces principes, l'ISO a identifié les besoins suivants :

- définir de manière non ambiguë un ensemble de types pour les objets utilisés dans le contexte de l'OSI ;
- assigner des noms aux occurrences d'objets appartenant à ces types ;
- informer les autres participants des enregistrements effectués.

Pour chacun de ces types, une autorité d'enregistrement, internationale ou nationale, est nécessaire afin de déterminer les noms des objets appartenant au monde OSI. Les autorités d'enregistrement de plus haut niveau sont les organismes de normalisation. La figure F.1 illustre la situation globale des domaines d'adressage.

Figure F.1
Domaines d'adressage



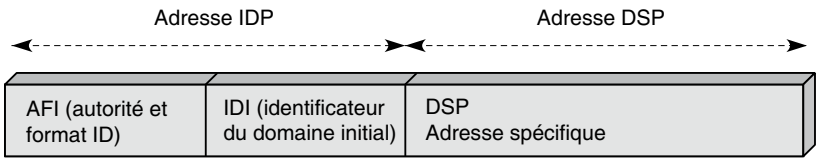
Structure des adresses ISO

La structure des adresses réseau est normalisée dans le document ISO 8348 (additif n° 2). Deux champs sont nécessaires :

- le domaine initial, ou IDP (Initial Domain Part) ;
- l'adresse spécifique, ou DSP (Domain Specific Part).

Cette structure est illustrée à la figure F.2.

Figure F.2
Format des adresses ISO



Le champ IDP est lui-même divisé en deux parties :

- Le champ AFI, qui indique l'autorité et le format utilisé.
- Le champ IDI d'identification du domaine initial. Plusieurs codes sont prédéfinis pour ce champ :

  36 ou 52 indique une adresse d'ETTD selon la norme X.121 (voir plus loin dans ce chapitre), codée en décimal. L'adresse est globale ou locale suivant le suffixe (36 : globale, 52 : locale).

  37 ou 53 indique une adresse d'ETTD selon la norme X.121, codée en binaire.

  38 indique une adresse d'ETCD selon la norme X.121, codée en décimal.

  39 indique une adresse d'ETCD selon la norme X.121, codée en binaire.

  40 ou 54 indique une adresse télex en décimal.

  41 ou 55 indique une adresse télex en binaire.

  42 ou 56 indique une adresse téléphonique en décimal.

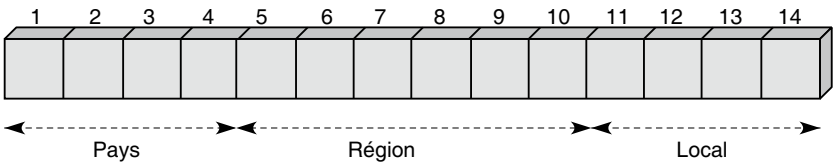
  43 ou 57 indique adresse téléphonique en binaire.

  44 ou 58 indique une adresse RNIS en décimal.

  45 ou 59 indique une adresse RNIS en binaire.

Le sous-adressage utilisé pour les réseaux de données longue distance est normalisé par le document X.121. Ce texte permet de déterminer les valeurs des champs IDP et DSP. La structure de cette adresse est illustrée à la figure F.3. Cette adresse tient sur 14 demi-octets, que nous avons numérotés de 1 à 14 ; deux demi-octets supplémentaires peuvent servir à des extensions. Sur un demi-octet, on peut représenter un chiffre décimal. L'adressage s'effectue dans ce cas sur 14 chiffres décimaux. Il est évident que ce choix est plus pénalisant que si la valeur avait été codée en binaire, prenant ainsi moins de place.

Figure F.3
Structure de l'adressage X.121



Les trois premiers demi-octets contiennent le code d'un pays. Au quatrième demi-octet correspond un numéro de réseau à l'intérieur du pays. Comme les grands pays ont plus de dix réseaux internes, plusieurs numéros sont donnés pour un même pays :

- 310 à 329 pour les États-Unis ;
- 302 à 307 pour le Canada ;
- 234 à 238 pour la Grande-Bretagne ;
- 208 à 212 pour la France.

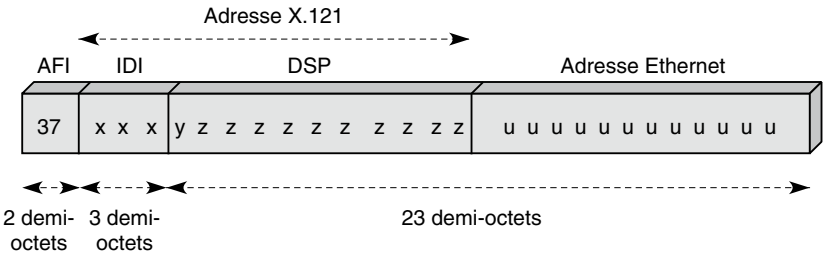
Pour les États-Unis, comme 20 numéros ont été spécifiés, il peut y avoir jusqu'à 200 sous-réseaux directement adressables.

Les demi-octets restants sont affectés à l'adresse dans le pays. Ils peuvent être découpés en deux tranches de 7 et 3 demi-octets, les sept premiers indiquant l'adresse du commutateur auquel le client est rattaché et les trois derniers l'adresse locale.

La figure F.4 illustre l'exemple d'un terminal OSI connecté à un réseau local de type Ethernet que l'on atteint *via* une passerelle connectée à un réseau X.25. L'adresse de ce terminal comporte le champ AFI, le champ X.121 et l'adresse Ethernet.

Figure F.4

Adresse d'un terminal OSI se comportant en ETTD distant



Le protocole X.25

Adopté en septembre 1976 par le CCITT, le protocole X.25, ou ISO 8208, résulte de l'expérience accumulée sur différents réseaux à commutation de paquets. Proposé au départ par quatre grands organismes, les PTT françaises, leur homologue britannique, TCTS (Trans Canada Telephone System) au Canada et Telenet Communication Corps aux États-Unis, il a été implémenté, entre autres, sur les réseaux publics de ces quatre compagnies sous la forme de Transpac, EPSS, Datapac et Telenet.

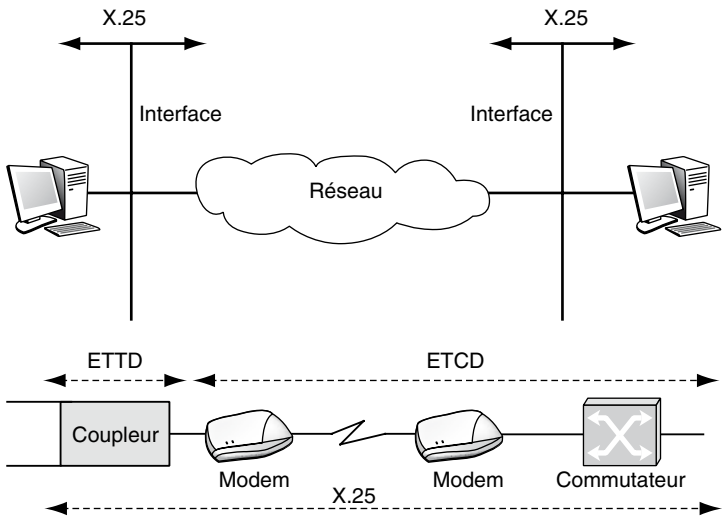
Les sections qui suivent décrivent en détail les fonctionnalités, la structure et le fonctionnement du protocole X.25.

Caractéristiques de X.25

Le protocole X.25 en lui-même contient les trois premières couches de protocole. Le niveau physique provient principalement de la norme X.21. Le niveau trame est constitué par le protocole LAP-B, un sous-ensemble de la norme HDLC, présentée au chapitre 7. Ici, c'est le niveau paquet de la norme X.25 qui nous intéresse.

La recommandation X.25 précise un protocole définissant l'interface entre un ETTD et un ETCD pour la transmission de paquets. X.25 est donc en premier lieu une interface locale entre un équipement informatique connecté au réseau et le réseau lui-même (*voir figure F.5*).

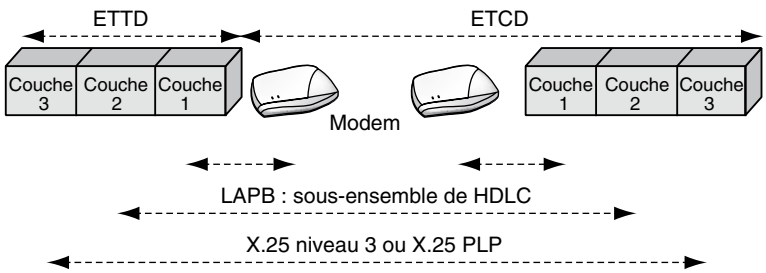
Figure F.5
Implémentation du protocole X.25



La définition de X.25 a été étendue pour prendre en compte des transmissions sur les interfaces soit d'entrée du réseau, entre la machine de l'utilisateur (ETTD) et l'équipement d'accès de l'opérateur (ETCD), soit de la machine de l'utilisateur à la machine distante (ETTD à ETTD).

Les trois premières couches du modèle de référence de l'architecture des réseaux informatiques sont prises en compte par X.25 (*voir figure F.6*).

Figure F.6
Niveaux et couches du protocole X.25

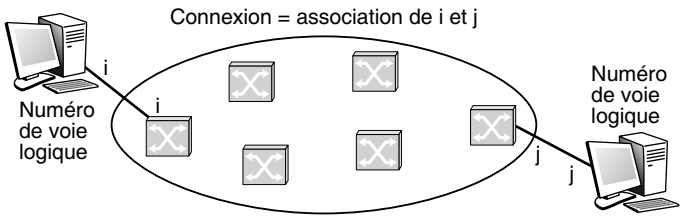


La recommandation X.25 du CCITT définit les types de paquets et leur format mais ne spécifie pas comment certaines informations de contrôle doivent être interprétées. En particulier, la fenêtre de contrôle de flux peut être interprétée au niveau local entre l'ETTD et l'ETCD ou au niveau global entre l'ETTD émetteur et l'ETTD récepteur. Ces imprécisions donnent naissance à des réseaux très différents les uns des autres.

X.25 utilise le mode avec connexion. La connexion est une association bidirectionnelle entre l'émetteur et le récepteur. En plus de cette connexion, l'ensemble des réseaux X.25 utilise un mode circuit virtuel, sans que ce soit une obligation de la norme. De ce fait, X.25 multiplexe sur la couche 2 les circuits virtuels passant par la même liaison. La

connexion entre deux adresses extrémité s'exprime par une correspondance entre deux références, appelées voies logiques, comme illustré à la figure F.7.

Figure F.7
Connexion X.25



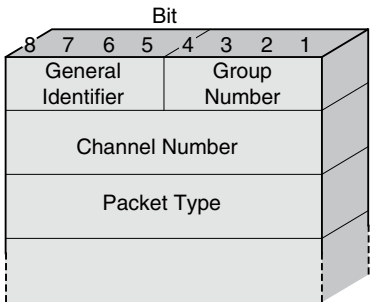
Le niveau paquet de X.25 permet un maximum de 16 groupes de 256 voies logiques entre un ETTD et un ETCD. L'en-tête du paquet contient un champ de 4 bits qui identifie le groupe et un champ de 8 bits pour le numéro de la voie logique. 4 095 voies logiques — la voie 0 joue un rôle particulier — sont donc utilisables sur une entrée. L'ETTD et l'ETCD partagent le même numéro de voie logique lors de la formation de la connexion.

On profite de la mise en place de la connexion pour réaliser un circuit virtuel, qui s'établit lors du routage du paquet d'appel. Ce circuit virtuel est emprunté par l'ensemble des paquets d'un même message. Le numéro de voie logique joue également le rôle d'une référence. L'ouverture du circuit virtuel peut s'accompagner d'allocations de ressources pour assurer le contrôle de flux et garantir le séquencement des paquets dans le réseau.

Format des paquets X.25

Le format général des paquets X.25 se présente sous la forme illustrée à la figure F.8.

Figure F.8
Format des paquets X.25



La zone identificateur de type de paquet (Packet Type) permet de déterminer la fonction du paquet. Elle ressemble à la zone de supervision de HDLC pour le contrôle de la connexion réseau. Le tableau F.1 répertorie les différents types de paquets rencontrés dans le protocole X.25.

Tableau F.1 • Types de paquets d'un environnement X.25

Type de paquet	Zone identificateur du type de paquet							
	8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
Paquet d'appel/Appel entrant *CALL REQUEST/INCOMING CALL*	0	0	0	0	1	0	1	1
Communication acceptée/Communication établie *CALL ACCEPTED/CALL CONNECTED*	0	0	0	0	1	1	1	1
Demande de libération/Indication de libération *CLEAR REQUEST/CLEAR INDICATION*	0	0	0	1	0	0	1	1
Confirmation de libération *CLEAR CONFIRMATION*	0	0	0	1	0	1	1	1
Paquet de données *DATA PACKET*	X	X	X	X	X	X	X	1
Demande d'interruption *INTERRUPT REQUEST*	0	0	1	0	0	0	1	1
Confirmation d'interruption *INTERRUPT CONFIRMATION*	0	0	1	0	0	1	1	1
Paquet RR *RECEIVE READY*	X	X	X	0	0	0	0	1
Paquet RNR *RECEIVE NOT READY*	X	X	X	0	0	1	0	1
Paquet REJ *REJECT*	X	X	X	0	1	0	0	1
Demande de réinitialisation/Indication de réinitialisation *RESET REQUEST/RESET INDICATION*	0	0	0	1	1	0	1	1
Confirmation de réinitialisation *RESET CONFIRMATION*	0	0	0	1	1	1	1	1
Demande de reprise/Indication de reprise *RESTART REQUEST/RESTART INDICATION*	1	1	1	1	1	1	0	1
Confirmation de reprise *RESTART CONFIRMATION*	1	1	1	1	1	1	1	1
Les bits X indiquent des informations de contrôle contenues dans le champ identificateur.								

Des paquets de diagnostic et d'enregistrement complètent cette panoplie de paquets.

La connexion X.25

La connexion entre deux utilisateurs et le circuit virtuel mis en place pour acheminer les paquets sur cette connexion permettent la circulation des données de contrôle et les

informations utilisateur. La figure F.9 illustre les différentes phases de la vie d'un circuit virtuel, que nous explicitons dans les sections suivantes.

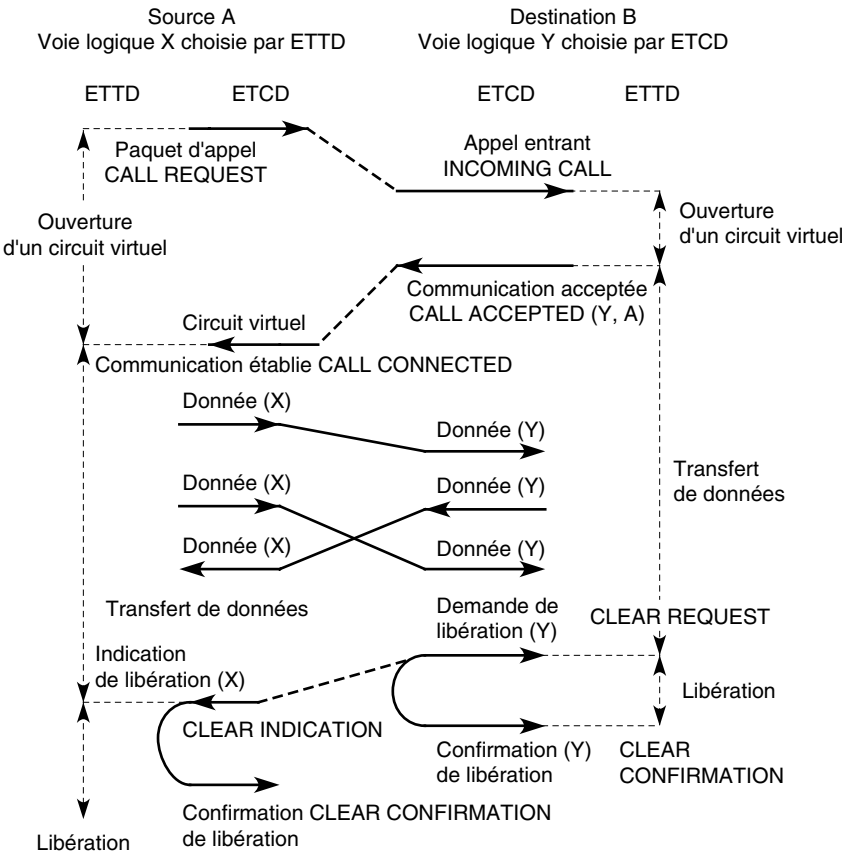


Figure F.9

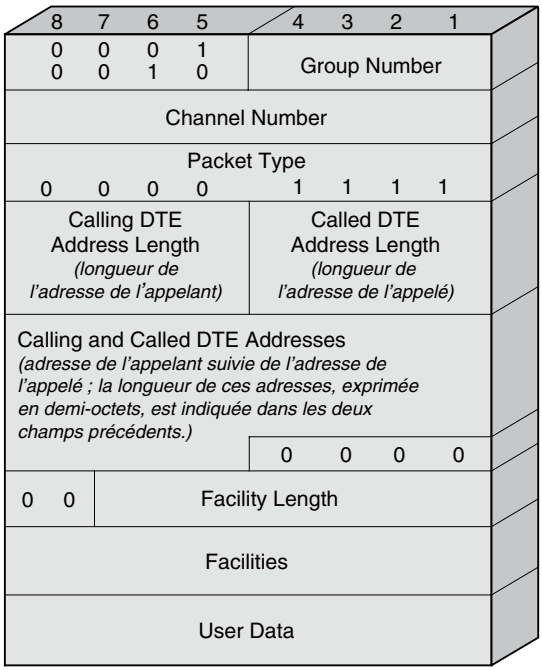
Phases de la vie d'un circuit virtuel

Ouverture et fermeture d'une connexion

Un utilisateur qui veut transmettre des paquets doit au préalable ouvrir une connexion et, en règle générale, un circuit virtuel. Pour ce faire, il émet une demande d'ouverture (CALL REQUEST). Le paquet contient le numéro de la voie logique obtenu par l'utilisateur (le plus grand disponible) et l'adresse réseau des abonnés (demandé et demandeur). Cette dernière est inscrite dans un champ dont la longueur, variable, est spécifiée par un champ de quatre bits en nombre de demi-octets (*voir figure F.10*). La recommandation X.121 normalise l'adresse sur 14 demi-octets. Comme le champ est de 4 bits, il permet d'obtenir une longueur de 16 demi-octets.

Figure F.10

Paquet d'appel (CALL REQUEST) et appel entrant (INCOMING CALL)



Le paquet contient un premier champ indiquant les options de contrôle du circuit virtuel et un second, de 64 octets au maximum, destiné à l'utilisateur. Ce dernier peut utiliser ce champ pour préciser, entre autres, des adresses complémentaires, si l'adresse du récepteur est un réseau local ou un autocommutateur privé, et des mots de passe.

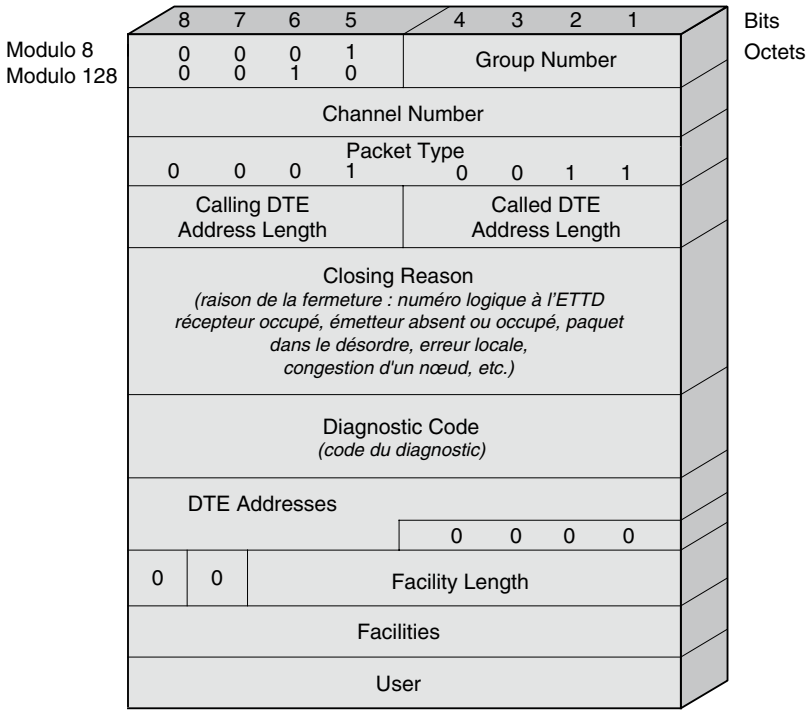
Lorsqu'il arrive à l'ETCD destinataire, le paquet d'appel capte le plus petit numéro de voie logique pour éviter la collision avec une demande d'ouverture de circuit virtuel qui pourrait arriver sur l'ETCD après avoir réservé le même numéro de voie logique sur l'ETTD, la demande entrante étant alors prioritaire. Si le récepteur accepte la communication, il retourne un paquet communication acceptée (CALL ACCEPTED). Sinon, il envoie une demande de libération (CLEAR REQUEST).

L'émetteur ou le récepteur peut mettre fin au circuit virtuel en envoyant une demande de fermeture (DTE INTERRUPT et DCE INTERRUPT), qui est acquittée au niveau local.

Le paquet de libération (DTE INTERRUPT CONFIRMATION et DCE INTERRUPT CONFIRMATION) peut contenir la raison de la demande : numéro logique à l'ETTD récepteur occupé, émetteur absent ou occupé, paquet dans le désordre, erreur locale, congestion d'un nœud, etc. Le format des trames de demande de libération et d'indication de libération est illustré à la figure F.11.

Figure F.11

Format des trames de demande de libération et d'indication de libération

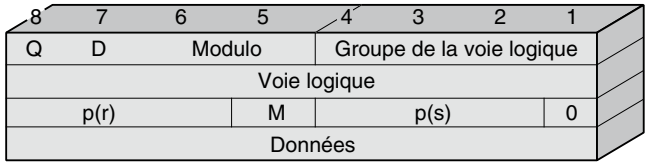


L'octet 5 indique le diagnostic et contient des informations supplémentaires. Les 256 possibilités sont utilisées et sont explicitées dans la norme CCITT ou ISO.

La figure F.12 illustre le format des paquets de données.

Figure F.12

Format des paquets de données



La phase de transfert

Une fois la phase d'ouverture effectuée, le circuit virtuel passe à la phase de transfert des paquets de l'utilisateur. Cette phase se termine par une demande de fermeture, qui démarre la phase de fermeture du circuit virtuel et de la connexion.

Les paquets de données sont transférés sur un circuit virtuel permanent ou commuté. Les numéros p(s) et p(r) servent pour le contrôle de flux. Comme nous l'indiquerons par la suite, il n'est pas précisé dans la norme à quoi s'appliquent les fenêtres : voie logique ou circuit virtuel. La valeur p(s) précise le numéro du paquet envoyé, tandis que p(r) indique le numéro du prochain paquet attendu par le récepteur. Ce dernier autorise l'émetteur à

envoyer plusieurs autres paquets selon l'ouverture de la fenêtre. Bien sûr, l'émetteur et le récepteur gardent en mémoire des numéros v(s) et v(r) analogues à ceux de HDLC.

Le bit Q indique que le paquet transporte des données qualifiées (Qualified Data). L'avis X.25 ne spécifie pas la nature des données qualifiées, mais l'intention sous-jacente est de distinguer les données de l'utilisateur des données de contrôle provenant de la couche supérieure. Si Q = 1, la zone de données transporte des messages de contrôle de la couche 4. C'est une signalisation dans la bande. Ce bit est notamment utilisé pour contrôler les PAD (Packet Assembler Disassembler), qui permettent la connexion de terminaux asynchrones sur un réseau X.25.

Le bit D précise la portée des acquittements. Si D = 0, le contrôle de flux s'effectue localement, et le champ p(r) est positionné par l'ETCD local. Si D = 1, le contrôle de flux est de bout en bout, et p(r) provient de l'ETTD récepteur. Le standard X.25 originel n'autorisait que la valeur D = 0. Plusieurs réseaux internationaux qui ont adopté la norme X.25 ne permettent pas au bit D d'être égal à 1.

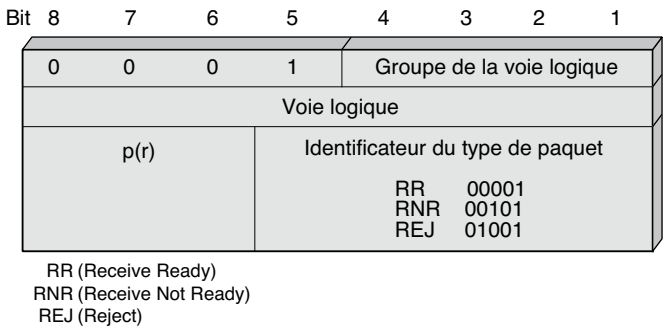
Dans l'identificateur général, les deux bits modulo indiquent le modulo de la séquence des numéros de paquet. Si c'est la suite 01, la numérotation est effectuée modulo 8 ; si la suite 10 est affichée, le modulo est en mode étendu porté à 128. Dans ce dernier cas, le champ de supervision est étendu à deux octets. Le bit M indique, s'il est à 1, que la NPDU fait partie d'une NSDU qui a été fragmentée et qu'il faut regrouper ces données avec celles du paquet précédent. Un 0 indique qu'il s'agit du dernier fragment du message.

La fenêtre qui gère l'avancement des compteurs p(r) et p(s) sert au contrôle de flux, le contrôle des erreurs étant assuré au niveau 2. Cette fenêtre limite le nombre de paquets circulant entre ses deux extrémités. Malheureusement, les extrémités de la fenêtre ne sont pas définies dans la norme, et deux interprétations très différentes régissent les implémentations de X.25. La compréhension de cette fenêtre peut être de bout en bout, c'est-à-dire de l'ETTD émetteur jusqu'à l'ETTD récepteur. Généralement, elle est interprétée comme locale entre l'ETTD et l'ETCD. Le contrôle de flux s'effectue dans ce dernier cas sur la voie logique et non plus sur le circuit virtuel. Les deux extrémités d'un circuit virtuel peuvent être gérées par des fenêtres distinctes, avec des longueurs de paquet différentes.

Les paquets utilisés par le contrôle de flux sont comparables à ceux de HDLC. Il s'agit des paquets RR, RNR et REJ, dont les formats sont illustrés à la figure F.13.

Figure F.13

Format des paquets de contrôle



Le paquet RR (Receive Ready) sert d'accusé de réception lorsque le récepteur n'a rien à transmettre. Il acquitte tous les paquets dont les numéros précèdent p(r). Le paquet RNR (Receive Not Ready) indique que le nœud qui l'envoie ne peut, pour des raisons diverses, recevoir de nouveaux paquets. Ce paquet RNR acquitte tous les paquets précédant celui numéroté p(r). Le récepteur détruit automatiquement tous les paquets qui lui parviennent. L'émetteur attend de recevoir un paquet RR doté du numéro p(r), indiquant que le prochain paquet attendu par le récepteur est celui numéroté p(r), pour reprendre sa transmission. C'est un contrôle de flux de ce type qui est utilisé dans le relais de trames.

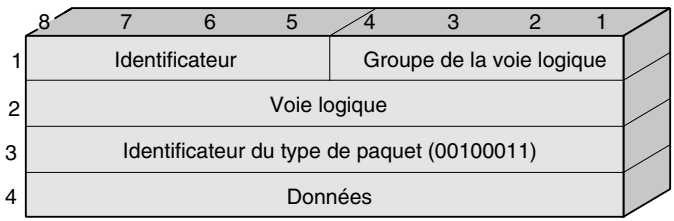
Seul l'ETCD utilise le paquet REJ pour demander, à la suite d'un problème, la retransmission de tous les paquets à partir du numéro p(r). En effet, le paquet ne contient pas de bloc de contrôle d'erreur, et l'ETCD ne peut détecter les erreurs qui auraient été laissées par la couche inférieure. Ce sont les erreurs sur les déséquencements ou les pertes de paquets qui sont prises en compte à ce niveau.

La longueur des paquets est spécifiée au moment de la demande d'ouverture du circuit virtuel. Le maximum recommandé par la norme est de 128 octets, mais les valeurs 16, 32, 256, 512, 1 024 ou même 255 octets sont permises. La longueur peut correspondre à un nombre quelconque d'octet, même non entier, si le tout est inférieur à la longueur maximale. Si la fenêtre de contrôle est locale, le nombre maximal d'octet d'un paquet peut être différent à chacun des bouts. À l'intérieur du réseau lui-même, les paquets peuvent être fragmentés ou réassemblés.

Les paquets de demande d'interruption

Les paquets de demande d'interruption ne sont pas soumis au contrôle de flux et n'ont donc pas de numéro p(s). Ils peuvent être envoyés lorsque la fenêtre de contrôle est atteinte. Ce sont en quelque sorte des paquets prioritaires pouvant transporter un octet de données. La figure F.14 illustre le format de ces paquets.

Figure F.14
Format des paquets d'interruption



Les demandes d'interruption sont acquittées par des paquets de confirmation d'interruption. Une seule demande peut circuler sur la voie logique. Les paquets de confirmation d'interruption comportent seulement 3 octets, et l'identificateur du type de paquet (troisième octet) est 00100111.

Les paquets de réinitialisation et de reprise

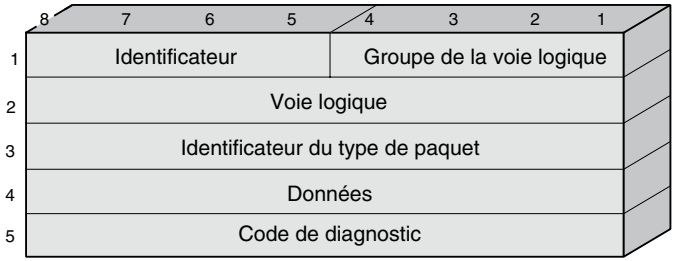
La procédure de réinitialisation permet de remettre le circuit virtuel dans un état connu, et ce dans les deux directions à la fois, c'est-à-dire de l'émetteur vers le récepteur et du

récepteur vers l'émetteur. En outre, elle détruit les paquets et les demandes d'interruption qui pourraient se trouver dans le circuit. Les compteurs p(s) et p(r) sont remis à 0. Une réinitialisation peut être demandée par chacun des deux bouts, généralement suite à une erreur de séquence ou suite à une erreur indiquée par la couche inférieure. Les réinitialisations sont acquittées au niveau local.

La reprise est une réinitialisation de tous les circuits virtuels en parallèle. Le format de ces paquets est illustré à la figure F.15.

Figure F.15

Format des paquets de réinitialisation et de reprise



Annexe G

8 : Le niveau message

Cette annexe détaille de façon plus formelle le niveau message de l'architecture OSI. Elle présente ensuite le standard OSI pour la couche 4, qui n'est plus utilisé, mais qui reste une bonne approche pour comprendre ce que l'on peut attendre d'une couche message. Enfin, nous présentons brièvement l'équivalent de la couche message dans le monde des réseaux ATM.

Le niveau message

L'architecture OSI n'est plus utilisée aujourd'hui, mais l'étude de son niveau message est intéressante à plus d'un titre. Elle donne un exemple de ce que pourrait être un niveau message bien étudié et explicite les fonctionnalités qu'il faut faire entrer dans toute couche complète de niveau 4.

Le protocole de transport doit pouvoir s'adapter à la demande de service de l'utilisateur et à la qualité de service fournie par les trois premières couches de l'architecture. Pour bien comprendre ces caractéristiques, les normalisateurs ont classé les services réseau en trois grandes catégories :

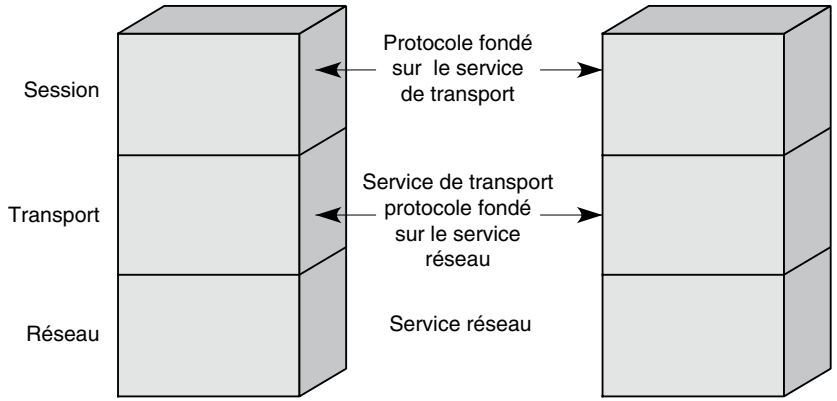
- Le type A représente un service de réseau qui possède un taux acceptable d'erreur résiduelle et un taux acceptable d'incident signalé par la couche réseau. L'exemple classique souvent proposé est celui d'une architecture utilisant le protocole LAP-B, qui garantit généralement que le taux d'erreur résiduelle est bas et acceptable, et le protocole X.25 au niveau réseau, qui assure un taux tolérable d'incident signalé. Cette architecture peut ne pas être classée dans le type A si l'utilisateur demande un service réseau d'une qualité supérieure.

- Le type B est déterminé par un taux acceptable d'erreur résiduelle, mais un taux inacceptable d'incident signalé. Dans cette catégorie, on peut placer un réseau qui posséderait un protocole de niveau trame avec une reprise sur correction d'erreur et un protocole de niveau paquet simplifié, comme IP. Cette architecture peut également se trouver dans une autre catégorie, suivant le service demandé par l'utilisateur.
- Le type C représente les réseaux qui ont un taux d'erreur résiduelle inacceptable. Un réseau qui possède un protocole de niveau trame sans reprise sur erreur dans un réseau de mauvaise qualité surmonté par un niveau paquet sans possibilité de reprise, comme le protocole IP, peut être classé dans cette catégorie.

Suivant le type du service réseau et la qualité que l'utilisateur souhaite pour le service de transfert, on détermine le protocole de transport à choisir. Le protocole de transport normalisé par l'ISO et l'UIT-T contient cinq classes, numérotées de 0 à 4, qui permettent de s'adapter aux demandes de l'utilisateur.

La relation classique que l'on observe entre la couche transport et les couches situées au-dessus et en dessous est illustrée à la figure G.1.

Figure G.1
Relations entre les couches dans le modèle OSI



La couche transport doit assurer un transfert transparent des données entre utilisateurs du service de transport. Les principales fonctionnalités de ce service sont les suivantes :

- choix d'une qualité de service ;
- indépendance par rapport aux ressources fournies par les trois couches inférieures ;
- contrôle de bout en bout de la communication ;
- adressage du service de transport.

Le protocole AAL

AAL (ATM Adaptation Layer) est un troisième exemple de protocole de niveau message. Il s'agit de la couche d'adaptation à l'ATM, qui se charge de l'interface avec les couches supérieures. Cet étage est lui-même subdivisé en deux niveaux, l'un prenant en

compte les problèmes liés directement à l'interfonctionnement avec la couche supérieure et l'autre ceux concernant la fragmentation et le réassemblage des messages en cellules.

Le rôle de cette couche est de transporter de bout en bout des messages dont le format est spécifié, leur taille maximale ne pouvant dépasser 64 Ko, comme dans Internet. Ce bloc doit être découpé en petits fragments de 48 octets pour entrer dans la cellule ATM. Ce découpage peut en fait descendre en dessous de 48 octets, par exemple 47 voire 44 octets, pour récupérer des octets de supervision dans la partie donnée.

Dans la couche AAL, quatre classes de services, 1, 2, 3 et 4, ont été définies, auxquelles correspondent quatre classes de protocoles. Cette subdivision a été modifiée en 1993 par le regroupement des classes 3 et 4 et par l'ajout d'une nouvelle classe de protocoles, la classe 5, qui définit un transport de données simplifié. Enfin, en 2000, la classe 2 a été transformée, ce qui a conduit à la définition de trois classes, 1, 2 et 5 :

- **Classe 1.** Correspond à une émulation de circuit, c'est-à-dire à la mise en place d'un circuit virtuel susceptible de transporter ce qui proviendrait d'un circuit et de redonner en sortie le même circuit. On se sert de cette classe pour transporter la parole téléphonique non compressée. Les opérateurs télécoms classiques ont des protocoles de ce type pour desservir toutes les demandes de circuit.
- **Classe 2.** Correspond au transport d'une information qui serait de type circuit au départ mais que l'on aurait compressée de telle sorte que le débit devienne variable. Cette classe transporte des applications comportant des contraintes de synchronisation, comme la classe A, mais avec un débit variable. On y trouve toutes les applications de parole téléphonique et de vidéo compressée. L'UMTS, en particulier, a choisi cette solution pour le transport de ses voies de parole.
- **Classe 5.** Permet de faire tout transiter sans ajouter de fonction supplémentaire, sauf éventuellement un contrôle d'erreur.

Le niveau message de l'architecture OSI

L'architecture OSI n'est plus utilisée aujourd'hui, mais l'étude de son niveau message est intéressante à plus d'un titre. Elle donne un exemple de ce que pourrait être un niveau message bien conçu et explicite les fonctionnalités qu'il faut faire entrer dans toute couche complète de niveau 4.

Le protocole de transport doit pouvoir s'adapter à la demande de service de l'utilisateur et à la qualité de service fournie par les trois premières couches de l'architecture. Pour bien comprendre ces caractéristiques, les normalisateurs ont classé les services réseau en trois grandes catégories :

- Le type A représente un service de réseau qui possède un taux acceptable d'erreur résiduelle et d'incident signalé par la couche réseau. L'exemple classique souvent proposé est celui d'une architecture utilisant le protocole LAP-B, qui garantit généralement que le taux d'erreur résiduelle est bas et acceptable, et le protocole X.25 au niveau réseau, qui assure un taux également tolérable d'incident signalé. Cette architecture

peut ne pas être classée dans le type A si l'utilisateur demande un service réseau d'une qualité supérieure.

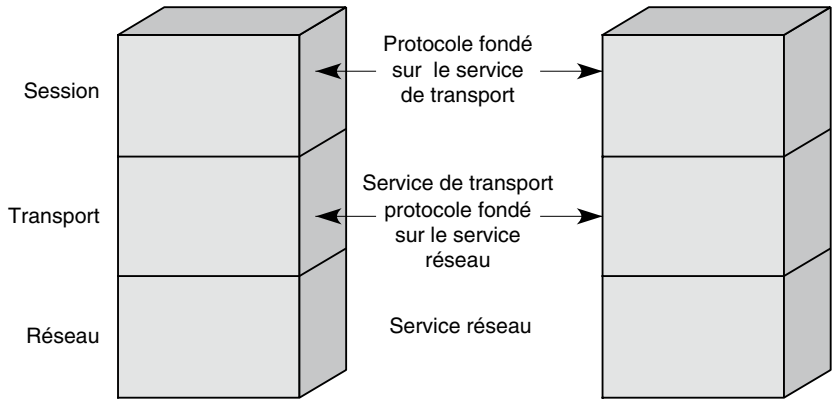
- Le type B est déterminé par un taux acceptable d'erreur résiduelle, mais un taux inacceptable d'incident signalé. Dans cette catégorie, on peut placer un réseau qui posséderait un protocole de niveau trame avec une reprise sur correction d'erreur et un protocole de niveau paquet simplifié, comme IP. Cette architecture peut également se trouver dans une autre catégorie, suivant le service demandé par l'utilisateur.
- Le type C représente les réseaux qui ont un taux d'erreur résiduelle inacceptable. Un réseau qui possède un protocole de niveau trame sans reprise sur erreur dans un réseau de mauvaise qualité surmonté par un niveau paquet sans possibilité de reprise, comme le protocole IP, peut être classé dans cette catégorie.

Suivant le type du service réseau et la qualité que l'utilisateur souhaite pour le service de transfert, on détermine le protocole de transport à choisir. Le protocole de transport normalisé par l'ISO et l'UIT-T contient cinq classes, numérotées de 0 à 4, qui permettent de s'adapter aux demandes de l'utilisateur.

La relation classique que l'on observe entre la couche transport et les couches situées au-dessus et en dessous est illustrée à la figure G.2.

Figure G.2

Relations entre les couches dans le modèle OSI



La couche transport doit assurer un transfert transparent des données entre utilisateurs du service de transport. Les principales fonctionnalités de ce service sont les suivantes :

- choix d'une qualité de service ;
- indépendance par rapport aux ressources fournies par les trois couches inférieures ;
- contrôle de bout en bout de la communication ;
- adressage du service de transport ;
- possibilité de mettre en place une connexion de transport capable de prendre en charge des TSDU et des TSDU expresses.

La connexion de transport est mise en œuvre classiquement par les primitives DEMANDE DE CONNEXION DE TRANSPORT et RÉPONSE À UNE DEMANDE DE CONNEXION DE TRANSPORT, l'émission des octets de données et enfin les indications de fin de TSDU.

La qualité de service est une des exigences du service de transport. Cette qualité de service, ou QoS, est négociée entre les utilisateurs et le fournisseur du service de transport. Cette négociation s'effectue par l'intermédiaire des primitives DEMANDE, INDICATION, RÉPONSE À UNE DEMANDE et CONFIRMATION DE CONNEXION DE TRANSPORT.

Les paramètres de qualité de service que l'on peut négocier sont les suivants :

- délai d'échec d'établissement d'une connexion de transport ;
- probabilité d'échec d'établissement d'une connexion de transport ;
- débit sur la connexion ;
- temps de transit ;
- taux d'erreur résiduelle ;
- probabilité de rupture de la connexion ;
- probabilité d'incident de transfert ;
- délai de libération de connexion ;
- probabilité d'échec d'une libération de connexion.

Nous allons détailler les trois paramètres les plus importants, à savoir le débit, le temps de transit et le taux d'erreur résiduelle.

Le débit moyen représente la cadence de transfert durant la vie de la connexion. Le débit maximal correspond à la cadence maximale à laquelle la connexion de transport peut prendre en charge les TSDU. La valeur du paramètre débit peut être définie à partir d'une séquence d'au moins deux TSDU arrivées correctement à destination. C'est le nombre d'octet de données utilisateur qui a pu être transféré divisé par le temps qui s'est écoulé entre la première et la dernière DEMANDE DE TRANSFERT DE DONNÉES DE TRANSPORT correspondant aux octets de données. Pour l'autre sens de la connexion, on considère le nombre d'octet de données entre la première et la dernière INDICATION DE TRANSFERT DE DONNÉES DE TRANSPORT. Si l'on se place sur un temps relativement court, correspondant à l'envoi de deux TSDU, on obtient un débit instantané qui peut s'approcher du débit maximal. Au contraire, sur une longue séquence de TSDU, on obtient le débit moyen.

Le temps de transit est le temps qui s'écoule entre une DEMANDE DE TRANSFERT DE DONNÉES DE TRANSPORT et L'INDICATION DE TRANSFERT DE DONNÉES DE TRANSPORT correspondante. Ce temps n'est valable que pour les TSDU dont le transfert s'est effectué correctement. Cette valeur varie énormément suivant les politiques de contrôle de flux et d'acquittement utilisées dans les différents niveaux de protocoles qui doivent être traversés.

Pour obtenir le taux d'erreur résiduelle, il faut calculer le rapport du nombre total de TSDU correctement remises à la couche supérieure sur le nombre total de TSDU transférées puis retrancher ce rapport de 1. Les erreurs peuvent provenir de TSDU perdues,

incorrectes ou en surnombre. À partir de cette valeur, on peut déduire la qualité du service rendu. Cette valeur intéresse davantage le fournisseur de services que l'utilisateur. En effet, le taux d'erreur résiduelle classiquement défini est assez différent, puisque c'est le nombre de bit erroné reçu par le destinataire sans qu'il s'en aperçoive. Cette dernière valeur donne à l'utilisateur une idée du nombre d'erreur qui n'a pu être détectée et qui peut perturber le déroulement correct de l'application.

Les unités de données (TPDU) du protocole de transport

- CR (Connection Request) : TPDU de demande de connexion ;
- CC (Connection Confirm) : TPDU de confirmation de connexion ;
- DR (Disconnect Request) : TPDU de demande de déconnexion ;
- DC (Disconnect Confirm) : TPDU de confirmation de déconnexion ;
- DT (Data) : TPDU de données ;
- ED (Expedited Data) : TPDU de données expresses ;
- AK (Data Acknowledge) : TPDU d'accusé de réception de données ;
- EA (Expedited Acknowledge) : TPDU d'accusé de réception de données expresses ;
- RJ (Reject) : TPDU de rejet ;
- ER (Error) : TPDU d'erreur.

Le service de transport en mode avec connexion (ISO 8073 ou X.224)

La norme X.224 du CCITT normalise le service qui doit être rendu par le niveau message. Elle définit les cinq classes de protocoles suivantes, qui s'adaptent aux services rendus par les trois couches inférieures et à la qualité de service éventuellement demandée par l'utilisateur :

- **Classe 0.** Représente le minimum nécessaire à la réalisation d'un service de transport. C'est la classe de base.
- **Classe 1.** Classe de base, à laquelle on a ajouté une reprise sur erreur au cas où celle-ci serait signalée par la couche 3.
- **Classe 2.** Classe de base, à laquelle on a ajouté une possibilité de multiplexage et de contrôle de flux.
- **Classe 3.** Offre les possibilités des classes 1 et 2.
- **Classe 4.** Permet, outre les possibilités précédentes, de détecter les erreurs et d'effectuer les reprises nécessaires pour les corriger.

À ces différentes classes, il faut ajouter les options négociées lors de l'établissement de la connexion.

La classe 0

La classe 0 doit pouvoir, avec un minimum de fonctionnalités, se placer au-dessus du service réseau. C'est la classe de base, qui assure la mise en place des connexions de transport. La connexion de transport correspond, dans ce cas, à la connexion réseau. L'établissement s'effectue grâce à la TPDU CR (Connection Request) et à la TPDU CC (Connection Confirm).

Les TPDU comportent trois paramètres : l'adresse (ID) du point d'accès au service de transport, ou TSAP (Transport Service Access Point), de l'entité appelante, l'adresse (ID) du TSAP de l'entité appelée et la taille de la TPDU proposée. Il n'est pas possible d'avoir quelques octets de données utilisateur. Les données utilisateur sont transportées dans la TPDU DT (Data) *via* la procédure de segmentation-réassemblage.

La libération de la connexion utilise en règle générale les TPDU DR (Disconnect Request) et les DC (Disconnect Confirm). Lorsqu'une extrémité reçoit une INDICATION DE DÉCONNEXION DE RÉSEAU ou une INDICATION DE RÉINITIALISATION DE RÉSEAU, la connexion de transport est automatiquement libérée. Pour les classes de protocoles de transport autres que 0 et 2, ces indications entraînent l'appel d'une procédure de reprise sur erreur. Le traitement des erreurs de protocole est effectué par la TPDU ER (Error), qui utilise les paramètres CAUSE DU REJET et TPDU NON VALIDE, ainsi que par la TPDU DR (Disconnected Request), qui porte le code de la cause de l'erreur.

Pour établir une connexion de transport, une entité de transport envoie une TPDU CR (Connection Request) à l'autre extrémité, qui répond par une TPDU CC (Connection Confirm). Toutes les informations et tous les paramètres nécessaires au fonctionnement des entités de transport doivent être échangés ou négociés au cours de l'échange des primitives d'ouverture. En particulier, chaque entité de transport choisit une référence sur 16 bits, qui permet d'identifier la connexion de transport. Lorsque la connexion est libérée, on peut geler la référence — pour un certain temps — afin que les TPDU qui n'offrent plus d'intérêt soient ignorées. Les références source et destination permettent de différencier les deux extrémités de la connexion.

Au cours de l'échange d'information, il est possible de recourir aux adresses indiquant les points d'accès au service de transport si les adresses réseau sont insuffisantes. Pour les classes de protocoles comportant un contrôle de flux, la valeur du crédit, c'est-à-dire le nombre de TPDU qui peut être envoyé sans acquittement, est indiquée explicitement. Ce n'est pas le cas dans la classe 0. La négociation de la classe de protocoles est également effectuée au cours de l'ouverture. L'émetteur propose une classe préférée et des classes de repli le cas échéant. La demande et la réponse doivent être compatibles avec les valeurs normalisées récapitulées au tableau G.1.

Par exemple, si la classe préférée est 4 et que la classe de repli soit 3, le récepteur peut choisir entre les classes 4, 3 et 2. Si l'émetteur ne précise aucune classe de repli, le récepteur a le choix entre les classes 4 et 2. Plusieurs classes de repli peuvent être proposées. Si la classe préférée est toujours 4 et que les classes de repli proposées soient 3 et 0, les classes possibles sont 0, 2 et 4, c'est-à-dire l'union des classes possibles correspondant aux classes de repli 0 et 3.

Tableau G.1 • Valeurs des classes de repli normalisées

Format du champ de contrôle	Élément binaire du champ de contrôle							
	1	2	3	4	5	6	7	8
Format I	0	N(S)			P	N(R)		
Format S	1	0	S	S	P/F	N(R)		
Format U	1	1	M	M	P/F	M	M	M

N(S)	numéro de séquence en émission (l'élément binaire 2 = élément binaire de poids faible).
N(R)	numéro de séquence en réception (l'élément binaire 6 = élément binaire de poids faible).
S	élément binaire de la fonction de supervision
M	élément binaire de la fonction de modification
P/F	élément binaire d'invitation à émettre lorsqu'il provient d'une commande ; élément binaire final lorsqu'il provient d'une réponse (1 = invitation à émettre/fin).
P	élément binaire d'invitation à émettre (1 = invitation à émettre)

La taille des TPDU se négocie au cours de la mise en place de la connexion. L'émetteur propose une taille maximale, et le récepteur peut accepter cette valeur ou demander une valeur comprise entre 128 octets et la taille maximale proposée. La taille maximale autorisée est de 8 192 octets, sauf en classe 0, où le maximum est de 2 048 octets. Mis à part la classe 0, pour laquelle seul le format normal est utilisé, de façon à permettre une numérotation de TPDU sur 7 bits, il est possible de choisir le format étendu, qui autorise une numérotation sur 31 bits.

Pour associer les TPDU aux connexions de transport, une procédure définie dans la norme permet d'utiliser des numéros de référence. Toutes les TPDU de toutes les classes de protocoles portent les numéros de référence source ou destination. Les paramètres RÉFÉRENCE DESTINATION et RÉFÉRENCE SOURCE sont utilisés pur cela. Ils identifient la connexion de transport au niveau de l'entité destinataire et de l'entité expéditrice. Pour la classe 0, une connexion de transport correspond à une connexion réseau, et les NSDU sont considérées comme constituant les TPDU, et *vice versa*. Dans les autres classes, des procédures de séparation et de concaténation peuvent être utilisées. Le paramètre RÉFÉRENCE DESTINATION sert à identifier la connexion de transport.

À partir de cet ensemble de fonctionnalités minimales, nous voyons que la classe 0 est apte à fonctionner sur un service réseau complet, puisqu'elle n'apporte aucune fonctionnalité supplémentaire. L'avantage d'une telle solution est son extrême simplicité, qui offre des performances optimales.

La classe 1

Outre les fonctionnalités de la classe de base, la classe 1 ajoute la possibilité de reprise sur erreur et un ensemble de procédures optimisant l'utilisation des ressources sous-jacentes. La connexion de transport s'effectue comme pour la classe 0.

Le transport de données utilise la segmentation et une numérotation des TPDU pour pouvoir effectuer un contrôle de flux ou une reprise sur une TPDU erronée. Dans la TPDU DT, on trouve un paramètre Numéro de TPDU. Cette numérotation s'effectue de

façon classique : on ajoute 1 au numéro de la TPDU précédente. Lorsqu'une TPDU est réexpédiée, elle doit avoir le même numéro que la première émise. Dans le cas du format normal, le champ de numérotation demande 7 bits, ce qui permet une numérotation modulo 2^7. Le format étendu requiert un champ de numérotation de 31 bits, ce qui permet une numérotation modulo 2^{31} (cette option n'existe pas dans la classe 0). Grâce à la numérotation, le réassemblage peut être facilement effectué.

La classe 1 permet d'émettre des données expresses. L'envoi d'une TPDU ED (Expedited Data) doit être confirmé par une TPDU d'accusé de réception de données expresses, la TPDU EA (Expedited Acknowledge), qui doit être unique sur la connexion. Les acquittements s'effectuent un à un. La possibilité d'utiliser des données expresses doit être négociée au cours de la mise en place de la connexion. Les libérations des connexions de transport s'effectuent de la même façon que pour la classe 0.

Outre les fonctionnalités décrites dans la classe 0, plusieurs fonctionnalités additionnelles sont disponibles dans la classe 1, notamment les suivantes :

- **Réaffectation après incident.** La réaffectation après incident permet une reprise à la suite d'une déconnexion signalée par le fournisseur du service réseau. Cette procédure s'applique lors d'une indication de déconnexion réseau. Deux temporisateurs sont utilisés :
  - TTR (Time to Try Resynchronization), ou temporisateur d'essai de réaffectation-resynchronisation ;
  - TWR (Time to Wait Resynchronization), ou temporisateur d'attente d'exécution de réaffectation-resynchronisation.

  Le TTR est utilisé par l'entité appelante. Sa valeur maximale normalisée ne peut excéder deux minutes moins la somme du délai maximal de propagation de déconnexion et du temps de transit maximal. Cette valeur peut être indiquée dans la TPDU CR de demande de connexion. La valeur du temporisateur TWR doit être supérieure à la somme de TTR, du délai maximal de propagation de déconnexion et du temps de transit maximal.

  Lorsqu'une indication de déconnexion réseau se présente alors que le temporisateur TTR n'est pas arrivé à échéance, on affecte la connexion de transport à une connexion différente, puisqu'on effectue une procédure de resynchronisation. Si le temporisateur TTR arrive à échéance, on considère que la connexion de transport est libérée.
- **Resynchronisation.** La resynchronisation permet de rétablir l'état normal de la connexion de transport, soit après une réinitialisation, soit à la suite d'une réaffectation. L'une des deux possibilités suivantes est réalisée : si le temporisateur TTR arrive à échéance, la connexion de transport est considérée comme libérée. Dans les autres cas, après avoir armé le temporisateur TTR, il faut, si nécessaire, réexpédier une TPDU CR, DR, ED ou RJ (Reject) ou attendre l'arrivée d'une TPDU avant la fin du temporisateur TWR puis envoyer à ce moment la réponse correcte. Le cas le plus classique est celui de l'envoi d'une TPDU RJ (Reject) dont le paramètre numéro de YR-TU (numéro de séquence en réponse) est celui de la prochaine TPDU attendue.

- **Gel de référence.** Le gel de référence permet de ne pas réaffecter le numéro de référence d'une connexion à une nouvelle connexion de transport tant que des TPDU correspondant à une connexion libérée risquent de circuler.

La classe 2

La classe 2 reprend les caractéristiques de la classe 0 et la plupart de celles de la classe 1, à l'exception des reprises sur erreur signalées à l'aide de la TPDU RJ. Elle permet d'effectuer en outre un multiplexage-démultiplexage et un contrôle de flux explicite.

Le multiplexage-démultiplexage permet à plusieurs connexions de transport d'utiliser la même connexion réseau pour optimiser les ressources des couches sous-jacentes. Pour effectuer le multiplexage, on concatène plusieurs TPDU correspondant à des connexions distinctes en une seule NSDU, qui est transférée par la couche réseau. À l'autre extrémité, on sépare la NSDU en plusieurs TPDU. Les connexions de transport correspondantes sont reconnues par les numéros de référence.

Pour le contrôle de flux, les TPDU sont numérotées dans le format normal (modulo 2^7) ou étendu (modulo 2^{31}). Au cours de l'établissement de la connexion, un crédit est envoyé dans la TPDU CR ou la TPDU CC. Ce crédit, qui peut être égal à 0, donne le nombre maximal de TPDU qu'il est possible de transmettre sans que les acquittements homologues soient arrivés. La fenêtre correspondant à ce crédit est augmentée chaque fois qu'une TPDU AK (Acknowledgement) revient à l'émetteur portant l'acquittement de une ou plusieurs TPDU DT. Dans le cas de la classe 2, la valeur du crédit est fixe et ne peut être modifiée au cours de la vie de la connexion (il en va différemment dans la classe 4).

La classe 3

La classe 3 couvre les possibilités des classes 0, 1 et 2. Nous ne décrivons ici que ses fonctionnalités additionnelles les plus importantes.

Une extrémité de la connexion peut effectuer à tout moment une reprise sur erreur en émettant une TPDU RJ (Reject). Cette TPDU demande à l'autre extrémité de réemettre toutes les TPDU à partir de celle qui est notée mais peut aussi demander de réduire le nombre de crédit alloué à l'autre extrémité ou, ce qui revient au même, de réduire la fenêtre indiquant le nombre de TPDU pouvant être émise vers lui. Le numéro de la trame YR-TU ne peut être qu'égal au plus grand des numéros déjà reçus + 1. Les nouvelles TPDU non en séquence ne sont pas admises, ce qui implique de la part de la couche réseau de remettre les NSDU dans l'ordre.

Dans le cadre du contrôle de flux, une réduction de crédit à travers une TPDU RJ peut engendrer la réception d'une TPDU qui ne se trouve plus dans la fenêtre gérée par l'émetteur. Cette possibilité ne doit pas être considérée comme une erreur de protocole. De même, au cours d'une reprise, des acquittements de TPDU émis avant l'arrivée de la demande de reprise RJ peuvent être pris en compte par l'émetteur, ce qui permet au récepteur de ne retransmettre que les TPDU qui n'ont pas été acquittées correctement.

La classe 4

C'est la classe la plus complète. Elle reprend toutes les fonctionnalités des quatre précédentes et comporte la possibilité de détecter les erreurs et d'effectuer des reprises à partir de cette détection. De même, les TPDU perdues, dupliquées ou hors séquence sont prises en compte dans les opérations de récupération. Des fonctionnalités supplémentaires sont disponibles en cas de défaillance du service réseau. Lors de ces reprises, la classe 4 utilise des procédures spécifiques, qui demandent la mise en place de temporisateurs.

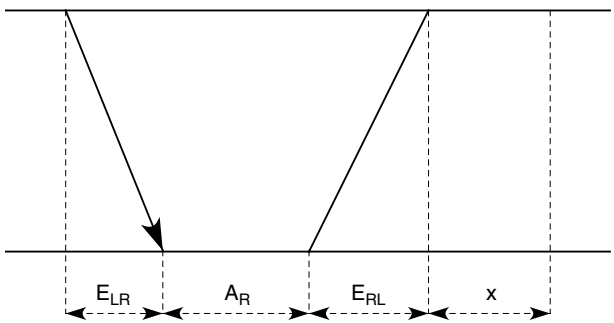
Les paramètres temporels utilisés en classe 4 sont définis dans la norme. Le tableau G.2 récapitule les symboles, noms et définitions exacte de ces valeurs.

Tableau G.2 • Paramètres temporels utilisés en classe 4

Symbole	Nom	Définition
M_{LR}	Durée de vie de NSDU, sens local-distant *(MAXIMUM TRANSIT DELAY)*	Temps maximal pouvant s'écouler entre l'expédition d'une NSDU par une entité de transport locale et la réception d'une copie de celle-ci par une entité distante
M_{RL}	Durée de vie de NSDU, sens distant-local *(MAXIMUM TRANSIT DELAY)*	Temps maximal pouvant s'écouler entre l'expédition d'une NSDU par une entité de transport distante et la réception d'une copie de celle-ci par une entitéde transport locale
E_{LR}	Temps de transit max. prévisible, sens local-distant *(EXPECTED MAXIMUM TRANSIT DELAY)*	Temps de transit acceptable pour l'ensemble des NSDU, à l'exception d'une faible fraction d'entre elles, transmises depuis l'entité de transport locale vers une entité de transport distante
E_{RL}	Temps de transit max. prévisible, sens distant-local *(EXPECTED MAXIMUM TRANSIT DELAY)*	Temps de transit acceptable pour l'ensemble des NSDU, à l'exception d'une faible fraction d'entre elles, transmises depuis une entité de transport distante vers l'entité de transport locale
A_L	Délai d'accusé de réception de l'entité locale *(ACKNOWLEDGEMENT TIME)*	Temps maximal pouvant s'écouler entre la réception par l'entité locale d'une TPDU provenant de la couche réseau et l'expédition de l'accusé de réception correspondant
A_R	Délai d'accusé de réception de l'entité distante *(ACKNOWLEDGEMENT TIME)*	Comme A_L, mais concerne l'entité distante.
T1	Délai de réexpédition de l'entité locale *(LOCAL TRANSMISSION TIME)*	Temps maximal d'attente, par l'entité locale, de l'accusé de réception d'une TPDU avant de réexpédier celle-ci
R	Délai de persistance *(PERSISTANCE TIME)*	Temps maximal pendant lequel l'entité de transport locale continue d'expédier une TPDU avec demande d'accusé de réception.
N	Nombre max. de réexpéditions *(MAXIMUM NUMBER OF TRANSMISSION)*	Nombre maximal de réexpéditions par l'entité de transport locale d'une TPDU avec demande d'accusé de réception.
L	Délai min. de réutilisation d'une référence d'un numéro de séquence *(BOUND ON REFERENCES AND SEQUENCE NUMBERS)*	Temps maximal écoulé entre l'expédition d'une TPDU et l'arrivée d'un accusé de réception de cette TPDU
I	Délai d'inactivité *(INACTIVITY TIME)* Note : ce paramètre est nécessaire pour se protéger des erreurs non signalées.	Délai au terme duquel une entité de transport qui ne reçoit aucune TPDU décide de lancer la procédure de libération pour mettre fin à la connexion de transport.
W	Délai de réexpédition d'informations de contrôle de fenêtre *(WINDOW TIME)*	Temps maximal d'attente d'une entité de transport avant de réexpédier des informations de contrôle de fenêtre actualisées.

Le temporisateur T1 illustré à la figure G.3 est défini par $T1 = E_{LR} + E_{RL} + A_R + x$. Son importance est capitale pour déterminer les performances du protocole. La valeur *x,* qui a été ajoutée dans T1, représente le délai de traitement local d'une TPDU. Le délai A_R dépend de la discipline d'acquittement des TPDU et du fonctionnement du récepteur. E_{LR} et E_{RL} représentent les délais de propagation aller-retour.

Figure G.3
Fonctionnement du temporisateur T1



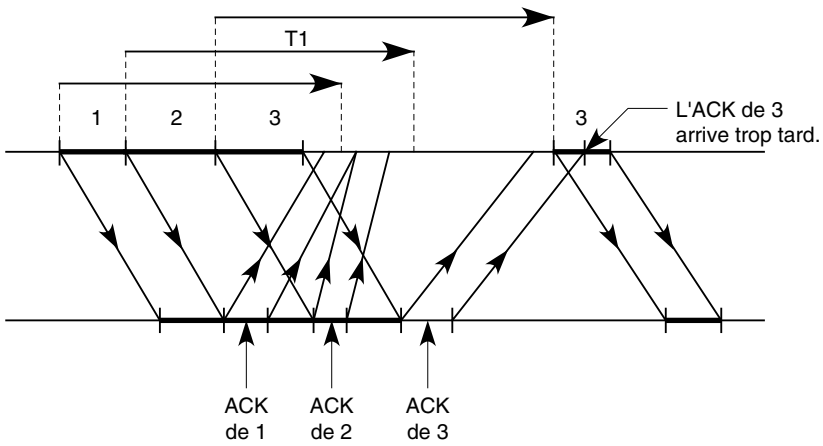
Comme dans la classe 4, on suppose que le taux d'erreur résiduelle est inacceptable. Chaque TPDU non acquittée est retransmise à l'échéance du temporisateur T1. On n'utilise pas d'acquittement négatif, puisqu'il n'est pas certain que les acquittements négatifs arrivent effectivement à l'émetteur.

Fonctionnement du temporisateur T1

On peut utiliser le temporisateur T1 de deux façons différentes :

- À chaque TPDU, on associe un temporisateur T1 au moment de son émission. À expiration de ce délai, la TPDU est réémise et le temporisateur T1 réinitialisé. Ce cas de figure est illustré à la figure G.4.

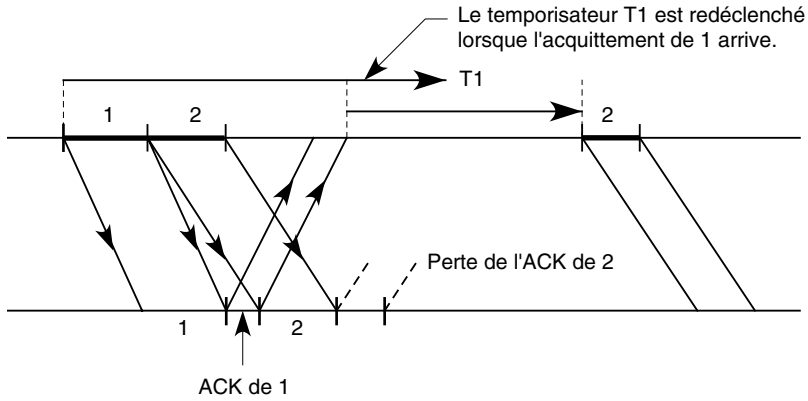
Figure G.4
Exemple où la TPDU 3 est réémise à la suite de l'échéance du temporisateur T1



- Un seul temporisateur est associé à la connexion de transport. Lors de l'émission d'une TPDU, le temporisateur T1 est armé s'il ne l'est déjà. S'il est en cours, l'émission d'une TPDU ne modifie rien. À réception d'un acquittement attendu, le temporisateur T1 est réarmé. Il est arrêté lors de la réception de la dernière TPDU attendue. Lorsque le temporisateur arrive à échéance, les TPDU non acquittées sont réémises. Ce cas de figure est illustré à la figure G.5.

Figure G.5

Reprise sur le temporisateur T1 lorsque celui-ci est affecté à une connexion de transport



La première solution permet de réémettre plus rapidement des TPDU erronées ou perdues mais exige davantage du logiciel, qui doit gérer autant de temporisateurs que de TPDU émises.

Un délai de persistance, R, est également utilisé : c'est le temps maximal pendant lequel l'entité de transport locale continue de réémettre les TPDU non acquittées. Si *N* émissions est la valeur que l'on se fixe pour arrêter les retransmissions d'une même TPDU, on prend R = *N* T1 + X, où X est une valeur fixe à déterminer localement et qui tient compte des délais internes pour réémettre la TPDU après expiration du temps T1.

La valeur de T1 est difficile à déterminer puisque l'émetteur peut avoir du mal à connaître la politique d'acquittement des TPDU. L'entité distante peut très bien attendre le temps A_R avant d'émettre l'acquittement, mais elle peut aussi le faire immédiatement. De plus, les temps de transit peuvent être très différents suivant le parcours des TPDU sur la connexion réseau. Enfin, le contrôle de flux du service réseau peut générer une attente de la TPDU dans l'émetteur local lorsque le temporisateur T1 arrive à échéance. Il est donc très difficile de contrôler le temps passé dans les logiciels exécutés sur les machines terminales.

Les TPDU de classe 4 peuvent porter une zone de détection d'erreur, appelée total de contrôle, mais ce n'est pas une obligation. L'algorithme qui est déroulé peut être adapté au type d'erreur attendu sur les connexions de transport. La norme définit l'algorithme ci-après, dont les paramètres sont transportés par les TPDU CR et DT. La valeur *L* représente le nombre d'octets de la TPDU et a_i la valeur de l'octet de position *i*.

Le premier octet du total de contrôle b_1 est déterminé par :

$$\sum_{i=1}^{L} a_i + b_1 = 0 \text{ (modulo 255)}$$

Le second octet du total de contrôle b_2 est déterminé par :

$$\sum_{i=1}^{L} i\,a_i + b_2 = 0 \text{ (modulo 255)}$$

Cette technique de détection d'erreur est extrêmement simple et peut être implémentée sans difficulté dans l'entité de transport. En revanche, elle ne détecte pas l'insertion de 0 en fin de TPDU.

La classe 4 se distingue encore par des échanges d'information supplémentaires lors de l'ouverture de la connexion. Comme pour les classes 1, 2 et 3, 32 octets de données utilisateur peuvent être transportés. Le délai d'accusé de réception, ainsi que les paramètres du total de contrôle et la possibilité d'ajouter des paramètres de sécurité définis par l'utilisateur sont transportés lors de l'ouverture.

Les tableaux G.3 et G.4 récapitulent les mécanismes utilisés dans le protocole X.224. Le tableau G.3 décrit certains éléments de procédure qui ne sont pas repris en détail au tableau G.4. Ce dernier précise, pour les cinq classes du protocole X.224, les mécanismes disponibles.

Tableau G.3 • Éléments de procédure disponibles dans les diverses classes X.224

x	Procédure faisant partie de la classe
m	Procédure négociable, mais dont l'équipement doit toujours permettre la mise en œuvre.
0	Procédure négociable, dont la possibilité de mise en œuvre par l'équipement est optionnelle.
ao	Procédure négociable, dont la mise en œuvre par l'équipement est optionnelle et dont l'utilisation dépend de sa disponibilité de la part du service de réseau.
(1)	Non applicable en classe 2 quand l'option Non utilisation du contrôle de flux explicite a été choisie.
(2)	L'utilisation du multiplexage peut conduire à une dégradation de la qualité du service dans le cas où l'option Non utilisation du contrôle de flux explicite a été choisie.
(3)	Cette fonction est offerte en classe 4 mais utilise des procédures différentes de celles qui ont été décrites dans le texte.

Tableau G.4 • Affectation des éléments de procédure dans chaque classe X.224

Mécanisme de protocole	Variante				
	0	1	2	3	4
Affectation à une connexion réseau	x	x	x	x	x
Transfert de TPDU	x	x	x	x	x
Segmentation et réassemblage	x	x	x	x	x
Concaténation et séparation		x	x	x	x
Établissement de connexion	x	x	x	x	x
Refus de connexion	x	x	x	x	x
Libération normale (implicite)	x	x	x	x	x
Libération sur erreur (explicite)	x	x	x	x	x
Association de TPDU à des connexions de transport	x	x	x	x	x
Numérotation de TPDU DT Normale Étendue		x	m(1) 0(1)	m 0	m 0
Données exprès Normale réseau Étendue réseau		m ao	x(1)	m	m
Réaffection après incident		x		x	(3)
Rétention jusqu'à accusé de réception de TPDU Confirmation réception AK	ao m		x	x	
Resynchronisation		x		x	(3)
Multiplexage et démultiplexage			x(2)	x	x
Contrôle de flux explicite			m	x	x
Total de contrôle					m
Gel de référence		x		x	x
Retransmission après temporisation					x
Remise en séquence					x
Détection d'inactivité					x
Traitement d'erreurs de protocole	x	x	x	x	x
Éclatement et recombinaison					x

Le tableau G.5 recense les TPDU valides pour chaque classe et le code des TPDU. La suite *xxxx* est indique la valeur du crédit pour les classes 2 à 4. Cette valeur est de 0000 pour les classes 0 et 1. La suite *zzzz* indique la valeur du crédit en classes 2 à 4. Cette valeur est de 1111 en classe 1.

Tableau G.5 • Codes des TPDU X.224

TPDU	0	1	2	3	4	Code
CR (Connect Request) : demande de connexion	x	x	x	x	x	1110 xxxx
CC (Connect Confirm) : confirmation de connexion	x	x	x	x	x	1101 xxxx
DR (Disconnect Request) : demande de déconnexion	x	x	x	x	x	1000 0000
DC (Disconnect Confirm) : confirmation de déconnexion		x	x	x	x	1100 0000
DT (DaTa) : données	x	x	x	x	x	1111 0000
ED (Expedited Data) : données exprès		x	NF	x	x	0001 0000
AK (data AcKnowledge) : accusé de réception de données		NRC	NF	x	x	0110 zzzz
EA (Expedited data Ack) : accusé de réception de données exprès		x	NF	x	x	0010 0000
RJ (ReJect) : rejet		x		x		0101 zzzz
ER (TPDU Errror) : erreur de TPDU	x	x	x	x	x	0111 0000

NF : non disponible quand l'option Non utilisation du contrôle de flux explicite a été adoptée.
NRC : non disponible quand l'option Confirmation de réception a été adoptée.

Annexe H

9. Les réseaux d'accès terrestres

Cette annexe détaille les accès *x*DSL, ainsi que leurs protocoles et leur utilisation. Elle se penche en outre plus en détail sur les accès par modem câble, qui sont assez peu utilisés en France, mais beaucoup aux États-Unis, et sur le passage de la vidéo sur la boucle locale.

Le protocole L2TP

Pour réaliser les communications entre les BAS et les serveurs, un protocole de tunneling doit être mis en place puisque ce chemin peut être considéré comme devant être emprunté par tous les paquets ou trames provenant des différents DSLAM et allant vers le même serveur. Le tunneling est une technique courante, qui ressemble à un circuit virtuel. Les trois protocoles utilisés pour cela sont PPTP (Point-to-Point Tunneling Protocol), L2F (Layer 2 Forwarding) et L2TP (Layer 2 Tunneling Protocol). Ces protocoles permettent l'authentification de l'utilisateur, l'affectation dynamique d'adresse, le chiffrement des données et éventuellement leur compression.

Le protocole le plus récent, L2TP, supporte difficilement le passage à l'échelle, ou scalabilité, et n'arrive pas à traiter correctement et suffisamment vite un nombre de flots dépassant les valeurs moyennes. Dans ce cas, on ajoute des concentrateurs d'accès L2TP, ou LAC (L2TP Access Concentrator), qui récupèrent tous les clients provenant d'un même DSLAM et allant vers un même BAS et les multiplexent sur un même circuit virtuel.

La figure H.1 illustre l'architecture protocolaire d'une communication d'un PC vers un serveur situé dans un réseau de FAI différent de celui de l'opérateur d'entrée. Le PC travaille sous TCP/IP et est connecté à un modem ADSL par le biais d'un réseau Ethernet.

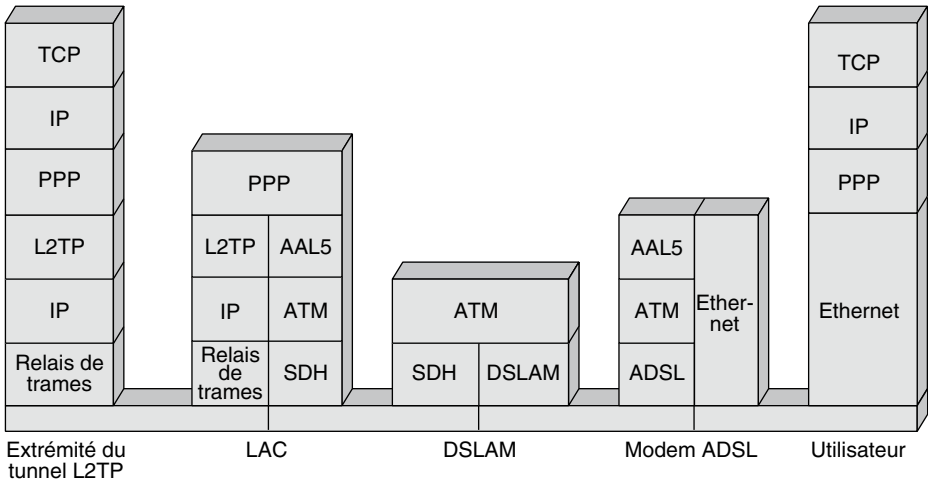


Figure H.1

Architecture protocolaire d'une communication ADSL

La parole et la vidéo sur *x*DSL

Nous avons vu qu'en *x*DSL la parole téléphonique était transportée parallèlement aux données sur la partie basse du spectre. Cette technologie convient très bien aux opérateurs historiques, aussi appelés ILEC (Incumbent Local Exchange Carrier). Les nouveaux venus, ou CLEC (Competitive Local Exchange Carrier), peuvent aujourd'hui espérer concurrencer les opérateurs historiques grâce à la déréglementation de la boucle locale.

Pour prendre en charge des clients sur la boucle locale de l'opérateur historique, ces opérateurs entrants peuvent faire passer la parole téléphonique sur la partie DSL. On appelle cette solution ToDSL (Telephony over DSL). Le passage de la parole sur la partie donnée s'apparente aux technologies de voix sur IP.

Les paquets de parole devant arriver au récepteur avant 150 ms, il faut qu'une priorité leur soit appliquée. Dans ce cas, la dizaine de kilobits par seconde de la parole compressée passe assez facilement. Il faut toutefois que la priorité puisse s'exercer non seulement sur la partie modem mais aussi sur les parties réseau précédant et suivant les deux modems. Cela suppose, pour la partie réseau d'entreprise, l'application d'une technique de priorité et, pour le réseau du FAI, la possibilité de négocier un SLA (Service Level Agreement) compatible avec le temps maximal de traversée de bout en bout.

Une autre solution, moins intégrée mais plus simple à mettre en œuvre, est commercialisée par de nombreux FAI pour offrir le service téléphonique ToDSL. Elle consiste à utiliser une bande spécifique du modem, de 4,3 MHz, donnant un débit de 32 Kbit/s. L'inconvénient de cette solution est que si la parole téléphonique n'est pas utilisée, la

bande passante correspondante est perdue. Cependant, comme la bande passante utilisée est très faible, cela ne pose pas vraiment problème.

La ligne DSL doit aussi convoyer la signalisation téléphonique, ce qui constitue la deuxième difficulté après la contrainte temporelle. Sur le modem, plutôt que d'utiliser une priorité sur les données, il est possible d'utiliser l'AAL-1, qui offre des fonctionnalités de synchronisation et de priorité. Cette solution, appelée VoATM (Voice over ATM), est complémentaire de la technologie ToDSL.

La télévision est une deuxième application qui est offerte aux utilisateurs de modems ADSL. Avec la première génération de modems ADSL, une bande passante spécifique est dévolue au canal de télévision, en général de 3 Mbit/s. Lorsque la télévision est en marche, le canal ne fait que transporter des signaux numériques de l'image de télévision. Lorsque la télévision est éteinte, les 3 Mbit/s sont alloués à la bande passante utilisée pour le transport des données. Dans la seconde génération, l'image de télévision est intégrée avec les autres flots, et les paquets transportant le flux d'images sont facilement repérables par une adresse spécifique correspondant à la prise sur le boîtier sur laquelle est branchée la télévision. Enfin, dans la troisième génération, le flot de paquets provenant de la télévision est un flot IP totalement intégré aux autres paquets, un marquage spécifique permettant de reconnaître les paquets pour leur donner une priorité acceptable pour la qualité de service nécessaire.

La vidéo est un autre service qui peut être offert par les modems DSL. S'il est encore difficilement imaginable de voir ce système supplanter la vidéo diffusée à grande échelle, la vidéo sur DSL, ou VoDSL (Video over DSL), commence à être déployée par de nombreux FAI pour des diffusions limitées et des services de VoD (Video on Demand).

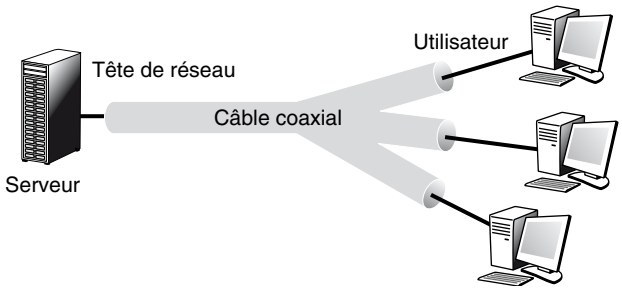
Les deux solutions que nous avons examinées pour la téléphonie sont possibles pour la vidéo : soit on intègre les paquets vidéo dans le flot en leur donnant si possible une priorité forte, soit on leur affecte un canal spécifique. Dans ce dernier cas, la largeur de la bande passante affectée à la vidéo diffère suivant les opérateurs pour aller de 800 Kbit/s à quelques mégabits par seconde. Pour une télévision à 800 Kbit/s, il suffit de récupérer 25 des 256 sous-bandes, chacune transportant 32 Kbit/s.

Dans le cas du multipoint, c'est-à-dire de la diffusion limitée à un petit nombre d'utilisateurs, la vidéo est compressée en MPEG-4 ou éventuellement en MPEG-2 et émise en utilisant un protocole multipoint. Le plus performant de ces protocoles est IP Multicast, puisque les paquets sont à l'origine IP. Cependant, comme il faut compresser au maximum les données vidéo, le choix du codec vidéo est capital pour que le flot arrive dans les temps.

Les modems câble

Les câblo-opérateurs disposent d'un environnement leur permettant de relier l'utilisateur à un ou plusieurs opérateurs. Ce câblage est réalisé à partir du câble coaxial CATV reliant la tête de réseau aux utilisateurs, comme l'illustre la figure H.2. Les canaux de télévision dans le sens descendant sont diffusés sur toutes les branches du câblage. Dans le sens montant, les canaux doivent se superposer sur le tronc de l'arbre.

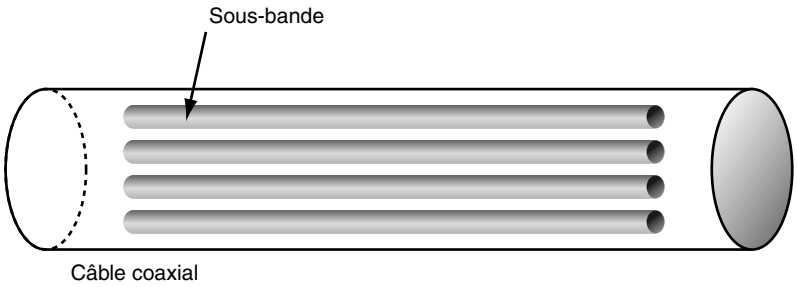
Figure H.2
Distribution de programmes TV par un câblo-opérateur



Le câblage part d'une tête de réseau pour atteindre l'utilisateur après une diffusion sur l'ensemble des branches. Dans le cadre de la diffusion de la télévision, les différents programmes sont poussés vers les utilisateurs. Chaque abonné reçoit l'ensemble des chaînes et en sélectionne une à visualiser. Cette technique est à l'opposé de l'ADSL, où seule la chaîne sélectionnée par l'utilisateur est acheminée.

Dans le CATV, un multiplexage en fréquence est utilisé pour le transport des différents canaux de télévision (*voir figure H.3*). La division en fréquence donne naissance à des sous-bandes, chaque sous-bande portant un canal de télévision.

Figure H.3
Multiplexage en fréquence dans le CATV



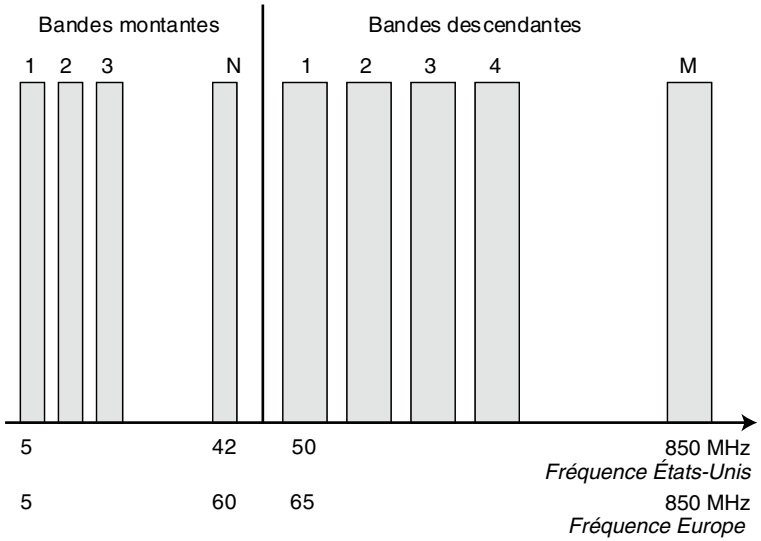
On peut affecter une bande étroite, de 32 ou 64 Kbit/s par utilisateur, pour transporter de la parole téléphonique entre le combiné de l'utilisateur et la tête de réseau qui est reliée à un opérateur télécoms.

Il est possible de réserver une sous-bande pour la connexion à un opérateur de type FAI. Cette sous-bande doit toutefois être suffisante pour supporter la somme des débits crêtes des utilisateurs. Par exemple, 1 000 utilisateurs connectés à 1 Mbit/s exigent un débit total potentiel de 1 Gbit/s. La solution à ce problème consiste à choisir sur le CATV une bande très large et à utiliser une technique de multiplexage pour faire passer un maximum d'utilisateurs simultanément.

La figure H.4 illustre un partage de la bande passante d'un CATV en Amérique du Nord et en Europe. Les bandes montantes en Europe se situent entre 5 et 42 MHz et ont une largeur de 200 kHz à 3,2 MHz. Les bandes descendantes se situent entre 50 et 850 MHz. La largeur des bandes de télévision est de 8 MHz. Le nombre de bandes montantes et

descendantes est laissé libre aux opérateurs. Les valeurs pour l'Amérique du Nord sont indiquées sur la figure. Les bandes de télévision sont de 6 MHz.

Figure H.4
Plage de fréquences dans un CATV



Pour réaliser le multiplexage des utilisateurs sur la bande commune, trois normes ont été proposées :

- IEEE 802.14, qui utilise une technologie ATM.
- MCNS-DOCSIS, qui est surtout utilisée en Amérique du Nord mais que les câblo-opérateurs européens ont adoptée par la suite.
- DVB-DAVIC, que nous détaillons un peu plus loin.

IEEE 802.14 et MLAP

La transmission numérique sur un CATV s'effectue d'une manière unidirectionnelle, de la station terminale vers la tête de réseau ou l'inverse. La bande passante du CATV est subdivisée en une bande montante vers la tête de ligne et une bande descendante vers les équipements terminaux.

Cette partie du câblage peut desservir entre 500 et 12 000 utilisateurs depuis la tête de réseau. Si chaque utilisateur veut effectuer une application de vidéo à la demande, ou VoD, la bande passante n'est pas suffisante, ou, du moins, chaque client doit se limiter à une partie de cette bande passante. Pour permettre une meilleure adéquation de la bande passante, surtout aux applications interactives, le groupe de travail IEEE 802.14 a développé le protocole MLAP (MAC Level Access Protocol), qui permet de distribuer le support entre les machines connectées.

La difficulté principale de ce système réside dans la technique d'accès. Comme les canaux sont unidirectionnels, l'équipement le plus en aval ne peut écouter les émissions des autres stations qu'après un certain laps de temps, qui correspond à la propagation du signal jusqu'à la tête de réseau et à celle en retour jusqu'à la station. La portée du CATV pouvant atteindre plusieurs dizaines de kilomètres, il faut trouver une solution intermédiaire entre les techniques satellite et les méthodes utilisées dans les réseaux locaux.

Le protocole MLAP repose sur une succession d'états correspondant à des actions découpées en cinq phases :

1. La station que l'on examine est inactive.
2. Elle devient active, c'est-à-dire qu'elle veut émettre des trames.
3. Elle avertit la tête de réseau par des primitives UP.FRAME et UP.REQ et par un mécanisme d'accès aléatoire.
4. La tête de réseau notifie à toutes les stations, par le biais du canal aval, les intervalles de temps pendant lesquels les stations peuvent émettre. Les canaux sont utilisés dans un mode avec contention. Cela signifie que l'allocation d'un canal ne se fait pas de façon unique du premier coup et que des collisions peuvent se produire. Associé à la tête de réseau, un contrôleur peut modifier l'allocation des canaux en tenant compte de la demande de qualité de service des stations. L'algorithme est alors réinitialisé, et les informations sont mises à jour. Une nouvelle allocation est ensuite déterminée. Les stations reçoivent une notification de la tête de réseau indiquant les nouveaux intervalles de temps qui leur sont alloués. Ce processus se poursuit jusqu'à ce que les stations aient leur canal réservé.
5. Si une station modifie sa demande de bande passante ou de qualité de service, la nouvelle demande s'effectue par les canaux partagés.
6. L'algorithme d'allocation de bande passante du contrôleur ne fait pas partie de la norme.

DVB-DAVIC

Le groupe DAVIC (Digital Audio VIsual Council) a été formé en 1994 pour normaliser les interfaces et les architectures des réseaux transportant de la vidéo. Le choix s'est dirigé en grande partie vers la norme DVB, qui permet le transport de tout type d'information, en particulier la vidéo.

Une version spécifique du DVB a été développée pour le câble. Elle utilise des bandes de 6 Mbit/s de débit et une technologie de modulation de phase et d'amplitude. Le DVB utilise la compression MPEG-2 pour la télévision numérique. MPEG-2 permet le multiplexage de plusieurs canaux numériques dans des trames spécifiques. Pour le transport des paquets MPEG, voire directement du paquet IP, puisque c'est permis par l'interface DAVIC, c'est la trame ATM qui est utilisée. Nous retrouvons là des techniques semblables à celles utilisées dans IEEE 802.14 et DOCSIS.

Le contrôle des paquets IP

Les normes IEEE 802.14 et DOCSIS assurent une bonne utilisation de la partie du câble affectée au transport des données. Nous avons vu que la norme associée au modem était l'ATM. En réalité, ces paquets ATM ne sont là que pour transporter des paquets IP, le paquet de base restant le paquet IP. Les paquets IP doivent être contrôlés, de telle sorte que chaque utilisateur n'en émette pas trop et que le réseau demeure fluide.

Le contrôle des flots IP s'effectue grâce à un algorithme, dit slow-start and congestion avoidance, qui limite la valeur de la fenêtre afin que chaque utilisateur puisse continuer à jouir de son débit, même lorsque le réseau est surchargé. Les paquets IP, dont le nombre est limité par la fenêtre, sont découpés pour cela en morceaux de 48 octets pour être introduits dans la zone de données de la trame ATM. Le nombre des cellules ATM dépend de la fenêtre IP.

Une difficulté de cette méthode provient de la couche d'accès au support physique, qui n'est pas corrélée au débit des trames ATM. Si la connexion n'a pas de débit, du fait que la demande d'accès n'a pas obtenu de réservation, les acquittements des paquets IP arrivent trop tard, et il en résulte un redémarrage du slow-start à la valeur 1 pour la fenêtre de contrôle. Même si la connexion reçoit une réservation réussie grâce à la technique d'accès, cette réservation est de nouveau perdue après l'émission des trames ATM en attente, qui ne sont qu'en petit nombre. En revanche, lorsque la technique d'accès a réussi à réserver un slot et que la valeur de la fenêtre de contrôle augmente, la connexion n'a plus de raison de perdre la main, et elle se met à très bien fonctionner.

Annexe I

10. Les réseaux d'accès hertziens

Cette annexe commence par détailler les bandes de fréquences utilisées dans les réseaux d'accès hertziens, avant d'examiner les réseaux WiMAX de première génération, qui n'ont guère rencontré le succès. C'est la raison pour laquelle WiMAX phase 2 a été développé, qui fait partie intégrante de la génération 4G. Nous examinons enfin des réseaux hertziens particuliers, comme WiBro, qui a été défini en Corée, et WRAN, qui est poussé par le groupe de travail IEEE 802.22 comme futur réseau régional.

WiMAX

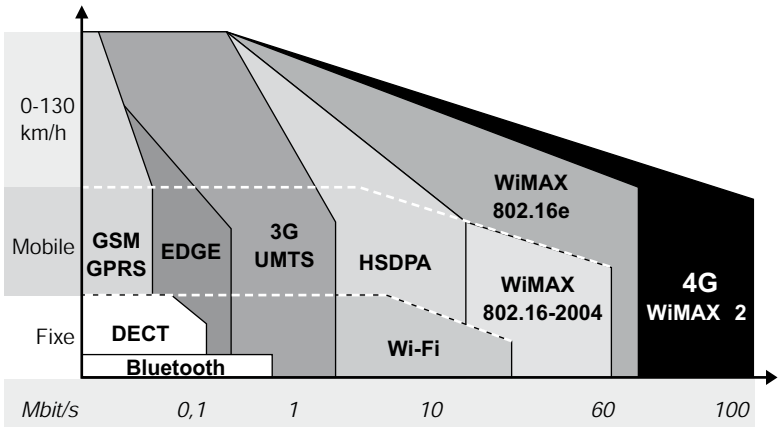
WiMAX (Worldwide Interoperability for Microwave Access) est issu d'une initiative lancée en 2001 par l'Alliance WiMAX. Son objectif était de promouvoir le standard 802.16 de l'IEEE en se proposant de vérifier la conformité et l'interopérabilité des équipements. Malheureusement, ce réseau n'a pas rencontré le succès escompté.

WiMAX se présente en deux versions, une version fixe, qui a été finalisée sous le nom de WiMAX IEEE 802.16-2004 et la version mobile IEEE 802.16e-2005.

L'utilisation de WiMAX est très semblable à celle d'un modem ADSL, si ce n'est qu'au lieu d'un câble téléphonique on utilise la voie hertzienne. C'est pourquoi l'on parle de WDSL (Wireless DSL) pour décrire la solution WiMAX fixe. En ce qui concerne la version mobile, son utilisation est identique celle d'un ADSL mobile. L'avantage évident de WiMAX mobile est qu'on l'a toujours sur soi. Avec un équipement muni d'une connexion WiMAX, il est possible de se connecter de partout, tout le temps, y compris en situation de mobilité.

La figure I.1 illustre la position de WiMAX dans le contexte de réseaux sans fil.

Figure I.1
Place de WiMAX dans les technologies hertziennes



Au sein du groupe 802.16, deux sous-groupes s'occupent des communications dans des fréquences situées, pour le premier, entre 1 et 11 GHz et, pour le second, entre 10 et 66 GHz. En Europe, la normalisation du même domaine s'effectue à l'ETSI (European Telecommunications Standards Institute), où le groupe de travail BRAN (Broadband Radio Access Networks) propose la norme HiperAccess (High-Performance Radio Access), ou HiperLAN 3, comme solution pour les réseaux d'accès à très haut débit. Cette proposition permet de réaliser des réseaux IP ou ATM offrant des débits de l'ordre de 25 Mbit/s.

Le groupe de travail 802.16 a mis en place des sous-groupes, qui se sont attaqués à des problèmes distincts. Le groupe de travail de base a normalisé un accès métropolitain dans la bande des 10-66 GHz avec une vue directe entre les antennes et un protocole point-à-point. Finalisée en 2001, la norme IEEE 802.16 a été complétée par la norme 802.16c de 2002, qui introduit des profils système WiMAX, et par une partie de la norme 802.16d de 2004, qui apporte des correctifs et des fonctionnalités supplémentaires autorisant la compatibilité avec la norme 802.16e.

Sortie en 2003, la norme 802.16a concerne la bande des 2 à 11 GHz, avec la possibilité d'utiliser des protocoles multipoint en plus de l'environnement point-à-point de base. La norme 802.16e a pour objectif d'étendre WiMAX à des machines terminales mobiles, impliquant la possibilité de réaliser des connexions *x*DSL vers des mobiles. Les fréquences utilisées se situent entre 2 et 6 GHz.

Les portées annoncées sont de 50 km à un débit de 70 Mbit/s, mais ces valeurs ne sont que théoriques, puisqu'elles nécessitent une très forte puissance avec une grande directivité et une vue directe. Dans les faits, la distance maximale est d'une dizaine de kilomètres et, suivant la puissance, la directivité et la vue directe, les débits se situent entre 40 et 50 Mbit/s. Plus classiquement, en partageant la ligne et en étant dans des conditions classiques avec des antennes de 90°, le débit maximal est plutôt de l'ordre de 30 Mbit/s.

On peut en déduire que le nombre de clients ADSL pouvant bénéficier d'un débit de l'ordre du mégabit par seconde peut atteindre la centaine en « surallouant » la ligne.

Pour augmenter les débits, il faut diminuer la portée en réduisant, par exemple, la puissance. Des débits d'une cinquantaine de mégabits par seconde sont dans ce cas possibles. Pour utiliser WiMAX en ville et bénéficier d'un grand nombre de clients, le diamètre des cellules ne doit pas dépasser 1 km environ.

Bandes de fréquences

Les bandes de fréquences attribuées pour les liaisons WLL varient suivant les pays et les continents. Une première bande fortement utilisée en France et en Europe concerne le DECT. Cette bande a été déterminée pour la téléphonie résidentielle et d'entreprise. Elle correspond à la partie du spectre située entre 1 880 et 1 900 MHz. Bien que particulièrement étroite, avec ses 20 MHz disponibles, cette bande peut être utilisée pour la BLR.

Le DECT se présente comme une solution potentielle pour la téléphonie mobile, mais au prix d'une limitation de la mobilité du terminal, qui doit rester dans une même cellule. Cette norme ETSI (European Telecommunications Standards Institute) de 1992 utilise une technique de division temporelle TDMA.

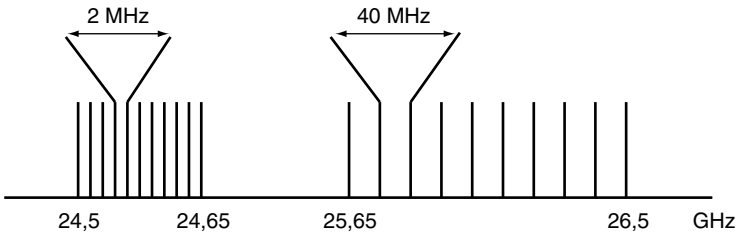
Une seconde bande, dédiée à la technologie MMDS, a été affectée aux techniques WLL. Cette bande était au départ dévolue à des canaux de télévision analogique en mode unidirectionnel, puisque la télévision est diffusée. Un canal de retour, permettant d'envoyer des commandes vers l'émetteur, était permis par l'utilisation du réseau téléphonique commuté. Cette bande sert maintenant à la BLR, mais de nouveau avec une bande passante assez faible. Les antennes réceptrices, d'un diamètre de 20 cm environ, doivent être quasiment en vue directe de l'antenne du fournisseur, sans obstacle entre les deux. Dans la bande des 3,5 GHz, les ondes réussissent à traverser les bosquets d'arbres et à être à peu près insensibles à la pluie. Les distances moyennes acceptables pour cette bande vont de 3 km dans les zones fortement urbanisées à quelque 10 km en zone rurale. La bande des 10,5 GHz est également disponible, mais une fois encore avec une très faible bande passante. Pour de réelles capacités, il faut utiliser des bandes au-dessus de 20 GHz, dont un grand nombre est disponible.

Les distances entre la station de base et l'antenne du client varient en fonction de la fréquence, du relief, de la météo, des obstacles, etc. Une vue directe entre les deux antennes qui communiquent est toujours nécessaire, cette directivité étant plus ou moins prononcée suivant la fréquence utilisée. La pluie peut devenir une contrainte forte compte tenu de la nature des ondes utilisées, dont la longueur est de l'ordre du millimètre, ce qui correspond à une fréquence d'environ 30 GHz. Toutes ces difficultés limitent la distance maximale entre l'émetteur et le récepteur à environ 3 km.

En France, deux licences nationales permettent l'utilisation des fréquences MMDS. Les licences régionales utilisent des fréquences dans la bande 24,5-26,5 GHz. Dans les DOM. Les licences concernent la bande des 3,5 GHz. Aux États-Unis, une bande de 1,3 GHz a été attribuée à cette technologie dans la gamme de fréquences 27,5-31,3 GHz. Sur une telle bande, une capacité de transmission au-dessus de 2 Gbit/s est envisageable. Une

partie de la bande 24,5-26,5 GHz sert à l'accès montant et une autre à l'accès descendant. Ces bandes sont illustrées à la figure I.2. D'une largeur de 150 MHz, la bande montante, c'est-à-dire de l'utilisateur vers la station de base, est divisée en sous-bandes de 2 MHz. La bande descendante, beaucoup plus large, avec 850 MHz, est découpée en sous-bandes de 40 MHz. Les canaux montants et descendants sont multiplexés en fréquence. Chaque sous-bande peut accueillir plusieurs utilisateurs multiplexés temporellement, c'est-à-dire se répartissant les tranches de temps entre eux. Nous détaillons le multiplexage temporel un peu plus loin.

Figure I.2
Canaux WLL de la bande 24,5-26,5 GHz



Couche physique et technique d'accès

La couche physique de WiMAX utilise la technologie OFDM (Orthogonal Frequency Division Multiplexing), qui découpe les fréquences en sous-fréquences orthogonales afin que deux fréquences voisines puissent être utilisées sans interférence.

Pour augmenter le débit des versions les plus évoluées, le MIMO (Multiple Input Multiple Output) est autorisé. Dans ce cas, comme expliqué au chapitre 23 pour IEEE 802.11n, plusieurs antennes peuvent émettre en parallèle sur la même fréquence en jouant sur les multiples chemins suivis par les signaux pour récupérer ces signaux à des instants légèrement différents.

WiMAX demande une technique d'accès puisque l'antenne joue le rôle d'équipement commun à tous les clients. La solution retenue est de type OFDMA (Orthogonal Frequency Division Multiple Access).

La technique d'accès de WiMAX est illustrée à la figure I.3.

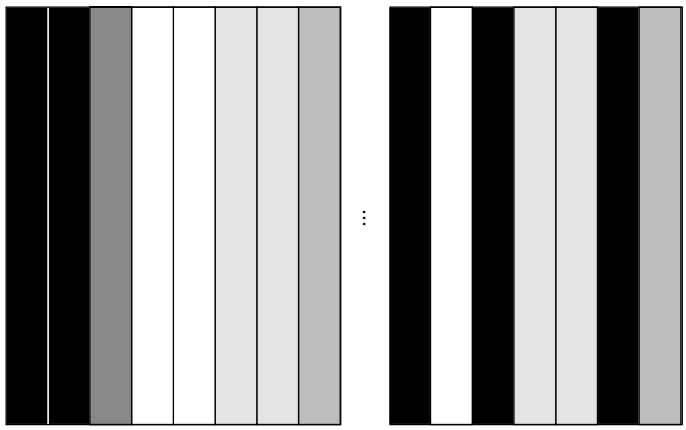
Dans cette figure, les tranches de temps sont données aux différents clients suivant des ordres de priorité. WiMAX possède quatre classes de priorités :

- UGS (Unsolicited Grant Service), la priorité la plus haute, a pour objectif de faire transiter des applications qui ont un débit constant en générant des paquets de longueur constante à des intervalles réguliers. Cette classe reçoit une allocation de tranches à intervalles réguliers de telle sorte que chaque paquet puisse être émis sans attente. Cette classe correspond aux applications de téléphonie classique qui produisent un débit constant. C'est une classe provenant de l'ATM mais un peu plus sophistiquée : le CBR (Constant Bit Rate). Les paramètres de qualité de service sont le Maximum Sustained Traffic Rate, c'est-à-dire le trafic moyen en période d'émission, le Minimum

Reserved Traffic Rate, c'est-à-dire le taux minimal à réserver pour que les paquets puissent passer et le Request/Transmission Policy, qui indique la politique de retransmission. Dans cette classe, si une tranche de temps est réservée, elle ne peut être préemptée par une autre classe. Il y a donc possibilité de perte de la tranche si le client ne l'utilise pas. Comme nous le verrons avec le WiMAX mobile, une autre classe a été ajoutée pour la téléphonie compressée.

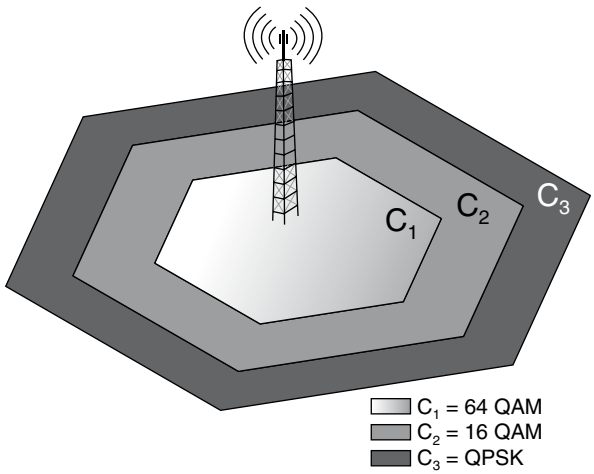
- rtPS (real-time Packet Service) correspond à la transmission d'applications de type vidéo. Cette classe prend en charge les applications qui produisent des trames de longueur variable à intervalles réguliers. Les tranches de temps qui ne seraient pas utilisées peuvent être réutilisées. Les paramètres de qualité de service sont les suivants : Maximum Sustained Traffic Rate, Minimum Reserved Traffic Rate, Request/Transmission Policy comme dans l'UGS et Maximum Latency Traffic Priority, qui indique le temps maximal entre deux trames prioritaires.
- nrtPS (non real-time Packet Service) correspond à des applications élastiques qui acceptent une variabilité du délai et dont les paquets ont des tailles variables, mais qui demandent un débit minimal. Cette classe de trafic est bien adaptée au transfert de fichiers et aux applications sans contraintes temporelles mais qui demandent malgré tout un débit minimal pour s'assurer d'être transmis après un temps correspondant à ce débit minimal. Les tranches de temps peuvent être volées par des classes de priorité supérieures si c'est nécessaire à la qualité de service de ces applications. Les paramètres définissant la qualité de service de sont Maximum Sustained Traffic Rate et Request/Transmission Policy ainsi que Minimum Reserved Traffic Rate, correspondant au trafic minimal souhaité par l'utilisateur, et Priority Traffic, correspondant au trafic des trames indispensables à l'application.
- BE (Best Effort) ne demande aucune qualité de service particulière et aucun débit minimal. Les paramètres de cette classe de service sont Maximum Sustained Traffic Rate, Traffic Priority, Request/Transmission Policy. Les services associés sont bien entendu ceux qui ne demandent aucune garantie sur le trafic, comme le trafic des applications Web.

Figure I.3
Technique d'accès de WiMAX



WiMAX utilise également une technique d'adaptation du codage à la qualité de la communication. Cette adaptation est illustrée à la figure I.4.

Figure I.4
Adaptation du codage à la qualité de la communication



Dans cette figure, le codage utilisé lorsque le client est assez près de l'antenne est le 64QAM, qui permet de faire passer 8 bits à chaque intervalle élémentaire. Si le client s'éloigne et que la qualité du signal se dégrade, ce qui est observé par le nombre de retransmissions, le codage passe au 16QAM et le transport à 4 bits par baud. Si le client est assez éloigné de l'antenne, une nouvelle dégradation implique le passage en QPSK et à l'émission de seulement 2 bits simultanément.

Ce comportement est assez sophistiqué puisqu'il implique une adaptation du terminal à la qualité du signal. Comme dans la plupart des réseaux de la gamme Wi-*xx,* cela crée des difficultés de gestion de la qualité de service des applications puisqu'il n'est pas possible de déterminer à l'avance le débit brut de l'antenne de l'opérateur. Ce débit dépend en fait des terminaux raccordés et non de l'antenne elle-même. Chaque terminal peut en effet transmettre à sa vitesse, allant du simple au quadruple. C'est une des raisons pour lesquelles les tests effectués autour de WiMAX affichent un débit beaucoup plus bas qu'attendu dès que la plupart des terminaux sont situés à des distances de plus de 5 km. C'est aussi pour cela qu'il est recommandé, si l'on veut obtenir un débit approchant 50 Mbit/s, de restreindre la taille des cellules WiMAX à des rayons de quelques kilomètres, idéalement deux ou trois.

La réception de WiMAX nécessite des antennes fixes qui relient la maison ou l'entreprise à l'antenne de l'opérateur. L'irrigation dans la maison ou l'entreprise peut se faire par le biais d'une autre technologie, comme Wi-Fi. Les ordinateurs personnels peuvent toutefois être dotés d'une carte spécifique incluant l'antenne. Des processeurs spécifiques intégrant les composants WiMAX sont également disponibles, mais ils ne sont encore que peu utilisés.

Pour voir se déployer des architectures WiMAX de bout en bout, il faudra attendre l'arrivée de processeurs multitechnologie permettant de se connecter à plusieurs antennes différentes simultanément.

Couche MAC

La couche MAC de WiMAX possède trois sous-couches :

- La sous-couche de convergence, qui permet d'utiliser la technologie IP que ce soit sur le relais de trames, Ethernet ou l'ATM.
- La sous-couche « Common part », qui permet l'accès au système et l'allocation de bande passante.
- La sous-couche sécurité, qui reprend un certain nombre d'éléments de chiffrement des techniques à l'œuvre dans les réseaux Wi-Fi.

La trame échangée entre l'équipement mobile et la station de base est illustrée à la figure I.5. Il s'agit d'une trame MAC générique, qui contient les requêtes de bande passante.

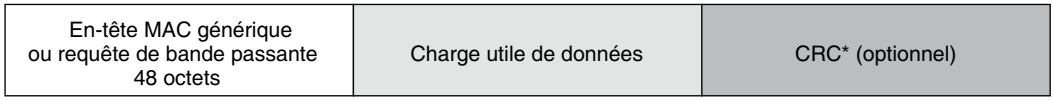


Figure I.5

La trame MAC WiMAX

Cette trame est composée de trois parties : l'en-tête, qui est soit un en-tête MAC générique, soit une requête de bande passante. La longueur de l'en-tête est de 48 octets. Viennent ensuite les données à transporter et une zone de détection d'erreurs optionnelle.

L'en-tête est illustré à la figure I.6.

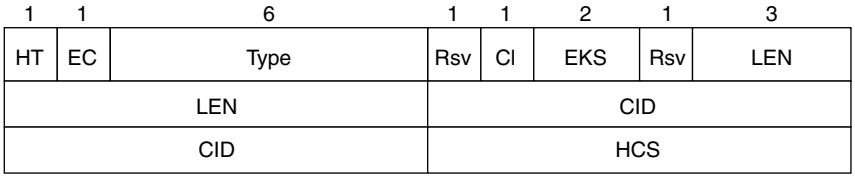


Figure I.6

En-tête de la trame MAC de WiMAX

Les valeurs possibles des différents champs sont les suivantes :

- Le bit HT est égal à 0 si l'en-tête est générique et à 1 si c'est une demande de bande passante.

- Le bit EC indique si la trame est chiffrée : si EC=0 les informations transportées ne sont pas chiffrées. Si EC=1, l'information est chiffrée. Il est à noter que EC doit être égal à 0 si HT=1.
- Le type, sur 6 bits, indique ce que contient le champ d'information. Si le premier bit est égal à 1, le réseau est un réseau mesh. Si le deuxième est égal à 1 c'est qu'un algorithme de ARQ Feedback Payload est appliqué. Si le troisième est égal à 1, une fragmentation du champ d'information ou bien une compression est acceptée. Les deux bits suivants indiquent si la fragmentation ou la compression est effectivement utilisée. Le sixième bit indique si un algorithme de Fast Feedback est utilisé.
- Les bits Rsv (reserved) sont positionnés à 0.
- Le bit CI est un indicateur d'existence d'un CRC. Si CI=0, il n'y a pas de CRC ; si CI=1, la zone de détection d'erreur CRC est présente dans la trame.
- La zone EKS (Encryption Key Sequence) n'a une valeur à prendre en compte que si EC=1. Dans ce cas, elle indique si une clé de chiffrement du trafic est utilisée, la clé TEK (Traffic Encryption Key), et s'il y a un vecteur d'initialisation.
- La zone LEN (Length) tient sur 11 bits, trois dans le deuxième octet et les huit bits du troisième octet. Cette zone indique la longueur en octets de la trame en y incluant l'en-tête et le CRC s'il y en a un.
- Le champ de deux octets CID (Connection Identifier) indique l'identificateur de la connexion.
- Le champ HCS (Header Check Sequence) sert de détection d'erreur pour l'en-tête. Le polynôme générateur est x^8+x^2+x+1.

En cas de demande de bande passante, l'en-tête se présente sous la forme illustrée à la figure I.7.

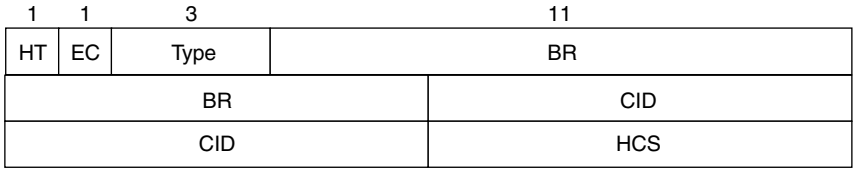


Figure I.7

Format de l'en-tête pour une demande de bande passante

Le champ HT est égal à 1 et le champ EC à 0 puisqu'il ne doit pas y avoir de chiffrement. Le champ Type indique le type de bande passante demandée par la trame. Pour le moment, seules sont admises les valeurs 000, pour indiquer une valeur incrémentale, et 001, pour une valeur agrégée. Le champ BR (Bandwidth Request) indique la demande d'une bande passante pour la voie montante en nombre d'octets. Cette demande n'inclut pas les overheads qui proviendraient de la couche physique.

La couche MAC comporte de nombreuses trames de gestion : quarante-neuf sont indiquées dans la norme IEEE 802.16-2004. La trame possède dans ce cas deux champs, le premier pour indiquer le type de message de gestion et le second pour préciser le contenu de l'information de gestion transportée.

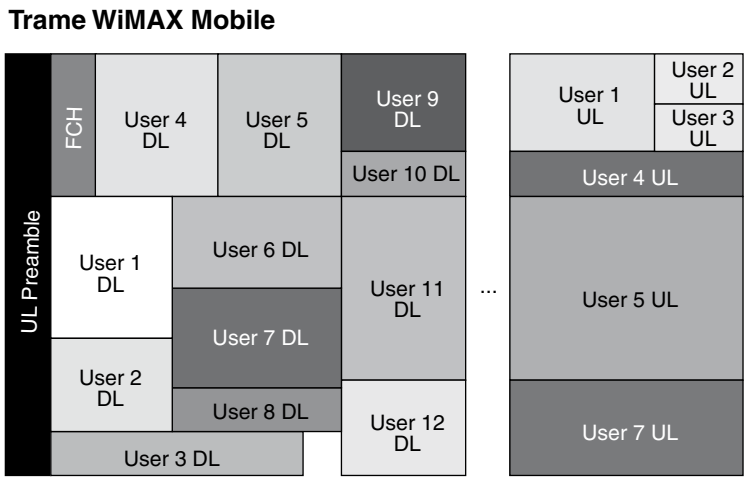
WiMAX mobile

WiMAX mobile correspond à la version mobile de WiMAX fixe. Il existe cependant d'importantes différences entre les deux technologies.

Dans WiMAX mobile, la couche physique OFDM donne naissance à un partage du support de type SOFDMA (Scalable OFDMA), dans lequel les clients prennent un ensemble de fréquences de l'OFDM pendant un certain nombre de tranches. Cette solution permet d'améliorer fortement l'utilisation du canal en récupérant des fréquences ou des tranches inutilisées.

La figure I.8 illustre cette technique d'accès de WiMAX mobile.

Figure I.8
Technique d'accès de WiMAX mobile



À un instant donné, plusieurs utilisateurs se partagent les fréquences du canal de communication. Ce partage s'effectue en fonction des besoins et des classes de clients. L'ordonnancement optimal n'est pas toujours simple à trouver, d'autant que certaines fréquences peuvent avoir un meilleur rendement grâce à une qualité supérieure de leur canal.

La couverture peut être améliorée par des antennes directives. WiMAX mobile utilise la diversité d'antenne ainsi qu'une méthode de retransmission automatique (H-ARQ). Cette technique de retransmission permet de garder en mémoire les paquets erronés de telle sorte que la confrontation de plusieurs paquets erronés puisse être suffisante pour rétablir le paquet correctement. Cette technique est fondamentalement différente de celles qui

retransmettent les paquets jusqu'à ce que le paquet arrive correctement en entier. Ces techniques sont également utilisées dans les réseaux de mobiles HSDPA et HSUPA.

La couverture et les débits, c'est-à-dire la diversité qui permet soit d'augmenter le débit, soit la qualité de la communication, sont également améliorés par l'utilisation du MIMO. De plus, différentes technologies de codage de nouvelle génération sont utilisées, comme les turbocodes et les LDCP (Low Density Parity Check). Ces solutions permettent d'adapter les communications d'un terminal vers l'antenne de l'opérateur en tenant compte de leurs caractéristiques propres et de la qualité de la transmission, lesquelles sont surtout dépendantes de l'éloignement de l'antenne et des atténuations dues au champ électromagnétique.

Dans WiMAX mobile, une classe de trafic supplémentaire a été introduite pour prendre en charge la parole téléphonique compressée de débit variable. Il s'agit de l'ertPS (enhanced real-time Packet Service). Cette classe correspond à de la téléphonie dans laquelle une compression rend le débit variable ou dans laquelle les silences sont supprimés de telle sorte que le débit devienne également variable. Les paramètres de qualité de service sont Maximum Sustained Traffic Rate, Minimum Reserved Traffic Rate, Maximum Latency Tolerated Jitter et Request/Transmission Policy. Ces paramètres sont les mêmes que dans l'UGS.

Une autre amélioration importante de WiMAX mobile provient de la compression des trames et plus généralement de l'utilisation intensive de la classe ertPS. Ces améliorations sont illustrées à la figure I.9.

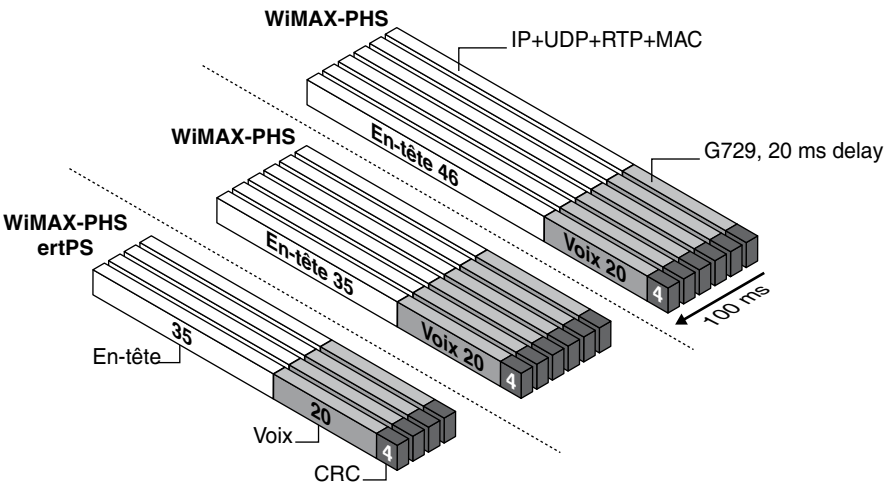


Figure I.9

Améliorations de WiMAX mobile

La première partie de la figure (en haut) illustre la transmission dans WiMAX (fixe) : les en-têtes font 46 octets de long, la zone de détection d'erreur (CRC 4), fait 4 octets et

le paquet (Voix) 20 octets de téléphonie. Dans la version WiMAX améliorée, WiMAX-PHS, l'en-tête est compressé, ce qui permet de faire descendre sa longueur de 46 à 35 octets. La partie basse de la figure illustre l'utilisation de la classe ertPS, qui permet de ne rien transmettre pendant les silences.

Comparaison avec les autres technologies

La figure I.10 situe la technologie WiMAX mobile par rapport aux versions UMTS et cdma2000, qui sont ses concurrentes directes. La différence fondamentale entre elles provient de la partie RAN (Radio Access Network). Dans les versions actuelles de l'UMTS ou du cdma2000, la technologie ATM est fortement utilisée pour l'optimisation de l'utilisation des supports physiques. L'AAL2 permet grâce à ses microtrames de bien remplir les trames ATM. Ce n'est pas le cas des paquets IP, qui ne permettent pas d'utiliser au mieux les capacités de transmission des supports fixes des réseaux WiMAX. Les paquets IP dans les techniques 3G (UMTS et cdma2000) sont transportés en tant qu'éléments binaires. Dans la solution WiMAX mobile, l'architecture est nativement Ethernet et IP.

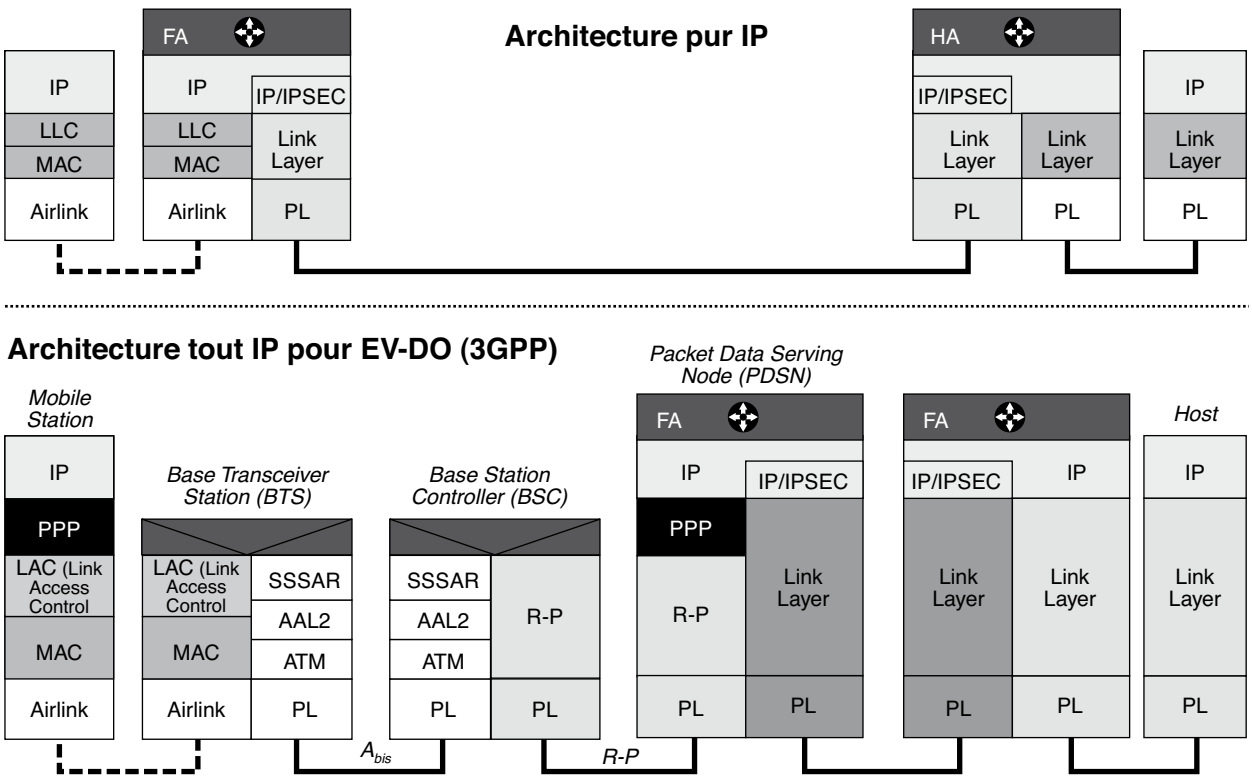


Figure I.10

Comparaison des technologies UMTS/cdma2000 et WiMAX mobile

La comparaison de ces deux architectures illustre la simplicité de WiMAX mobile mais aussi la difficulté à garantir la qualité de service si les canaux ne sont pas de bonne qualité, puisque c'est l'environnement Ethernet/IP qui doit prendre en charge la communication.

Globalement, la compétition entre les deux technologies risque d'être très forte puisque l'objectif est le même : réaliser du multimédia en mobilité avec des débits de quelques mégabits par seconde.

La différence fondamentale entre WiMAX fixe et WiMAX mobile réside dans la gestion des handovers. Trois mécanismes ont été définis dans la norme avec une latence inférieure à 50 ms :

- Hard handoff : le passage d'une cellule à une autre est instantané, et à aucun moment le terminal n'est en communication avec les deux cellules simultanément.
- FBSS (Fast Base Station Switching) : la connexion reste maintenue avec le réseau cœur (core network).
- MDHO (Macro Diversity Handover) : possibilité de réaliser un handover sans couture (*seamless handoff*) qui n'est pas visible du terminal.

Le tableau I.1 compare les caractéristiques de WiMAX mobile à celles des technologies cellulaires de même génération, c'est-à-dire HSDPA/HSUPA et 1x EV-DO Rev A.

Tableau I.1 • Comparaison des techniques cellulaires de nouvelle génération

Attribut	1X EV-DO REVA	HSDPA/HSUPA	WIMAX MOBILE
Standard de base	cdma2000/IS 95	WCDMA	IEEE 802.16e-2005
Méthode de duplexage	FDD	FDD	TDD
Canal descendant	TDM	CDM-TDM	OFDMA
Canal montant	CDMA	CDMA	OFDMA
Largeur de bande du canal	1,25 MHz	5 MHz	5, 7, 8,75, 10 MHz
Taille de la trame descendante	1,67 ms	2 ms	5 ms
Taille de la trame montante	6,67 ms	2,1 ms	5 ms
Modulation sur le canal descendant	QPSK, 8PSK, 16QAM	QPSK, 16QAM	QPSK, 16QAM, 64QAM
Modulation sur le canal montant	BPSK, QPSK, 8PSK	BPSK, QPSK	QPSK, 16QAM
Codage	Turbo	CC, Turbo	CC, Turbo
Vitesse maximale du canal descendant	3,1 Mbit/s	14 Mbit/s	32, 46 Mbit/s
Vitesse maxilae du canal montant	1,8 Mbit/s	5,8 Mbit/s	7, 4 Mbit/s
H-ARQ	Fast 4-channel Synchronous IR	Fast 6-channel Asynchronous CC	Multi-channel Asynchronous CC
Ordonnancement	Fast scheduling sur le canal descendant	Fast scheduling sur le canal descendant	Fast scheduling sur le canal descendant et montant
Handover	Virtual Soft Handover	Network Initiated hard handover	Network optimized hard hanover
MIMO	Simple Open Loop Diversity	Simple Open&Closed Loop Diversity	STBC, SM
Beamforming	Non	Non	Oui

Comme on peut le voir sur ce tableau, de nombreuses propriétés sont communes aux différentes technologies de nouvelle génération correspondant à des réseaux commercialisés

en 2007-2008. Parmi ces technologies, AMC (Adaptive Modulation and Coding), H-ARQ (Hybrid ARQ), FS (Fast Scheduling) et BEH (Bandwidth Efficient Handover).

La première caractéristique commune concerne le codage et la modulation adapatative en fonction de la qualité du canal. La technologie proposée par WiMAX est plus puissante, grâce à la possibilité d'utiliser la technologie AMC sur des paquets de taille variable, aussi bien dans le sens montant que descendant.

La technique de correction des erreurs par une méthode H-ARQ permet, en conservant les paquets erronés, de déterminer le paquet exact sans que l'ensemble des éléments binaires doivent arriver correctement au destinataire. Les techniques de H-ARQ CC (Chase Combining) et H-ARQ IR (Incremental Redundancy) sont les plus utilisées. Dans la première, les paquets retransmis sont les mêmes que ceux transmis la première fois. Dans la seconde, le paquet erroné peut être retransmis à la suite de nouveaux paquets du même flot. Cette solution est beaucoup plus complexe, mais elle permet de continuer à transmettre sans attendre la réussite d'une retransmission.

L'algorithme Fast Scheduling permet de distribuer l'allocation de la bande passante aux clients en tenant compte de la qualité du canal. Il est beaucoup plus efficace de servir les clients qui disposent d'un bon canal que de s'attarder sur ceux dont le canal est de mauvaise qualité.

Les solutions pour effectuer du « Bandwidth Efficient Handover » sont diverses. La technique du soft handover pourrait paraître la plus séduisante. Elle n'est toutefois pas toujours la meilleure, car elle oblige l'équipement terminal à être connecté simultanément sur deux stations de base. Cela exige une gestion de la bande passante plus complexe. Le hard handover est généralement plus efficace et demande moins de ressources.

WiBro et IEEE 802.20

WiBro est une solution très semblable à WiMAX développée par la Corée du Sud au tout début des années 2000. En 2004, Intel et LG Electronics se sont mis d'accord pour réaliser une interopérabilité entre les deux techniques. La solution est fortement orientée WiMAX mobile puisque WiBro a choisi de modifier son interface radio pour prendre le SOFDMA.

Le groupe de travail IEEE 802.20 a un objectif semblable. Formé pour réaliser un réseau MBWA (Mobile Broadband Wireless Access), il devait venir en complément de WiMAX, conçu au départ pour être uniquement fixe. Lorsque le groupe 802.16e s'est mis en place, le groupe 802.20 a été suspendu afin de ne pas dupliquer les efforts. Finalement, il a été remis en marche pour aboutir à une proposition de standard pour la très grande mobilité, jusqu'à 500 km/h, et le très haut débit.

Une proposition de Kiocera a été normalisée dans le cadre d'un groupe très restreint d'industriels. En réponse, les industriels de WiMAX ont lancé le groupe IEEE 802.16m et WiMAX phase 2 avec un objectif similaire à celui du groupe 802.20. Comme l'environnement WiMAX est le sixième système inclus dans l'IMT 2000, la technologie IEEE 802.20 n'a quasiment aucune chance de se développer.

WRAN

Le groupe de travail IEEE 802.22 a démarré ses activités en 2004 dans l'objectif de réaliser un réseau hertzien régional. Les bandes de fréquences utilisées viennent en premier lieu du dividende numérique, c'est-à-dire des bandes de fréquences qui seront libérées lorsque la télévision passera totalement et définitivement en numérique. En France, c'est prévu pour 2010. Dans le reste du monde, cela devrait s'étaler entre aujourd'hui et 2015.

Les études portent sur les « canaux blancs » de la télévision, c'est-à-dire les fréquences ou les bandes de télévision qui ne sont pas utilisées ou qui le sont très mal. L'idée est d'introduire une transmission opportuniste qui utilise les bandes inutilisées à certains instants par la télévision en prenant soin de ne pas brouiller les canaux de télévision.

Les fréquences utilisées se situent en dessous de 1 GHz. Elles possèdent les propriétés des bandes de télévision : pénétration par les murs, très bonne portée et haut débit.

Les clients seront munis de systèmes GPS ou Galileo pour localiser l'émetteur. Après interrogation d'une base de données centrale, ils recevront la fréquence sur laquelle ils peuvent émettre avec la puissance et la directivité voulues.

Ces principes de radio « cognitive » sont étudiés depuis quelques années afin d'utiliser beaucoup mieux le spectre. L'état du réseau et le comportement de l'utilisateur pourront impliquer une modification de la fréquence, de la puissance, etc.

En résumé, la radio cognitive définit la possibilité d'utiliser une bande avec licence sans que l'opérateur qui l'utilise soit gêné. Comme de nombreuses bandes sont peu utilisées, il est possible de récupérer une bande passante considérable.

On peut définir deux types de radio cognitive :

- Full Cognitive Radio, où tous les paramètres utilisables le sont.
- Spectrum Sensing Cognitive Radio, où seulement la fréquence radio utilisée est prise en compte.

Deux sous-ensembles sont également discernables :

- utilisation de la radio cognitive dans un environnement sous licence, comme celle proposé par l'IEEE 802.15.2 ;
- utilisation des fréquences d'une bande sans licence, comme celle proposée par l'IEEE 802.19.

La radio cognitive a été surtout développée dans le cadre de la radio logicielle (Software-Defined Radio) et s'est surtout intéressée à la solution Spectrum Sensing Cognitive Radio dans les bandes de télévision. La difficulté essentielle est évidemment de détecter l'utilisation de la bande par son détenteur légal, puis d'arrêter les émissions secondaires et détecter que la bande est de nouveau non utilisée. La détection de l'énergie n'est pas vraiment suffisante pour être sûr que l'on ne va pas perturber les signaux licenciés. L'utilisation s'effectue par une technologie OFDM, dans laquelle seules les sous-bandes correspondant aux bandes libres sont utilisées.

IEEE 802.22 travaillant en mode point-à-multipoint, un signal peut être diffusé sur une large surface et s'adresser simultanément à un ensemble de points. Le système est formé

de stations de base, ou BS (Base Station), et d'équipements terminaux. La station de base reçoit de la part des équipements terminaux des rapports réguliers de l'écoute des porteuses. À partir de ces informations, la station de base peut décider de changer ou non de fréquence et définir la puissance d'émission des équipements terminaux.

Le support physique travaille en OFDM et détermine les sous-bandes à utiliser, et le codage de la modulation. Les essais montrent que l'émission sur un canal de télévision de la station de base permet d'acheminer une vingtaine de mégabits par seconde sur 30 km.

Annexe J

13. Les réseaux de niveau physique)

Cette annexe revient sur la transmission des trames ATM et sur les supports physiques qui ont été fortement utilisés sur les supports plésiochrones. Elle aborde ensuite une interface de signalisation du monde de la fibre optique avant de terminer par la technique PON (Passive Optical Network), qui est utilisée par de nombreux grands opérateurs sur la boucle locale.

Transmission des trames ATM

La transmission de trames ATM illustre ce qui se passe dans la couche 2 lorsque la longueur de la trame est constante. La trame ATM est également appelée *cellule* pour bien dénoter ce cas particulier. L'en-tête des cellules contient une zone de 1 octet ayant pour rôle de protéger les 4 octets de supervision précédents. Il s'agit de la zone HEC (Header Error Control). Elle permet de détecter les erreurs de transmission et d'effectuer automatiquement la correction si le nombre d'erreur est limité à un. Lorsque les erreurs arrivent de façon aléatoire, la plupart du temps avec une probabilité très faible, le taux d'erreur est excellent. Il arrive que le taux d'erreur s'emballe lorsqu'une forte perturbation des signaux en cours de transmission se produit dans un laps de temps très court, générant une succession de cellules en erreur. C'est la raison pour laquelle on préfère, dès que l'on découvre plus de deux erreurs sur une même cellule, que le HEC devienne détecteur plutôt que correcteur de l'erreur, puisqu'il y a toutes les chances pour que la zone d'information soit erronée.

Le HEC permet également de délimiter des cellules. Le récepteur est constamment à la recherche des 4 octets, correspondant à la zone HEC. Dès qu'il trouve une séquence qui satisfait le HEC, il vérifie que les zones correspondantes des cinq cellules suivantes sont également correctes. Si tel est le cas, le récepteur passe en mode synchronisé. S'il ne réussit pas à cadrer le HEC avec les cinq cellules suivantes, il reste dans un état non synchronisé. Il faut sept détections consécutives d'erreur pour considérer que le cadrage est perdu. Les valeurs 5 et 7 sont valables pour une transmission synchrone. Pour une transmission asynchrone, ces valeurs sont définies respectivement à 6 et 8.

L'adaptation au débit synchrone de la liaison permet de synchroniser les horloges de l'émetteur et du récepteur, de sorte que les bits émis à la vitesse de l'horloge de l'émetteur puissent être récupérés exactement au bon moment par le récepteur. Ces deux fonctions dépendent du support physique utilisé pour transmettre la trame.

L'acheminement des cellules ATM par l'intermédiaire de trames SONET ou SDH est surtout réservé aux opérateurs et aux grands réseaux. Deux solutions s'imposent actuellement : celle du transport des trames sur les lignes exploitées par les opérateurs et celle fondée sur le transport direct de la trame sur le support physique, sans aucune trame sous-jacente. La solution la plus simple pour une mise en œuvre rapide consiste à utiliser des liaisons PDH (Plesiochronous Digital Hierarchy). En Europe, il est possible d'acheminer les cellules sur des liaisons à 2 et 34 Mbit/s, suivant les recommandations G.804 et G.832 de l'UIT-T. Les cellules sont insérées dans le corps des trames qui circulent toutes les 125 µs. Un adaptateur est nécessaire à cette insertion afin d'ajuster la transmission des cellules à la vitesse de l'interface et à insérer des cellules vides pour maintenir la synchronisation.

L'interface standard de l'ATM

Le standard le plus classique de l'ATM correspond à un débit de 155 Mbit/s. Grâce au codage 8B/10B, qui utilise 10 bits pour transporter 8 bits de l'utilisateur, le débit peut atteindre 194,4 Mbit/s. La gestion du support physique est effectuée par des cellules OAM (Operation And Maintenance). On trouve une cellule de gestion après vingt-six cellules d'information transmises par l'émetteur. Le débit réel ATM descend de ce fait à 149,76 Mbit/s.

Les supports plésiochrones

Pour parvenir au multiplexage simultané de plusieurs paroles téléphoniques sur un même circuit, les Américains ont adopté un standard permettant de multiplexer 24 voies de 64 Kbit/s sur un support à 1 544 Kbit/s. Ce canal est nommé DS-1. Les Européens ont répondu à cette technique par le canal E-1, un multiplexage de 30 canaux de parole sur un support à 2 048 Mbit/s. À partir de ce multiplexage de base, toute une hiérarchie a été définie, qu'elle soit multiple du canal de base, comme dans le cas européen, ou un peu plus complexe, comme dans le cas américain, en raison d'une zone de supervision dépendant du débit.

Ces hiérarchies sont appelées PDH (Plesiochronous Digital Hierarchy). La hiérarchie européenne est la suivante :

- E-1 = 2 Mbit/s
- E-2 = 8 Mbit/s
- E-3 = 34 Mbit/s
- E-4 = 140 Mbit/s
- E-5 = 565 Mbit/s

La hiérarchie américaine est assez semblable mais moins régulière. Elle ne correspond pas à un multiple du canal de base, car les bits de synchronisation ne sont pas proportionnels au nombre de voies transportées. La racine *plesio* de *plesiochronous* vient du grec et signifie presque.

Les supports physiques étant passés en mode numérique, une hiérarchie spécifique a dû être développée sous le nom de SDH (Synchronous Digital Hierarchy) en Europe et de SONET (Synchronous Optical Network) en Amérique du Nord. Cette nouvelle hiérarchie prend toujours en compte la numérisation de la parole avec un échantillonnage toutes les 125 µs, mais elle est complètement synchrone. Une trame, d'une longueur dépendant de la vitesse, est émise toutes les 125 µs. SONET et SDH sont les deux techniques utilisées pour acheminer des transmissions numériques aussi différentes que la parole et les données. Cette technique peut donc transporter tous les types de paquets ou de trames, trame ATM, paquet IP, trame Ethernet, etc.

SONET est une interface standardisée par l'ANSI (American National Standards Institute), l'organisme de normalisation nord-américain. Son rôle était au départ d'introduire un très grand nombre de voies téléphoniques sur un même support physique de façon à relier entre eux les réseaux de deux opérateurs.

SDH est une généralisation de SONET normalisée par l'UIT-T, qui donne une définition de la zone de données qui traverse l'interface beaucoup plus précise que celle introduite dans SONET. Cette zone de données porte le nom de *container*.

La hiérarchie plésiochrone

Le standard PDH, en français hiérarchie plésiochrone, c'est-à-dire presque synchrone, a été défini par les organismes de normalisation s'occupant du téléphone pour faire transiter simultanément sur une même ligne physique plusieurs voies téléphoniques. Les termes « presque synchrone » indiquent que cette hiérarchie travaille en synchrone. Cependant, l'instant de départ de la communication est asynchrone. En d'autres termes, la communication est synchrone, une fois l'instant de départ décidé.

Des canaux de différents débits ont été définis :

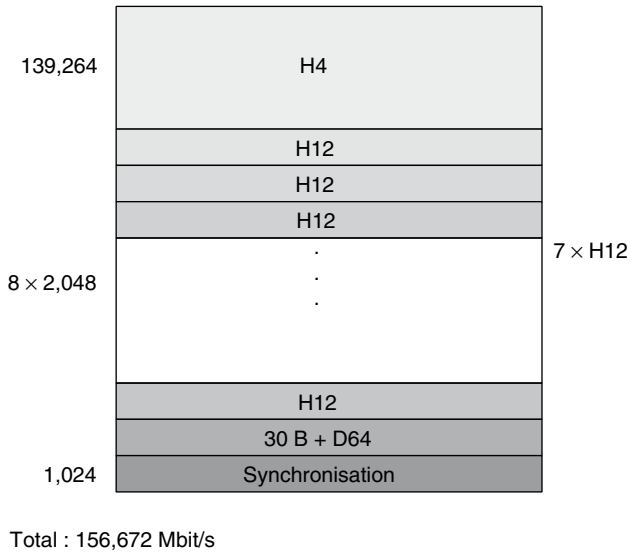
- B : canal circuit à 64 Kbit/s, qui correspond à une voie téléphonique.
- H_0 : canal circuit à 384 Kbit/s, ce qui représente une superposition de 6 canaux B.
- H_{11} : canal circuit à 1 472 Kbit/s, c'est-à-dire une superposition de 23 canaux B.
- H_{12} : canal circuit à 1 920 Kbit/s, c'est-à-dire une superposition de 30 canaux B.

- H_2 : canal à 6,312 Mbit/s ou 8,448 Mbit/s.
- H_3 : canal à 32,064 Mbit/s ou 34,368 Mbit/s ou 44,736 Mbit/s.
- H_4 : canal à 97,728 Mbit/s ou 139,264 Mbit/s.

Une autre solution, qui a été développée sans être normalisée, consiste à superposer différentes catégories de circuits. En particulier, le multicircuit illustré à la figure J.1 a souvent été cité comme une référence pour l'intégration de services à très haute vitesse. Ce multicircuit est une superposition de dix circuits : un circuit H4, sept circuits H12 et deux canaux B. On a ajouté à cette superposition de circuits un canal D, canal multipoint en commutation de paquets, et un canal de synchronisation. Au total, il y a donc douze circuits qui doivent transiter simultanément sur le multicircuit.

Figure J.1

Exemple de canal multicircuit pour l'intégration de services à très haute vitesse



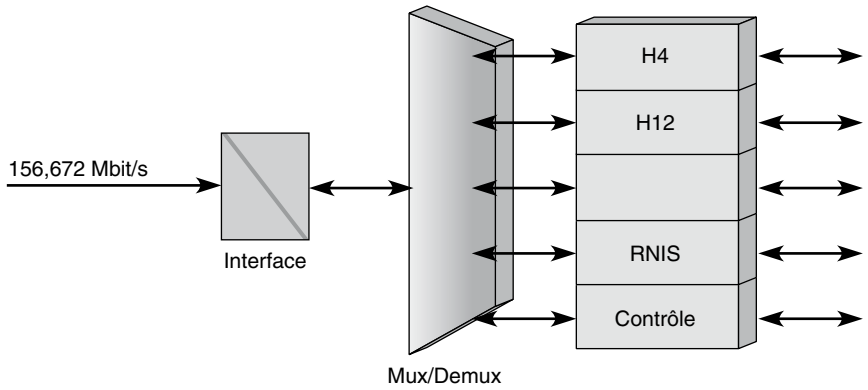
La difficulté principale de ce multicircuit réside dans la gestion du circuit multipoint. Il faut développer une interface unique avec l'utilisateur susceptible de multiplexer les données provenant des différentes sources et de les démultiplexer dans le sens opposé.

La figure J.2 illustre ce multiplexage. Sur la voie de droite arrive un flot à 156,672 Mbit/s. Ce flot doit être décomposé en dix sous-flots, plus des informations de contrôle et de synchronisation. Dans le sens contraire, les douze flots qui arrivent simultanément sur le multiplexeur doivent trouver leur place sur la liaison à 156,672 Mbit/s. Cela implique une mise en série des éléments binaires. En d'autres termes, les bits arrivant en même temps sur le multiplexeur doivent se placer les uns derrière les autres.

La gestion du multiplexage des canaux est complexe, ce qui occasionne la perte d'une partie de la bande passante pour des raisons autres que la transmission des données. La commutation multicircuit est la technique utilisée dans le RNIS bande étroite. Dans l'interface de base, on fournit à l'utilisateur deux canaux B à 64 Kbit/s, qui doivent être

partagés entre les différents équipements terminaux de l'utilisateur : combiné téléphonique, PC, fax, terminal vidéotex, etc.

Figure J.2
Exemple de multiplexage-démultiplexage

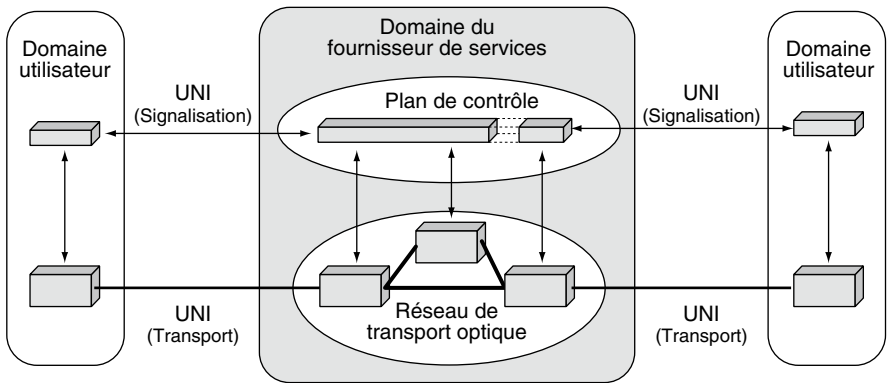


La signalisation OIF (Optical Internetworking Forum)

Si les opérateurs de télécommunications ont tous adopté la technique DWDM pour le cœur de leur réseau, le contrôle des grands réseaux reste une affaire délicate. Pour le moment, la solution trouvée est essentiellement liée au surdimensionnement.

L'interconnexion de deux réseaux d'opérateurs distincts pose problème à cause de leurs systèmes de contrôle respectifs, qui sont généralement incompatibles. Une solution possible à ce problème consiste à adopter MPLS (MultiProtcol Label-Switching) et GMPLS (Generalized MPLS) pour uniformiser les processus de gestion. L'OIF (Optical Internetworking Forum) propose d'ailleurs sous le nom d'OIF UNI 1.0 une signalisation pour les réseaux optiques permettant d'établir une connexion optique dynamiquement en utilisant la procédure de signalisation de GMPLS. Cette signalisation est illustrée à la figure J.3.

Figure J.3
Introduction d'une signalisation OIF UNI entre le service et l'utilisateur



En plus de la signalisation, les spécifications de l'UNI contiennent deux autres fonctionnalités destinées à simplifier la gestion du réseau optique. La première concerne un mécanisme de découverte des voisins, qui permet aux deux extrémités d'une fibre optique de s'identifier et de construire une carte complète du réseau. La seconde est un mécanisme de découverte des services disponibles dans le réseau optique. Globalement, l'interface UNI simplifie le fonctionnement du réseau optique, engendrant une baisse sensible des coûts de contrôle et de gestion.

L'interface permettant la signalisation OIF UNI est une révolution dans le monde des interfaces, en ce qu'elle autorise la mise en place d'une connexion adaptée à l'application.

EPON (Ethernet Passive Optical Network)

Une nouvelle direction de développement a vu le jour avec la migration de la technologie Ethernet vers les réseaux métropolitains et étendus. La trame Ethernet est de fait une des plus efficaces qui soit, avec son préambule simple, qui permet de reconnaître facilement le début de la trame. De plus, les vitesses des coupleurs Ethernet s'étalant de 10 Mbit/s à 10 Gbit/s, il est facile de trouver la bonne valeur pour un réseau de type métropolitain.

Une raison supplémentaire à l'adoption de la trame Ethernet pour les longues distances réside dans l'utilisation massive de cartes coupleurs Ethernet dans les entreprises. Aujourd'hui, plus de 98 % des réseaux d'entreprise sont de type Ethernet. Les cartes coupleurs génèrent une trame Ethernet, et il semble naturel de garder cette trame tout au long du chemin plutôt que de la transformer en d'autres trames avant de revenir à la trame Ethernet dans le réseau d'arrivée.

Le transfert de trames Ethernet présente un dernier avantage car il peut être de type routé ou commuté. Pour la commutation, il suffit de considérer l'adresse Ethernet comme une référence associée à la route menant à la carte coupleur portant cette adresse et d'y ajouter une vraie référence, le shim-label. Nous examinons cette solution en détail au chapitre 15, dédié à MPLS.

La technologie PON (Passive Optical Network) a été définie pour réaliser des boucles locales sur fibre optique. C'est une technique point-à-multipoint sans élément actif, c'est-à-dire alimenté électriquement. Elle offre une large couverture à haut débit et une maintenance réduite, puisqu'il n'y a pas d'élément actif. La normalisation de la technologie EPON est effectuée par le groupe IEEE 802.3ah. Ce groupe vise plusieurs objectifs, dont celui d'introduire Ethernet dans la boucle locale sous le nom d'EFM (Ethernet in the First Mile). L'allocation de bande passante s'effectue par le biais d'un algorithme spécifique, développé par les équipementiers, en utilisant la méthode d'accès TDMA (Time Division Multiple Access), qui définit des slots à l'intérieur d'une longueur d'onde.

Un EPON permet d'émettre des trames Ethernet à partir d'unités de réseau optique, ou ONU (Optical Network Unit), vers une tête de réseau, ou OLT (Optical Line Termination). La tête de réseau est connectée à un FAI pour permettre l'émission des paquets IP encapsulés dans les trames Ethernet.

La figure J.4 illustre une architecture d'EPON en boucle.

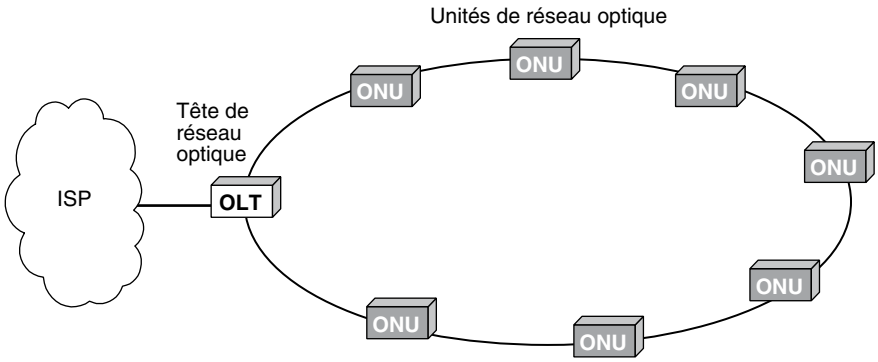


Figure J.4
Architecture d'un EPON

Le standard FSAN (Full Service Access Network) définit un réseau d'accès en fibre optique qui utilise la technologie ATM. Un GPON utilise une technique très similaire, mais avec des trames OTN à la place de trames ATM.

Annexe J

14 : Les réseaux Ethernet et ATM)

La normalisation des réseaux ATM, à la fin des années 1980, avait pour ambition de proposer une solution capable de remplacer tous les autres réseaux et de permettre le passage de la parole téléphonique et de toutes les applications à fortes contraintes de temps réel. Cette solution a pris pour nom la commutation de cellules afin de la différencier de la commutation de trames classique.

Avant l'ATM, le relais de trames peut être vu comme une solution pré-ATM puisque assez similaire mais pas avec toutes les possibilités de qualité de service de l'ATM.

Cette annexe présente d'abord le relais de trames en tant que solution pré-ATM puis examine la commutation de cellules ATM avant de décrire l'architecture générale des réseaux ATM et les protocoles qui y sont mis en œuvre.

Le relais de trames

Le relais de trames a pris la succession du protocole X.25 en faisant descendre la commutation du niveau 3 au niveau 2. Dans le même temps, il a été doté de nouvelles fonctionnalités qui l'apparentent à une technologie pré-ATM, notamment la possibilité de garantir une qualité de service. Les sections qui suivent examinent ces fonctionnalités.

La commutation de niveau trame

L'objectif d'une commutation de niveau trame est d'améliorer les performances de la commutation de niveau paquet, comme X.25, en diminuant le nombre de niveaux de

l'architecture à traverser à chaque nœud. En plaçant la commutation au niveau trame de l'architecture, on n'est pas obligé de décapsuler la trame pour retrouver le paquet. En effet, dans un transfert de paquets, on attend de recevoir correctement une trame, avec des retransmissions potentielles. Une fois la trame décapsulée, on examine le paquet pour déterminer la direction dans laquelle on va l'émettre.

La commutation implique la mise en place d'un chemin ou circuit virtuel, qui est appelé liaison virtuelle dans le relais de trames puisque nous sommes au niveau 2. Des références placées dans la structure de la trame sont utilisées pour commuter les trames. Sans signalisation préalable, la liaison virtuelle est permanente, et les références sont posées une fois pour toutes pour toute la période d'abonnement.

Dans le relais de trames, les abonnements sont généralement effectués sur une base mensuelle. Ces liaisons permanentes peuvent être considérées comme des liaisons spécialisées, ou circuits, attribuées par un opérateur et mises en place à la demande d'un utilisateur pour aller à un point précis. Les ressources y sont affectées une fois pour toutes, et seules les deux extrémités peuvent les utiliser.

L'avantage d'un circuit virtuel permanent est de ne pas utiliser les ressources du réseau lorsque les deux utilisateurs sont silencieux, à l'exception des tables de commutation, lesquelles restent ouvertes en permanence.

Le relais de trames peut être considéré comme un cas particulier de commutation de trames, doté de simplifications supplémentaires permettant de gagner encore en débit. Les simplifications se trouvent principalement dans les algorithmes de reprise sur erreur et dans les contrôles de flux, qui ne sont effectués que dans les points extrémité. Dans le relais de trames, les contrôles d'erreur et de flux sont reportés aux extrémités de la connexion. Cette simplification du travail des nœuds intermédiaires est très importante puisqu'il n'y a plus à mettre en œuvre d'algorithmes complexes. On considère que l'on gagne en performance au moins un ordre de grandeur — multiplication par 10 du débit — pour une puissance d'équipement donnée par rapport à l'équivalent en commutation de paquets. Le débit de base du relais de trames est de 2 Mbit/s contre 64 Kbit/s dans une commutation de paquets de type X.25 avec des nœuds de même complexité.

La normalisation du relais de trames

La commutation de trames et le relais de trames ont été normalisés par l'ANSI et l'UIT-T dans le cadre du RNIS. La recommandation I.122 (Framework for Providing Additional Packet Mode Bearer Services) introduit les éléments de base. La principale recommandation technique se trouve dans le document Q.922 et figure également dans la recommandation I.441 ou dans le document T1.618 de l'ANSI. Elle limite à 2 Mbit/s le débit de cette technique de commutation. Dans les faits, rien n'empêche d'aller beaucoup plus vite. Cette limitation peut s'expliquer par le manque de visibilité à long terme de cette technique au moment de sa normalisation. En effet, la technique de transfert recommandée à l'époque étant l'ATM, le relais de trames n'était envisagé que comme une étape transitoire, capable de combler un trou de quelques années entre la commutation de paquets et la commutation de cellules ATM.

Un autre organisme, le Frame Relay Forum, ou FR Forum, a eu un impact important sur le relais de trames. Né du regroupement de quatre constructeurs, DEC, Northern Telecom, Cisco Systems et Stratacom, le FR Forum a surtout repris les recommandations de l'UIT-T, en modifiant parfois quelques éléments mais sans toucher aux principes de base. La différence principale avec la norme réside dans l'utilisation du relais de trames indépendamment du RNIS.

Deux modes, dénommés FR1 et FR2, sont décrits dans la normalisation. Dans le mode FR1, le contrôle de flux et la reprise sur erreur sont laissés à la charge de l'équipement terminal. Dans le mode FR2, ils sont effectués aux extrémités du réseau.

On peut considérer le relais de trames comme une amélioration décisive de la recommandation X.25, puisqu'il simplifie considérablement le travail des nœuds intermédiaires. Malgré cette simplification, on retrouve les mêmes services de transport de l'information, mais avec des capacités de transport bien supérieures.

Le relais de trames est bien adapté au transfert de fichiers de gros volume, aux applications interactives par bloc, comme les applications graphiques de CAO (conception assistée par ordinateur) ou d'images, ou encore au transport de voies haute vitesse multiplexant un grand nombre de voies basse vitesse.

La commutation de trames pure a rapidement été remplacée par le relais de trames dans les réseaux des opérateurs et est aujourd'hui inusitée pour le transport de données. Nous la présentons toutefois en premier de façon à conserver l'ordre chronologique d'introduction de ces techniques.

La commutation de trames (Frame Switching)

Comme expliqué précédemment, dans la commutation de trames, les trames sont transportées d'un bout à l'autre du réseau sans avoir à remonter au niveau paquet. Il faut utiliser un protocole de niveau trame suffisamment puissant pour permettre l'acheminement des trames en ne tenant compte que des informations de supervision disponibles dans la structure de la trame. En particulier, un adressage de niveau trame doit remplacer l'adressage de niveau paquet. De plus, les fonctions du niveau 2 doivent être maintenues.

Dans la commutation de trames et dans le relais de trames, il est nécessaire de retrouver les grandes fonctionnalités du niveau paquet, comme l'adressage, le routage et le contrôle de flux, reportées au niveau trame. Pour effectuer le transfert, on utilise l'adresse du niveau trame sans remonter au niveau paquet, contrairement à ce que préconise le modèle de référence. Cet adressage sert à ouvrir le circuit virtuel sur lequel les trames sont commutées. Le nom exact de ce circuit virtuel est liaison virtuelle, comme nous l'avons vu dans l'introduction de ce chapitre, puisque nous sommes au niveau 2. Nous revenons un peu plus loin sur le problème de l'adressage et de la mise en place des références.

L'architecture d'un réseau à commutation de trames est illustrée à la figure K.1. Cette figure montre que les nœuds de commutation intermédiaires ne possèdent que les deux premières couches de l'architecture du modèle de référence, à savoir la couche physique et la couche liaison utilisant le protocole Q.922 normalisé par l'UIT-T. Q.922 est le protocole

de niveau trame qui est mis en œuvre dans les réseaux à commutation de trames. Ce protocole utilise la trame LAP-F, que nous décrivons dans une section ultérieure.

Dans les nœuds de commutation, on cherche la référence de niveau 2 autorisant la commutation de la trame vers le destinataire. La zone de détection d'erreur portée par la trame est examinée à chaque nœud du réseau. En cas de détection d'erreur, une demande de retransmission est lancée, et la trame est retransmise à partir du nœud précédent.

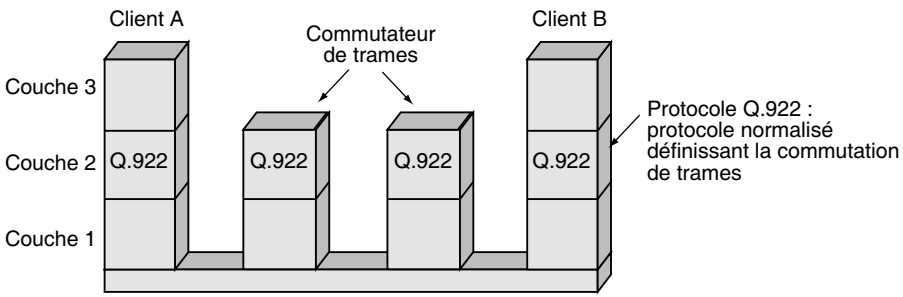


Figure K.1

Commutation de trames

Fonctionnement du relais de trames (Frame Relay)

Le relais de trames apporte une simplification supplémentaire à la commutation de trames. Dans les nœuds intermédiaires, les trames sont vérifiées grâce à une zone de détection d'erreur et détruites si une erreur est détectée. En revanche, il n'y a pas d'algorithme pour effectuer la récupération de la trame perdue. Les nœuds de commutation ne prennent donc en charge que les trames valides. La retransmission des trames erronées est effectuée par le nœud de sortie du réseau en demandant une retransmission à l'autre extrémité du réseau.

Cette solution permet de simplifier énormément les nœuds intermédiaires et d'atteindre des capacités de transmission se chiffrant en mégabit par seconde. Elle n'est toutefois viable que si le taux d'erreur est faible puisque les retransmissions sont beaucoup plus lentes que dans une reprise de nœud à nœud, comme cela se produit dans un transfert de niveau 3.

La normalisation du relais de trames s'appuie sur l'avis Q.922 de l'UIT-T et plus particulièrement sur le noyau de base de cette recommandation, Core Q.922. On utilise les fonctionnalités complètes de la recommandation aux extrémités de la connexion et celles du noyau dans les nœuds intermédiaires.

Les grandes fonctionnalités normalisées par cette recommandation sont les suivantes :

- Délimitation, alignement et transparence des trames.
- Multiplexage et démultiplexage des trames à l'aide du champ de référence.

- Inspection de la trame pour vérifier qu'elle possède un nombre entier d'octet avant insertion ou après extraction des 0 intégrés pour la transparence.
- Inspection de la trame pour vérifier qu'elle n'est ni trop courte, ni trop longue.
- Demande de retransmission dans les éléments extrémité de la connexion.
- Fonction de contrôle de flux de bout en bout.

Les deux dernières fonctions ne font pas partie du noyau et ne sont donc entreprises qu'aux extrémités de la connexion.

Le relais de trames a pour rôle de diminuer au maximum le temps passé dans les commutateurs en n'effectuant qu'un travail minimal, en l'occurrence l'examen de la zone de détection d'erreur et de la référence de niveau 2 et l'émission de la trame vers le nœud suivant.

Le relais de trames possède deux plans, c'est-à-dire deux réseaux logiques multiplexés sur un même réseau physique : le plan utilisateur et le plan de contrôle. Le plan utilisateur gère l'acheminement des trames qui transportent des données utilisateur tandis que le plan de contrôle se charge des trames qui transportent de la signalisation.

L'architecture du relais de trames en ce qui concerne le plan utilisateur est illustrée à la figure K.2. Nous verrons plus loin l'architecture pour les informations de supervision et de gestion. Dans cette figure, le niveau paquet est conservé aux deux extrémités et ce qui symbolise le relais de trames c'est la disparition d'une partie de la couche 2, correspondant aux reprises sur erreur, dans les nœuds intermédiaires. La partie de la couche 2 qui reste provient de la norme Q.922 de l'UIT-T et plus précisément le noyau de cette couche. La partie complémentaire de Q.922 se retrouve dans les nœuds extrémité. Cette partie complémentaire peut éventuellement être remplacée par une autre procédure spécifiée par l'utilisateur.

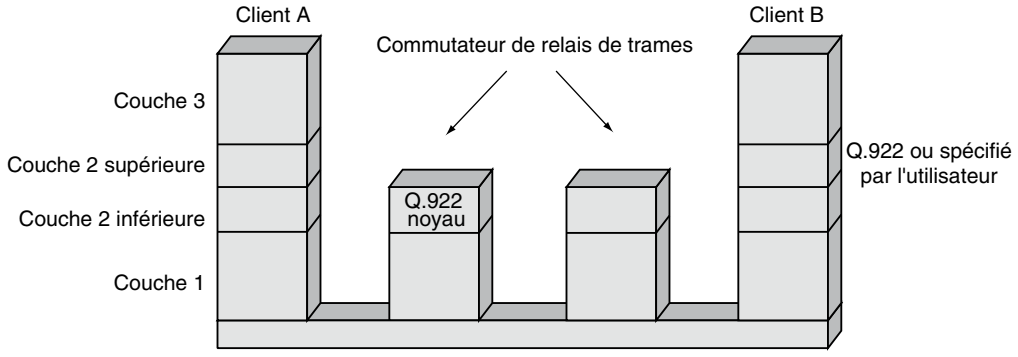


Figure K.2

Architecture du plan utilisateur du relais de trames

Le noyau de la recommandation Q.922, ou Q.922 Core, décrit les fonctions de base, la délimitation de la trame, la transparence par rapport aux délimiteurs, le multiplexage des

trames sur les liaisons physiques par un numéro de référence, appelé DLCI (Data Link Connection Identifier), la vérification du nombre d'octet, qui doit être un entier, et la vérification de la longueur totale de la trame.

La figure K.3 illustre l'architecture complète du relais de trames au niveau extrémité, c'est-à-dire les plans utilisateur et contrôle. La mise en place de la liaison virtuelle s'effectue en dehors du plan utilisateur par un plan spécifique, le plan de contrôle. La supervision du réseau en relais de trames doit être assurée par un environnement distinct de celui du réseau utilisateur, même si l'infrastructure de ce dernier est utilisée.

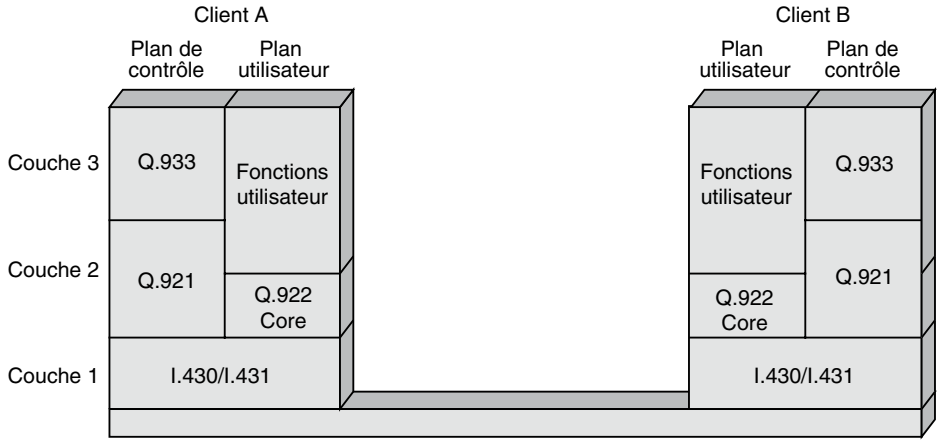


Figure K.3

Architecture complète du relais de trames

L'avis Q.922 de l'UIT-T

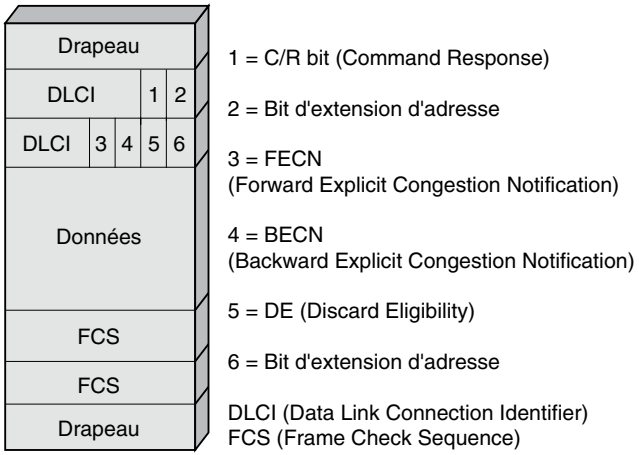
Le format de la trame véhiculée dans le relais de trames est illustré à la figure K.4. Cette trame correspond à celle du LAP-D légèrement modifiée pour tenir compte du contexte du relais de trames. La zone DLCI remplace les zones SAPI (Service Access Point Identifier) et TEPI (Terminal End Point Identifier), à l'exception des bits 3, 4 et 5. La zone de données peut atteindre 4 096 octets. Le drapeau est le même que dans la norme HDLC : 01111110. On utilise la procédure d'insertion de 0 en présence de la succession 011111, afin d'éviter de retrouver la valeur du drapeau à l'intérieur de la trame.

Dans le LAP-F (Link Access Protocol-Frame), la référence est spécifiée dans la zone DLCI. Ce champ compte 6 bits + 4 bits = 10 bits. Il peut donc y avoir jusqu'à $2^{10} = 1\,024$ valeurs pour le DLCI. Cette quantité est notoirement insuffisante si l'on veut réaliser des réseaux un tant soit peu complexes et encore plus insuffisante si l'on considère un contexte national dans lequel on souhaite que les réseaux en relais de trames aient assez de références pour permettre un grand nombre de liaisons virtuelles. C'est la raison pour laquelle deux extensions supplémentaires, de 1 ou 2 octets, ont été effectuées pour le relais de trames, aboutissant à des références sur 16 ou 23 bits. Dans le premier cas, un

troisième octet d'adressage est ajouté. Sur cet octet, 6 bits sont dédiés à l'extension de longueur de la référence. Dans le deuxième cas, un quatrième octet est ajouté, 7 de ses bits concernant l'extension de la longueur de la référence. Le huitième bit des octets 3 et 4 indique si un octet de supervision supplémentaire est à prendre en considération. Les octets d'extension se trouvent soit au milieu des deux octets de base, soit derrière eux.

Figure K.4

Format de la trame du relais de trames

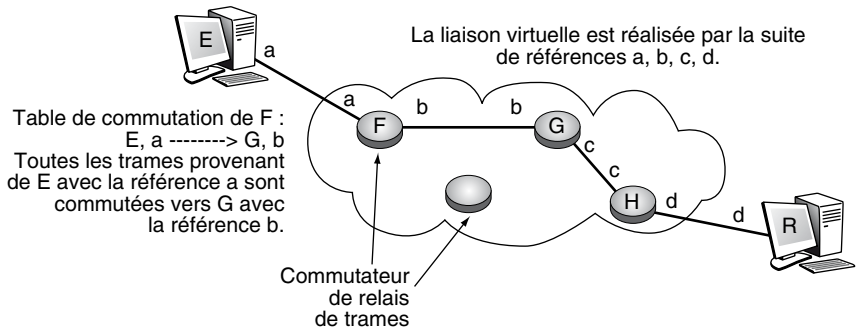


Le transfert des trames vers le nœud suivant s'effectue grâce à la valeur transportée dans le champ DLCI. La valeur du DLCI est modifiée lors de la traversée de chaque nœud. La nouvelle valeur de la référence se trouve dans la table de commutation. L'acheminement de la trame s'effectue par le chaînage des références DLCI. Les trames d'un même client allant de la machine terminale d'émission à la machine terminale de réception doivent toujours suivre un même chemin, à savoir la liaison virtuelle.

Lorsqu'un client veut émettre une suite de trames, il commence par mettre en place une liaison virtuelle. Cette dernière se réalise par l'intermédiaire d'une signalisation passant par le plan de contrôle lorsque la connexion est commutée ou l'utilisation des références placées sur une base mensuelle lorsque la liaison virtuelle est permanente. La figure K.5 illustre une liaison virtuelle déterminée par la succession des numéros DLCI a, b, c et d.

Figure K.5

Liaison virtuelle dans le relais de trames



Le commutateur de trames change la valeur du DLCI au passage, suivant les indications fournies par la table de commutation.

La procédure de commutation des trames sur la liaison virtuelle est en tout point similaire à la commutation de niveau paquet sur le circuit virtuel de la recommandation X.25.

Le contrôle de flux

Dans les premières versions du relais de trames, le contrôle de flux était pratiquement éliminé. Avec l'accroissement de la taille de ces réseaux, il a fallu ajouter un certain nombre d'éléments capables de réguler les flux. Les solutions retenues reposent sur un accord entre l'utilisateur et l'opérateur quant au débit moyen à respecter, ou CIR (Committed Information Rate), qui définit un flux à ne dépasser que sous certaines conditions. On définit aussi un CBS (Committed Burst Size), qui, pour le temps *T,* précise la quantité d'informations maximale à transporter sans dépasser le seuil garanti CIR : CBS = CIR × *T.*

Comme le relais de trames procède selon une méthode statistique, l'utilisateur a le droit de dépasser par moments le débit CIR. Cependant, ces dépassements peuvent mettre l'opérateur en difficulté, puisqu'il n'a réservé de ressources que pour la valeur garantie. C'est la raison pour laquelle l'autorisation de dépassement est accompagnée d'une indication relative aux données en surplus et spécifiée dans la trame. Cela permet à l'opérateur, en cas de difficulté dans son réseau, de détruire les données supplémentaires. Il n'y a donc pas de garantie de service pour les données en surplus.

Les dépassements peuvent se faire suivant un additif au contrat de base, par la détermination d'un débit maximal, ou EIR (Excess Information Rate), et d'une valeur nommée EBS (Excess Burst Size). Si l'utilisateur dépasse le seuil CIR, l'opérateur laisse entrer les données supplémentaires jusqu'à la valeur EIR, ces valeurs étant indiquées par la mise à 1 d'un bit du champ de la trame, le bit DE (Discard Eligibility). La valeur 1 du bit DE correspond aux données en excès. Cette indication a aussi pour signification que la trame peut être détruite par l'opérateur, suite à des problèmes de congestion du réseau.

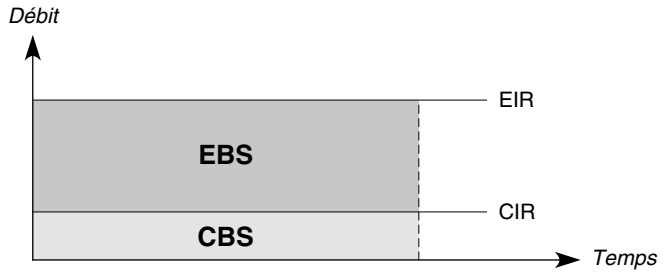
La valeur EBS indique la quantité d'information supplémentaire que l'opérateur transmet lorsque le seuil CIR est dépassé. Pour le temps *T,* cette quantité est définie par (EIR – CIR) × *T.*

En résumé, le dépassement de la valeur de base CIR est accepté par le réseau jusqu'à une limite maximale définie dans le contrat de trafic par la valeur EIR. Au-delà de cette limite, les trames sont détruites à l'entrée du réseau. La figure K.6 illustre ces différents paramètres de contrôle de flux.

Le contrôle de flux effectué par le contrat de trafic est complété par des notifications effectuées aux extrémités et spécifiées dans les trames elles-mêmes. Les deux notifications possibles sont :

- FECN (Forward Explicit Congestion Notification)
- BECN (Backward Explicit Congestion Notification)

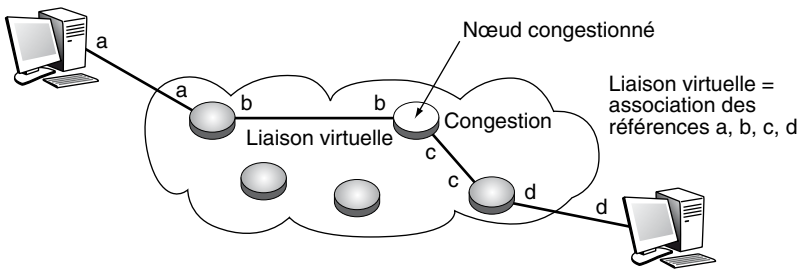
Figure K.6
Paramètres du contrôle de flux dans le relais de trames



Supposons qu'un nœud soit en période de congestion. Cette congestion est déterminée par des seuils définis par l'opérateur. Lorsqu'une trame passe par un nœud congestionné, elle est marquée soit par le bit FECN = 1, soit par le bit BECN = 1, suivant la direction de la trame, vers le récepteur ou l'émetteur. La notification vers l'avant correspond à un avertissement envoyé au récepteur pour l'informer que le réseau comporte un point saturé. La seconde notification repart vers l'émetteur pour lui indiquer qu'il serait souhaitable qu'il diminue provisoirement son débit.

Les normes ne donnent aucune indication sur l'usage effectif de ces notifications. Cependant, l'unité de raccordement, ou FRAD (Frame Relay Access Device), peut réduire son débit tout en avertissant les couches supérieures. La figure K.7 fournit un exemple de liaison virtuelle passant par un nœud congestionné notifiant la surcharge à ses extrémités. Le problème posé par cette notification collective vient de la demande effectuée à toutes les machines extrémité de réduire leur trafic, indépendamment des connexions fautives.

Figure K.7
Liaison virtuelle avec point de congestion



La commutation de cellules ATM

Une première caractéristique importante des réseaux ATM est qu'on utilise le mode avec connexion pour la transmission des cellules. Une cellule n'est transmise que lorsqu'un circuit virtuel est ouvert, ce circuit virtuel étant marqué à l'intérieur du réseau par des références précisées dans les tables de commutation placées dans chaque nœud traversé. Nous verrons à la fin de ce chapitre comment mettre en place ce circuit virtuel grâce au réseau de signalisation.

Deux interfaces ont été définies dans le monde ATM suivant que la cellule provient de l'extérieur du réseau ou passe d'un nœud de commutation à un autre à l'intérieur du réseau :

- L'interface NNI (Network Node Interface), qui se situe entre deux nœuds du réseau.
- L'interface UNI (User Network Interface), qui est utilisée pour entrer dans le réseau ou pour en sortir.

Ces deux noms d'interface, UNI et NNI, sont maintenant utilisés dans la plupart des réseaux, mêmes s'ils ne sont pas ATM.

Les références destinées à permettre la commutation des trames ATM sont composées de deux numéros : le numéro VCI (Virtual Channel Identifier), ou identificateur de voie virtuelle, et le numéro VPI (Virtual Path Identifier), ou identificateur de conduit virtuel. Ces numéros permettent d'identifier le circuit virtuel entre deux nœuds. Nous parlons de circuit virtuel, car c'est la terminologie utilisée dans l'ATM, bien que nous ayons affaire à une liaison virtuelle puisque le niveau ATM est un niveau trame.

La référence d'un circuit virtuel comporte donc deux parties : le numéro de conduit virtuel (*virtual path*) et le numéro de voie virtuelle (*virtual channel*). La différence entre ces deux valeurs est explicitée un peu plus loin.

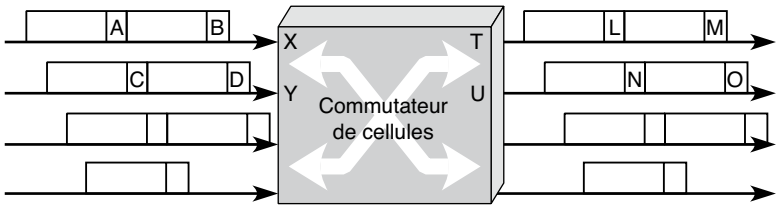
ATM étant en mode avec connexion, avant toute émission de cellule, une connexion doit être mise en place. Pour cela, une association entre les références d'entrée et de sortie du réseau doit être définie. Cette technique est déjà utilisée dans les réseaux X.25.

Le routage de la cellule de supervision, qui met en place le circuit virtuel, est effectué par des tables de routage, lesquelles déterminent vers quel nœud est envoyée la cellule de supervision avec l'adresse du destinataire final. Cette cellule de supervision détermine pour chaque nœud l'association entre le port d'entrée et le port de sortie. Ces associations sont regroupées dans la table de commutation.

La figure K.8 illustre l'association effectuée entre la référence et le port d'entrée dans un nœud de commutation et la référence et le port de sortie de ce même commutateur. Par exemple, si une cellule se présente à la porte d'entrée X avec la référence A, elle est transmise à la sortie T avec la référence L. La deuxième ligne du tableau de commutation constitue un autre exemple : une cellule qui entre sur la ligne X avec la référence B est envoyée vers la sortie U, accompagnée de la référence N de sortie.

Des connexions multipoint sont prévues dans la normalisation. Il suffit d'associer à une ligne et à une référence en entrée plusieurs lignes et des références en sortie. Les références permettant de commuter les cellules sont appelées, comme nous l'avons vu, VCI et VPI pour ce qui concerne la voie et le conduit. Dans un commutateur ATM, on commute une cellule en utilisant les deux références. Dans un brasseur, on ne se sert que d'une seule référence, celle du conduit. Par exemple, on peut commuter un ensemble de voies virtuelles en une seule fois en ne se préoccupant que du conduit. Dans ce cas, on a un brasseur de conduit, ou cross-connect, et l'on ne redescend pas au niveau de la voie virtuelle.

Figure K.8
Commutation des cellules dans un nœud de commutation

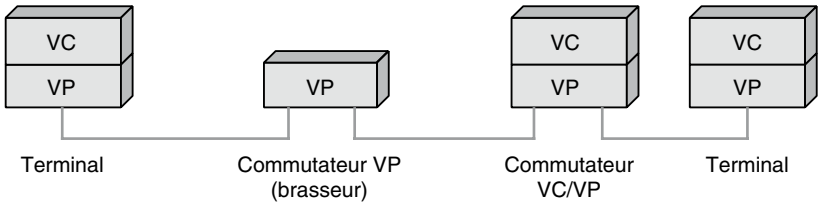


Les trames arrivant sur la porte d'entrée X avec la référence A sont dirigées sur la sortie T avec la référence L.

Ligne d'entrée	Référence d'entrée	Ligne de sortie	Référence de sortie
X	A	T	L
X	B	U	N
Y	C	T	M
Y	D	T	O
.			

La figure K.9 illustre un circuit virtuel avec un commutateur ATM et un brasseur.

Figure K.9
Circuit virtuel avec brasseur et commutateur ATM



Dans un brasseur de conduits, on commute simultanément toutes les voies virtuelles à l'intérieur du conduit. On a donc intérêt à regrouper les voies virtuelles qui vont vers la même destination de façon à les intégrer dans un même conduit. Cela simplifie grandement les problèmes de commutation à l'intérieur du réseau. La figure K.10 illustre, de façon assez symbolique, un même conduit partagé par un ensemble de voies. Le long du conduit, des brasseurs VP peuvent se succéder.

Figure K.10
Multiplexage de VC dans un VP

Longueur de la cellule ATM

La longueur de la zone de données, de 48 octets, est le résultat d'un compromis passé entre les Européens, qui souhaitaient 32 octets, et les Américains, qui désiraient 64 octets. Ce compromis a bien entendu un sens, que nous expliciterons.

La très faible longueur de la cellule est aussi explicable par une autre raison. Prenons l'exemple de la transmission de la parole téléphonique, qui demande une liaison à 64 Kbit/s. C'est une application isochrone qui possède deux contraintes :

- Une synchronisation très forte des données : un octet part de l'émetteur toutes les 125 µs, et les octets doivent être remis au codeur-décodeur de l'autre extrémité toutes les 125 µs.
- Un délai de propagation qui doit rester inférieur à 28 ms si l'on veut éviter les problèmes liés à la transmission de signaux sur une longue distance (suppression des échos, adaptation, etc.).

Si nous regardons le temps de transit des octets pour la parole sortant d'un combiné téléphonique, nous avons :

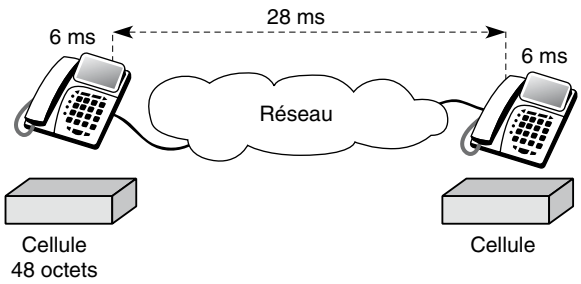
- Un temps de remplissage de la cellule par les octets qui sortent du combiné téléphonique toutes les 125 µs. Il faut donc exactement 6 ms pour remplir la cellule de 48 octets de longueur.
- Le temps de transport de la cellule dans le réseau.
- Encore 6 ms pour vider la cellule à l'extrémité, puisqu'on remet au combiné téléphonique un octet toutes les 125 µs.

Comme le temps total ne doit pas dépasser 28 ms, on voit que, si l'on retranche le temps aux extrémités, il n'y a plus que 16 ms de délai de propagation dans le réseau lui-même. En supposant que le signal soit transmis sur un câble électrique à la vitesse de 200 000 km/s, la distance maximale que peut parcourir le signal sans que l'écho soit détecté est de 3 200 km. Cette distance peut bien évidemment être augmentée si l'on ajoute des équipements adaptés (suppression des échos, adaptation, etc.). Comme le territoire nord-américain est très étendu, il a fallu mettre en place tous ces types de matériels dès les premières générations. C'est pourquoi les Américains préconisaient une meilleure utilisation de la bande passante en allongeant la zone de données des cellules par rapport à la partie supervision.

En Europe, pour éviter d'avoir à adapter le réseau terrestre, on aurait préféré une taille de cellule plus petite, de 32, voire 16 octets, de façon à gagner du temps aux extrémités. Ces contraintes sont illustrées à la figure K.11.

Figure K.11

Contraintes de propagation de la parole téléphonique



Performance des réseaux ATM

Les réseaux ATM n'ont que peu d'originalité. On y retrouve de nombreux algorithmes utilisés dans les réseaux classiques à commutation de paquets. Cependant, la hiérarchie des protocoles utilisés est assez différente de celle de la première génération de réseaux.

Dans les réseaux ATM, le temps d'émission d'une cellule demande quelques nanosecondes, ce qui est négligeable par rapport au temps de propagation sur le support, qui s'exprime généralement en microseconde. On peut donc considérer que la ligne physique, surtout si elle est un peu longue, représente une mémoire de plusieurs mégabits par seconde. Dans la structure des réseaux ATM, il faut toutefois tenir compte du temps d'attente dans les files de sortie des nœuds. Si l'on veut des portées de l'ordre de plusieurs milliers de kilomètres, il faut impérativement minimiser ces temps d'attente, de façon qu'ils restent relativement négligeables par rapport au délai de propagation.

Cette problématique est illustrée à la figure K.12. Si l'on suppose une liaison d'une longueur de 2 000 km et un débit de 1 Gbit/s, le temps de propagation est de 1 ms et le temps d'émission d'une cellule de 424 ns. Il y a donc 2 358 cellules en cours de propagation sur la liaison.

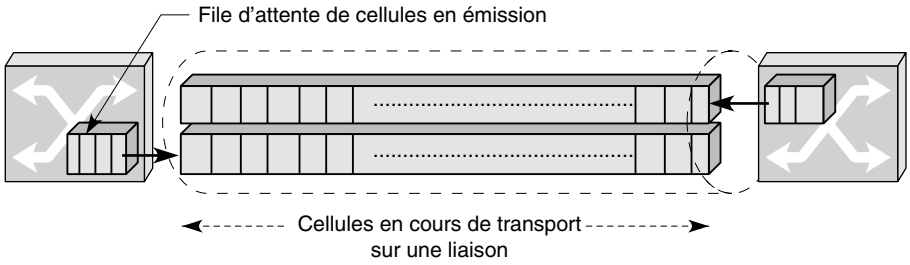


Figure K.12

Capacité de la ligne de transmission

Le réseau ATM est asynchrone, mais cet asynchronisme est faible du fait du rapport entre le temps de transmission et le délai de propagation. Ces contraintes de temps sont illustrées à la figure K.13, qui les compare avec la commutation de paquets. Le paquet, ici fragmenté en cinq cellules, arrive bien avant le paquet transporté en commutation de paquets.

La commutation de cellules a pour objectif de remplacer à la fois la commutation de circuits et la commutation de paquets. Pour ce faire, les principes des deux techniques doivent être respectés. Si l'on considère que l'ATM utilise des vitesses de transmission très élevées, le temps de transmission est très petit et même négligeable par rapport au temps de propagation du signal. Prenons l'exemple de lignes de communication à 1 Gbit/s. Pour émettre les 53 octets de la cellule, il faut un peu moins de 500 ns. Si l'on suppose qu'il faut ajouter quelques microsecondes pour franchir le commutateur, la somme du temps de traversée du commutateur et du temps de transmission est négligeable en comparaison du délai de propagation, qui vaut approximativement 1 ms pour 250 km, soit 10 ms pour 2 500 km.

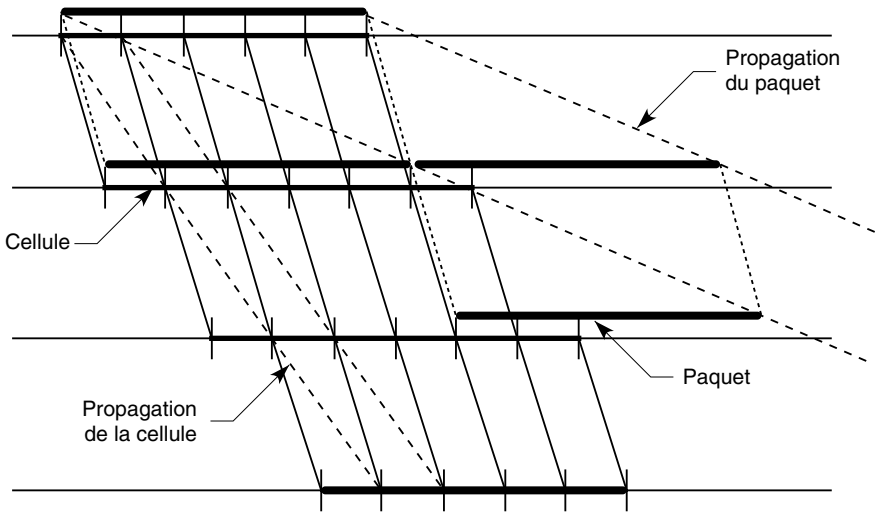


Figure K.13

Comparaison de la commutation de paquets et de cellules

Avantage de la séparation entre administration et établissement

La séparation entre l'administration de la bande passante et l'établissement des connexions de conduits virtuels procure les avantages suivants :

- Diminution des tâches d'administration : les tâches d'administration sont nécessaires uniquement pour les conduits virtuels, et non pour tous les circuits virtuels transitant dans les brasseurs. Une étude sur l'utilisation des conduits virtuels indique que, lorsque le brassage seul est utilisé, le nombre d'instructions diminue de 90 % par rapport à une commutation VP/VC.
- Facilité du contrôle de la bande passante dynamique : les changements de bande passante d'une connexion de conduit virtuel n'étant pas indiqués aux nœuds intermédiaires du conduit, le contrôle de la bande passante peut être réalisé plus facilement.
- Utilisation efficace de la bande passante : le contrôle dynamique permet d'utiliser efficacement la bande passante. Par exemple, la capacité d'un conduit virtuel réservé mais non utilisé peut être mise à zéro ou ramenée à une valeur déterminée à l'avance. De plus, la bande passante disponible peut être allouée aux conduits virtuels saturés.

Le concept de conduit virtuel permet d'avoir des services de ligne louée (*leased line services*). La figure K.14 illustre un réseau privé construit autour de deux réseaux locaux, ou CPN (Customer Premise Network), reliés par un conduit virtuel. Les connexions sont multiplexées sur le conduit virtuel et se partagent la bande passante disponible. L'augmentation ou la diminution de la bande passante d'un circuit virtuel étant simple à réaliser, l'utilisateur peut adapter son débit, étant entendu que la bande passante totale en utilisation ne peut dépasser la bande passante réservée au conduit virtuel.

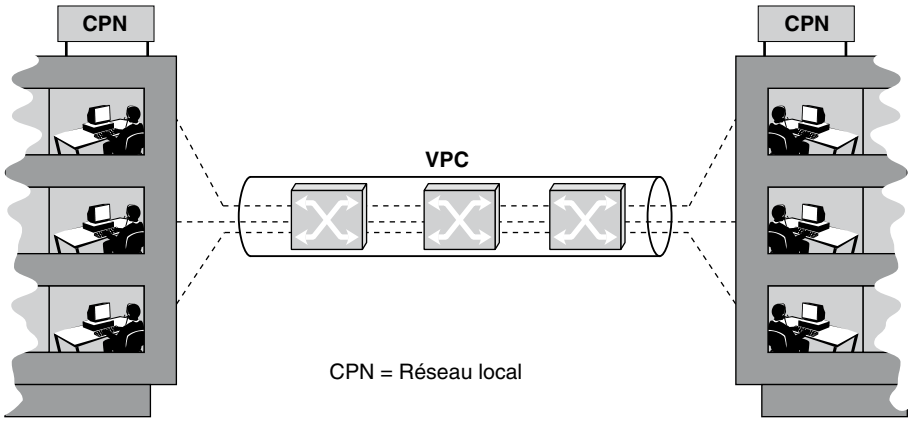


Figure K.14
Réseaux locaux reliés

La réduction des tables de commutation est l'une des raisons les plus importantes de ce découpage en VP et VC. Une fois le circuit virtuel établi, les cellules doivent être commutées d'une ligne d'entrée vers une ligne de sortie. Si la table de commutation compte plus de 4 000 entrées, le temps de commutation devient incompatible avec les temps de traversée des commutateurs souhaités par les opérateurs. Pour réduire cette table de commutation, la subdivision de l'adresse en deux parties permet de ramener le champ à examiner à 12 bits sur la partie intérieure au réseau. Pour les réseaux locaux, dans lesquels le nombre de clients connectés est bien moindre, le problème est différent, et des tables de commutation employant des références VP/VC sont permises.

Le champ PTI (Payload Type Identifier)

Le champ PTI permet d'identifier deux types d'informations de la cellule (*voir tableau K.1*). Les codes PTI, pour les cellules utilisateur, contiennent deux indications additionnelles :

- indication de congestion (référencée par le bit n° 3) ;
- indication d'utilisateur de la couche ATM à un autre utilisateur distant (référencée par le bit n° 2).

Tableau K.1 • Définition des identificateurs de capacité utile

0	Contrôle	0 1	Identificateur d'utilisateur	0 1	Notification de congestion
1	Gestion	0	Flux OAM F5 Gestion de CV	0	Locale
				1	De bout en bout
		1	Gestion de ressources	0	De ressources
				1	Réservé

Pour les cellules de gestion, les codes PTI permettent de distinguer les cellules du flux OAM (Operation And Maintenance) pour la gestion de CV des cellules de gestion de ressources. Les cellules appartenant au flux OAM sont également divisées en deux classes : de bout en bout et locale.

Le bit CLP (Cell Loss Priority)

Le bit CLP indique la priorité de la cellule. Si le bit est marqué (CLP = 1), la cellule est détruite en cas de congestion dans le réseau. S'il ne l'est pas (CLP = 0), la cellule est prioritaire par rapport aux cellules marquées. Le bit CLP permet de différencier deux classes de cellules d'une même connexion et de disposer de deux qualités de service en termes de perte de cellules ou de temps de transfert. Par exemple, dans le cas du service vidéo, les cellules de synchronisation peuvent être prioritaires.

Le bit CLP a une signification assez complexe puisqu'il peut être utilisé par l'opérateur pour marquer les trames en surplus après dépassement du seuil de débit négocié entre l'utilisateur et l'opérateur. De ce fait, un bit CLP marqué à 1 à l'intérieur du réseau peut avoir deux significations : soit l'utilisateur considère la cellule comme peu importante, soit la cellule est importante mais elle fait partie d'un surplus.

De par cette double signification, les équipementiers ont dû introduire des différences de gestion assez importantes dans leur architecture de contrôle au détriment de la compatibilité. C'est la raison pour laquelle on essaye de ne plus utiliser le bit CLP, dont la signification véritable est généralement incompatible entre équipementiers.

Le champ HEC (Header Error Control)

Le champ HEC est utilisé par la couche physique pour la délimitation de la cellule et le contrôle d'erreur dans l'en-tête.

La première fonction du HEC est de déterminer le début des cellules. Tant que la synchronisation n'a pas été trouvée, le coupleur génère le polynôme formé des quatre derniers octets reçus et le divise par le polynôme générateur. Si le reste correspond à ce qui se trouve dans le cinquième octet, ce sont bien les cinq premiers octets d'une cellule qui ont été trouvés, et cela correspond au début d'une cellule. Comme la cellule est elle-même transformée par un code de mixage, il est quasiment impossible de détecter un début de cellule qui n'en soit pas un. Rappelons que la cellule est une trame, et non un paquet, puisqu'il est possible de détecter son début et sa fin.

Les normalisateurs ont considéré que le taux d'erreur en ligne pour l'en-tête de la cellule n'était pas suffisant sur les lignes utilisées par la commutation ATM. Le HEC sert donc également à détecter les erreurs et à les corriger. Plus exactement, deux modes de fonctionnement ont été placés dans la norme. En mode normal, le mode par défaut, le HEC sert à détecter si un seul bit est en erreur et à corriger cette erreur. Si plusieurs erreurs sont détectées, la cellule est détruite, et l'on passe en mode de détection. Toutes les cellules avec une ou plusieurs erreurs sont alors détruites. On repasse en mode normal dès qu'une cellule est reçue sans erreur.

Le champ HEC est calculé à l'aide du polynôme constitué par les bits du champ de contrôle, à l'exception du champ HEC. Ce polynôme est divisé par le polynôme générateur $x_8 + x_2 + x + 1$. Le reste est introduit dans le HEC.

La couche d'adaptation ATM (AAL)

La couche AAL (ATM Adaptation Layer) a pour rôle de gérer l'interface avec les couches de protocole situées chez l'utilisateur. Ses fonctions dépendent des exigences de la couche supérieure. L'AAL doit supporter les besoins des différents utilisateurs du service d'AAL et donc des protocoles multiples.

L'AAL est composée de deux sous-couches : la sous-couche de convergence, CS (Convergence Sublayer), et la sous-couche de segmentation et de réassemblage, SAR (Segmentation And Reassembly). La fonction essentielle de la couche SAR est de segmenter les données des couches supérieures en un ensemble de segments de données correspondant à la taille des cellules. Au niveau du destinataire, la couche SAR rassemble les cellules pour restituer des données aux couches supérieures. La sous-couche CS dépend du service qui doit être rendu à l'utilisateur. Elle fournit le service de l'AAL au SAP (Service Access Point), ou point d'accès au service. Selon le protocole de niveau AAL, les sous-couches peuvent être vides si la couche ATM est suffisante pour les exigences des utilisateurs.

Les classes de services

L'UIT-T répartit les services du réseau ATM en quatre classes, fondées sur la relation de temps entre la source et le destinataire, le débit constant ou variable et le mode de connexion :

- Pour les services de classe A, le débit est constant et le service en mode avec connexion. Le service de type parole téléphonique à 64 Kbit/s en est un exemple typique. La relation de temps existe entre la source et la destination.
- Pour les services de classe B, le débit est variable. Un service typique peut être une parole téléphonique ou une vidéo compressée.
- Les classes C et D correspondent aux applications de transfert de données. Le débit est variable, et la relation de temps n'est pas nécessaire. Les transferts de données des classes C et D sont respectivement en mode avec connexion et sans connexion.

L'UIT-T recommande quatre types de protocoles AAL pour supporter ces classes de services (ces protocoles ayant été modifiés en 1993, nous donnons ici les dernières versions) :

- **AAL-1.** Supporte les services de la classe A et fournit de ce fait un service d'émulation de circuit en permettant d'utiliser toute la souplesse de l'ATM. Cependant, il n'exploite pas toute l'efficacité de l'ATM résultant du multiplexage statistique. Le service rendu par l'AAL-1 s'appelle CBR (Constant Bit Rate).
- **AAL-2.** L'histoire de ce protocole est plus complexe. Il a été défini au départ pour supporter les services de la classe B. Le service vidéo à débit variable en est un exemple.

Il permet d'exploiter non seulement la flexibilité mais aussi l'efficacité de l'ATM. Le service rendu par cette classe s'appelle VBR (Variable Bit Rate). L'AAL-2 a été abandonné au cours des années 95 pour être redéfini dans le cadre d'applications ayant des contraintes temporelles fortes et un débit variable. Pour arriver à paquétiser suffisamment rapidement, on a commencé à multiplexer plusieurs connexions sur le même circuit virtuel. Ce protocole est utilisé, par exemple, sur la partie accès de l'UMTS. C'est la raison pour laquelle ce nouvel AAL-2 est présenté au chapitre 41, consacré à la téléphonie IP. Son rôle, dans ce cas, est de permettre le multiplexage de plusieurs connexions bas débit sur une connexion ATM de façon à tenir compte aux mieux des contraintes temporelles.

- **AAL-3/4.** Supporte les services de données en mode avec ou sans connexion, à débit variable et sans relation de temps. Le contrôle de flux entre les extrémités et la retransmission des fragments perdus ou altérés sont possibles. Les exemples de services que peut rendre ce type d'AAL sont nombreux : X.25, relais de trames (FMBS, Frame Mode Bearer Services), signalisation, etc. Cette classe n'est plus utilisée depuis 2005.
- **AAL-5.** L'autre nom de ce type d'AAL est SEAL (Simple Efficient Adaptation Layer). Il permet de transporter des trames de données non superposées en mode avec connexion (service de classe C). Le service rendu est de type élastique et utilise le service ABR (Available Bit Rate).

À ces quatre types correspondent quatre structures de trames de la couche SAR, appelées SAR-PDU (Segmentation And Reassembly-Protocol Data Unit).

La couche SAR (Segmentation And Reassembly)

Cette sous-couche définit les structures qui serviront réellement au transport de l'information. Les services CBR (Constant Bit Rate), VBR (Variable Bit Rate), ABR (Available Bit Rate), GFR (Generic Frame Rate) et UBR (Unspecified Bit Rate) sont définis sur les classes 1, 2, 3-4 et 5, qui introduisent une segmentation spécifique à chaque classe de services.

En résumé, le niveau AAL d'adaptation, et plus particulièrement sa sous-couche SAR, doit rendre les services suivants :

- assembler et désassembler les cellules ;
- compenser le délai variable de la méthode ATM ;
- prendre en charge les cellules perdues ;
- récupérer la synchronisation horloge.

L'unité de données du niveau SAR, la SAR-PDU, dépend du service qui doit être rendu, c'est-à-dire de la classe de transport de données.

AAL-1

La classe 1, qui correspond au service CBR, possède une SAR-PDU relativement simple, illustrée à la figure K.15.

Les champs SN (Sequence Number) et SNP (Sequence Number Protection) sont découpés suivant le schéma illustré à la figure K.16.

Figure K.15
SAR-PDU de type 1

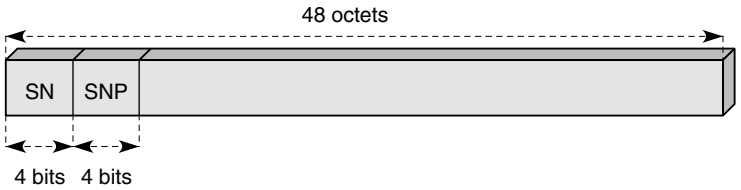
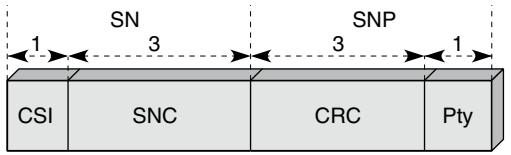


Figure K.16
Champ de supervision de l'AAL-1



CSI (Convergence Sublayer Information)
SNC (Sequence Number Counter)
CRC (Cyclic Redundancy Check)
Pty (Parity bit)

Le champ SNC (Sequence Number Counter) numérote la cellule sur 3 bits, c'est-à-dire de 0 à 7. En règle générale, l'émetteur émet plusieurs centaines de cellules avant que l'acquittement revienne, si bien qu'une numérotation de 0 à 7 apparaît très insuffisante. Les cellules sont numérotées en séquence de 0 à 7, et une cellule perdue est détectée par un trou dans la numérotation. Par exemple, si le récepteur reçoit la séquence 0, 1, 2, 4, 5, il en déduit que la cellule 3 a été perdue. S'il reçoit la séquence 2, 3, 4, 7, 0, 1, le récepteur comprend que les cellules 5 et 6 ont été perdues. Si huit cellules successives sont perdues, il n'y a plus aucun moyen de s'en apercevoir. On compte sur le fait que la probabilité de perdre plus de deux ou trois cellules successives est négligeable.

La zone SNP doit protéger le numéro de séquence afin de ne pas avoir à détecter d'erreur de déséquencement dues à une erreur sur la zone de numérotation elle-même. Ce champ est composé d'une zone de détection d'erreur sur 3 bits et d'un bit de parité paire.

Le bit CSI (Convergence Sublayer Information) permet de transporter une marque de temps RTS (Residual Time Stamp) pour caler l'horloge du récepteur ou délimiter des blocs de données. La marque de temps est sur 4 bits, transportée par le bit CSI d'une cellule sur deux (les cellules impaires d'une suite de huit cellules).

La vitesse d'arrivée des marques autorise le calcul d'un temps moyen entre deux arrivées, ce qui permet de synchroniser la restitution des cellules. Si la vitesse d'arrivée augmente, la restitution des cellules augmente aussi. C'est la technique SRTS (Synchronous Residual Time Stamp).

Pour le transfert isochrone de données à $n \times 64$ Kbit/s, un cadrage est effectué par un pointeur qui occupe le premier octet de la zone de données (il reste 46 octets de données).

Ce pointeur est indiqué par le bit CSI, présent dans les cellules d'ordre pair pour préserver la compatibilité avec la technique SRTS. Lorsque le bit CSI est à 1 dans une cellule paire (numérotée 0, 2, 4, 6), il indique l'existence d'un pointeur qui permet de connaître le degré de remplissage des 46 + 47 octets (93 octets) de la cellule paire, suivie de la cellule impaire. Dans l'octet du pointeur, seuls 7 bits sont utilisés, le huitième étant réservé à des développements futurs.

Une technique d'entrelacement d'octets (*byte interleave*) peut être ajoutée pour éviter la perte successive d'octets, une faute grave dans une transmission isochrone. Par exemple, si 47 octets sont en erreur, au lieu de perdre 47 octets successifs, on perd un octet tous les 47 octets. Dans le transport de la parole, il vaut mieux perdre un échantillon tous les 47 échantillons que 47 échantillons de suite.

La technique d'entrelacement est illustrée à la figure K.17.

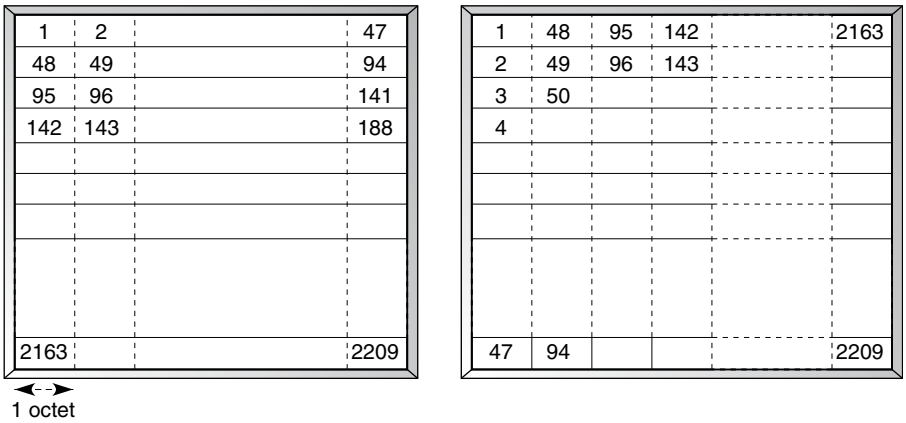


Figure K.17

Entrelacement des octets dans l'AAL-1

AAL-2 de 1990

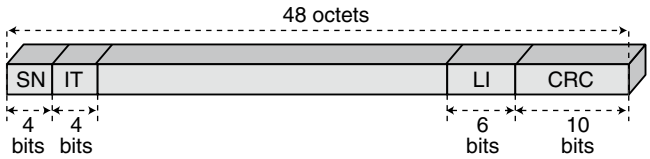
Nous présentons ici la version AAL-2 définie au début des années 1990 pour le service VBR.

Pour les services VBR, le rôle de la couche SAR est assez semblable à celui des services CBR :

- division et récupération des trames d'information ;
- prise en charge des cellules en partie remplies ;
- adaptation du débit ;
- prise en charge des cellules perdues.

La SAR-PDU de la classe 2 est illustrée à la figure K.18.

Figure K.18
SAR-PDU de type 2



Dans la structure de la SAR-PDU, on trouve quatre zones de supervision :

- SN (Sequence Number), sur 4 bits, qui permet de numéroter les trames modulo 16. Cette numérotation permet de détecter les trames perdues.
- IT (Information Type), sur 4 bits, qui indique le début, la continuation ou la fin d'un message.
- LI (Length Indicator), sur 6 bits, qui permet de détecter la zone de données effectivement occupée sur les 45 octets disponibles. Si ce champ porte la valeur 16, cela indique que les 16 premiers octets sont des données de l'utilisateur et que les 29 octets suivants ne sont pas utilisés.
- CRC (Cyclic Redundancy Check), sur 10 bits, qui permet de détecter des erreurs au cours du transfert.

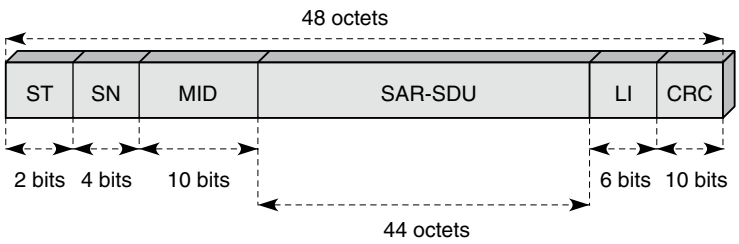
Ce protocole n'a pu être réellement utilisé à cause des évolutions technologiques sur la compression des applications vidéo. En effet, si la compression est extrêmement forte, une détection et une correction d'erreur doivent être ajoutées. En revanche, si la compression n'est pas trop poussée, le protocole n'a pas à se soucier d'une correction d'erreur. Devant ces incertitudes, les choix de l'AAL-2 n'ont pas résisté, et une nouvelle version tournée vers le transport de la parole et de la visioconférence dans l'UMTS est apparue en 2000.

AAL-3/4

Les types 3 et 4 ont été rassemblés dans une classe unique pour le transport sécurisé des données. Dans chaque cellule, une partie du message est transmise, et chaque partie est sécurisée par un CRC, permettant de détecter les erreurs qui peuvent survenir pendant le transport. Il y a donc, dans chaque cellule, tout un ensemble de zones de supervision, ce qui rend la procédure peu efficace.

La figure K.19 illustre la classe 3/4 de la couche AAL.

Figure K.19
SAR-PDU de type 3/4



Le champ ST (Segment Type) permet de structurer la communication. Quatre possibilités sont recensées :

- BOM (Beginning Of Message) – Début 10
- COM (Continuation Of Message) – Continuation 00
- EOM (End Of Message) – Fin de segment 01
- SSM (Single Segment Message) – Segment simple 01

Le champ SN (Sequence Number) permet la numérotation des cellules modulo 16. Le champ MID (Multiplexing IDentifier) est utilisé pour identifier les SAR-PDU appartenant à différentes SAR-SDU. S'il n'y a pas de multiplexage, ce champ est mis à 0. Le champ LI (Length Indicator) indique la longueur de la zone de données utilisée. Le reste du champ de données (*payload field*) est mis à 0.

Le polynôme permettant la détection des erreurs et générant le champ CRC est :

$1 + x + x_4 + x_5 + x_9 + x_{10}$

Assez complexe, la classe 3/4 comporte de nombreux champs de contrôle. Une nouvelle classe a été introduite en 1993, la classe 5, pour compléter le transport de données dans un cadre simple. Son rôle était au départ de permettre l'interconnexion de réseaux locaux. Sa conception a pris en compte la facilité de découpage de l'information provenant de la couche supérieure.

AAL-5

Le rôle de la classe 5 est de prendre l'entité de niveau supérieur et de la découper en tronçons de 48 octets pour l'introduire dans la zone de données de la cellule ATM. Ce schéma de découpage provient d'études préalables de la part de l'UIT-T sur le protocole SEAL (Simple Efficient Adaptation Layer).

La structure de la cellule SAR-5 et le découpage de l'entité de niveau supérieur sont illustrés à la figure K.20. Il y a un minimum de perte, puisque la CPCS-PDU (unité de données du protocole commun de la couche CS) est directement découpée en fragments de 48 octets.

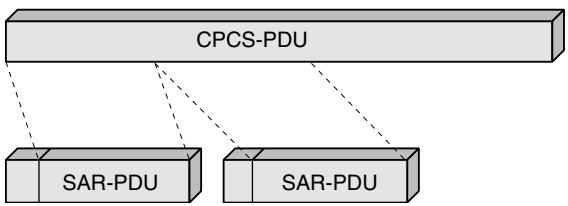


Figure K.20
Découpage de l'information dans la classe 5

La couche CS (Convergence Sublayer)

La couche CS se trouve au-dessus de la couche SAR. Elle définit le bloc d'information qui doit être transporté de bout en bout par la couche ATM après fragmentation dans la couche SAR. Pour les classes 1 et 2, la couche CS délimite un bloc qui sera découpé suivant les principes exposés à la section précédente. Pour les classes 3/4 et 5, des fonctionnalités supplémentaires peuvent être introduites. Pour ces deux classes, la recommandation I.363 propose un découpage de la couche CS en deux sous-couches, la couche supérieure, SSCS (Service Specific Convergence Sublayer), et la couche inférieure, CPCS (Common Part Convergence Sublayer). La couche SSCS peut être vide.

La couche CPCS prend en charge les fonctions suivantes :

- délimitation ;
- séquencement ;
- réservation de mémoire aux extrémités ;
- détection d'erreur (en classe 5).

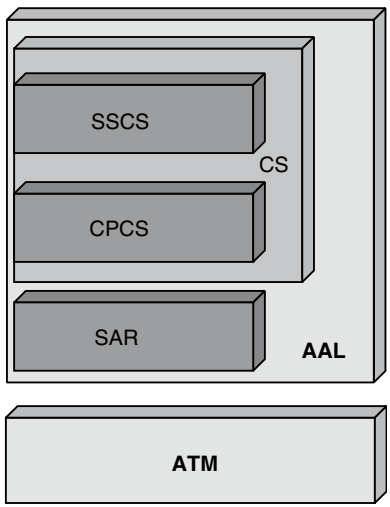
Les fonctionnalités de SSCS sont les suivantes :

- segmentation-réassemblage ;
- blocage-déblocage ;
- correction d'erreur ;
- contrôle de flux ;
- remise optionnelle des segments de ce niveau au niveau supérieur ;
- mode assuré, restreint aux communications point-à-point.

La taille maximale de la CS-PDU est de 65 535 octets.

L'architecture globale de la couche AAL est illustrée à la figure K.21.

Figure K.21
Architecture de la couche AAL

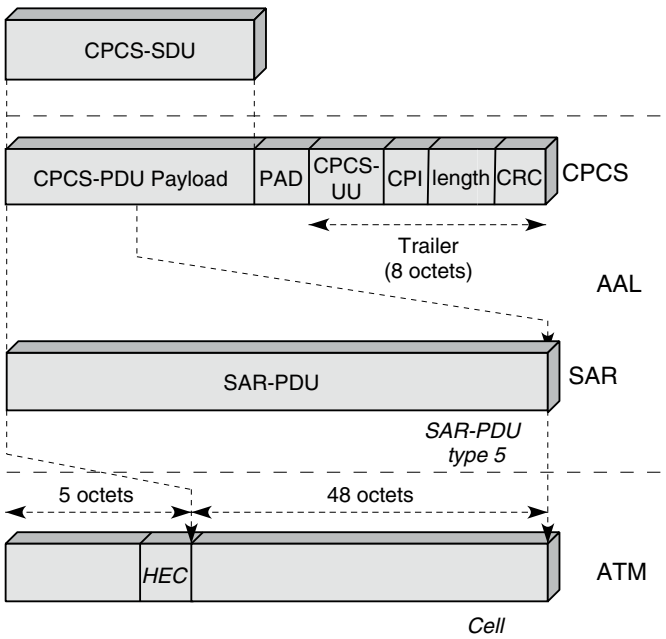


La couche CS-5

La figure K.22 illustre l'empilement des protocoles pour la classe 5.

Le champ PAD permet d'obtenir un champ de données d'une longueur multiple de 48 octets. Le découpage doit fournir des fragments d'une longueur de 48 octets. Il y a donc entre 0 et 47 octets mis à 0. Le champ CPCS-UU (CPCS User-to-User indication) permet d'indiquer le début, la continuation et la fin de la CPCS-PDU.

Figure K.22
Empilement des protocoles dans la couche CS-5



On retrouve dans le champ de supervision de fin de trame la zone Length, qui indique la longueur de la CPCS-SDU, et la zone CPI. La zone CRC, sur 4 octets, permet de détecter les erreurs sur la CPCS-PDU.

Les classes de services ATM

La technique de transfert ATM s'est stabilisée vers la fin des années 1990, après plus de dix années de normalisation intensive. La technologie a tellement évolué entre 1988 et aujourd'hui qu'il a fallu adapter les possibilités de l'ATM. La qualité de service constitue un point particulièrement sensible, puisque c'est l'élément qui permet de distinguer l'ATM des autres types de protocoles. Pour arriver à donner une qualité de service, il faut allouer des ressources, lesquelles sont parfois fortement sous-utilisées. Les recherches ont été nombreuses, et la solution a fini par être trouvée, sous la forme de classes de services.

La vision du contrôle des informations dans le réseau a beaucoup varié. Au départ, elle était fortement liée aux classes de services de la couche AAL définies dans les recommandations de l'UIT-T. L'ATM Forum a ensuite proposé cinq classes de services, définies dans un contexte un peu différent. Du coup, l'idée étant bonne, les opérateurs de télécommunications l'ont reprise en essayant de l'améliorer.

Les cinq classes de services de l'ATM Forum sont les suivantes (*voir aussi le tableau K.2*) :

- CBR (Constant Bit Rate), qui correspond à une émulation d'un circuit virtuel avec une bande passante fixe. Les services de cette classe incluent la voix et la vidéo temps réel sans compression.
- VBR (Variable Bit Rate), qui correspond à un circuit virtuel pour des trafics d'intensité variable dans le temps et plus spécifiquement les services par à-coups *(bursty).* Les services de cette classe incluent les transports d'applications vocales ou vidéo mais compressées ainsi que les services d'interconnexion de réseaux locaux ou le transactionnel. Il existe une classe VBR RT (Real-Time), qui doit prendre en compte les problèmes de temps réel.
- ABR (Available Bit Rate), qui permet d'utiliser la bande passante restante pour des applications aux débits variables et sensibles aux pertes. Un débit minimal doit être garanti pour que les applications puissent passer en un temps acceptable. Le temps de réponse n'est pas garanti dans ce service.
- GFR (Guaranteed Frame Rate), qui correspond à une amélioration du service ABR en ce qui concerne la complexité d'implantation de ce dernier sur un réseau. Le service GFR se fonde sur l'utilisation d'un trafic minimal. Si un client respecte son service minimal, le taux de perte de ses cellules doit être très faible. Le trafic dépassant le trafic minimal est marqué, et, si le réseau est en état de congestion, ce sont ces cellules qui sont perdues en premier. Le contrôle des paquets s'effectue sur la trame : si une cellule de la trame est perdue, le mécanisme de contrôle essaie d'éliminer toutes les cellules appartenant à la même trame.

Tableau K.2 • Comparaison des classes de services de l'ATM Forum

	Garantie de bande passante	Garantie de variance du délai	Garantie de débit	Retour d'indication de congestion
CBR	Oui	Oui	Oui	Non
VBR	Oui	Oui	Oui	Non
UBR	Non	Non	Non	Oui
ABR et GFR	Non*	Non	Oui	Oui

* Un minimum peut être garanti.

- UBR (Unspecified Bit Rate), qui correspond au service best-effort. Il n'y a aucune garantie ni sur les pertes ni sur le temps de transport. Le service UBR, qui n'a pas de garantie de qualité de service, n'est d'ailleurs pas accepté par les opérateurs télécoms,

qui ne peuvent se permettre de proposer un service sans qualité de service. Le service UBR correspond au service offert sur Internet. Cependant, la solution est totalement différente ici, puisque la priorité de plus basse qualité de service qu'offre l'UBR est appliquée non à l'ensemble des utilisateurs mais uniquement aux clients qui se partagent le résidu des ressources délaissées par les autres classes.

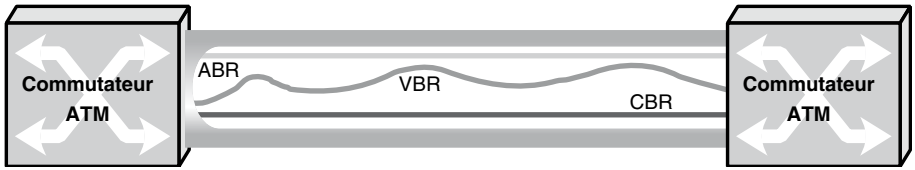


Figure K.23

Allocation des classes de services entre deux nœuds

La figure K.23 illustre l'allocation des classes de services. Dans un premier temps, les classes CBR et VBR sont allouées avec des ressources permettant une garantie totale de la qualité de service des données qui transitent dans les circuits virtuels concernés. Pour cela, on peut allouer les ressources sans restriction, puisque tout ce qui n'est pas utilisé peut être récupéré dans le service ABR. La partie basse de la figure indique la bande passante occupée par les clients CBR et celle du dessus la partie de la bande prise par les clients VBR. La partie supérieure est celle qui est laissée libre, et donc prise par les clients ABR. Si, dans les bandes CBR et VBR, une partie des bandes n'est pas utilisée, cette partie est affectée aux clients ABR.

Les classes de services de l'UIT-T

L'UIT-T a repris la proposition de l'ATM Forum en modifiant parfois légèrement les classes et en proposant une classe supplémentaire, ABT. Elle a supprimé l'UBR car les opérateurs ne souhaitaient pas offrir de service sans garantie.

Les quatre classes de l'UIT-T sont les suivantes :

- DBR (Deterministic Bit Rate). La bande passante est allouée sur la base du débit crête, ou PCR (Peak Cell Rate). C'est l'équivalent du service CBR de l'ATM Forum.
- SBR (Statistical Bit Rate). La bande passante est allouée sur la base du débit crête, du débit moyen, ou SCR (Sustainable Cell Rate), et de la longueur de la crête déterminée par l'IBT (Intrinsic Burst Tolerance). Le SCR fournit la moyenne en dehors des pointes. L'IBT donne une idée de la durée pendant laquelle le débit est au niveau crête.
- SBR + SBR RT (Statistical Bit Rate Real-Time). C'est le même type de service que le précédent, mais avec une contrainte de temps primordiale.
- ABR (Available Bit Rate). C'est le même service que dans l'ATM Forum.
- ABT (ATM Block Transfer). C'est un nouveau service normalisé par l'UIT-T. Il apporte une certaine souplesse tout en conservant une garantie complète aussi bien sur le taux d'erreur que sur le temps de réponse. Le service s'effectue sur des blocs de cellules

pour lesquels on doit indiquer le débit moyen. Le service ABT est similaire au service DBR mais pour un temps limité au bloc. Deux cas se produisent : soit le bloc est long, et l'opérateur peut effectuer une réservation de ressources pour garantir la qualité de service, soit le bloc est très court, et le temps de réservation devient long par rapport au temps d'émission des cellules du bloc. Dans ce dernier cas, la solution proposée par l'UIT-T consiste à envoyer le bloc sans réservation, en comptant sur la capacité statistique du réseau à supporter ce léger à-coup. Les deux services suivants sont appelés :

– ABT/DT (ABT with Delayed Transmission) ;

– ABT/IT (ABT with Immediate Transmission).

Le tableau K.3 récapitule les garanties fournies par les différents services de niveau ATM.

Tableau K.3 • Garanties des services de niveau ATM

	Service du niveau ATM					
Attribut	**DBR**	**SBR Real-Time**	**SBR Non-Real-Time**	**ABR**	**UBR**	**ABT**
Taux de perte de cellules	Spécifié (sauf pour CLP = 1)			Spécifié	Non spécifié	Spécifié
Délai de transfert de cellules Gigue	Spécifié	Spécifié	Spécifié Non spécifié	Non spécifié	Non spécifié	Spécifié
Débit crête	Spécifié	Spécifié	Spécifié	Spécifié	Spécifié	Spécifié
SCT/IBT	Non applicable	Spécifié	Spécifié	Non applicable	Non applicable	Spécifié
Contrôle temps réel par cellule RM	Non	Non	Non	Oui	Non	Oui

Comme nous le verrons, il faut ajouter un contrôle de flux, associé au service ABR, pour s'assurer que le taux de perte des cellules est négligeable. Le contrôle de flux choisi est de type rate-based.

La qualité de service ATM

Si l'ATM a été choisi comme mode de transfert pour le RNIS large bande plutôt que son concurrent, le mode de transfert temporel synchrone, ou STM (Synchronous Transfer Mode), c'est parce qu'il apporte un gain économique grâce au multiplexage statistique. Cependant, le multiplexage statistique de trafic en rafale peut provoquer des problèmes de congestion. Les travaux de l'UIT-T et de l'ATM Forum ont visé à minimiser cette congestion et à maximiser le taux d'utilisation du réseau, tout en garantissant la qualité de service spécifiée par l'utilisateur. Ces efforts ont abouti à la définition d'un contrat de trafic dépendant de la qualité de service requise et à la normalisation de fonctions de gestion de trafic.

Avant de regarder plus avant ces fonctions, nous allons définir précisément la qualité de service.

Une classe de qualité de service doit préciser des paramètres de performance (QoS spécifiée). Il est possible de ne spécifier aucun paramètre (QoS non spécifiée). Dans ce dernier cas, comme la QoS n'est pas précisée, on parle de la technique du meilleur effort possible de la part du réseau, ou service best-effort, pour satisfaire la demande de l'utilisateur. Comme expliqué au chapitre 7, le réseau Internet n'a jusqu'à présent proposé que ce service du fait des limitations de la première génération du protocole IP, IPv4. Si un utilisateur entre dans le réseau, on lui attribue une partie des moyens du réseau en les prélevant sur les ressources de tous les autres utilisateurs. Il y a donc partage des ressources. Il en ira autrement avec IPv6, qui permet une certaine qualité de service. Dans le cas de l'ATM, pour garantir une qualité de service, on préfère ne pas admettre de nouveaux clients, qui pourraient dégrader la qualité de service des autres utilisateurs.

Si la QoS est spécifiée par des paramètres de performance, on adopte, entre autres, les paramètres suivants :

- taux d'erreur par cellule (cell error ratio) ;
- taux de perte de cellules (cell loss ratio) ;
- délai de transfert par cellule (cell transfer delay) ;
- variation du délai de transfert par cellule, ou gigue (cell delay variation) ;
- taux de cellules mal insérées (cell misinsertion rate) ;
- délai moyen de transfert par cellule (mean cell transfer delay).

Un contrat de trafic est négocié entre l'utilisateur et l'opérateur du réseau ATM via l'interface UNI. Ce contrat de trafic doit contenir :

- une classe de QoS ;
- un descripteur de trafic sur la connexion demandée ;
- une définition de la conformité (on utilise également le mot anglais *conformance*).

La conformité (conformance) se réfère aux paramètres permettant d'être conforme à la demande de service d'un utilisateur. La classe de services peut être spécifiée ou non. Si elle ne l'est pas, cela correspond au service best-effort.

Le descripteur de trafic est un sous-ensemble des paramètres de trafic qui servent à décrire les caractéristiques du trafic des cellules sur la connexion. Ce descripteur contient les variables suivantes, qui diffèrent suivant les recommandations de l'UIT-T ou les propositions de l'ATM Forum :

- Descripteur du trafic source, qui peut lui-même contenir :
  - le débit crête, ou PCR (Peak Cell Rate) ;
  - le débit projeté, ou SCR (Sustainable Cell Rate) ;
  - la durée des rafales tolérée, ou BT (Burst Tolerance) ;
  - la tolérance de gigue, ou CDV tolerance (Cell Delay Variation tolerance).

- Algorithme déterminant le taux de génération des cellules, ou GCRA (Generic Cell Rate Algorithm), qui définit la conformité du trafic. Deux paramètres sont utilisés : le temps minimal entre deux émissions de cellule et la capacité maximale de mémorisation. Lorsqu'une cellule se présente et que la capacité maximale est atteinte (cellule non conforme), cette cellule doit soit être détruite, soit être émise en surplus, soit prendre la place d'une autre cellule, qui, elle-même, peut être détruite ou envoyée en surplus. C'est là que le bit CLP devient opérationnel : si la cellule est envoyée en surplus, elle est marquée par le bit CLP = 1, qui permet à un nœud interne du réseau de la détruire en cas de congestion. Il y a donc deux classes de priorité : CLP = 0, qui correspond aux cellules les plus prioritaires, et CLP = 1, pour les cellules pouvant être détruites dans le réseau.
- Paramètres expérimentaux, qui permettent de faire passer dans la demande des caractéristiques spécifiques, correspondant le plus souvent à des propriétés particulières à des constructeurs.

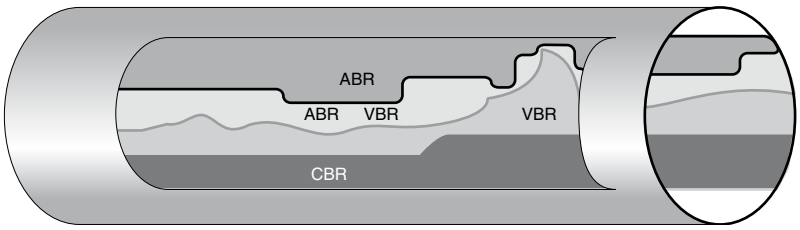
Le contrôle de flux

La conception des mécanismes de contrôle de flux efficaces pour ATM, permettant d'utiliser au mieux les ressources du réseau et de satisfaire la qualité de service requise, a été un véritable défi.

Toute la difficulté est située dans le temps de réaction des extrémités. Pour arriver à un contrôle relativement simple des flux ATM, l'ATM Forum, suivi par l'UIT-T, a décidé de regrouper les flux en différentes classes, comme expliqué précédemment. L'idée sous-jacente est la suivante : certains peuvent demander des tuyaux correspondant à des modes circuit, dans lesquels la garantie est complète, aussi bien en temps de réponse qu'en taux de perte, et d'autres se contenter de prendre l'espace laissé libre dans les tuyaux, un espace minimal étant toutefois réservé, même en cas de tuyaux complètement saturés.

La figure K.24 illustre cette idée de base. On y voit, en fonction du temps, le débit demandé par les clients CBR (la ligne interne la plus basse) et VBR (la ligne interne la plus haute), ainsi que la somme CBR plus VBR réellement utilisée (la ligne située entre les deux). Le trafic ABR peut atteindre cette ligne intermédiaire (débit CBR plus VBR réellement utilisé).

Figure K.24
Répartition des débits en fonction des classes de services



La répartition des informations par classe s'effectue de la façon suivante :

1. On affecte tout d'abord la bande passante au trafic CBR, et l'opérateur ne fait qu'additionner les bandes passantes demandées par les clients. On suppose que la bande passante ainsi réservée est bien utilisée.
2. Si ce n'est pas le cas, la place restant libre est réaffectée au trafic ABR.
3. Une fois cette affectation réalisée, l'opérateur retient une bande passante pour y faire transiter le trafic VBR. Cette réservation correspond, sur la figure K.24, à la somme des zones notées VBR et ABR VBR.

Cette réservation est à la charge de l'opérateur, qui peut l'effectuer de différentes façons, par exemple en réservant la somme des débits crêtes ou, après calcul, en faisant une surallocation, sachant qu'il y a peu de chance que tous les clients aient besoin du débit crête en même temps. Cela est du ressort de l'opérateur. Le client, quant à lui, doit pouvoir considérer qu'il dispose quasiment du débit crête pour que les garanties de ce service puissent être réalisées à coup sûr.

Dans la réalité, l'utilisation de cette bande passante réservée est largement inférieure à la réservation faite par l'opérateur. La zone utilisée est, sur la figure, la zone non hachurée notée VBR. La partie hachurée est la partie réservée mais non utilisée par le trafic VBR et qui est donc réaffectée au trafic ABR.

On comprend pourquoi le contrôle de flux est indispensable au trafic ABR. En effet, le rôle de ce trafic est de remplir, le plus près possible des 100 %, le tuyau global. Comme, à chaque instant, le volume de trafic avec garantie varie, il faut transmettre plus ou moins de trafic ABR de façon à être capable de dire à l'émetteur à tout instant quelle quantité de trafic ABR il faut laisser entrer pour optimiser l'utilisation des tuyaux de communication dans le réseau. Comme le trafic ABR n'a pas de garantie sur le temps de réponse, on peut se dire que si le contrôle de flux est parfait, on est capable de remplir complètement les voies de communication du réseau.

En d'autres termes, l'opérateur affecte l'équivalent de circuits aux utilisateurs qui veulent une garantie de temps de réponse et de taux de perte. Ces équivalents circuits correspondent à des cellules qui seront prioritaires dans les nœuds du réseau et pour lesquelles il n'y aura pas d'attente, si ce n'est l'arrivée simultanée de plusieurs cellules allant dans la même direction. Les cellules étant très courtes, cela entraîne un retard extrêmement faible, de quelques microsecondes. Il n'y aura donc pas de problème lors de la resynchronisation extrémité. Ensuite, toute la bande passante qui n'est pas utilisée par ces équivalents circuits est affectée au trafic ABR. On voit bien de la sorte que la technique de contrôle dans les réseaux ATM est devenue simple grâce à l'apparition de la structure en classes.

La quatrième classe, UBR, non illustrée à la figure K.24, peut fournir les données à transporter, sans aucune garantie de service, et remplir définitivement les tuyaux si, par hasard, le contrôle de flux ABR ne permettait pas d'arriver au niveau de 100 %.

Le contrôle de flux ABR

La méthode de contrôle de flux ABR (Available Bit Rate) a été introduite par l'ATM Forum. C'est une méthode réactive, qui essaye d'adapter nœud par nœud le débit provenant

de la source pour contrôler le niveau du débit sur chaque circuit virtuel. Il faut définir un débit maximal, le PCR (Peak Cell Rate), un débit minimal, le MCR (Minimum Cell Rate), un débit initial, ICR (Initial Cell Rate), un accroissement de débit, AIR (Additive Increase), un facteur de décroissance, RDF (Rate Decrease Factor), et un nombre de cellules Nrm entre deux cellules de gestion de ressource RM (Resource Management).

La source envoie une cellule de gestion de ressource RM toutes les Nrm cellules et, au pire, toutes les 100 ms. Cette source ne peut émettre à un débit supérieur à PCR et doit émettre au débit d'au moins MCR. Lors de l'initialisation de la source, un débit d'au moins ICR doit être émis. Une cellule RM est envoyée avant le début de la transmission. Suivant le débit entre deux cellules RM, la station source augmente son débit par AIR jusqu'au maximum PCR ou le diminue par RDF jusqu'à son minimum MCR.

La difficulté avec cette politique consiste à optimiser les paramètres d'augmentation et de diminution du débit sur chaque circuit virtuel et à faire remonter les informations de contrôle jusqu'à la source sans toutefois perdre trop de bande passante. L'obstacle majeur réside dans l'éloignement des nœuds puisque la méthode est réactive.

Considérons une liaison de 2 000 km, impliquant un délai de propagation de 10 ms, et un circuit virtuel au débit de 34 Mbit/s. Supposons que le dernier nœud du circuit virtuel décide de passer d'un débit ABR de valeur 34 Mbit/s à la valeur 0. Pour avertir l'émetteur de cette nouvelle valeur de débit acceptable dans le circuit virtuel, un temps de 10 ms est nécessaire. Cependant, il faut attendre 10 ms supplémentaires pour que le débit devienne nul à l'entrée du dernier nœud. Un temps aller-retour est en effet nécessaire pour que le débit ABR devienne effectivement nul, ce qui représente dans notre exemple 20 ms. Pendant ce temps, la quantité d'information arrivée au nœud congestionné correspond à 680 Kbit. Il suffit que ce nœud possède une mémoire de 85 Ko pour qu'aucun débordement n'ait lieu, ce qui représente une quantité relativement minime pour un canal à 34 Mbit/s.

On peut reprendre cet exemple de la façon suivante : si un nœud de commutation ATM possède un débit total de 34 Gbit/s, correspondant, par exemple, à 1 000 canaux de 34 Mbit/s, et si les nœuds extrémité, qui contrôlent les débits, sont situés en moyenne à 2 000 km, il faut une mémoire de 85 Mo pour garantir qu'aucune cellule ne sera perdue. Cette quantité est à la fois importante, à cause du coût des mémoires rapides (la mémoire doit absorber le débit de 34 Mbit/s), et faible par rapport à ce que l'on sait faire.

Cet exemple nous permet de comprendre les implémentations réalisées : placer dans les nœuds de grosses mémoires, capables de stocker les cellules lors d'une baisse du trafic ABR due au trafic prioritaire. Cette solution n'est toutefois pas compatible avec la conception des premiers commutateurs.

Un second problème est la reconnaissance du type de flux qui doit passer dans le commutateur. Si le flux est de type prioritaire, il faut traiter ses cellules immédiatement, en mettant en attente les cellules des flots ABR. La difficulté réside dans la possibilité de discerner instantanément les différents types de flux. Une première solution a consisté à noter le type de flux dans la table de commutation VPI/VCI au moment de l'ouverture du circuit virtuel. La qualité de service est alors inscrite dans la table de commutation par

la cellule de signalisation. Malheureusement, cette solution extrêmement lourde ne peut mener à de très hauts débits dans les commutateurs.

Une solution à ce problème consisterait à ce que la cellule porte en elle un indice permettant de détecter directement la qualité de service. C'est ce que font les paquets IPv6 dans les quatre premiers octets. Dans l'en-tête de la cellule ATM, les bits disponibles sont rares, voire inexistants. On pourrait penser que la zone Payload Type pourrait jouer ce rôle, mais il n'en est rien, cette zone se chargeant de transporter des notifications ou des flux de gestion F5 (niveau circuit virtuel). De plus, le bit CLP n'a plus vraiment d'intérêt avec le contrôle ABR et des mémoires tampons en nombre suffisant.

Le contrôle de flux du service ABR est très complexe à mettre en œuvre dès que le nombre de circuits virtuels passant par un nœud est important. En effet, pour déterminer les valeurs à faire remonter vers les sources, on utilise des algorithmes complexes, dits du max-min, qui demandent une forte puissance de calcul et qui n'optimisent pas les valeurs qui remontent. Pour les réseaux locaux, l'ABR est plus facile à mettre en œuvre. Devant cette difficulté, l'ATM Forum réfléchit à de nouvelles solutions plus aisées à mettre en œuvre.

Parmi ces solutions, la plus souvent citée est l'UBR+, qui offre une qualité de service supérieure à celle de l'UBR mais inférieure à celle de l'ABR. L'idée de base de cette solution consiste à contrôler le flux essentiellement à l'entrée du réseau. Dans l'UBR+, on définit deux seuils. Lorsque le premier seuil est franchi, une première limitation du flux entrant est effectuée. Au-dessus du second seuil, le débit d'entrée est plus fortement limité, et les paquets les moins importants sont détruits.

Gestion des réseaux ATM

Comme expliqué précédemment, dans l'ATM, le plan utilisateur doit être complété par deux autres plans : le plan de gestion et le plan de contrôle. Pour la partie gestion de réseau, la principale contribution de l'UIT-T est la recommandation I.610. Cette recommandation concerne à la base la maintenance de l'interface UNI et les accès au réseau. Son rôle est de décrire les fonctions permettant de maintenir le niveau physique et l'accès au niveau de l'interface ATM.

La recommandation I.610 se préoccupe des opérations de contrôle et de maintenance, ou OAM (Operation And Maintenance). Cinq environnements sont privilégiés : la gestion de performance, la détection de pannes, la protection du système, l'information sur les pannes et les performances et enfin la localisation des fautes.

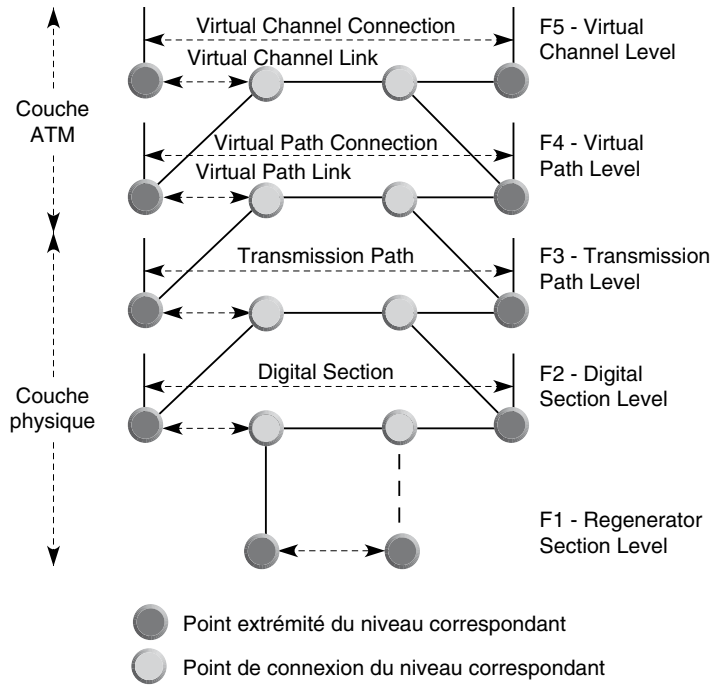
Les fonctions OAM sont réalisées dans le réseau par l'intermédiaire de cinq niveaux hiérarchiques OAM, associés aux deux niveaux ATM et PMD du modèle de référence UIT-T. Ces fonctions de contrôle et de gestion sont effectuées par des flots de données bidirectionnels : les flots F1, F2, F3, F4 et F5, dont voici la description :

- F1 : niveau section de régénération des signaux ;
- F2 : niveau section numérique ;
- F3 : niveau de transmission sur le chemin ;

- F4 : niveau du conduit virtuel ;
- F5 : niveau de la voie virtuelle.

Seuls les deux niveaux les plus élevés concernent la partie ATM. Toutes les autres fonctions s'appliquent au niveau physique. Nous avons représenté ces cinq niveaux de contrôle à la figure K.25.

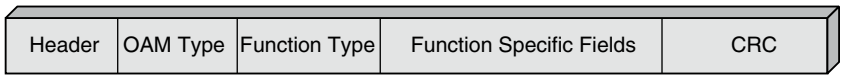
Figure K.25
Niveaux de contrôle et de gestion



Le flot F5 concerne le niveau de la voie virtuelle. Les cellules OAM du flot F5 sont identifiées par le champ PT (Payload Type), qui se trouve dans la zone de supervision. Ce champ indique une valeur PTI (Payload Type Identifier). La cellule OAM, pour chaque direction du flot F5, doit suivre une même route physique, de telle sorte que chaque nœud soit au courant de toutes les informations transportées dans un sens ou dans l'autre.

Les cellules OAM peuvent être insérées ou extraites aux différents points de connexion des VCC (Virtual Channel Connection).

Le flot F4 se préoccupe du niveau des conduits virtuels et a en charge le contrôle des VPC (Virtual Path Connection). Le flot F4 est bidirectionnel, comme le flot F5. Il est identifié par une valeur du VPI préassignée, généralement la valeur VCI = 3 pour le flux F4 sur un segment et VCI = 4 de bout en bout. Ses propriétés sont identiques à celles du flot F5. Cependant, le flot F5 est identifié par le format de la cellule OAM. Ce format est illustré à la figure K.26. En travaillant sur la gestion des performances, il est possible d'engendrer des messages qui transmettent les informations vers le récepteur ou vers l'émetteur.



OAM Type		Function type	
0001	Fault Management	0000	AIS (Alarm Indication Signal)
		0001	RDI (Remote Defect Indication)
		0010	Loopback
		0100	Continuity Check
0010	Performance Management	0000	Forward Monitoring
		0001	Backward Reporting
		0010	Monitoring and Reporting

Figure K.26

Format des cellules OAM

L'ATM Forum a défini une interface de gestion, nommée ILMI (Interim Local Management Interface). Cette interface permet à l'utilisateur d'obtenir des informations concernant les VP et les VC de l'interface UNI. Le protocole ILMI se fonde sur le standard de fait SNMP. Le mot intérim indique que ce standard n'est considéré que comme transitoire en attendant les recommandations de l'UIT-T. Cependant, il risque de devenir définitif puisque l'UIT-T est partie dans une direction différente en reprenant les standards CMIS/CMIP et TMN.

Le protocole ILMI est défini dans la RFC 1695.

Les principales fonctions du protocole ILMI sont les suivantes :

- indiquer le statut, la configuration et les informations de contrôle des niveaux liaison et physique de l'interface UNI ;
- gérer les adresses au travers de l'UNI.

La base de données de gestion de l'interface UNI fournit différents types d'informations, en particulier :

- des statistiques sur le niveau physique ;
- des informations sur le niveau ATM ;
- des statistiques sur les connexions VP et VC ;
- des informations sur les adresses enregistrées.

Le protocole ILMI supporte toutes les interfaces physiques définies par l'ATM Forum. Les deux extrémités de l'interface UNI gèrent un ensemble d'attributs, appelés UME (UNI Management Entities).

Les informations contenues dans les bases de données VPC ILMI MIB (VCC ILMI MIB) renseignent sur la connaissance de l'UME en fournissant des informations de configuration et les paramètres de QoS. Les enregistrements d'adresse permettent l'échange d'informations d'adresse et d'identificateur.

Annexe L

15. MPLS et GMPLS

Cette annexe introduit l'environnement IP sur ATM, qui a longtemps été considéré comme la solution de base des opérateurs de télécommunications, et décrit les diverses technologies qui se sont succédé depuis une vingtaine d'années pour parvenir à la technologie MPLS.

IP sur ATM

L'environnement IP est devenu le standard de raccordement à un réseau pour tous les systèmes distribués provenant de l'informatique. De son côté, la technique de transfert ATM a incarné la solution préférée des opérateurs pour relier deux routeurs entre eux avec une qualité de service. Il était donc plus que tentant d'empiler les deux environnements pour permettre l'utilisation à la fois de l'interface standard IP et de la puissance de l'ATM. Cette opération a donné naissance aux architectures dites IP sur ATM.

La difficulté de cette solution se situe au niveau de l'interface entre IP et ATM, avec le découpage des paquets IP en cellules, et lors de l'indication dans la cellule d'une référence correspondant à l'adresse IP du destinataire. En effet, le client que l'on souhaite atteindre est connu par son adresse IP, alors que les données doivent transiter par un réseau ATM. Pour ouvrir le chemin, ou circuit virtuel, il faut nécessairement connaître l'adresse ATM du client récepteur. La problématique vient de la correspondance d'adresses : en connaissant l'adresse IP du destinataire, comment trouver son adresse ATM ?

On peut regrouper les solutions à ce problème en trois grandes classes :

- Les techniques d'émulation, lorsque la correspondance d'adresses utilise un intermédiaire, l'adresse MAC.
- Le protocole CIOA (Classical IP over ATM), lorsqu'il n'y a qu'un seul sous-réseau ATM.
- Les techniques de serveur de routes MPOA (MultiProtocol Over ATM), PNNI (Private Network Node Interface) et NHRP (Next Hop Resolution Protocol), lorsqu'il y a plusieurs sous-réseaux ATM potentiels à traverser.

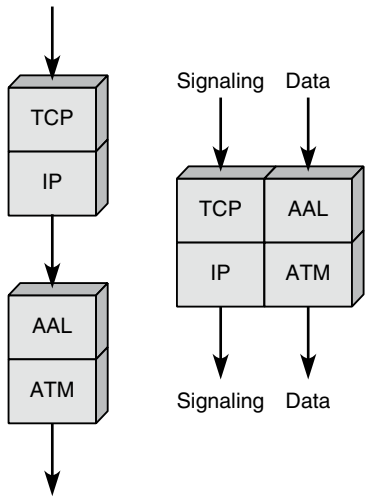
Ces trois techniques sont de plus en plus remplacées par un protocole beaucoup plus homogène, normalisé par l'IETF sous le nom de MPLS (MultiProtocol Label-Switching). Comme Ethernet et ATM, MPLS utilise des techniques de commutation de références, ou label-switching, mais avec d'autres types de trames, comme LAP-F ou PPP. MPLS fait appel à un chemin LSP (Label Switched Path), qui n'est autre qu'un circuit virtuel. Les paquets qui suivent ce chemin sont commutés dans les nœuds.

Pour le monde des opérateurs de télécommunications et, de façon plus fragmentaire, pour les très grandes sociétés internationales dotées de leur propre réseau, MPLS est devenu la technique de base depuis le début de la décennie.

Des extensions à MPLS ont été apportées avec GMPLS (Generalized MPLS), qui introduit de nouveaux paradigmes de commutation. Ce chapitre commence par décrire les techniques IP sur ATM avant de détailler MPLS puis GMPLS.

La figure L.1 illustre deux architectures potentielles pour IP sur ATM. L'architecture de gauche (IP over ATM) est celle qui a été retenue par la quasi-totalité des constructeurs et des opérateurs. L'architecture de droite est une solution non implémentée, qui consiste à mettre en parallèle une infrastructure ATM et une pile TCP/IP. L'idée est de faire passer la signalisation par le plan TCP/IP et les données par le plan ATM. L'intérêt de cette solution est d'utiliser l'universalité de l'adressage IP et la puissance de transfert de l'ATM.

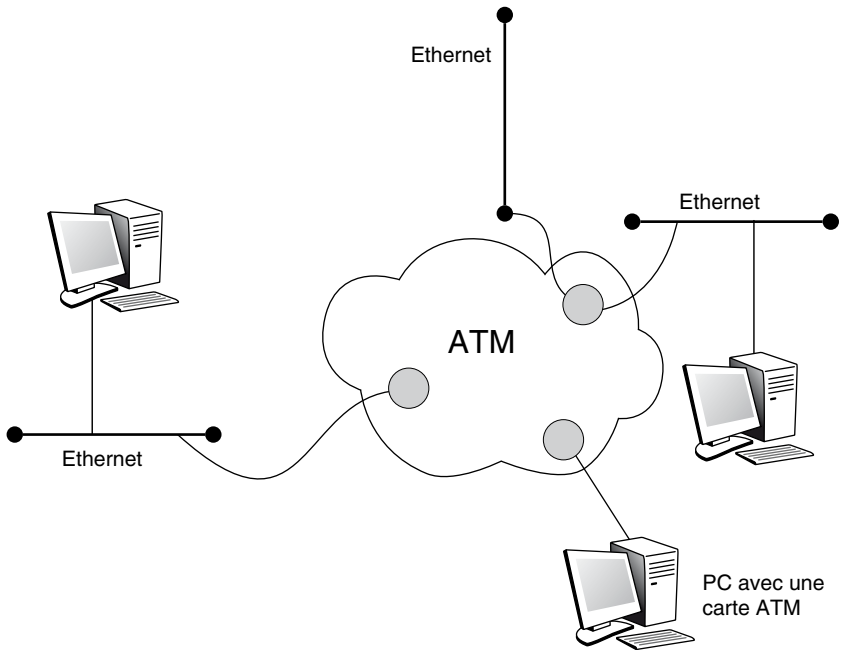
Figure L.1
Deux architectures IP sur ATM



Son inconvénient est de devoir mettre sur pied un double réseau et de ne pas avoir d'interface native ATM. C'est cette architecture qui va servir de base à MPLS.

Une troisième solution, de moins en moins utilisée, est ce que l'on appelle l'émulation de réseau, ou LANE (LAN Emulation). Elle est illustrée à la figure L.2. Dans cette solution, on se sert d'une adresse Ethernet comme intermédiaire entre l'adresse IP et l'adresse ATM. Cela permet d'ajouter une infrastructure ATM sans que les équipements terminaux aient à s'en soucier. C'est une façon d'introduire de l'ATM dans l'entreprise de manière transparente pour l'utilisateur. Nous en donnons ci-après quelques caractéristiques.

Figure L.2
Architecture LANE



LANE (LAN Emulation)

Le protocole LANE poursuit trois objectifs :

- remplacer un sous-réseau par un réseau ATM ;
- conserver les interfaces utilisateur ;
- faire communiquer des équipements terminaux ATM avec des équipements terminaux LAN.

L'un des inconvénients majeurs de cette solution est qu'elle nécessite une double correspondance IP-MAC et MAC-ATM.

Il existe de nombreuses façons de définir une émulation, dont l'une des meilleures est proposée par l'ATM Forum sous le sigle L-UNI (LAN emulation User-to-Network

Interface). Comme elle est de niveau MAC, cette émulation supporte toutes les applications existantes.

L'émulation L-UNI comporte quatre parties :

- L'émulation client, ou LEC (LAN Emulation Client), qui travaille comme un délégué pour le terminal ATM.
- L'émulation serveur, ou LES (LAN Emulation Server), qui résout la correspondance des adresses MAC et ATM.
- L'émulation serveur pour les applications multipoint, ou BUS (Broadcast and Unknown Server), qui résout la correspondance des adresses multipoint.
- L'émulation serveur de configuration, ou LECS (LAN Emulation Configuration Server), qui permet de mettre à jour une station qui se connecte.

Le logiciel LEC, que doit posséder toute station ou tout routeur qui veut être émulé, détient une adresse ATM d'accès. Le LES mémorise toutes les adresses MAC des stations des réseaux locaux qui sont logiquement attachés et leur adresse ATM associée. Le BUS est un serveur du même type que le LES mais pour les adresses de diffusion et multipoint. Enfin, le LECS possède les informations de configuration, comme l'adresse du LES du réseau émulé auquel appartient une station qui s'active.

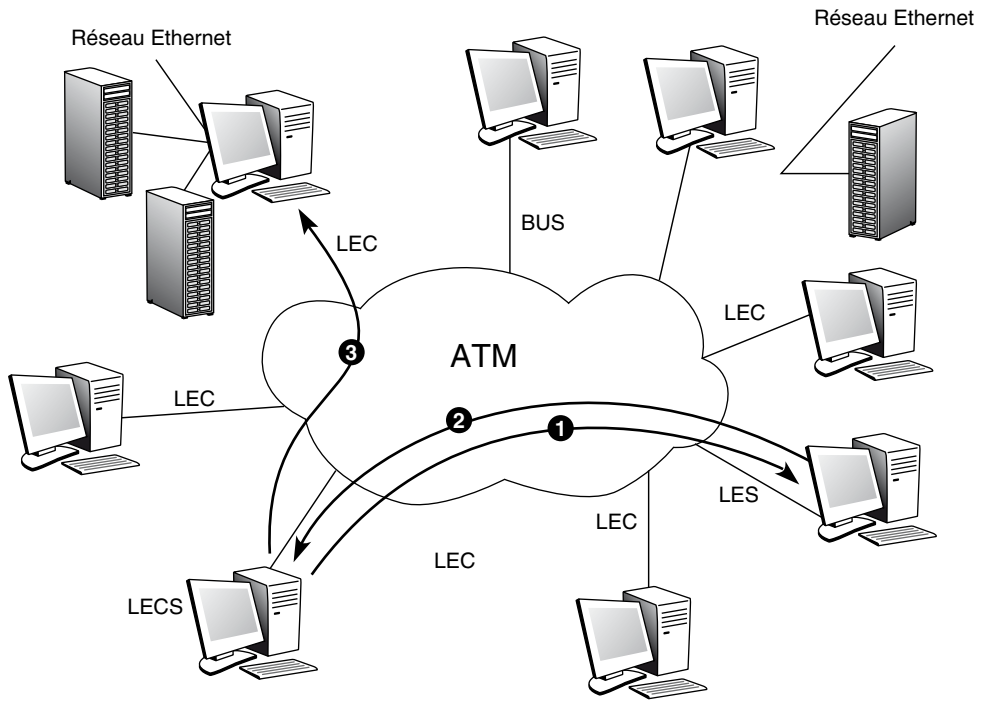
Quand un client désire envoyer une trame vers une autre station, il fait parvenir au serveur LES une requête sur l'adresse ATM correspondant à l'adresse MAC de la station destinataire. Le serveur répond avec l'adresse ATM du LEC auquel la station destination est connectée. Ensuite, le LEC ouvre un circuit virtuel avec son correspondant, déterminé par l'adresse ATM que lui a procurée le LES, et convertit la trame MAC en plusieurs trames ATM et envoie les cellules. Au LEC d'arrivée, les cellules sont converties en trames MAC, qui sont alors envoyées vers le terminal approprié.

Le cheminement des flots s'effectue de la façon illustrée à la figure L.3. Le parcours 1 correspond à l'envoi par le client d'une requête, portant une demande de conversion d'une adresse IP en une adresse ATM, envoyée au serveur LES. Le parcours 2 illustre la réponse à cette requête. Le client connaissant maintenant l'adresse ATM de son correspondant, il peut lui envoyer un flot de paquets IP encapsulés dans des trames ATM et circulant sur le circuit virtuel ouvert vers l'adresse ATM du destinataire. Le parcours 3 correspond à l'ouverture du circuit virtuel avec la machine distante dont l'adresse ATM a été obtenue grâce à la conversion effectuée.

Si le serveur LES n'est pas capable d'effectuer la traduction d'adresse, il faut envoyer une demande de traduction au BUS. Celui-ci émet en diffusion cette demande vers l'ensemble des récepteurs du réseau ATM. La station de réception qui se reconnaît comme étant le correspondant, grâce à l'adresse IP incluse dans la demande, renvoie son adresse ATM à l'émetteur, qui peut enfin ouvrir un circuit virtuel, où transitera le flot des paquets IP.

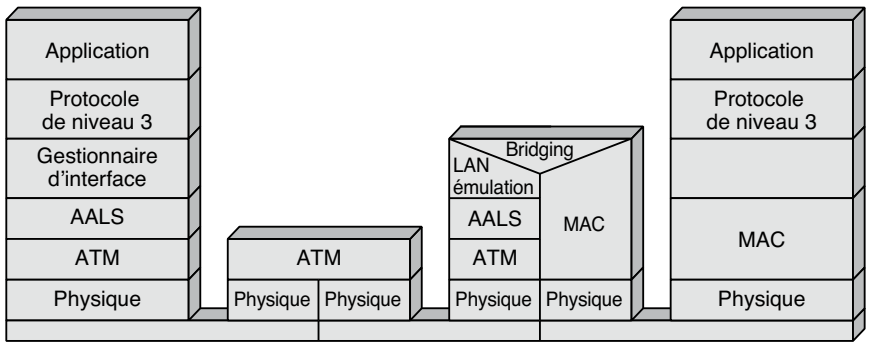
Le serveur BUS est également utilisé lorsque l'adresse IP du récepteur est multicast. Le serveur BUS possède pour cela des circuits virtuels ouverts avec l'ensemble des machines participant au réseau ATM.

Figure L.3
Émulation L-UNI



La figure L.4 illustre l'architecture du LANE. La pile protocolaire de droite représente une machine terminale connectée à un réseau local. Celui-ci mène à un équipement de connexion au réseau ATM. La pile protocolaire de gauche représente une station ATM attachée directement au réseau ATM mais travaillant en émulation LAN. Les piles protocolaires du milieu représentent, à droite, un commutateur ATM et, à gauche, la passerelle de passage entre le réseau local et le réseau ATM.

Figure L.4
Architecture de l'émulation de réseaux locaux LANE



LANE 2.0 introduit une évolution notable par rapport à cette première génération en ajoutant le respect de la qualité de service et le support d'applications multipoint. Cette

génération n'a cependant pas eu le temps de s'étendre, du fait de l'arrivée de MPLS, que nous détaillons dans la suite de ce chapitre.

CIOA (Classical IP over ATM)

La solution CIOA permet de transporter les paquets IP par l'intermédiaire d'un réseau ATM sans émulation de réseau local. Pour ce faire, l'adresse IP est traduite directement dans une adresse ATM. Pour réaliser le transport de l'information, il suffit d'encapsuler les paquets IP dans des cellules ATM. À la différence de la solution précédente, on ne passe pas par une première encapsulation dans une trame Ethernet, elle-même encapsulée dans des cellules ATM.

Issue du groupe de travail ION (Internetworking Over NBMA), chargé par l'IETF en 1996 de redéfinir les environnements IP sur ATM, CIOA est la solution la plus répandue aujourd'hui. Le sigle NBMA (Non Broadcast Multiple Access) a été attribué à tous les réseaux qui n'offrent pas une diffusion au niveau physique, comme celle obtenue dans un réseau Ethernet partagé. Un réseau ATM est un NBMA au même titre qu'un réseau relais de trames.

Pour réaliser la correspondance d'adresses, comme dans le couple IP-Ethernet, il faut un protocole de type ARP (Address Resolution Protocol), ici ATMARP (ATM's Address Resolution Protocol). Ce protocole est défini dans la RFC 1577, qui précise la notion de sous-réseau IP, ou LIS (Logical IP Subnetwork). Tous les utilisateurs connectés sur un LIS ont un préfixe d'adresse en commun. Un LIS regroupe l'ensemble des machines et des routeurs IP appartenant au même sous-réseau au sens IP. Un LIS comporte un serveur ATMARP, connu de toutes les machines connectées sur le LIS et contenant les correspondances d'adresses IP et ATM des stations du LIS.

Une station qui veut communiquer avec une autre station sur le LIS envoie une requête au serveur (phase 1), lequel, dans le cas standard, lui communique l'adresse ATM correspondante (phase 2), permettant à la station source d'ouvrir un circuit virtuel avec la station destination (phase 3). Ces trois phases sont illustrées à la figure L.5

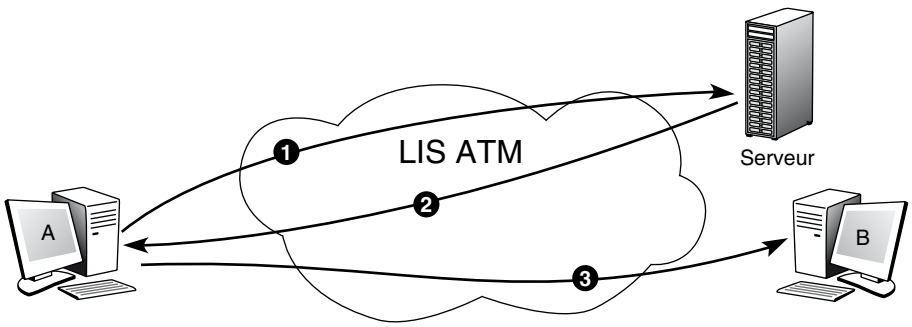
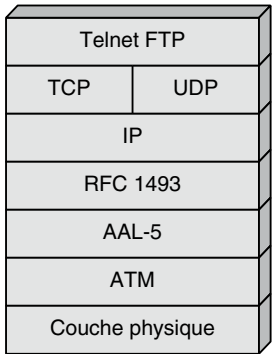


Figure L.5
Connexion CIOA

Les paquets IP sont encapsulés dans des cellules ATM au moyen d'une fragmentation effectuée par l'AAL-5. Les spécifications de la fragmentation et du réassemblage sont indiquées dans les RFC 1577 et 1483. L'architecture protocolaire de l'encapsulation CIAO est illustrée à la figure L.6.

Figure L.6

Architecture protocolaire de l'encapsulation CIAO



CIOA se place au niveau 3 de l'architecture OSI et utilise une résolution d'adresse IP directement en ATM. La résolution d'adresse de l'émulation LAN opère pour sa part au niveau MAC. Ce sont bien sûr deux solutions incompatibles. CIOA est beaucoup plus simple que l'émulation LAN, mais elle ne permet pas de gérer la diffusion.

De nombreuses autres possibilités d'encapsulation ont été proposées, dont les plus connues sont les suivantes :

- TULIP (TCP and UDP Lightweight IP), RFC 1932 ;
- TUNIC (TCP and UDP over a Non-existing IP Connection), également décrite dans la RFC 1932.

Le rôle de ces deux encapsulations concernant deux stations appartenant au même LIS est de simplifier les traitements dans le niveau IP en supprimant en grande partie l'en-tête.

Comme nous venons de le voir, la corrélation d'adresses dans CIOA se fait au niveau IP-ATM, ce qui simplifie la recherche de la correspondance d'adresses mais limite son utilisation aux réseaux IP. Avec la deuxième génération du protocole CIOA, la résolution d'adresse s'effectue par un mécanisme InATMARP (Inverse ATM's ARP), qui est une extension du mécanisme RARP (Reverse ARP) d'Internet. Dans CIOA 2, le protocole NHRP, que nous détaillons à la section suivante, peut être utilisé.

Le groupe ION de l'IETF a mis au point le système MARS (Multicast Address Resolution Server) pour émuler le multicast au-dessus d'ATM. Ce service est étendu à tous les protocoles de la couche réseau au-dessus des réseaux NBMA. Le système MARS comporte un serveur et des clients. Dans le cadre d'IPv4, MARS ne travaille que sur un LIS. Il est possible d'ajouter des serveurs spécialisés MCS (Multicast Cluster Server) pour remplacer le serveur MARS dans la distribution des paquets et de la gestion des applications multicast. Il n'est toutefois pas évident de trouver l'architecture optimale entre une

centralisation dans un serveur MARS unique et une distribution totale dans un réseau de serveurs MCS.

Avec l'arrivée d'IPv6, le protocole ATMARP ne peut plus être exploité. IPv6 au-dessus d'ATM remplace le processus ATMARP par ND (Neighbor Discovery), ce qui empêche le fonctionnement du protocole CIOA tel que nous l'avons décrit. De ce fait, l'IETF a normalisé dans les RFC 2491 et 2492 deux nouveaux protocoles pour le remplacer. Ces protocoles spécifient la mise en place d'IPv6 au-dessus de réseaux NBMA. Le protocole MARS est repris mais étendu pour transporter du trafic IPv6 unicast. Dans ce nouvel environnement, les LIS sont remplacés par des LL (Logical Link). Le serveur MARS réalise les fonctions auparavant réalisées par le serveur ATMARP.

NHRP et MPOA

Les deux solutions décrites précédemment, LANE et CIOA, s'appliquent facilement à un LIS (Logical IP Subnetwork) unique. Les protocoles utilisés par le BUS ou la procédure ATMARP requièrent une diffusion. Si les requêtes peuvent traverser des passerelles, la diffusion devient difficile à maîtriser. Il faut donc un protocole pour rechercher l'adresse du destinataire sans diffusion afin que l'environnement IP puisse se mettre au-dessus d'un ensemble de sous-réseaux ATM.

Considérons un ensemble de LIS ATM formant un NBMA. Chacun des réseaux ATM interconnectés a donc des utilisateurs possédant un préfixe d'adresse en commun et formant un LIS. Connaissant l'adresse IP du destinataire, il est possible de déterminer l'adresse ATM correspondante. La figure L.7 illustre le processus consistant à trouver l'adresse ATM du destinataire en connaissant son adresse IP alors qu'il ne se trouve pas sur le même réseau.

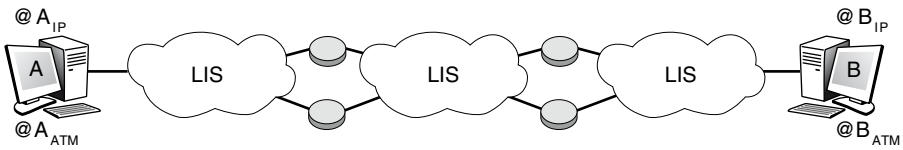


Figure L.7

IP sur plusieurs LIS interconnectés

NHRP (Next Hop Resolution Protocol)

Le protocole NHRP provient du monde Internet et est décrit dans la RFC 1932. Il permet de rechercher l'adresse ATM correspondant à une adresse IP dans un réseau NBMA composé de plusieurs LIS. Plus précisément, NHRP permet la résolution d'une adresse IP d'une station de travail se trouvant sur un LIS distant en une adresse du réseau NBMA (adresse ATM, relais de trames, etc.).

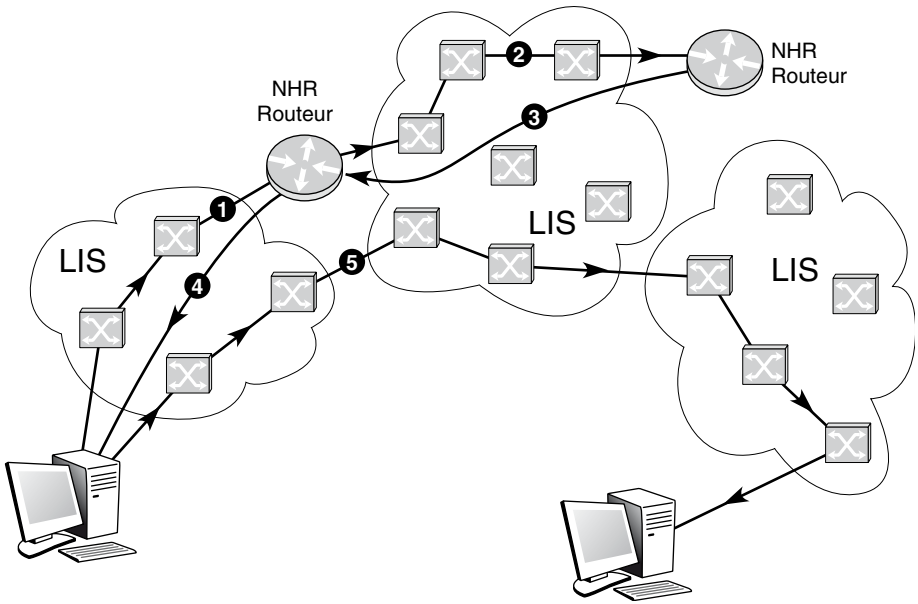
Chaque LIS possède un serveur de route, appelé NHS (Next Hop Server), souvent situé dans un routeur. Lorsqu'un client demande une connexion, il s'adresse au NHS du LIS

auquel il appartient pour obtenir les informations de routage sur son paquet. Si le NHS local ne peut résoudre le problème de la localisation, il adresse une requête vers les NHS connexes, et ainsi de suite jusqu'à arriver au LIS auquel le destinataire appartient.

Cette solution permet de trouver une route beaucoup plus directe que le passage par les différents NHS, comme l'illustre la figure L.8. La phase 1 correspond à la demande de conversion d'adresse au NHR Routeur du premier LIS, lequel s'adresse avec la phase 2 au NHR Routeur du LIS dont dépend l'utilisateur distant. Les phases 3 puis 4 correspondent au retour de la conversion d'adresse. Avec l'adresse ATM le client ouvre un circuit virtuel avec le distant : c'est la phase 5. On peut ainsi obtenir une connexion directe en mode ATM de deux stations appartenant à des LIS distants, sans qu'il soit nécessaire de remonter au niveau IP du routeur.

Figure L.8

Mise en place d'une route par NHRP



MPOA (MultiProtocol Over ATM)

MPOA est un protocole mis au point par l'ATM Forum. Plus complexe que NHRP, il se sert des techniques décrites aux sections précédentes en les unissant et en les complétant pour réaliser le transport de paquets IP ou de paquets d'autres protocoles, comme IPX, sur une interconnexion de réseaux ATM. La route peut être déterminée soit par une solution centralisée de type serveur de route, soit par une solution distribuée utilisant les protocoles PNNI ou NHRP.

Le rôle de MPOA est toujours de trouver l'adresse ATM du correspondant pour ouvrir une connexion directe, ou shortcut, entre deux stations ATM qui ne se connaissent au départ que par leur adresse IP.

Les deux composantes de MPOA sont les suivantes :

- MPC (MPOA Client), qui, à la demande d'un client, recherche la meilleure route pour ouvrir un circuit virtuel avec un client dont il connaît l'adresse IP.
- MPS (MPOA Server), situé dans un routeur, qui, à l'aide d'un routage classique, tel que RIP (Routing Information Protocol), OSPF (Open Shortest Path First), etc., achemine les requêtes NHRP de demandes de correspondance.

La figure L.9 illustre le fonctionnement de MPOA. La phase 1 correspond à la demande de conversion d'adresse qui remonte jusqu'au serveur MPS connaissant la réponse. La phase 2 transporte la réponse à la demande de conversion qui permet l'ouverture du circuit virtuel vers le distant.

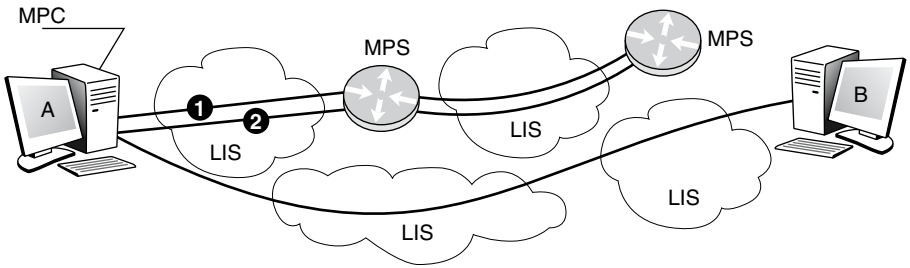


Figure L.9
Fonctionnement de MPOA

PAR et I-PNNI

Issu de l'ATM Forum, le protocole PNNI a pour fonction de mettre en place une connexion entre deux utilisateurs en subdivisant le réseau en sous-réseaux, chaque sous-réseau possédant un nœud leader capable de connaître l'état des autres sous-réseaux et de renvoyer ces informations à ses propres nœuds dans son sous-réseau.

Lorsque des routeurs IP sont interconnectés par un ensemble de réseaux ATM, il est difficile de déterminer le chemin à suivre. Une solution pour trouver un chemin consiste à utiliser le protocole PNNI. Les mécanismes PAR et I-PNNI ont pour objet d'établir cette jonction entre les routeurs et le protocole PNNI.

- PAR (PNNI Augmented Routing) permet d'élire un serveur de route sur une machine de chaque sous-réseau ATM. Ce routeur est appelé DR (Designated Router). C'est lui qui est capable de faire la résolution d'adresse entre la partie IP et le réseau ATM et qui déclenche le protocole PNNI pour mettre en place une route sur l'interconnexion de réseaux ATM.
- I-PNNI (Integrated PNNI) étend le protocole PNNI de sorte qu'il puisse être utilisé sur les sous-réseaux IP. Dans chaque sous-réseau LIS, on indique en ce cas un leader.

Les solutions pré-MPLS

Introduite par la société Ipsilon, IP-switching a été la première version du label-switching. Dans cette architecture, la route est déterminée par le flot IP.

Les autres solutions, principalement le tag-switching de Cisco Systems et ARIS (Aggregate Route-based IP Switching) d'IBM, utilisent des routes déterminées par la topologie et non plus par le flot. La norme MPLS a également choisi cette solution du choix de la route déterminée par la topologie pour des raisons de passage à l'échelle. Le tag-switching a été proposé quelques mois après l'annonce de l'IP-switching. Cisco a essayé de promouvoir sa solution *via* l'IETF, et de nombreuses RFC sont disponibles sur le type de sous-réseaux — ATM, PPP, Ethernet — à utiliser, ainsi que sur la possibilité de faire du multicast et d'utiliser le protocole RSVP.

La proposition ARIS d'IBM a été soumise à l'IETF sous forme de RFC. Comme dans le tag-switching, la mise en place des routes s'effectue par un algorithme dépendant de la topologie du réseau et non par une signalisation utilisant le premier paquet du flot de données. Les routes sont donc déterminées à l'avance.

Ces solutions reposent sur le principe de la détermination d'une route entre l'émetteur et le récepteur, cette route étant établie par des serveurs de route. Les fragments de paquets IP sont étiquetés à l'entrée du réseau pour suivre la route déterminée. La route peut traverser des réseaux divers, aussi bien ATM que relais de trames ou Ethernet. La référence se trouve dans la zone VPI/VCI de la cellule ATM, dans la zone DLCI de la trame LAP-F d'un réseau relais de trames ou dans une zone supplémentaire de la trame Ethernet. On retrouve là la solution de mise en place d'une route à l'intérieur du réseau et de commutation de trames le long de cette route.

Les différences d'implémentation proviennent des antécédents des constructeurs. Si le constructeur propose des routeurs à son catalogue, il doit ajouter la partie ATM pour commuter les cellules ATM. Si le constructeur provient de l'environnement ATM, c'est un serveur de route IP qui est ajouté.

Annexe M

16. Les réseaux IP : architecture

Cette annexe décrit l'évolution d'Internet, depuis ses débuts et sa normalisation jusqu'à la solution actuelle, puis détaille certaines techniques de NAT.

Les débuts du réseau Internet

L'adoption quasi universelle de l'environnement IP en fait son principal intérêt. La DARPA (Defense Advanced Research Projects Agency) a développé un concept de réseaux interconnectés, Internet, au milieu des années 1970, avec une architecture et des protocoles qui ont acquis leur forme actuelle vers 1977-1979.

À cette époque, la DARPA est connue comme le premier centre de recherche sur les réseaux à transfert de paquets avec la création d'ARPAnet, à la fin des années 1960. Il est à noter qu'un projet assez semblable est développé en même temps en France sous le nom de Cyclades. Malheureusement, ce projet est arrêté pour laisser place au protocole X.25.

La disponibilité des fonds de recherche de la DARPA attire l'attention et éveille l'imagination de plusieurs groupes de chercheurs, notamment ceux qui ont déjà l'expérience du transfert de paquets dans ARPAnet. La DARPA organise des rencontres informelles avec les chercheurs pour mettre en commun des idées et discuter des expérimentations effectuées. À partir de 1979, il y a tant de chercheurs impliqués dans TCP/IP que la DARPA fonde un comité de coordination, appelé ICCB (Internet Control and Configuration Board). Le groupe se réunit régulièrement jusqu'en 1983, année où il est réorganisé.

Le réseau Internet démarre en 1980, quand la DARPA commence à convertir les protocoles du réseau de la recherche à TCP/IP. La migration vers Internet est complète en

1983, quand le bureau du secrétariat de la Défense rend obligatoires les protocoles pour tous les hôtes connectés aux réseaux grande distance. Au même moment, ARPAnet est scindé en deux réseaux séparés, un pour la recherche, qui garde le nom d'ARPAnet, et un plus grand, réservé aux militaires, appelé Milnet.

Pour encourager les chercheurs à adopter les nouveaux protocoles, la DARPA propose des implémentations à bas prix. La plupart des ordinateurs des universités utilisent une version UNIX de l'Université de Californie, de Berkeley Software Distribution, appelée UNIX Berkeley. En fondant la société Bolt Beranek et Newman pour implémenter les protocoles et en finançant Berkeley pour intégrer TCP/IP dans ses produits, la DARPA réussit à couvrir 90 % des ordinateurs des universités scientifiques. Ce succès avec les ordinateurs scientifiques produira un effet d'entraînement sur les autres communautés.

En 1985, la NSF (National Science Foundation) commence à développer un programme destiné à mettre en place un réseau autour de ses six centres de supercalculateurs. En 1986, elle crée un réseau longue distance fédérateur, le NSFNET, pour relier tous ses centres de calcul et se connecter à ARPAnet. L'ensemble de ces réseaux interconnectés forme Internet, auquel viennent se greffer peu à peu de nouveaux réseaux.

Internet se développe alors rapidement pour interconnecter des milliers de réseaux aux États-Unis et en Europe et connaît un taux de croissance d'environ 15 % par an en 1987 avant d'atteindre le rythme de 60 % par an.

L'adoption des protocoles d'Internet s'élargit ensuite aux entreprises privées, qui commencent à se relier à Internet, avant de s'étendre aux réseaux privés d'entreprise, même s'ils ne sont pas connectés à Internet. Ces réseaux privés prennent le nom d'intranet.

La normalisation des réseaux IP

De nos jours, des centaines de sociétés importantes commercialisent des produits TCP/IP. Ce sont elles qui décident de la mise sur le marché de nouvelles technologies, et non plus les chercheurs, comme à l'origine. La gouvernance de l'Internet a été totalement repensée à la fin des années 2000. L'autorité sur les fonctions de coordination centrales d'Internet est exercée par l'IANA (Internet Assigned Numbers Authority). En fait, c'est Jon Postel qui exerçait cette charge jusqu'à son décès en 1998. Aujourd'hui c'est l'ICANN qui exerce cette fonction.

L'ICANN (Internet Corporation for Assigned Names and Numbers) est une organisation à but non lucratif domiciliée en Californie. Ses principales missions sont l'attribution des plages d'adresses de l'environnement IP, la sélection des paramètres des protocoles utilisés, la gestion du DNS (Domain Name System) et la gestion du nœud racine américain. Il est à noter qu'il existe un deuxième réseau Internet, indépendant de celui géré par l'ICANN, et qui est l'Internet chinois, doté de son propre nœud racine. Les Européens songent fortement à mettre en place également leur propre réseau Internet avec un nœud racine en Europe.

L'ICANN est géré par un conseil d'administration composé de 20 membres. À l'ICANN sont associées trois organisations, nommées SO (Supporting Organization), et des

comités consultatifs. Les trois organisations SO sont responsables de missions pour le compte de l'ICANN :

- DNSO (Domain Name SO) s'occupe des questions liées aux noms de domaines ;
- ASO (Address SO) prend en charge la gestion des adresses IP ;
- PSO (Protocol SO) traite des protocoles Internet.

Les comités consultatifs sont les suivants :

- Government Advisory Committee
- Root Server System Advisory Committee
- Budget Advisory Group
- Membership Implementation Task Force
- At-Large Member Study Committee

Nous ne détaillons ici que le PSO, qui s'occupe de la partie technique d'Internet. Le PSO (Protocol Supporting Organization) a pour mission de soumettre au conseil d'administration de l'ICANN des avis et recommandations pour toutes les questions touchant aux protocoles utilisés sur Internet, aux standards techniques permettant aux équipements d'extrémité d'échanger des informations et de gérer les communications sur Internet. Les signataires du décret de mise en place du PSO sont l'IETF, le W3C (World-Wide Web Consortium), l'UIT, l'ETSI et l'ICANN.

Quatre organismes sont regroupés dans le PSO :

- IETF
- IAB (Internet Activities Board)
- ISOC (Internet Society)
- IESG (Internet Engineering Steering Group)

L'IETF est un groupe d'individus qui se réunit trois fois par an pour contribuer au développement et à l'évolution d'Internet. Ses missions consistent à proposer des solutions aux problèmes techniques, formaliser les solutions retenues, les porter auprès de l'IESG en vue de la standardisation des protocoles et de leur utilisation sur Internet et être un forum de discussions. L'IETF n'est pas une organisation de standardisation au sens classique du terme, puisque tout le monde peut y participer et qu'il n'y a pas de représentation des organismes officiels de normalisation. Cependant, ses spécifications deviennent des standards.

La première réunion de l'IETF a lieu en janvier 1986 à San Diego. Seules 15 personnes y participent. Le quatrième meeting de l'IETF, en Californie également, en octobre 1986, est le premier à accueillir des participants étrangers. Le concept des groupes de travail est introduit lors du cinquième meeting, tenu toujours en Californie en février 1987. La barre des 100 participants est atteinte dès le septième meeting, tenu en Virginie en juillet 1987. En juillet 1989, lors du quatorzième meeting, tenu à Stanford, la structure de l'IETF est profondément remaniée, avec la séparation des activités de l'IAB en deux pôles distincts : l'IETF et l'IRTF (Internet Research Task Force), qui se préoccupe des projets de

recherche à long terme. Après la formation de l'ISOC en janvier 1992, l'IAB passe sous son autorité.

L'IAB a pour objectif d'arbitrer et de conseiller les autres organismes en ayant une vue d'ensemble de l'architecture Internet. Il peut aussi, dans le cadre de la procédure de définition des standards d'Internet, juger en appel de décisions prises par l'IESG. L'IAB est responsable de la sélection des membres de l'IESG parmi les nominés proposés par le comité de nomination de l'IETF.

L'ISOC est une association de professionnels qui s'intéresse à la croissance et à l'évolution d'Internet dans le monde en termes sociaux, politiques et techniques. Les responsables de l'ISOC doivent sélectionner les membres de l'IAB parmi les nominés proposés par le comité de nomination de l'IETF.

L'IESG supervise les activités techniques de l'IETF et le processus de définition des standards. Dépendant de l'ISOC, il applique les règles définies par cet organisme. L'IESG est directement responsable de la définition des standards, depuis le choix des propositions jusqu'à leur validation finale.

Les documents de travail, propositions et normes Internet sont édités dans une série de rapports techniques, appelés RFC (Request For Comments). Ces dernières peuvent couvrir des sujets précis ou vastes et faire figure de normes ou seulement de propositions. Les normes et la documentation relatives aux protocoles peuvent être obtenues auprès du site de l'IETF.

Chaque protocole Internet a un état et un statut. L'état du protocole spécifie l'avancement des travaux de normalisation :

- Initial (*initial*) : le protocole est soumis pour être examiné.
- Norme proposée (*proposed standard*) : le protocole est proposé comme norme et subit la procédure initiale.
- Norme de travail (*draft standard*) : le protocole a passé l'examen initial et peut être considéré comme étant dans sa forme semi-finale. Au moins deux implémentations indépendantes sont produites. Le document les décrivant est étudié par le groupe de travail *ad hoc*. Des modifications sont souvent introduites avant la norme finale.
- Norme (*standard*) : le protocole examiné est accepté comme une norme complète. Il fait officiellement partie de TCP/IP.
- Expérimental (*experimental*) : le protocole n'est pas soumis à normalisation mais reste utilisé dans des expérimentations.
- Historique (*historic*) : le protocole est périmé et n'est plus utilisé.

Normalement, les protocoles soumis doivent être passés en revue par le groupe de travail correspondant de l'IETF puis par les organismes cités plus haut avec une formalisation par l'IAB d'un statut. Le statut du protocole indique sous quelles conditions le protocole doit être utilisé :

- Exigé (*required*) : toutes les machines et les passerelles doivent implémenter le protocole.

- Recommandé (*recommended*) : toutes les machines et les passerelles sont encouragées à implémenter le protocole.
- Facultatif (*elective*) : on peut choisir d'implémenter ou non le protocole.
- Utilisation limitée (*limited use*) : le protocole n'est pas spécifié pour une utilisation générale, comme dans le cas d'un protocole expérimental.
- Non recommandé (*non recommended*) : l'utilisation du protocole n'est pas recommandée, par exemple pour un protocole périmé.

Le tableau M.1 récapitule les normes principales du monde Internet.

Tableau M.1 • Normes Internet

Nom	Description	Statut/RFC
ARP	Address Resolution Protocol	Elect. 826
RARP	Reverse ARP	Elect. 903
IP	Internet Protocol	Req. 791
ICMP	Internet Control Message Protocol	Req. 792
IGMP	Internet Group Multicast Protocol	Rec. 1112
UDP	User Datagram Protocol	Rec. 768
TCP	Transmission Control Protocol	Rec. 793

Les trois catégories de NAT

Le mécanisme de NAT que nous avons pris comme exemple précédemment, consistant à jouer sur les ports pour masquer plusieurs terminaux avec une adresse IP unique, est un cas particulier. Il repose sur une translation de port appelée NPT (Network Port Translation). Lorsqu'elle se combine avec le NAT, on parle de NAPT (Network Address and Port Translation).

Bien que les concepts soient différents, le processus de NAT inclut fréquemment par abus de langage le processus de NPT. En réalité, il faut distinguer trois formes de NAT, le NAT statique, le NAT dynamique et NATP. Ces formes peuvent se combiner selon les besoins de chaque utilisateur et les politiques d'administration établies dans un réseau. D'autres formes de classification du NAT sont possibles. La RFC 3489 en recense quatre types, par exemple. Nous nous contenterons de détailler dans les sections suivantes les formes les plus courantes.

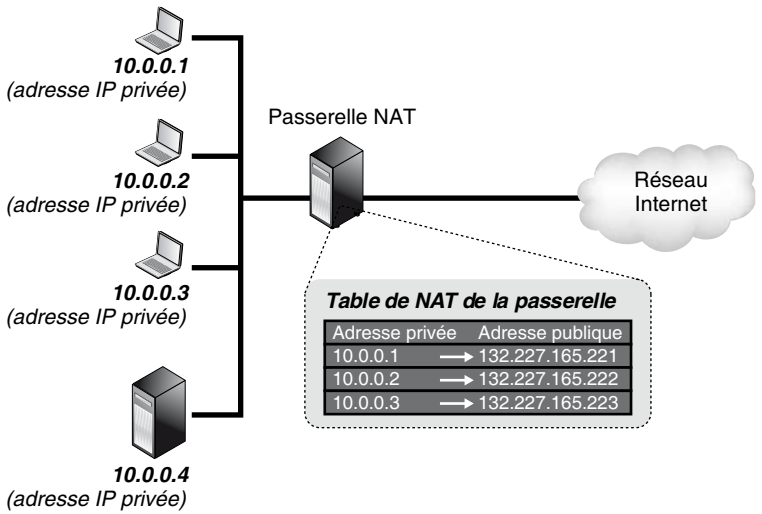
Le NAT statique

Dans le NAT statique, à toute adresse IP privée qui communique avec l'extérieur, une adresse IP publique fixe lui est affectée. Avec ce type de NAT, les utilisateurs du réseau local sont joignables de l'extérieur, car la passerelle réalise la correspondance d'une adresse IP locale en une adresse IP publique dans les deux sens. C'est un avantage

indéniable, en particulier pour la téléphonie, car un utilisateur à l'extérieur du réseau privé peut appeler un abonné à l'intérieur du réseau privé puisqu'il connaît son adresse IP fixe.

Ce cas de figure est illustré à la figure M.1. Le terminal ayant l'adresse IP privée 10.0.0.4 n'a pas de correspondance d'adresse IP publique, car c'est un serveur interne. Les administrateurs font l'économie d'une adresse IP pour ce serveur et s'assurent en outre que ce dernier n'est pas joignable directement de l'extérieur. Un changement de FAI ne remet pas en cause le plan d'adressage en local.

Figure M.1
Le NAT statique



Le NAT dynamique

Avec le NAT dynamique, une plage d'adresses IP publiques est disponible et partagée par tous les utilisateurs du réseau local. Chaque fois qu'une demande d'un utilisateur local (avec une adresse privée) parvient à la passerelle NAT, celle-ci lui concède dynamiquement une adresse IP publique. Elle maintient cette correspondance pour une période fixe, mais renouvelable selon l'activité de l'utilisateur, qui assure le suivi des communications.

Avec ce type de NAT, les utilisateurs locaux ne sont joignables de l'extérieur que s'ils ont une entrée dans la table de la passerelle NAT, autrement dit que s'ils entretiennent une activité avec le réseau Internet. En effet, les correspondants externes ne peuvent s'adresser qu'à la passerelle NAT pour envoyer leur flux. Or tant que le correspondant interne n'a pas d'activité réseau, aucune entrée ne lui est attribuée dans la table de NAT. De plus, l'adresse IP qui leur est affectée est temporaire et peut être différente à la prochaine connexion, ce qui restreint les possibilités d'être joignable de l'extérieur.

Il existe même une forme de NAT particulière, appelée NAT symétrique ou « full cone » dans la RFC 3489, qui consiste à établir une correspondance entre l'adresse IP privée et publique selon la destination d'une communication. Autrement dit, un utilisateur du

réseau local aura une certaine adresse IP publique lorsqu'il communique avec un correspondant extérieur et une autre adresse IP publique lorsqu'il communique avec une autre destination.

Le modèle dynamique offre une plus grande souplesse d'utilisation que le modèle statique puisque les associations d'adresses IP privées et publiques n'ont pas besoin d'être mentionnées statiquement par l'administrateur, mais sont attribuées automatiquement. En outre, il présente l'avantage d'optimiser au maximum les ressources. Si un utilisateur n'exploite pas sa connexion Internet et se contente de sa connexion locale, la passerelle NAT n'a pas besoin de lui attribuer une adresse IP. Le NAT dynamique est cependant plus complexe puisqu'il impose à la passerelle NAT de maintenir les états des connexions pour déterminer si les utilisateurs exploitent leur adresse IP publique ou s'il est possible, passé un certain délai, de les réutiliser.

Ce modèle ressemble à celui déployé avec la téléphonie RTC. Le nombre de lignes sortantes d'un commutateur téléphonique d'entreprise et même d'immeubles de particuliers est généralement inférieur au nombre de lignes entrantes. Autrement dit, tous les abonnés disposent d'un téléphone, mais tous ne peuvent appeler en même temps. Dans la pratique, il est assez exceptionnel que tous les abonnés appellent en même temps, si bien que ces derniers ne perçoivent pas cette restriction, qui permet aux opérateurs de limiter le nombre de lignes. Avec le NAT dynamique, les notions sont différentes, mais le principe est le même : l'attribution des adresses IP se fait à la demande, avec les limitations du nombre d'adresses IP publiques disponibles que cela suppose.

Le NAPT

Variante du NAT dynamique, le NAPT (Network Address Port Translation) est en fait celui que nous avons présenté précédemment sans le nommer. Il consiste à attribuer une même adresse IP à plusieurs utilisateurs d'un même réseau local.

Comme nous l'avons expliqué, pour associer une même adresse IP publique à deux terminaux ayant une adresse privée distincte, la passerelle NAT joue sur les ports des applications : une requête envoyée à partir du port A d'une source est retransmise avec le port B de la passerelle, tandis qu'une requête émise à partir du port C d'une autre source est retransmise avec le port D de la passerelle. De cette manière, la passerelle peut contrôler et distinguer chacune des demandes qui lui parviennent.

L'inconvénient de cette méthode est que seuls les utilisateurs du réseau local peuvent amorcer une communication vers l'extérieur. Autrement dit, ils ne peuvent répondre à une communication qu'ils n'ont pas préalablement initiée. Les correspondants externes à la passerelle NAT ne possèdent en effet des entrées que pour une adresse IP et un port source privés. Or si le port source est mentionné, c'est qu'une application a déjà été ouverte par le terminal du réseau local. Le correspondant externe n'a aucun moyen d'établir une telle association en lieu et place du terminal dont il ignore la véritable adresse IP.

Le NAPT est sans conteste la méthode la plus économe puisqu'elle permet de masquer tout un réseau local avec une seule adresse IP. Elle est la plus couramment employée chez les particuliers et les petites et moyennes entreprises.

Les problèmes engendrés par le NAT

Pour être pratiques et courantes, les fonctionnalités du NAT n'en posent pas moins des problèmes de différente nature, comme les protocoles dits « sensibles » au NAT, la difficulté de recevoir une connexion derrière un NAPT ou la sécurité.

Les sections suivantes détaillent chacun de ces problèmes.

Les protocoles sensibles au NAT

Le problème le plus important à considérer concerne les protocoles dits « sensibles » au NAT. C'est le cas des principaux protocoles de signalisation utilisés pour les échanges multimédias, dont H.323, SIP et MGCP, mais également de bien d'autres protocoles, comme Kerberos, SNMP, DNS, ICMP ou encore les protocoles de partage de fichiers tels que FTP et les protocoles de mobilité tels que Mobile IP.

Ces protocoles ne se contentent pas de mentionner leur adresse IP dans l'en-tête des paquets qu'ils envoient, mais ils l'indiquent également dans le corps de leurs messages. Par exemple, avec le protocole SIP, un message d'invitation INVITE comporte dans le paquet des informations sur l'adresse IP de la source. Ces informations permettent d'établir entre les correspondants la connexion dans laquelle les données véritables (la voix ou la vidéo notamment) sont transmises. Dans cette situation, même si le boîtier NAT modifie l'adresse IP source du paquet, le récepteur ne peut répondre correctement à la requête puisque cette dernière comporte une adresse IP source initiale, qui est une adresse privée. Le récepteur envoie donc sa réponse vers l'adresse IP source spécifiée qui ne lui est pas accessible, et le paquet de réponse n'arrive jamais à son destinataire.

Cette contrainte ne se pose pas pour toutes les applications. Par exemple, les flux d'application Web utilisent le protocole HTTP, dont les paquets ne contiennent pas l'adresse IP de la source à l'origine de la requête. En conséquence, le récepteur peut répondre sans connaître de problème de routage. Ce cas est en fait celui de la majorité des protocoles.

Recevoir une connexion derrière un NAPT

Ce problème est spécifique au NAPT, qui translate les utilisateurs à la fois selon une adresse IP et selon un port. La question qui se pose est de savoir comment solliciter une entité masquée derrière un boîtier NAPT.

Nous avons vu le cas où un terminal en adressage local effectuait une demande de connexion. La table de NAPT est alors mise à jour conformément à la demande du terminal local, et la connexion avec l'extérieur peut se poursuivre. Mais comment faire si ce n'est pas le terminal local au boîtier NAPT qui initie la connexion, mais un terminal distant ? Dans ce cas, le terminal distant ne sait pas vers où envoyer sa demande de connexion, puisque la seule adresse publique est celle du boîtier NAPT et que la table de NAPT ne contient à ce stade aucune entrée permettant de déterminer à qui est destinée cette communication.

Une solution élémentaire à ce problème pourrait consister à connaître le port d'écoute d'une application et à configurer sur le boîtier NAPT une règle de redirection des paquets externes à destination de ce port d'écoute vers une machine locale en particulier. Par

exemple, tous les paquets reçus d'Internet à destination du port 34567 sont systématiquement redirigés vers le terminal dont l'adresse IP est 10.0.0.2. Si ce dernier a configuré son application pour utiliser le port 34567 comme port d'écoute, la connexion devient possible.

Malheureusement, cette solution n'est guère satisfaisante. Deux applications qui tournent sur deux terminaux distincts ne sont pas adressables simultanément. En outre, la procédure n'est pas automatique, et il est nécessaire de configurer statiquement les règles de redirection, ce qui rend le mécanisme contraignant pour l'administrateur du réseau, en plus de ne pas être toujours une fonctionnalité disponible sur les boîtiers NAPT. Sur la majorité des équipements, les règles de redirection sont configurées au moyen d'une interface Web propriétaire et non compatible selon les différents constructeurs.

La sécurité avec le NAT

Comme les codes de contrôle (checksums) inclus dans les en-têtes TCP d'un paquet sont calculés en fonction de l'adresse et du port du terminal source, ils deviennent invalides lorsque la passerelle NAT a modifié l'un ou l'autre de ces deux éléments. Si le destinataire reçoit le paquet avec le code de contrôle initial, il considère le paquet comme corrompu et demande sa réémission. En conséquence, la passerelle NAT doit recalculer les codes de contrôle et remplacer les originaux afin que les paquets restent valides et ne soient pas considérés par le destinataire comme corrompus.

Pour cette raison, le mécanisme de NAT est davantage une parade à la pénurie d'adresses IP qu'une véritable solution. Il ne se met en place qu'au prix de traitements sensibles et pas toujours réalisables. Par exemple, si l'émetteur crypte ses flux avec une couche IPsec, il devient impossible pour la passerelle NAT d'accéder aux en-têtes TCP des paquets relayés et donc de les modifier, si bien qu'ils sont transmis de manière erronée aux destinataires, qui les refusent.

On peut considérer le NAT comme une forme de « hack », en ce qu'il impose une rupture entre un émetteur et son récepteur et ne respecte pas les en-têtes d'origine des paquets, puisqu'il doit retravailler certains champs pour que les paquets demeurent conformes aux spécifications des protocoles.

En résumé

Conçue essentiellement pour faciliter l'administration d'un réseau et offrir une solution alternative aux restrictions d'adressage du protocole IP dans sa version 4, la translation d'adresses est aujourd'hui largement déployée, à la fois chez les particuliers et dans les entreprises, sous différentes formes, plus ou moins restrictives. Elle fait néanmoins intervenir, de manière obligatoire, une entité tierce intermédiaire entre l'émetteur et le récepteur. Cette technique impose donc des traitements supplémentaires sur les flux. Or ces traitements ne sont pas toujours compatibles avec d'autres protocoles. En particulier, le NAPT bloque la réception d'appel. Et surtout, les protocoles de signalisation les plus courants ne prennent pas en compte la translation d'adresse qui sera appliquée aux flux et insèrent dans leur message des adresses privées, invalides pour un récepteur distant.

Le passage des pare-feu

Les pare-feu constituent des remparts indispensables pour se protéger des attaques extérieures. Ils sont aujourd'hui couramment employés, à la fois par les particuliers et par les entreprises. Par le biais de règles de filtrage, ils inspectent tous les paquets qui transitent et vérifient s'ils sont conformes à la politique de sécurité implémentée. Si c'est le cas, les paquets sont autorisés à traverser le pare-feu et à poursuivre leur cheminement vers leur destinataire. Si ce n'est pas le cas, ils sont détruits.

Les pare-feu les plus classiques distinguent cinq éléments qui caractérisent les flux : l'adresse IP de la source, le port utilisé par la source, l'adresse IP du destinataire, le port utilisé par le destinataire et enfin le protocole de transport spécifié dans un paquet. Une règle de filtrage mentionne donc la valeur de chacun de ces cinq éléments et ordonne une action à entreprendre lorsque toutes ses valeurs sont validées.

L'action entreprise revient soit à autoriser, soit à interdire le paquet, c'est-à-dire respectivement à laisser passer le paquet ou à le détruire. Typiquement, un pare-feu adopte pour politique de bloquer tous les paquets pour lesquels aucune règle d'acceptation ne convient. La politique inverse, consistant à autoriser tous les paquets pour lesquels aucune règle d'interdiction ne convient, est trop permissive.

L'état d'une connexion peut être un sixième élément à prendre en compte par un pare-feu. Lorsqu'une communication est établie avec les cinq éléments précédemment mentionnés, on considère que la connexion est à l'état actif ou établi. Autrement, l'état est considéré comme inactif.

On distingue ainsi deux catégories de pare-feu :

- Les pare-feu sans état (*stateless*), qui ne maintiennent aucun état des connexions et se contentent des cinq éléments caractéristiques d'un flux, précédemment cités pour autoriser ou interdire les flux qui transitent dans le réseau.
- Les pare-feu avec état (*statefull*), qui maintiennent l'état des connexions et sont capables de distinguer si une communication s'effectue sur un port déjà ouvert ou sur un port que le paquet demande d'ouvrir.

La notion d'état est utile pour les protocoles à ports dynamiques. Avec des applications exploitant ces protocoles, une communication s'établit sur un port fixe vers un destinataire (canal de contrôle). Lorsque ce dernier est contacté, il convient avec l'émetteur de poursuivre la communication sur un autre port dynamiquement et arbitrairement sélectionné (canal de données). De cette façon, il reste disponible pour servir un autre correspondant qui tenterait de le joindre ultérieurement sur le port fixe. Face à une telle situation, seul un pare-feu avec état est capable d'autoriser l'usage du port dynamique. Pour cela, il lui faut analyser les paquets et déterminer s'ils sont liés ou non à une connexion préalablement établie.

Imaginons à titre d'exemple un protocole dans lequel un destinataire demande à la source de remplacer le port statique initial par un port dynamique qu'il lui impose. Les trois étapes suivantes sont nécessaires :

- La source émet un premier paquet vers un port fixé du destinataire.

- Le destinataire lui répond en précisant le port sur lequel il souhaite poursuivre la communication.
- La source reprend la communication en utilisant le port mentionné.

Pour le pare-feu sans état, seules les deux premières étapes sont possibles puisqu'elles peuvent correspondre à une règle statique simplement fondée sur le « 5-uplets » initial. L'ouverture d'un port dynamique lui est impossible, car aucune règle n'en permet la définition, sauf à être totalement permissive et d'ouvrir tous les ports possibles, ce qui constituerait une piètre politique de sécurité.

Pour le pare-feu avec état, la troisième étape est possible. En effet, ce type de pare-feu est capable d'analyser les flux et de déterminer que le port dynamique sur lequel la source tente de communiquer correspond à la demande qui a été faite précédemment par la destination. La gestion des états offre une performance accrue dans le traitement des paquets, mais cela a un coût en ce qu'elle introduit une latence supplémentaire pour le pare-feu, qui doit en outre savoir analyser les protocoles correctement et, pour cela, connaître leur syntaxe.

L'état est facilement discernable avec le protocole TCP, puisque ce dernier positionne des bits indiquant si la connexion est nouvelle, se poursuit ou se termine. Au contraire, le protocole UDP ne fournit pas ces indications. Pourtant, le pare-feu ne peut attribuer éternellement le statut d'actif à une connexion UDP. Il alloue généralement le statut actif à une connexion UDP pendant un certain délai. Passé ce délai, la connexion est considérée comme perdue et devient par conséquent inactive.

Cette manière de procéder est cependant très approximative et ne convient pas aux applications de voix sur IP, qui utilisent très majoritairement le protocole UDP pour transporter leurs données. Si, lors d'une communication, les intervenants cessent de parler, le silence correspondant n'est pas transmis, et aucun paquet n'est transmis durant cet intervalle de temps. Le pare-feu risque de considérer ce silence comme une terminaison de la communication, ce qui est erroné.

Un pare-feu est utile pour centraliser la politique de sécurité au sein d'un équipement unique. De cette manière, la gestion du contrôle des applications autorisées n'est pas laissée au libre choix des utilisateurs, mais est à la charge du réseau, ce qui réduit les possibilités de contournement des règles édictées au sein de l'entreprise.

Les fonctionnalités de NAT sont souvent implémentées en parallèle avec les fonctionnalités de pare-feu. En effet, l'opération réalisée par le NAT comme par le pare-feu doit s'appliquer au niveau d'une passerelle, point de jonction entre le réseau local privé et le réseau public. En outre, dans ces deux fonctions, une notion de filtrage est requise. Lorsque les flux traversent le réseau, le boîtier NAT détecte l'adresse IP source privée et la translate avec une adresse IP publique, tandis que le pare-feu inspecte l'adresse IP source pour savoir si l'utilisateur est autorisé à émettre des flux. Dans le même temps, le pare-feu détecte les ports et protocoles utilisés par l'application pour opérer un filtrage avec une granularité plus forte. Autrement dit, l'analyse des paquets est un mécanisme partagé par les fonctions de NAT et de pare-feu, ce qui justifie leur couplage.

Annexe N

18. Les réseaux de mobiles 2G et 3G

Cette annexe décrit la première génération de réseaux de mobiles puis la deuxième, avec le GSM, GPRS et Edge, et introduit les versions américaines, avec l'IS.

Les systèmes cellulaires de première génération

Les systèmes cellulaires de première génération sont caractérisés par des terminaux analogiques dotés d'une mobilité restreinte et de services limités. Deux standards ont été développés, le CT0 (Cordless Telephone), principalement utilisé aux États-Unis et au Royaume-Uni, et le CT1, utilisé en Europe, notamment en Allemagne et en Italie.

Les réseaux cellulaires de première génération ont été les premiers à permettre à un utilisateur mobile d'utiliser un téléphone de façon continue, n'importe où dans la zone de service d'un opérateur.

Les systèmes téléphoniques sans fil

Les premiers terminaux sans fil sont introduits avec la technologie CT0 aux États-Unis et en Europe au cours des années 1970 pour remplacer les téléphones filaires. Ces terminaux offrent des performances modestes, le canal radio étant fortement parasité et de nombreuses interférences avec les installations électriques environnantes perturbant la qualité des émissions.

Les téléphones sans fil, très chers dans les années 1970, souffrent alors d'un manque de sécurité, d'une faible autonomie et d'une qualité de restitution de la parole en dessous

de la moyenne. Cependant, la flexibilité et la portabilité qu'ils proposent les rendent rapidement populaires.

Une nouvelle génération de technologie sans fil, le CT1, est développée au début des années 1980 et est utilisée dans une douzaine de pays européens. Malheureusement, chaque pays en commercialise une version spécifique, ce qui oblige les constructeurs à concevoir autant de versions que de pays. De plus, le CT1 ne permet pas aux terminaux sans fil de communiquer avec des stations de base provenant d'autres constructeurs et souffre de limitations importantes concernant l'itinérance et le handover. Ces téléphones sans fil analogiques fonctionnent autour de 900 MHz. Leur marché n'a jamais été à la hauteur des ambitions des constructeurs, essentiellement à cause de leur prix élevé et de la non-compatibilité entre constructeurs et entre versions de la norme.

Des recherches sur les systèmes sans fil fondés sur la technologie numérique sont menées à partir des années 85 afin de fournir plus de capacité et une meilleure qualité de service. La deuxième génération voit ainsi apparaître une téléphonie à faible mobilité, le Télépoint, reposant sur le standard CT2 (Cordless Telephone of 2nd Generation).

Les systèmes cellulaires

Le concept cellulaire est introduit dans les années 1970 par les Bell Labs. Les systèmes cellulaires sont conçus pour augmenter la mobilité des terminaux. Une cellule est une zone géographique couverte par une antenne de transmission. Un utilisateur est en mesure de passer d'une cellule à une autre sans coupure de la communication. Ce passage, appelé handover ou handoff, permet au terminal de changer de cellule sans interruption. À cette fin, le terminal doit embarquer tous les composants nécessaires à la gestion de la communication.

Le premier système cellulaire opérationnel, l'AMPS (Advanced Mobile Phone System), se met en place aux États-Unis à la fin des années 1970. En Europe du Nord, des opérateurs de télécommunications et des constructeurs lancent une génération assez similaire, le NMT (Nordic Mobile Telecommunication system). Le NMT est développé en Suède, en Norvège, au Danemark et en Finlande au début des années 1980.

D'autres réseaux, fondés sur les concepts de l'AMPS et du NMT, sont également commercialisés, comme le TACS (Total Access Communication System) au Royaume-Uni ou des versions du NMT en France. France Télécom introduit Radiocom 2000 en 1985 et SFR met en place son service en 1989. Tous ces systèmes cellulaires reposent sur une transmission de la voix analogique avec une modulation de fréquence dans les bandes des 450 et 900 MHz.

Les réseaux téléphoniques sans fil

En raison de la faible qualité du CT1, plusieurs constructeurs européens ont développé, en 1984, le système CT2 de téléphonie sans fil de deuxième génération. Dans le but d'autoriser un service de Télépoint, c'est-à-dire un service de téléphonie public fondé sur le CT2 dans lequel le client est quasiment immobile, une interface commune, connue sous

le nom de CAI (Common Air Interface) est spécifiée en 1988. Son objectif est de fournir une norme uniforme pour le Télépoint public, qui permette aux utilisateurs de changer de réseau et d'opérateur tout en gardant le même terminal.

Le Télépoint

Cette norme concerne l'accès au réseau téléphonique commuté par une interface air en faible mobilité, le terminal ne pouvant effectuer de handover entre deux cellules. Les systèmes de type Télépoint ne fournissent pas de couverture nationale mais peuvent être installés en des endroits où le trafic d'appel est important, comme les gares, aéroports, centres commerciaux et restaurants. Le Télépoint est le premier exemple d'un service de téléphonie personnelle peu onéreux, utilisable en résidentiel, au bureau ou dans des lieux publics, car il se sert du réseau téléphonique existant. En outre, le coût de l'implémentation d'un réseau de stations de base Télépoint est très bas.

Le Télépoint donne donc la possibilité d'établir un réseau public à faible coût, comparativement aux systèmes cellulaires, qui nécessitent une intelligence sophistiquée incluant la gestion de la mobilité. Plusieurs réseaux de Télépoint ont été créés en Europe, tels Rabbit au Royaume-Uni, Bi-Bop en France, Greenpoint aux Pays-Bas et CITEL en Belgique. Le principal inconvénient du Télépoint réside dans l'incapacité quasi permanente des terminaux à recevoir des appels. Il est également impossible avec de tels systèmes d'avoir une conversation continue en déplacement. Tous ces éléments ont empêché le lancement commercial du CT2 dans de bonnes conditions, et la plupart des services de Télépoint européens ont été des échecs.

Le DECT

Le DECT est un standard de télécommunications sans fil conçu par l'ETSI. La plupart des concepts ayant présidé à son lancement s'inspirent d'un système suédois, connu sous le nom de DCT (Digital Cordless Telephone) ainsi que du CT2. Les Suédois ont conçu le DCT parce qu'il leur fallait une nouvelle norme, mieux appropriée que le CT1 aux environnements à grande capacité, comme les PABX sans fil. Le DECT bénéficie en Europe d'une bande de fréquences de 1 880 à 1 900 MHz et offre des services qui vont au-delà de ceux fournis par les systèmes précédents. En particulier, l'environnement radio DECT est conçu pour des applications résidentielles et professionnelles ainsi que pour un accès public. De plus, l'interfonctionnement des systèmes DECT dans les zones publiques et privées est fiable.

Développé au Japon à partir de 1989 sur des bases légèrement différentes des systèmes européens, le PHS est un système sans fil offrant un accès public, aussi bien pour un usage domestique que professionnel, à la fois à l'intérieur et à l'extérieur, avec un terminal de poche à très faible coût. Le système PHS est introduit commercialement au Japon en 1995 comme un système d'accès public. Des fonctionnalités supplémentaires sont rapidement ajoutées, comme la mise en place de boucles locales sans fil, la transmission de données à des débits que l'on peut qualifier d'importants (32 ou 64 Kbit/s) et l'itinérance, ou roaming.

Aux États-Unis, plusieurs standards sont également définis au milieu des années 1990 :

- PCI (Personal Communications Interface), qui s'appuie sur le CT2.
- PWT (Personal Wireless Telecommunications), qui repose sur le DECT.
- PACS-UA (Personal Access Communications System), élaboré à partir du PHS.

Les objectifs de tous ces systèmes sont de fournir une couverture extérieure totale dans les zones urbaines ainsi qu'une continuité de service entre les zones publiques et privées et de permettre aux utilisateurs d'émettre et de recevoir des appels. Pour ce type d'application, la technologie sans fil est une solution de rechange aux technologies cellulaires numériques.

Fonctionnement du DECT

Le DECT définit une technique d'interface radio pour des télécommunications sans fil à courte portée. La mobilité offerte par un système DECT est donc réduite. Le DECT couvre seulement l'interface air entre le terminal, ou PP (Portable Part), et la partie fixe, ou FP (Fixed Part), équivalente à une station de base du GSM. L'élément principal de la normalisation du DECT consiste en l'IC (Interface Control), qui définit le fonctionnement de l'interface air et prévoit un ensemble complet de protocoles.

Le DECT ne fournit aucun service. Il procure la connexion radio à un environnement capable de proposer des services, comme le réseau téléphonique, un PABX, le RNIS, un réseau de données d'opérateur, Internet ou tout autre réseau. L'objectif est de permettre la connexion de terminaux sans fil à un PABX ou à un site central dans un environnement cellulaire.

Les cellules sont de taille variable, leur rayon variant de 10 m à 5 km, selon les obstacles susceptibles de freiner la propagation des ondes. Le DECT fournit des services de voix d'une qualité équivalente à celle rencontrée dans les réseaux fixes ainsi qu'un large ensemble de services de données, incluant la connexion au RNIS ou à Internet. Il peut être implémenté comme un simple téléphone sans fil résidentiel ou comme un système complet, capable de prendre en charge tous les services classiques de téléphonie.

Le DECT prévoit tous les outils nécessaires à la mobilité. Les procédures liées à l'identification, aux droits d'accès, à l'allocation de clés, à la récupération de données, à l'authentification, au chiffrement, au transfert intercellulaire, à la recherche de l'abonné et à la localisation du terminal sont décrites dans la norme. Ses recommandations portent essentiellement sur l'interface radio. En tant que technique permettant l'accès à de nombreux réseaux, et donc aux services correspondants, l'interface DECT doit être indépendante des caractéristiques techniques de ces réseaux tout en étant capable de laisser passer les commandes adaptées aux réseaux à atteindre. C'est ce qu'on désigne sous le terme de profil.

Chacun des profils DECT décrit la façon dont l'interface commune est utilisée pour une application particulière. Un profil est un ensemble de commandes et de procédures fournissant une description non ambiguë de l'interface air pour accéder à des services et à des applications spécifiques. Dans la réalité, la plupart de ces profils ont pour objet

l'interfonctionnement et l'interopérabilité. L'interfonctionnement désigne la capacité d'utiliser plusieurs systèmes ensemble, tandis que l'interopérabilité se réfère à la possibilité d'utiliser ensemble des équipements de différents fabricants fonctionnant sous des systèmes différents. Le GAP (Generic Access Profile) et le profil d'interfonctionnement entre le DECT et le GSM constituent deux exemples importants de profils.

Le GAP permet l'interopérabilité entre les équipements terminaux et les stations de base. Un terminal d'un premier constructeur peut être compatible avec une station de base d'un second constructeur, à condition que ces deux équipements respectent le profil GAP. Le profil GAP est le profil DECT de base. Il contient les fonctionnalités nécessaires pour supporter des applications telles que la voix, pour des téléphones sans fil domestiques, les PABX sans fil professionnels et les applications à partir d'un accès public. Il inclut la gestion de la mobilité et le contrôle des appels. Les protocoles gérant le contrôle des appels sont fortement liés à la fourniture des services de voix. Les protocoles traitant la gestion de la mobilité couvrent notamment le traçage de la localisation, les identités et les aspects de sécurité.

Les normes DECT spécifient des protocoles autorisant la mobilité mais ne définissent pas comment les éléments de réseau gardent trace de la localisation d'un terminal DECT ni comment délivrer un appel entrant à un terminal. Ces aspects sont en dehors de la norme DECT, qui n'est qu'une technologie d'accès. L'interface DECT permet d'accéder à de nombreux réseaux, même à des systèmes cellulaires comme le GSM. Pour les réseaux GSM, la mobilité étant une fonctionnalité bien définie, il est possible d'utiliser cette fonctionnalité pour fournir la mobilité à travers une interface air DECT. Les composants spécifiques de l'interface commune nécessaires à l'interfonctionnement entre un terminal DECT et un réseau GSM, en particulier l'interface A, sont définis dans le profil d'interfonctionnement DECT/GSM.

L'ETSI a défini les besoins du protocole de l'interface air et la façon dont les protocoles DECT s'interconnectent avec les protocoles GSM au niveau de l'interface A. Ce profil permet à un équipement DECT d'être compatible GSM, c'est-à-dire de bénéficier des services du réseau GSM, tels que grande mobilité, sécurité ou services de messages courts SMS (Short Message Service). La normalisation de ce profil implique des modifications dans la norme DECT afin qu'elle supporte les services GSM.

D'autres profils ont été définis par l'ETSI, comme l'interfonctionnement entre le DECT et le RNIS. Ce dernier profil permet d'accéder à des services du RNIS, avec des transferts de données d'un débit maximal de 64 Kbit/s.

Vers la 2G

Avec les terminaux DECT et PHS, il est possible d'appeler et d'être appelé, donc de transmettre et recevoir des données. Cependant, ces terminaux n'offrent pas une mobilité globale. Les systèmes sans fil s'appuyant sur les réseaux fixes, la mobilité du terminal n'est pas totale. L'utilisateur d'un terminal DECT peut certes se déplacer, mais cette mobilité n'est pas comparable à celle qui caractérise les terminaux GSM.

L'interfonctionnement entre les systèmes sans fil et cellulaires n'a pas fait l'objet d'études approfondies. Par exemple, si un utilisateur veut bénéficier du même service à partir de son terminal DECT et de son terminal GSM, il doit interrompre sa communication pour changer de terminal. Aujourd'hui, des terminaux multimodes GSM/DECT sont disponibles chez certains fabricants de terminaux, mais, la plupart du temps, ces terminaux correspondent à un terminal GSM et à un terminal DECT réunis.

La technologie DECT semble dotée du potentiel nécessaire à une mobilité locale extérieure, mais elle est inadaptée à une mobilité large. Le DECT permet à un utilisateur d'accéder à des services avancés, implémentés dans les réseaux fixes, à l'aide du réseau intelligent (*voir le chapitre 31*) dans le cadre du concept CTI (Computer Telephony Integration). Le GSM offre une mobilité large mais nécessite l'aide des réseaux intelligents CAMEL (Customized Applications for Mobile Network Enhanced Logic) pour implémenter de nouveaux services, plus spécifiques des opérateurs. Au finale, les solutions GSM et DECT sont davantage complémentaires que concurrentes.

La figure N.1 illustre l'évolution des systèmes mobiles de première, deuxième et troisième générations.

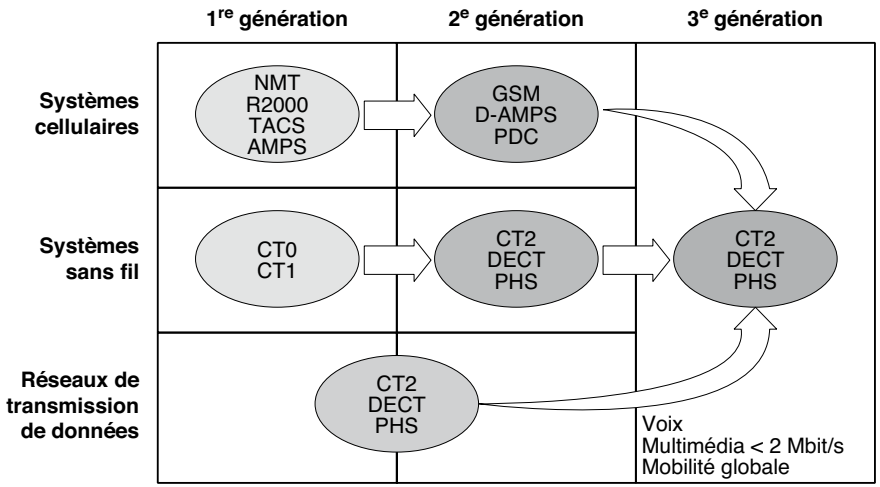


Figure N.1

Évolution des systèmes de communication mobile

Même si les systèmes cellulaires et sans fil ont évolué dans le but de répondre aux besoins des utilisateurs, les systèmes actuels ne proposent pas tous les services attendus par ces derniers. Le manque de compatibilité entre systèmes est également à souligner. Par exemple, il est difficile de connecter un terminal DECT au réseau GSM, bien qu'un profil DECT/GSM soit défini.

En conclusion, de nouveaux systèmes étaient nécessaires pour une meilleure prise en compte des besoins de l'utilisateur. Ces réseaux devaient être plus universels, en intégrant

le cellulaire et le sans-fil. Cela nécessitait de nouveaux standards, dits de deuxième génération et demie et de troisième génération, qui font l'objet des sections suivantes.

Les protocoles des réseaux de mobiles

Les protocoles utilisés dans les réseaux de mobiles s'appliquent à quatre types d'interfaces, que nous allons décrire. Nous ne détaillons dans la suite que les protocoles de l'interface air, qui constituent la spécificité des réseaux de mobiles.

L'architecture de l'IMT 2000 peut être décrite par ses interfaces (*voir figure N.2*). Les quatre interfaces suivantes sont définies :

- **UIM-MT** (User Identity Module-Mobile Terminal). Située entre la carte à puce, qui détermine l'identité de l'utilisateur, et le terminal mobile, cette interface authentifie l'utilisateur et permet de facturer correctement le client qui effectue une communication.
- **MT-RAN** (Mobile Terminal-Radio Access Network). Située entre le terminal mobile et l'antenne, cette interface est aussi appelée interface radio ou interface air. Lorsqu'on parle de réseaux de mobiles, on pense immédiatement à cette interface, car c'est là que réside la spécificité de ces réseaux.
- **RAN-CN** (Radio Access Network-Core Network). Située entre l'antenne et le réseau cœur du réseau de mobiles, cette interface permet, une fois l'antenne atteinte, de transporter les signaux vers l'utilisateur distant par l'intermédiaire d'un réseau terrestre, que l'on appelle le réseau cœur.
- **CN-CN** (Core Network-Core Network). Située entre deux nœuds de transfert du réseau cœur, cette interface est aussi appelée interface NNI (Network Node Interface).

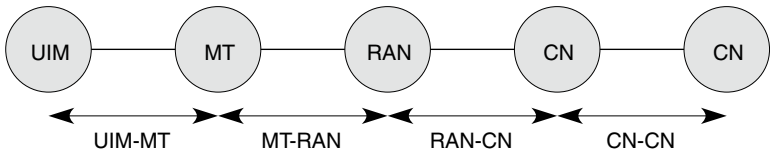


Figure N.2

Interfaces de l'architecture IMT 2000

Un réseau de mobiles d'opérateur doit posséder toutes ces interfaces. Un réseau privé de mobiles peut ne pas disposer d'interfaces UIT-MT et CN-CN.

L'interface UIM-MT, ou SIM-MT, se situe entre la carte à puce et le terminal mobile. Son rôle principal est de sécuriser la communication qui s'établit à partir du mobile. Une carte à puce est insérée dans le terminal à cet effet. Il existe des cartes à puce sans contact, que l'on porte sur soi et qui communiquent directement avec le terminal, les contrôles d'accès et les vérifications s'effectuant par le biais de cette interface. À mesure que les performances des puces s'accroissent, d'autres services peuvent être mis en place et sécurisés, tel le VHE.

L'interface MT-RAN relie le terminal mobile, de type GSM, UMTS ou autre, à l'antenne ou éventuellement à un autre terminal. Dans le cas des systèmes satellitaires, cette interface permet la connexion directe du terminal au satellite. Elle concerne la traversée de la partie air du réseau et définit comment un terminal accède à l'antenne et réciproquement. L'interface air, ou interface radio, est celle que l'on met en avant dans les réseaux de mobiles et sans fil.

Des algorithmes permettent de déterminer quel terminal est en train de transmettre ou comment le signal est transmis, dans le cas où plusieurs terminaux émettent en même temps tout en restant compréhensibles par l'antenne. Dans le GSM, les stations mobiles parlent à tour de rôle, tandis que dans l'UMTS les mobiles peuvent parler en parallèle. Les interfaces air présentent des différences, qui servent souvent à caractériser une technologie, bien que ce ne soit qu'une des quatre interfaces nécessaires pour obtenir un système complet.

L'interface radio constitue souvent le point le plus sensible du réseau, car les ressources y sont faibles et doivent être optimisées. De nombreux défauts peuvent entacher par ailleurs la qualité de service délivrée par cette interface. Les puissantes rivalités politiques et économiques suscitées par la mise en place de l'interface radio n'ont pas permis aux différents continents de se mettre d'accord sur les grandes directions à emprunter. C'est la raison pour laquelle, par exemple, le GSM n'est pas compatible avec les systèmes américains.

L'interface RAN-CN concerne la transmission de l'antenne au premier commutateur du réseau cœur. Cette interface regroupe plusieurs antennes pour permettre de gérer ces dernières collectivement. Dans le cas de l'antenne satellite, l'interface est interne au satellite puisque l'antenne et le commutateur sont tous deux situés dans le satellite.

Cette interface assure la gestion des appels, en acheminant correctement chaque appel arrivant sur le commutateur du réseau cœur de liaison vers l'antenne adéquate, laquelle diffuse l'information de façon qu'elle soit captée par le client destinataire. Cette interface doit également gérer la mobilité, puisque le client se déplace et peut se trouver connecté à une autre antenne, soit à l'intérieur du même sous-système, soit au sein d'un sous-système indépendant.

L'interface CN-CN décrit les protocoles utilisés entre deux nœuds de la partie fixe d'un réseau de mobiles ou d'un réseau satellite, dans le cas d'une constellation de satellites. Les nœuds du réseau sont constitués par les commutateurs du réseau cœur. Cette interface définit, entre autres choses, la technologie réseau utilisée pour acheminer les informations. La technologie réseau du GSM est la commutation de circuits, tandis que celle du GPRS superpose commutation de circuits et commutation de paquets. L'UMTS met en œuvre la commutation de paquets, d'abord ATM, pour la première génération attendue, puis IP. Dans les environnements satellitaires l'interface est de type ATM.

L'interface CN-CN est également importante dans les constellations de satellites, dans lesquelles les interconnexions des satellites forment par elles-mêmes le réseau fixe. La limitation de cette interface provient de l'impossibilité d'offrir une qualité de service garantie.

L'interface radio

L'antenne d'émission-réception, généralement unique pour chaque cellule, est un élément critique des réseaux de mobiles. Si deux mobiles émettent en même temps, l'antenne ne peut généralement capter qu'un des deux messages. Comme dans les réseaux locaux, il faut une technique d'accès pour sérialiser les arrivées des messages sur l'antenne. Les techniques d'accès sont semblables à celles que l'on trouve dans les réseaux locaux.

Les réseaux satellite présentent la même problématique, avec pour différence essentielle une distance très grande entre les stations.

Les méthodes le plus souvent utilisées dans les réseaux de mobiles sont le FDMA, le TDMA et le CDMA. Ces trois méthodes étant décrites au chapitre 10, nous ne ferons ici que rappeler brièvement leurs différences. Dans la technique CDMA, tous les utilisateurs parlent en même temps, l'antenne étant capable de récupérer correctement tous les signaux qui lui arrivent grâce au code de puissance. Chaque terminal émet sur une fréquence donnée avec une puissance déterminée par le code. Il faut respecter la puissance arrivant au récepteur pour que le déchiffrage soit possible.

L'avantage évident de cette technique est de permettre de garder son code, et donc sa bande passante, sur des cellules connexes. En revanche, une première difficulté consiste à fournir des codes suffisamment différents à chaque utilisateur connecté pour qu'il n'y ait pas d'interférences et que l'antenne soit capable de récupérer les émissions qui s'effectuent en parallèle. Une seconde difficulté consiste à contrôler précisément la puissance d'émission, de façon que le récepteur qui se trouve plus ou moins loin reçoive le signal avec la bonne puissance. La figure N.3 présente une comparaison des trois grandes techniques d'accès. Dans le CDMA, la bande passante est partagée par les cinq terminaux suivant un code, c'est-à-dire un niveau de puissance de réception.

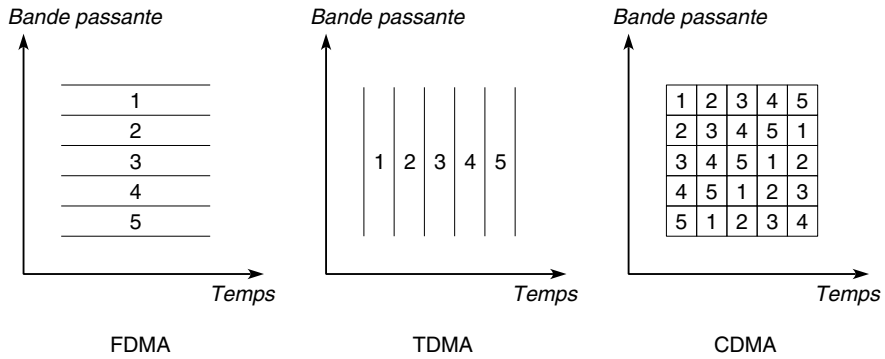


Figure N.3

Comparaison des techniques d'accès

Les techniques que nous venons de décrire peuvent se superposer. Par exemple, un découpage en fréquences (FDMA) peut être suivi d'un TDMA sur chaque fréquence, comme dans le GSM. Dans l'UMTS, un découpage en fréquence est associé sur chaque

fréquence à un TDMA puis sur chaque slot à un CDMA. Le cdma2000 divise la bande passante en grandes sous-bandes auxquelles est appliqué un CDMA. Enfin, le WCDMA (Wideband-CDMA) utilise toute la bande passante en CDMA.

La deuxième génération (2G)

Les réseaux cellulaires de deuxième génération, tels IS-95 et le GSM pour les réseaux de mobiles et le DECT pour les réseaux sans fil, sont caractérisés par l'introduction de la technologie numérique.

Le DECT (Digital Enhanced Cordless Telecommunications) et le PHS (Personal Handyphone System) offrent une couverture radio permettant une utilisation en résidentiel (station de base domestique), au bureau (PABX sans fil) et dans la rue (station de base publique). La complexité technique pour accéder au service est assez faible. Le système ne sachant pas effectuer de handover, l'utilisateur doit se trouver impérativement dans une cellule et y rester.

Plusieurs technologies numériques cellulaires font leur apparition au début des années 1990 :

- GSM (Global System for Mobile communications), en Europe, fonctionnant à 900 MHz ;
- DCS 1800 (Digital Cellular System 1800), système équivalent au GSM, mais fonctionnant à des fréquences plus élevées (1 800 MHz) ;
- PCS (Personal Communication System) 1900 et D-AMPS, version numérique de l'AMPS, aux États-Unis ;
- PDC (Pacific Digital Cellular) au Japon.

Les systèmes cellulaires numériques de deuxième génération favorisent la mise au point d'un terminal portable doté d'une autonomie acceptable.

Le GSM

Le GSM a été déployé au départ en Europe et partout dans le monde, à l'exception de l'Amérique, avant d'être adopté par plusieurs opérateurs américains.

La CEPT (Conférence européenne des Postes et Télécommunications) entreprend en 1970 d'établir une norme unique en matière de communication avec les mobiles. Dans le même temps, elle affecte une bande de 25 MHz dans la bande des 900 MHz pour réaliser un réseau cellulaire. Un groupe de travail, le groupe spécial mobile (GSM), est constitué pour réaliser ces études. En 1987, treize pays européens se mettent d'accord pour développer un réseau GSM. En 1990, une adaptation de la bande des 1 800 MHz est mise en place sous le nom de DCS 1800 (Digital Communication System 1 800 MHz). À cette époque, l'ETSI remplace la CETP pour finaliser la normalisation du GSM900 et du DCS 1800. De leur côté, les Américains reprennent une version du GSM dans la

bande des 1 900 MHz, sous le nom de DCS1900. Les principes généraux du GSM sont les mêmes pour les trois adaptations.

Le GSM est un environnement complet, rassemblant l'interface air, mais aussi les interfaces entre le système radio et le système de commutation et l'interface utilisateur. Les appels sont contrôlés par la norme Q.931, déjà rencontrée dans le RNIS et le relais de trames.

La station mobile est constituée de deux éléments, le terminal portatif et la carte SIM. Cette carte à puce contient les caractéristiques de l'utilisateur et les éléments de son abonnement.

L'interface radio travaille dans les bandes 890-915 MHz dans le sens montant et 935-960 MHz dans le sens descendant. Une version GSM étendue, le E-GSM, travaille dans les bandes 880-915 MHz dans le sens montant et 925-960 MHz dans le sens descendant. Le réseau DCS 1800 utilise un sens montant entre 1 710 et 1 785 MHz et un sens descendant de 1 805 à 1 880 MHz. Enfin, le PCS1900 se place entre 1 850 et 1 910 MHz dans le sens montant et 1 930 à 1 990 MHz dans le sens descendant. Chaque porteuse radio exige 200 kHz, de telle sorte que 124 porteuses sont disponibles en GSM900, 174 en E-GSM, 374 en DCS 1800 et 298 en DCS1900.

De nombreux canaux sont disponibles sur l'interface radio GSM pour la transmission des données et des différents contrôles :

- Le canal plein débit TCH/FS (Traffic CHannel/Full Speed), au débit net de 13 Kbit/s, pour la transmission de la parole ou des données. Ce canal peut être remplacé par :
  - Le canal demi-débit TCH/HS (Traffic CHannel/Half Speed) à 5,6 Kbit/s.
  - Le canal plein débit pour les données à 9,6 Kbit/s, pour la transmission de données à un débit net de 12 Kbit/s.
  - Le canal demi-débit pour les données à 4,8 Kbit/s, pour la transmission de données à un débit net de 6 Kbit/s.
- Le canal SDCCH (Standalone Dedicated Control CHannel), au débit brut de 0,8 Kbit/s, qui sert à la signalisation (établissement d'appel, mise à jour de localisation, transfert de messages courts, services supplémentaires). Ce canal est associé à un canal de trafic utilisateur.
- Le canal SACCH (Standalone Access Control CHannel), au débit brut de 0,4 Kbit/s, qui est un canal de signalisation lent associé aux canaux de trafic. Son rôle est de transporter les messages de contrôle du handover.
- Le canal FACCH (Fast Access Control CHannel), qui est obtenu par un vol de trames (c'est-à-dire qui utilise la place de certaines trames d'un autre canal) sur le canal trafic d'un utilisateur, dont il est chargé d'exécuter le handover. Il est associé à un canal de trafic et peut servir à des services supplémentaires, comme l'appel en instance.
- Le canal CCCH (Common Control CHannel), qui est un canal de contrôle commun aux canaux de trafic pour faire transiter des demandes d'établissement de communication ou des contrôles de ressources.

- Le canal BCCH (Broadcast Control CHannel), au débit de 0,8 Kbit/s, qui gère le point-à-multipoint.
- Le canal AGCH (Access Grant CHannel), ou canal d'allocation des accès, qui s'occupe de la signalisation des appels entrants.
- Le canal RACH (Random Access CHannel), qui s'occupe de la métasignalisation, correspondant à l'allocation d'un premier canal de signalisation.
- Le canal FCCH (Frequency Control CHannel), qui prend en charge les informations de correction de fréquence de la station mobile.
- Le canal SCH (Synchronous CHannel), qui est dédié aux informations de synchronisation des trames pour la station mobile et pour l'identification de la station de base.

Le protocole de niveau trame chargé de la gestion de la transmission sur l'interface radio provient du standard HDLC, avec quelques modifications pour s'adapter à l'interface air. Plus précisément, ce protocole est appelé LAP-Dm (Link Access Protocol on the Dm channels). Il transporte des trames avec une fenêtre de 1, la reprise éventuelle s'effectuant sur un temporisateur.

Le protocole de niveau paquet est lui-même divisé en trois sous-niveaux :

- La couche RR (Radio Resource), qui se préoccupe de l'acheminement de la supervision.
- La couche MM (Mobility Management), qui prend en charge la localisation continue des stations mobiles.
- La couche CM (Connection Management), qui gère les services supplémentaires, le transport des messages courts SMS et le contrôle d'appel. Ce dernier contrôle reprend en grande partie la recommandation Q.931 du réseau numérique à intégration de services.

Le GSM définit les relations entre les différents équipements qui constituent le réseau de mobiles :

- sous-système radio BSS ;
- sous-système réseau NSS (Network SubSystem), avec ses bases de données pour la localisation des utilisateurs HLR et VLR ;
- relations entre les couches de protocoles et les entités du réseau ;
- interfaces entre sous-système radio (BSS) et sous-système réseau (NSS) ;
- itinérance (roaming).

L'IS-95

L'IS-95 est la principale version normalisée pour la deuxième génération américaine. L'interface air utilise la technologie CDMA. La version IS-95A est celle qui est déployée en Amérique du Nord. La version 1999, IS-95B, augmente les débits numériques. C'est elle que nous prenons comme référence dans cette section.

Le canal de contrôle descendant regroupe le canal pilote, le canal de paging et le canal de synchronisation. Le canal réservé au trafic des utilisateurs est multiplexé avec les canaux

de contrôle par des trames de 20 ms. La trame est ensuite codée pour être transportée sur l'interface air. Le canal de synchronisation travaille à la vitesse de 1,2 Kbit/s. Chaque utilisateur possède un canal en division par code (CDMA) et jusqu'à 7 canaux de trafic supplémentaires. Deux taux de trafic ont été définis, l'ensemble 1 propose des débits de 9,6, 4,8, 2,4 et 1,2 Kbit/s, et l'ensemble 2 des débits de 14,4, 7,2, 3,6 et 1,8 Kbit/s. Les trames de 20 ms sont divisées en seize groupes de contrôle de puissance d'une durée de 1,25 ms.

La structure du canal montant est différente. Ce canal est subdivisé en deux canaux, le canal de trafic et le canal de gestion de l'accès. Les trames font également 20 ms et prennent en charge l'ensemble du trafic.

L'IS-95 a trois mécanismes différents pour le contrôle de puissance. Sur le lien montant, un contrôle en boucle ouverte et un contrôle en boucle fermée sont disponibles. Sur le lien descendant, un contrôle en boucle plus lent est implémenté.

Deux technologies de codage de la parole sont utilisées, l'une à 8 Kbit/s et l'autre à 13 Kbit/s. Ce dernier codage utilise le taux de 14,4 Kbit/s du canal de transmission. Le premier codage utilise un codec EVRC (Enhanced Variable Rate Codec) à 8 Kbit/s, s'adaptant aux canaux à 1,2, 2,4, 4,8, et 9,6 Kbit/s pour des décompositions éventuelles du canal dans les débits de 1, 2, 4 et 8 Kbit/s.

L'IS-136

L'IS-136 est une norme américaine pour les téléphones mobiles de deuxième génération utilisant le TDMA. Moins développée que l'IS-95, cette norme offre cependant une base intéressante pour la troisième génération.

Une première amélioration intermédiaire, ressemblant au GPRS, examiné à la section suivante, concerne l'augmentation du flux de données jusqu'à une valeur de 384 Kbit/s. La version suivante introduira des microcellules et des picocellules sur lesquelles l'utilisateur pourra récupérer un grand nombre de tranches dans le TDMA pour atteindre des débits de 2 Mbit/s.

Le GPRS

L'activité majeure de développement de la phase 2+, ou 2,5G, du GSM concerne le GPRS. Ce dernier incarne une nouvelle génération du standard GSM, rendant possible la prise en charge des applications de données à moyen débit dans le cadre de la mobilité. Il constitue en outre une transition vers la troisième génération, caractérisée par le passage d'un débit de 14,4 Kbit/s (9,6 Kbit/s utilisable) à un débit beaucoup plus important, pouvant être multiplié par 8 au maximum.

Le GPRS utilise la même infrastructure que le GSM mais avec un double réseau cœur, celui du GSM, c'est-à-dire d'un réseau à commutation de circuits, et celui d'un réseau à transfert de données. Si l'utilisateur téléphone, l'information transite par le réseau cœur de type circuit téléphonique. Si l'utilisateur émet des paquets, ces derniers sont

acheminés par le réseau cœur de type paquet. Le réseau cœur utilise une technique de relais de trames. Nous ne considérons dans la suite que la partie paquet ajoutée au GSM.

Le terminal intègre les composants nécessaires au traitement de la parole téléphonique pour la numériser de façon plus ou moins compressée et se complète d'un modem, qui émet les paquets de l'utilisateur vers le réseau cœur paquet. La traversée de l'interface radio utilise les slots du TDMA qui ne sont pas utilisés par la parole téléphonique.

L'architecture du GPRS est illustrée à la figure N.4. Cette architecture est composée de divers types de nœuds :

- Les SGSN (Serving GPRS Support Node), qui sont des routeurs connectés à un ou plusieurs BSS.
- Les GGSN (Gateway GPRS Support Node), qui sont des routeurs acheminant le trafic vers des réseaux de données GPRS ou externes.

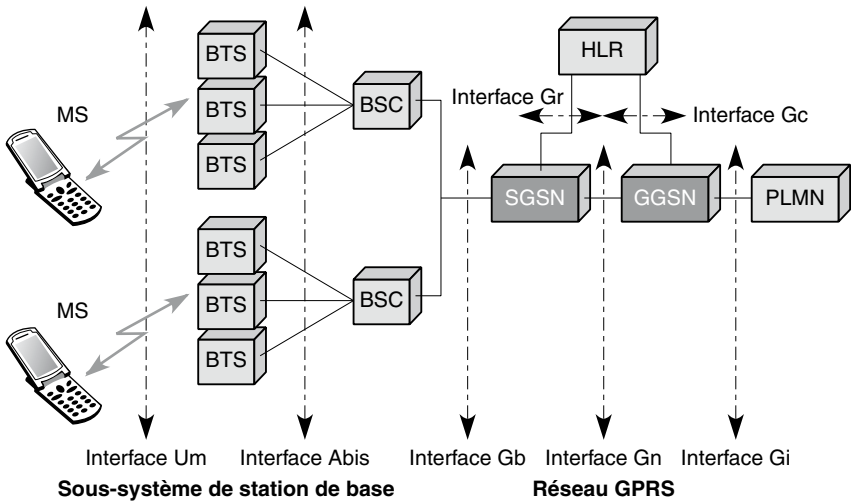


Figure N.4

Architecture du GPRS

Le réseau GPRS possède deux plans, le plan utilisateur et le plan de signalisation. Les couches de protocoles du plan utilisateur sont illustrées à la figure N.5.

Par rapport au GSM, le GPRS requiert de nouveaux éléments pour créer un mode de transfert de paquets de bout en bout. De plus, le HLR est amélioré pour les clients qui demandent à transporter des données. Deux services sont permis :

- le point-à-point PTP (Point-To-Point) ;
- le point-à-multipoint PTM (Point-To-Multipoint).

Les transferts de paquets et le routage s'effectuent, comme nous venons de l'indiquer, par les nœuds logiques SGSN. Ils utilisent les passerelles GGSN avec les réseaux de transfert

de paquets externes. Dans le réseau GPRS, les unités de données sont encapsulées par le SGSN de départ et décapsulées dans le SGSN d'arrivée. Entre les SGSN, le protocole IP est utilisé. L'ensemble de ce processus est défini comme le tunneling du GPRS.

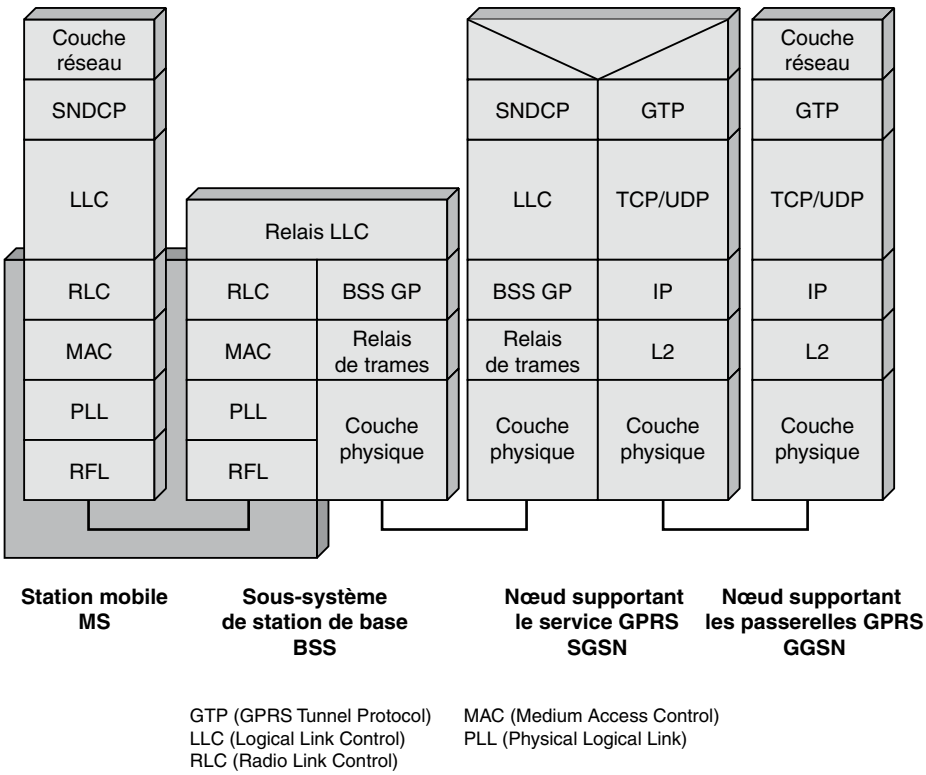


Figure N.5

Couches de protocoles du réseau GPRS

Le GGSN maintient les informations de routage pour réaliser les tunnels et les maintenir. Ces informations sont stockées dans le HLR. Le protocole en charge de ce travail, le GTP (GPRS Tunnel Protocol) utilise TCP et UDP pour effectuer le transport effectif. Entre le SGSN et les MS, le protocole SNDCP (SubNetwork Dependent Convergence Protocol) effectue le multiplexage de niveau paquet, le chiffrement, la segmentation et la compression. Entre les MS (Mobile Station) et les BSS, le niveau trame est subdivisé en deux sous-couches, la couche LLC (Logical Link Control) et la couche RLC/MAC (Radio Link Control/Medium Access Control).

La couche LLC se sert du protocole LAP-Dm, déjà utilisé pour la signalisation dans l'environnement GSM. Le RLC/MAC s'occupe du transfert physique de l'information sur l'interface radio. Ce protocole prend en charge les retransmissions éventuelles sur erreur par une technique BEC (Backward Error Correction), consistant en une retransmission

sélective des blocs en erreur. La technique d'accès s'effectue par le protocole slotted aloha, ou aloha en tranches. Le protocole RLC/MAC s'appuie sur un protocole de niveau physique effectuant la transmission des éléments binaires sur le support physique et prenant en charge le codage, la récupération de certaines erreurs physiques et même un contrôle de flux.

EDGE (Enhanced Data for GSM Evolution)

En utilisant plusieurs slots dans le GPRS, un utilisateur peut augmenter son débit. Le GPRS offre de surcroît différents taux de codage, permettant d'augmenter le débit lorsque les conditions de propagation sont correctes. Néanmoins, le débit brut sur un slot reste celui du GSM, c'est-à-dire environ 270 Kbit/s. EDGE (Enhanced Data for GSM Evolution) permet de s'affranchir de cette limite, moyennant l'introduction d'une nouvelle modulation, de nouveaux schémas de codage et la généralisation du principe de l'adaptation de lien (*link adaptation*).

L'association de EDGE et de GPRS est aussi connue sous le nom de E-GPRS (Enhanced-General Packet Radio Service). L'E-GPRS est souvent considéré comme un système de troisième génération. De leur côté, les principes d'EDGE ont été repris et adaptés pour l'évolution de l'IS-136, le standard TDMA américain. Cette évolution est connue sous le nom d'UWC136 ou d'EDGE Compact.

EDGE est issu de la constatation que, dans un système cellulaire, tous les mobiles ne disposent pas de la même qualité de transmission. Le contrôle de puissance tente de pallier ces inégalités en imposant aux mobiles favorisés une transmission moins puissante. Cela permet plutôt d'économiser les batteries des terminaux que d'augmenter les capacités de transmission. Nous verrons qu'avec l'UMTS, qui utilise un accès par répartition en code tel que CDMA, ce contrôle de puissance a un rôle autrement plus important.

EDGE permet à ses utilisateurs de bénéficier de transmissions plus efficaces, augmentant par conséquent le trafic moyen offert dans la cellule. En réalité, EDGE fait correspondre à chaque condition radio rencontrée le schéma de modulation et de codage, ou MCS (Modulation and Codage Scheme), le plus approprié en regard de la qualité de service requise sur la liaison. Pour cela, EDGE a évidemment introduit de nouveaux MCS, en comparaison de ceux existant dans le GSM ou le GPRS.

Le cdma2000

Le cdma2000 adopté par les Américains ressemble au WCDMA, à quelques notables différences près. En particulier, au lieu de faire du CDMA sur l'ensemble de la bande, la bande passante allouée à la troisième génération est découpée en plusieurs sous-bandes, et le CDMA est appliqué à chacune de ces sous-bandes.

La transition entre la deuxième génération IS-95, que l'on appelle encore IS-95A, et le cdma2000 s'effectue par l'intermédiaire de la norme IS-95B. Cette dernière reste compatible avec l'IS-95A mais augmente fortement les débits des données par l'intégration de plusieurs codes simultanés, huit au maximum, pour un même utilisateur. Un terminal haut

débit a la possibilité de gagner jusqu'à sept codes supplémentaires pendant la période de débit crête. Le canal peut être asymétrique, avec des canaux montant et descendant différents. Le contrôle de puissance pour les canaux supplémentaires n'est pas indépendant du canal de base. Le débit total offert dans la version IS-95B est de 76,8 ou 115,2 Kbit/s, suivant que l'on compte le débit total ou le débit utile du canal de base.

L'interface radio du cdma2000 reprend les attributs de l'IS-95 mais avec une largeur de bande de 5 MHz. Elle peut regrouper un nombre de codes supérieur à 8. Un pilote de gestion du canal a été ajouté, permettant des gains significatifs de performances, notamment par une réduction du temps nécessaire au contrôle de puissance. Des turbocodes peuvent être utilisés à la place des codes de convolution.

Des débits pouvant atteindre jusqu'à 2 Mbit/s sont accessibles sur des picocellules à l'intérieur des bâtiments, jusqu'à 384 Kbit/s pour les piétons restant dans une même cellule et jusqu'à 144 Mbit/s pour les véhicules qui effectuent des changements de cellules.

La technique d'accès au support hertzien est fortement modifiée entre l'IS-95 et le cdma2000. Alors qu'il n'y avait que deux états possibles de l'interface IS-95, il y en a quatre avec le cdma2000.

La troisième génération (3G)

Les systèmes de télécommunications mobiles de troisième génération fournissent toute une gamme de services de télécommunications aux utilisateurs fixes et mobiles, situés dans une variété d'environnements autour de la bande de fréquences des 2 GHz. En 1985, l'UIT a commencé ses études des réseaux FPLMTS (Future Public Land Mobile Telephone System), renommés IMT 2000 (International Mobile Telecommunications system for the year 2000) en 1993. L'ETSI a entamé les siennes pour l'Europe en 1990 avec l'UMTS. L'UMTS n'est qu'une des cinq normes de la famille IMT 2000, qui inclut également WCDMA, cdma2000, EDGE et DECT de troisième génération.

Ces systèmes mobiles de troisième génération se présentent comme des concurrents des infrastructures de deuxième génération déjà déployées. Il a toutefois fallu penser à la transition entre les deux générations, qui ne pouvait être instantanée, et à la possibilité de créer un maximum de services communs. La troisième génération améliore la précédente par une qualité du service rendu au moins comparable à celle fournie par les réseaux fixes. De plus, les réseaux IMT 2000, comme l'UMTS, cherchent à fournir de nouvelles avancées significatives incluant l'itinérance mondiale, une large gamme de services, à haut débit ou non, des services audiovisuels et l'utilisation d'un seul terminal dans différents environnements radio. La gamme des services de télécommunications doit pouvoir s'adapter de façon flexible aux besoins des utilisateurs et leur permettre de communiquer indépendamment de leur localisation et de leur méthode d'accès.

Un autre objectif des réseaux de troisième génération est de rendre les services fixes et mobiles compatibles pour former un service transparent de bout en bout pour les utilisateurs.

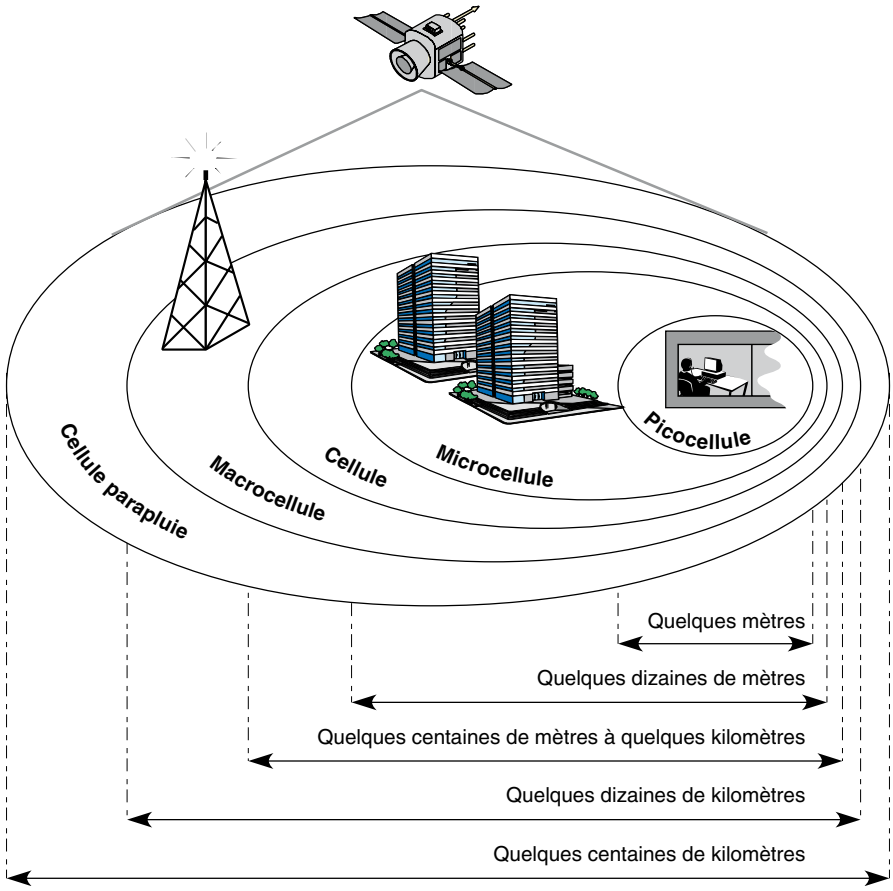
La liste suivante, extraite de la norme UMTS, présente quelques-unes des conditions requises pour ces réseaux :

- Fournir un seul système intégré, dans lequel l'utilisateur peut facilement accéder aux services UMTS d'une façon uniforme dans tous les environnements, qu'ils soient résidentiels, de bureau ou cellulaires, avec un même équipement, à condition que le terminal soit adapté.
- Fournir des services accessibles à des terminaux portatifs, qu'ils soient portables, montés dans des véhicules, transportables ou fixes, incluant ceux qui sont normalement connectés aux réseaux fixes, dans les environnements aussi bien résidentiels, que publics ou radio.
- Fournir une large gamme de services de télécommunications, incluant ceux fournis par les réseaux fixes, caractérisés par des débits utilisateur pouvant atteindre 2 Mbit/s, ainsi que les services propres aux communications mobiles. Ces services doivent être supportés par les environnements résidentiels, publics et de bureau, dans des zones de densité de population diverses. La qualité, particulièrement en ce qui concerne la voix, doit être comparable à celle fournie par les réseaux fixes comme le RNIS.
- Supporter des services audio, vidéo, texte et graphique, c'est-à-dire les éléments essentiels d'un appel multimédia, et de données.
- Offrir des débits de 64 à 144 Kbit/s en forte mobilité, 384 Kbit/s en mobilité moyenne et 2 à 10 Mbit/s en faible mobilité.
- Supporter la mobilité globale, à savoir la mobilité du terminal, comme dans le GSM, la mobilité personnelle universelle et la mobilité des services, le service étant assuré quels que soient l'accès et le lieu.
- Supporter les utilisateurs itinérants en leur permettant d'accéder aux services de leurs fournisseurs de façon toujours identique, même s'ils se déplacent.
- Permettre la différenciation entre les offres de services des différents réseaux et fournisseurs de services.
- Séparer les concepts de fournisseur de services et d'opérateur.
- Offrir un numéro unique, indépendant du réseau et du fournisseur de services.
- Permettre à un utilisateur piéton d'accéder à tous les services normalement accessibles par les réseaux fixes.
- Permettre à un utilisateur piéton d'accéder à tous les services normalement accessibles par PABX et réseaux locaux.
- Favoriser de petits terminaux, faciles à utiliser, dotés d'une grande autonomie et peu coûteux.
- Introduire facilement des services peu onéreux.
- Optimiser l'utilisation des ressources, en particulier du spectre radio.
- Partager les ressources spectrales entre les multiples opérateurs de réseaux publics et privés.
- Garantir une couverture radio transparente et globale.

- Garantir un accès satellite direct.
- Utiliser la bande de fréquences définie par la Conférence administrative mondiale des radiocommunications en 1992 (1 885-2 025 et 2 110-2 200 MHz).
- Adopter un système ouvert pour accélérer la création et la personnalisation de nouveaux services.
- Supporter une large gamme de services pouvant s'adapter aux souhaits de l'utilisateur.
- Introduire des recommandations dans l'IMT 2000 pour aboutir à une compatibilité entre les différentes normes (UMTS, WCDMA, cdma2000, etc.).

Plusieurs de ces conditions requièrent un seul système intégrant plusieurs environnements fonctionnant de façon concertée. Les services seront disponibles dans toutes les situations dans lesquelles pourra se trouver l'utilisateur, à l'intérieur ou à l'extérieur des zones urbaines denses, même dans les bureaux, dans le cas d'une utilisation intensive, dans les zones reculées, suburbaines et rurales. La figure N.6 illustre les différents environnements définis pour les réseaux IMT 2000.

Figure N.6
Environnement des réseaux IMT 2000



Chacune des quatre zones représentées sur la figure caractérise un environnement spécifique. La première zone, de quelques mètres, correspond à un environnement de grande densité, comme le centre d'une ville, avec des picocellules dans lesquelles le trafic est très important. Dans ce type d'environnement, le débit maximal peut atteindre 2 à 10 Mbit/s, rejoignant, voire dépassant celui des offres ADSL. Dans les deux zones suivantes, de quelques dizaines à quelques centaines de mètres, la mobilité augmente tandis que le débit diminue. Dans la dernière zone, de quelques dizaines à quelques centaines de kilomètres, caractérisée par le composant satellite, la mobilité est globale, avec un débit pouvant atteindre 2 Mbit/s. Les situations terrestre, maritime et aéronautique sont incluses dans les objectifs de ces cellules parapluie. De ce fait, l'utilisateur se trouvant dans un véhicule, sur un bateau ou dans un avion bénéficie d'une disponibilité continue des services.

Les réseaux IMT 2000 utilisent simultanément les techniques cellulaires et sans fil ainsi que le composant satellite, complément des réseaux fixes et mobiles, qui fournit une couverture globale, à l'intérieur et à l'extérieur des bâtiments, ce que ne permet pas un déploiement terrestre conventionnel.

Les services de l'IMT 2000

En principe, les services de l'IMT 2000 doivent être compatibles avec ceux des réseaux de télécommunications fixes en matière de fonctionnalités, d'interface utilisateur, de coût et de qualité. Les réseaux IMT 2000 étendent les services multimédias multipartites, comme ceux fournis par les réseaux fixes, au domaine mobile. Ce point est important, car un utilisateur équipé d'un téléphone mobile peut de la sorte bénéficier avec plus de liberté des services auxquels il a souscrit, sans souffrir d'une perte de qualité de service.

Les services fournis vont de l'audio à la vidéo, en passant par les données et le multimédia. L'utilisateur d'un même terminal doit pouvoir établir et maintenir plusieurs connexions simultanément. Il doit de plus se voir offrir des applications réclamant des paramètres différents de qualité de service. Les services proposés dépendent des propriétés, ou capacités, du terminal ainsi que de l'offre de l'opérateur concerné. Les services demandant de hauts débits de transmission sont concentrés dans les zones de grande densité, comme les centres d'affaires, plutôt que dans les zones suburbaines. Les utilisateurs d'IMT 2000 ne se rendront pas compte qu'un lien radio connecte leur terminal aux réseaux mondiaux de télécommunications.

La stratégie déployée pour intégrer de nouveaux services dans les réseaux IMT 2000 ressemble à ce qui a été conçu dans le cadre des réseaux intelligents. Elle consiste à définir des capacités de service et non les services eux-mêmes. Les capacités de service concernent les techniques de transport nécessitées par les paramètres de qualité de service ainsi que les mécanismes nécessaires à leur réalisation. Ces mécanismes incluent les fonctionnalités fournies par les différents éléments de réseau, la communication entre eux et le stockage des données associées. Ces capacités normalisées fournissent une plate-forme supportant la voix, la vidéo, le multimédia, les messages, les données et autres téléservices, des applications utilisateur et des services supplémentaires. Elles permettent la

création d'un marché pour des services déterminés par les utilisateurs et les fournisseurs de service.

La mobilité globale est impossible à réaliser aujourd'hui du fait de la multiplicité des systèmes et des réseaux. Il est quasiment impossible pour un utilisateur de bénéficier des mêmes services dans les mêmes conditions dans son réseau d'abonnement et dans les réseaux visités. Lorsqu'elle deviendra une réalité, la mobilité des services permettra aux utilisateurs de disposer des mêmes services dans les mêmes conditions, quelle que soit leur localisation. L'itinérance, ou mobilité du terminal, permettra de construire un réseau universel. Les futurs réseaux supporteront de surcroît le concept de VHE (Virtual Home Environment), qui vise à offrir à l'utilisateur un ensemble complet de services ayant une même apparence, que ce dernier se trouve dans son réseau d'abonnement ou dans un autre réseau.

L'offre de mobilité personnelle n'est possible que si l'utilisateur IMT 2000 possède un identificateur indépendant du réseau et du fournisseur de services. Les opérateurs de réseau et les fournisseurs de service pouvant être deux entités distinctes, le fait de posséder un numéro spécifique avec chacune de ces entités rend plus compliquée la fourniture des services, en particulier le routage des appels. C'est pourquoi l'identificateur de l'utilisateur doit être unique. Grâce à ce numéro personnel unique, le seul connu par les appelants, l'utilisateur peut être joint n'importe où dans le monde.

Les réseaux IMT 2000 supportent la portabilité des numéros aux niveaux à la fois du fournisseur de services, de la localisation et des services. La portabilité des numéros au niveau du fournisseur de services implique qu'un identificateur, appelé IMUN (International Mobile User Number), est alloué à chaque nouvel abonné IMT 2000. Un abonné peut changer de fournisseur de services tout en gardant son IMUN, à condition que le nouveau fournisseur de services offre le service concerné dans la même zone géographique. De même, un fournisseur de services peut changer d'opérateur réseau tout en conservant son IMUN. La portabilité de la localisation signifie que chaque abonné peut être appelé indépendamment de sa localisation, et donc de sa mobilité. La portabilité du numéro signifie que le numéro à composer pour joindre un utilisateur est indépendant du service requis.

Le spectre radio doit être utilisé de façon efficace et éventuellement partagé entre différents opérateurs dans le but d'offrir une couverture radio globale, transparente pour l'usager, avec la portion satellite. Il doit être possible pour un terminal IMT 2000 de s'adapter à l'interface radio fournie dans une région spécifique et de déterminer les capacités de services disponibles dans celle-ci. De plus, comme plus d'une interface radio est disponible dans une région donnée, la norme doit prévoir un mécanisme qui permette à un terminal IMT 2000 de sélectionner les interfaces radio capables de fournir les capacités de services appropriées.

Les clients individuels possèdent un profil de services particulier, avec une définition des types de services souscrits, incluant, par exemple, le moment de la journée où ces services sont utilisés. Le fournisseur de services a la charge du contrôle de tous les aspects de service de l'abonné et de l'utilisateur. Quand l'abonné et l'utilisateur sont des entités distinctes, l'abonné contrôle le profil de services de l'utilisateur dans les limites

de l'abonnement. L'abonné peut facilement modifier ce profil et décider si l'utilisateur détient le contrôle de l'activation-désactivation des services définis dans le profil de services de l'utilisateur. Tout changement du profil de services doit être effectué de façon sécurisée. Les informations concernant l'utilisateur, nécessaires pour l'identifier sans ambiguïté et permettre son enregistrement pour un service sont enregistrées sur sa carte, de type circuit intégré et comportant l'USIM.

Le concept de profil multiple est introduit dans les réseaux IMT 2000. Un profil multiple permet à un utilisateur d'obtenir certains services de la part d'un fournisseur de services et d'autres services de la part d'un autre fournisseur, et ce à l'aide d'une même carte. Dans le cas où des abonnements multiples sont possibles sur la même carte, si ceux-ci concernent plusieurs fournisseurs de services, un numéro différent est alloué pour chacun d'eux. Pour les appels sortants, l'utilisateur doit être capable de sélectionner le fournisseur de services qu'il préfère pour chaque appel ou en fonction de son abonnement. Plusieurs abonnements multiples peuvent être actifs simultanément. Le standard permet en outre de supporter l'enregistrement multiple sur un même terminal par l'insertion de cartes à puce multiples.

La sécurité des futurs réseaux de mobiles sera un critère essentiel de leur réussite. Les réseaux IMT 20000 prévoient une sécurité mutuelle : le réseau peut authentifier l'utilisateur afin de vérifier qu'il est bien celui qui est autorisé à utiliser les services, et l'utilisateur peut demander à authentifier le réseau au moment de son enregistrement et avant d'initier un service. De même, les réseaux peuvent s'authentifier entre eux. D'autres relations d'authentification seront définies dans les réseaux et seront détaillées par la suite. Ces nouveaux services seront flexibles afin d'être les plus proches possibles des souhaits de l'utilisateur.

Les normes IMT 2000 devront être cohérentes pour garantir la compatibilité entre réseaux. Les futurs réseaux de mobiles seront compatibles avec les systèmes mobiles de deuxième génération, qui continueront à fonctionner (GSM, DCS 1800, DECT, etc.) à pleine capacité, afin d'autoriser le déplacement des utilisateurs à travers le monde. Les réseaux IMT 2000 intégreront les réseaux de mobiles cellulaires et satellite et les réseaux fixes dans un seul système afin de fournir une couverture globale, à l'intérieur et à l'extérieur, de façon uniforme, permettant aux utilisateurs d'accéder aux services, quels que soient le terminal et le réseau qu'ils utilisent et leur emplacement géographique.

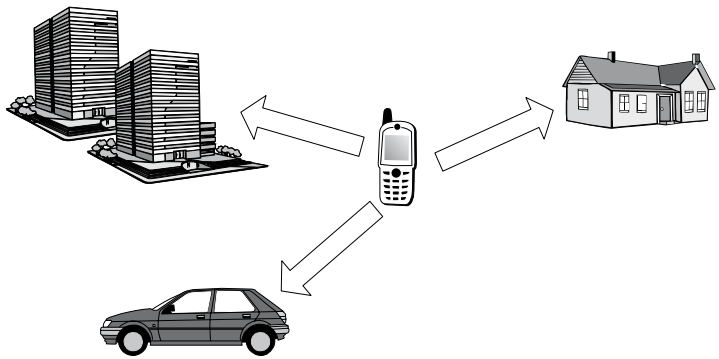
En résumé, l'utilisateur d'une technologie de troisième génération bénéficiera d'une offre complète de services grâce à l'intégration des réseaux fixes et mobiles. L'intégration et la compatibilité entre les différents réseaux correspondant à des normes différentes (UMTS, WCDMA, cdma2000, GSM, etc.) autoriseront l'itinérance et l'interfonctionnement. L'utilisateur pourra se déplacer entre réseaux de troisième génération de façon transparente, tout en gardant la continuité des services, même si, dans certains cas, la qualité pourra en pâtir du fait des caractéristiques d'un nouvel environnement radio. Si des accords d'itinérance n'existent pas entre le fournisseur de services de l'utilisateur et le réseau visité par ce dernier, il sera possible d'établir de tels accords. Lorsque plus d'un réseau visité sera disponible, l'utilisateur aura la possibilité de sélectionner manuellement ou automatiquement un réseau particulier, en fonction de son profil de services.

La mobilité dans les réseaux de troisième génération

Le fait d'offrir une mobilité globale, rassemblant mobilité du terminal, mobilité personnelle et mobilité des services, représente l'atout décisif des réseaux de troisième génération.

La mobilité du terminal correspond à la capacité du terminal à accéder aux services de télécommunications, quels que soient l'endroit où il se trouve et sa vitesse de déplacement. Cette mobilité, illustrée à la figure N.7, implique que le réseau est capable d'identifier, de localiser et de suivre les utilisateurs, indépendamment de leurs mouvements, puis de router les appels vers eux. Un enregistrement précis de la localisation de l'utilisateur et de son terminal associé doit être maintenu. L'itinérance est liée à la mobilité du terminal, puisqu'elle permet à un utilisateur de se déplacer d'un réseau à un autre.

Figure N.7
Mobilité du terminal

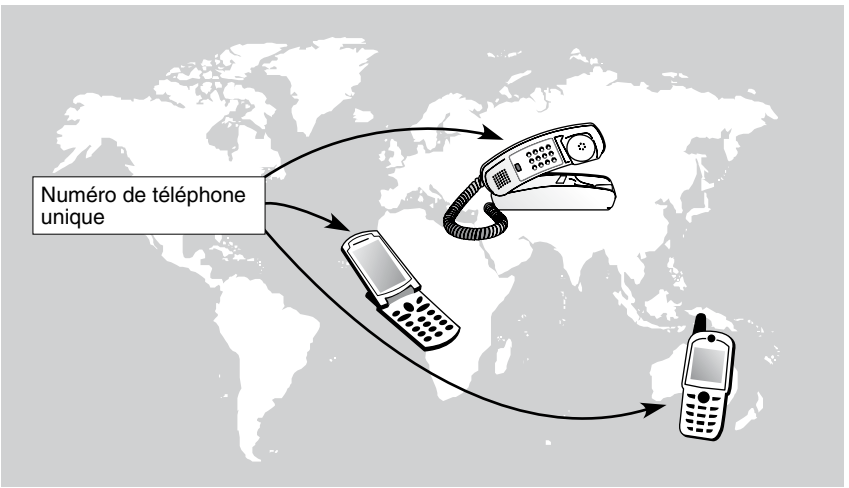


La mobilité personnelle correspond à la capacité d'un utilisateur à accéder aux services de télécommunications entrants et sortants sur tout terminal, à n'importe quel endroit. Sur la base d'un numéro personnel unique, l'utilisateur peut initier et recevoir des appels à partir de n'importe quel terminal. La mobilité personnelle implique la capacité du réseau à identifier les utilisateurs lorsqu'ils se déplacent afin de leur fournir des services en fonction de leur profil de services et de localiser le terminal associé à l'utilisateur pour adresser, acheminer et facturer les appels de l'utilisateur. Cette mobilité personnelle est symbolisée à la figure N.8.

Figure N.8
Mobilité personnelle

La mobilité des services, aussi appelée portabilité des services, se réfère à la capacité du réseau à fournir les services souscrits à l'endroit où se trouvent le terminal et ses utilisateurs. Cette mobilité est décrite à la figure N.9. Les services exacts que l'utilisateur peut demander sur son terminal dépendent de la capacité du terminal à cette localisation et du réseau qui dessert ce terminal. La portabilité des services est assurée par des mises à jour régulières du profil de services de l'utilisateur et l'interrogation de ce profil si nécessaire. La mobilité des services associe les services à un utilisateur et non à un accès particulier du réseau. Les services doivent suivre les utilisateurs lorsque ceux-ci se déplacent.

Figure N.9
Mobilité des services



Lié à la mobilité des services, le VHE (Virtual Home Environment) prend en charge les utilisateurs itinérants en leur permettant d'accéder aux services fournis par leurs fournisseurs de services toujours de la même façon, même s'ils se déplacent. Grâce au VHE, l'utilisateur peut utiliser ses services dans n'importe quel réseau qu'il visite, de la même manière et avec les mêmes caractéristiques que lorsqu'il se trouve dans son propre réseau d'abonnement. Il dispose ainsi d'un environnement personnalisé de services, qui le suit partout où il se déplace. Le VHE sera fourni à condition que les différents réseaux visités par l'utilisateur soient capables de proposer les mêmes fonctionnalités que le réseau d'abonnement.

On regroupe parfois dans le concept de mobilité de l'utilisateur la mobilité du terminal et la mobilité personnelle.

Annexe O

21. Les réseaux personnels

Cette annexe décrit l'environnement de la norme UWB supportée par la WiMedia Alliance. Cette norme ne s'est pas développée comme prévu du fait de la consommation électrique des terminaux mobiles dotés de batteries standards, qui n'a pu être ramenée à une valeur acceptable.

UWB (Ultra Wide Band)

UWB est une technologie radio sans fil pour la transmission point-à-point entre équipements électroniques grand public, les périphériques PC et les dispositifs mobiles, sur de courte distance et à très grande vitesse, tout en consommant peu de puissance. Elle est bien adaptée au transfert de données multimédias, tel que la transmission sans fil de vidéos à partir d'un magnétoscope numérique vers une télévision haute définition dans le salon ou d'un PC mobile vers un vidéo-projecteur dans une salle de conférence pour réaliser une présentation sur grand écran.

Une grande valeur est attachée à la mise en place de dispositifs permettant aux équipements de se découvrir automatiquement et de communiquer, d'imprimer ou de demander un service sans intervention des utilisateurs. En règle générale, cette découverte automatique est impossible au travers d'un environnement câblé utilisant des interfaces incapables de communiquer entre elles.

L'adoption rapide des communications UWB dépendra de leur facilité d'utilisation et de leur coût. Les utilisateurs sont en outre en droit d'attendre un système fiable et fortement testé.

L'interopérabilité est une question clé pour permettre des opérations transparentes pour l'utilisateur, indépendamment des fabricants choisis. Par conséquent, il est crucial que la

standardisation des protocoles soit effectuée et que l'ensemble des protocoles soit incorporé dans une plate-forme unifiée, notamment les suivants :

- USB (Universal Serial Bus). Conçue au départ pour raccorder par câble des périphériques à un PC, cette interface est surtout utilisée pour le transfert de données.
- IEEE 1394, également connu sous le nom de FireWire. Spécifiquement conçu pour transmettre des flots multiples de types divers, comme l'audio et la vidéo, cette norme a été adoptée dans beaucoup de foyers pour remplacer les systèmes hétérogènes de diffusion audio, vidéo et de jeu.
- Bluetooth. L'objectif de cette technologie était de remplacer les câbles mais à des débits relativement faibles, tels qu'on en trouve dans les téléphones portables, ordinateurs personnels, PDA, écouteurs, etc.

Si chacun de ces protocoles correspond à des segments de marché différents, les consommateurs en souhaitent l'interopérabilité sans couture. À cet effet, des consortiums d'industriels, comme DLNA (Digital Living Network Alliance), essayent de définir des solutions d'interopérabilité complète à l'intérieur de la maison.

Parmi les applications ciblées, citons notamment les suivantes :

- Téléchargement depuis un caméscope vers un PC pour traitement, puis vers la télévision.
- Synchronisation des données d'un PDA vers un PC.
- Chargement de jeux audio/vidéo vers un PDA.
- Liaison d'un ordinateur portable vers une console de jeu.
- Passerelle résidentielle vers un serveur de jeux.
- Transfert de fichiers audio vers un lecteur MP3 à partir d'une base de données située sur un serveur de la maison.
- Télévision haute définition (HDTV) depuis ou vers le téléviseur pour stocker ou jouer des films. Cette application demande un débit de l'ordre de 20 Mbit/s.
- Communication d'un téléphone portable vers une oreillette.
- Transferts de photos d'un appareil numérique ou d'un téléphone portable.
- Téléchargement de jeux ou de films d'un point d'accès sans fil à un portable dans un lieu public tel qu'une gare.
- Téléchargement d'une présentation vers un vidéo-projecteur.

La partie du spectre choisie par l'UWB est également utilisée pour des applications telles que les radars de contrôle de collision et de découverte d'obstacles, les systèmes de positionnement de personnes, les systèmes d'inventaire automatique et les systèmes de transport intelligent. Plusieurs sociétés développent des technologies pour satisfaire des besoins spécifiques de communication sans fil robuste et sécurisée dans divers secteurs, tels que la santé, les opérations d'urgence ou les environnements militaires.

Dans le domaine de la santé, la localisation des équipements de diagnostic ou le transfert des données des patients dans les milieux hospitaliers peuvent être réalisés par le biais

de plates-formes logicielles/matérielles en indiquant le cheminement des objets grâce à un contact radio permanent par le biais d'un réseau de capteurs placés dans le bâtiment.

Dans les opérations de secours, ces systèmes peuvent permettre le positionnement de personnes physiques prises dans un feu ou un accident de produits toxiques ou lors d'un acte de terrorisme. Dans ce dernier cas, signalons que le NASC (Naval Air Systems Command) américain a commandé des systèmes d'intercommunication entre avions par UWB nommés AWICS (Aircraft Wireless Intercommunication Systems).

Annexe P

22. Les réseaux Wi-Fi

Cette annexe se penche sur un certain nombre de problèmes qui peuvent survenir en matière de supervision, de qualité de service, de contrôle de la mobilité ou de gestion de l'énergie avec le standard IEEE 802.11e.

Parmi les fonctionnalités examinées, nous aborderons successivement les solutions pour prendre en charge les stations cachées, les problèmes de fragmentation-réassemblage, l'introduction de priorités avec IEEE 802.11e, le contrôle des handovers et la gestion de la mobilité

La réservation RTS/CTS et le problème de la station cachée

Dans Wi-Fi, l'écoute du support se fait à la fois au niveau de la couche physique, avec le PCS (Physical Carrier Sense), et au niveau de la couche MAC, avec le VCS (Virtual Carrier Sense). Le PCS détecte la présence d'autres stations Wi-Fi en analysant toutes les trames passant sur le support hertzien et en détectant l'activité sur le support grâce à la puissance relative du signal des autres stations.

Le VCS est un mécanisme de réservation fondé sur l'envoi de trames RTS/CTS (Request to Send/Clear to Send) entre une station source et une station destination avant tout envoi de données. Une station source qui veut transmettre des données envoie un RTS. Toutes les stations du BSS entendant le RTS lisent le champ TTL du RTS et mettent à jour leur NAV. La station destination ayant reçu le RTS répond, après avoir attendu pendant un SIFS, en envoyant un CTS. Les autres stations entendant le CTS lisent le champ de durée du CTS et mettent à nouveau à jour leur NAV. Après réception du CTS par la station source, cette dernière est assurée que le support est stable et réservé pour sa transmission de données.

Cela permet à la station source de transmettre ses données ainsi que de recevoir l'ACK sans collision. Comme les trames RTS/CTS réservent le support pour la transmission d'une station, ce mécanisme est habituellement utilisé pour envoyer de grosses trames pour lesquelles une retransmission serait trop coûteuse en terme de bande passante.

La figure P.1 illustre le processus d'émission d'une trame lorsque la station destination est cachée.

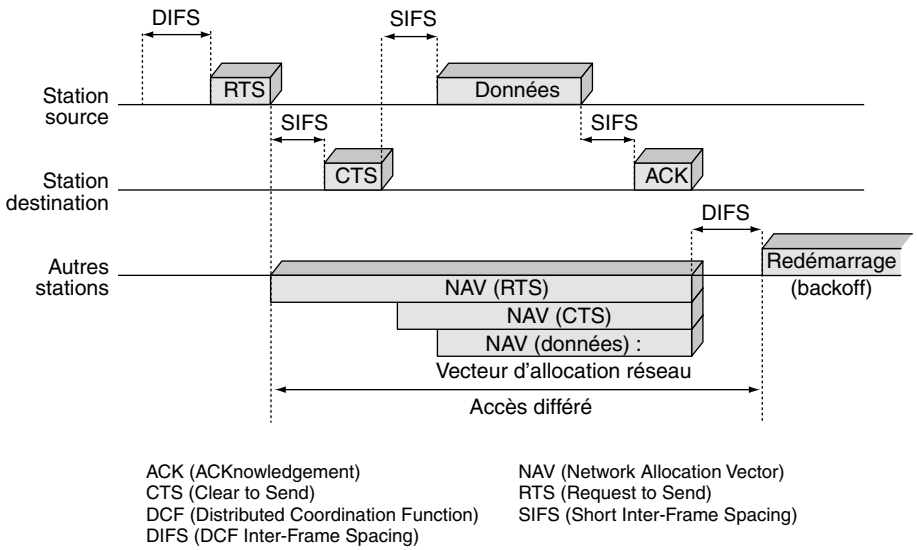


Figure P.1

Transmission en utilisant les trames RTS/CTS

Les stations peuvent choisir d'utiliser le mécanisme RTS/CTS ou de ne l'utiliser que lorsque la trame à envoyer excède une variable RTS_Threshold ou encore de ne jamais l'utiliser.

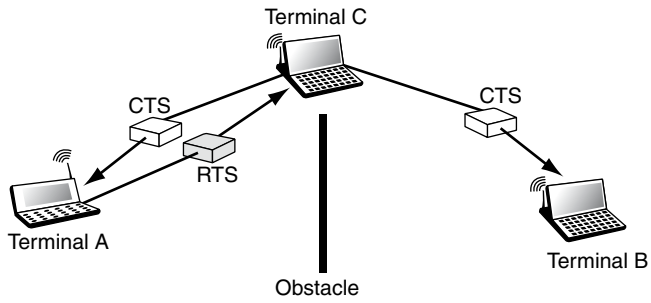
Le problème de la station cachée

Un problème spécifique du monde sans fil est le problème de la station cachée. Deux stations situées chacune à l'opposé d'un point d'accès (AP) ou d'une autre station peuvent entendre l'activité de cet AP mais ne pas s'entendre l'une l'autre du fait que la distance entre les deux est trop grande ou qu'un obstacle les empêche de communiquer entre elles. Le mécanisme de réservation RTS/CTS permet de résoudre ce problème.

La figure P.2 illustre une station B cachée de la station A mais pas de la station C. La station A transmet des données à la station C, mais la station B ne détecte pas l'activité de la station A. Dans ce cas, la station B peut transmettre librement, sans interférer avec la transmission de la station A. Toutefois, si A et C s'échangent des RTS et des CTS, la

station B, bien que n'écoutant pas directement la station A, est informée par l'envoi par la station C d'un CTS que le support est occupé. Elle n'essaie donc pas de transmettre durant la transmission entre A et C. Ce mécanisme ne permet pas d'éviter les collisions, puisque des RTS peuvent être envoyés simultanément par A et par B, mais une collision de RTS ou de CTS ne gaspille pas autant de bande passante qu'une collision de données, étant donné que les trames RTS et CTS sont relativement petites.

Figure P.2
Problème de la station cachée



En conclusion, le CSMA/CA permet de partager l'accès. Le mécanisme d'acquittement supporte en outre efficacement les problèmes liés aux interférences et, d'une manière générale, tous les problèmes liés à l'environnement radio. Le mécanisme de réservation RTS/CTS évite les problèmes de la station cachée. Tous ces mécanismes entraînent toutefois l'ajout aux trames Wi-Fi d'en-têtes, que les trames Ethernet ne possèdent pas. C'est pourquoi les réseaux Wi-Fi montrent toujours des performances plus faibles que les réseaux locaux Ethernet.

Fragmentation-réassemblage

Nous venons d'introduire le protocole CSMA/CA, qui permet à une station d'accéder au support hertzien pour émettre sa trame. Une question en suspens concerne la taille de la trame. Plus la taille d'une trame est importante, plus elle a de chance d'être corrompue. La fragmentation d'une trame en plusieurs trames de taille inférieure accroît la fiabilité de la transmission. Cette solution a pour effet de réduire le besoin de retransmettre des données dans de nombreux cas et d'augmenter ainsi les performances globales du réseau. La fragmentation est utilisée notamment dans les liaisons radio, dans lesquelles le taux d'erreur est important.

Wi-Fi utilise un système à saut de fréquence (Frequency Hop), dans lequel le support s'interrompt toutes les 20 ms pour changer de fréquence. Si la trame est petite, la probabilité pour que la transmission soit interrompue est faible. Pour savoir si une trame doit être fragmentée, on compare sa taille à une valeur seuil, appelée Fragmentation_Threshold.

Si la taille de la trame est plus grande que ce seuil, la trame est fragmentée. Les fragments ont une taille équivalente à la valeur du seuil Fragmentation_Threshold, sauf pour le dernier, qui peut avoir une taille plus petite.

Quand une trame est fragmentée, tous les fragments sont transmis de manière séquentielle. Le support n'est libéré qu'une fois tous les fragments transmis avec succès ou lorsque la station source ne réussit pas à recevoir l'acquittement d'un fragment transmis. La station destination acquitte chaque fragment reçu avec succès en envoyant un ACK à la station source. La station source garde le contrôle du support pendant toute la durée de la transmission d'une trame en attendant un temps SIFS après la réception d'un ACK ou après la transmission d'un fragment. Si un ACK n'est pas correctement reçu, la station source arrête la transmission et essaie d'accéder de nouveau au support. Lorsque la station source accède au support, elle commence à transmettre à partir du dernier fragment non acquitté.

Si les stations utilisent le mécanisme RTS/CTS, seul le premier fragment envoyé utilise les trames RTS/CTS pour réserver le support. Les autres stations dans le BSS maintiennent leur NAV en extrayant l'information de durée de vie dans les différents fragments et ACK.

La figure P.3 illustre le processus suivi par l'émetteur pour transmettre une suite de fragments provenant d'une même trame.

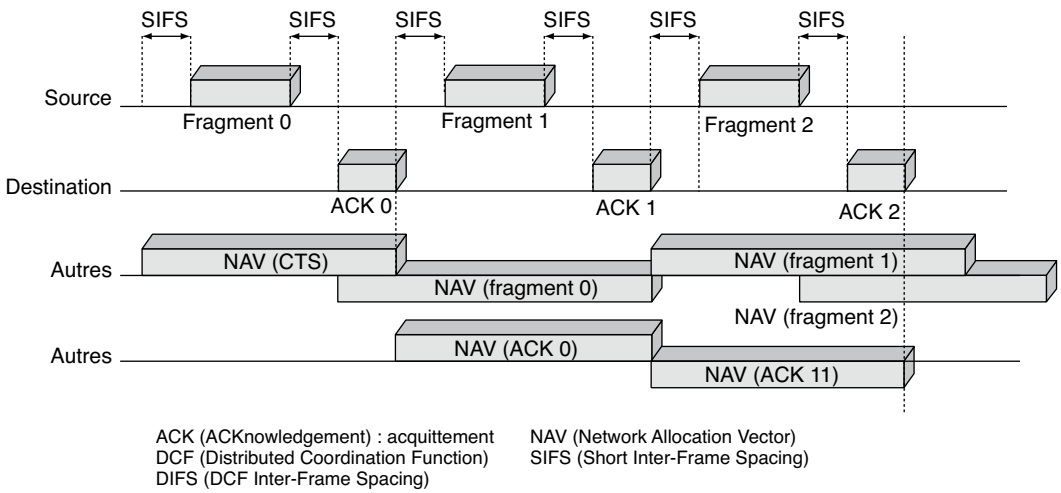


Figure P.3

Transmission d'une trame fragmentée

La trame est assemblée lorsque la station destination a reçu tous les fragments de la station source.

IEEE 802.11e

La qualité de service est indispensable pour assurer le transfert temps réel de données comme la voix ou la vidéo. De tels services demandent des transferts isochrones, c'est-à-dire des transferts de données qui permettent de faire varier le délai entre les différentes trames d'une même transmission. Dans le cas d'une application vidéo, par exemple, plus ce délai est important, plus la qualité se dégrade, qu'elle soit sonore ou visuelle. Pour minimiser ce délai, des mécanismes de priorité ont été introduits par une extension au standard 802.11, appelée 802.11e.

Wi-Fi et la qualité de service

Wi-Fi est utilisé comme un réseau local permettant d'échanger et de transmettre des données. Compte tenu des nombreux avantages apportés par ce type de réseau, il était normal de vouloir l'utiliser pour transmettre de la voix et même de la vidéo. Avec un débit théorique de 54 Mbit/s, IEEE 802.11g est capable de faire passer un trafic de type MPEG-4 ou même MPEG-2 sans aucun problème.

Il faut toutefois modérer cet optimisme, comme nous l'avons indiqué à la section précédente. Dans un tel cas, il faudrait qu'aucun autre trafic, par exemple de données, ne circule sur le réseau et que les stations qui utilisent l'application multimédia soient proches du point d'accès de façon que le mécanisme de variation de débit ne soit pas utilisé, évitant ainsi une chute de performance. Cela fait beaucoup de contraintes pour une simple transmission vidéo. Les mécanismes proposés par 802.11e améliorent justement la qualité de service.

Le taux de perte dans un réseau sans fil est de l'ordre de 10^{-3}, soit le taux de perte minimal pour appliquer une QoS. Le débit de Wi-Fi dépend du nombre de stations situées dans la cellule. La garantie de débit impose donc de limiter le nombre de stations connectées au point d'accès ainsi que de n'autoriser que des débits théoriques élevés. Le paramètre essentiel à prendre en compte est le délai entre les trames envoyées ainsi que sa variation, ou gigue.

La plupart des applications multimédias (voix et vidéo) demandent un trafic temps réel. Si les données d'une application multimédia n'arrivent pas à temps, cela peut stopper le processus de lecture ou engendrer des erreurs, que l'oreille et l'œil humain peuvent facilement voir ou entendre. L'oreille, par exemple, peut tolérer un temps de latence (délai) de 150 ms. Si ce temps augmente, la voix semble lointaine. Il en va de même de la vidéo. Si le délai n'est pas respecté, la vidéo peut apparaître pixellisée, ralentir, comporter des décalages entre le son et l'image, etc., la rendant difficile ou impossible à visionner.

Pour avoir un processus de lecture constant, l'instauration d'un système de priorité permettant de jouer sur le temps de réponse permet de mieux gérer ce type de trafic.

Les approches IntServ et DiffServ ne sont pas envisageables dans les réseaux Wi-Fi. En effet, ces mécanismes sont définis au niveau 3, niveau réseau, et il n'existe aucun lien, ou mapping, entre le niveau 3 et le niveau 2. Si l'on implémente DiffServ dans un réseau 802.11b souhaitant offrir à une station un débit de 3 Mbit/s, ce débit ne peut être

assuré que si la station est seule dans la cellule. Le débit maximal utile d'une station étant de 5 Mbit/s, en supposant un débit théorique de 11 Mbit/s, si une autre station essaye d'émettre sur le support, le débit est partagé entre les deux stations, soit 2,5 Mbit/s. Le débit de 3 Mbit/s ne peut plus être garanti, et DiffServ ne fonctionne pas.

Une solution à ce problème pourrait consister à appliquer un mécanisme de réservation en dehors du réseau Wi-Fi. Comme illustré à la figure P.4, il serait de la sorte possible de classifier le trafic entrant et sortant pour chaque station du réseau. Le problème est que la somme des débits alloués à chaque station ne devrait pas dépasser le débit maximal utile d'une cellule Wi-Fi. Dans l'exemple de la figure P.4, le réseau Wi-Fi étant en 802.11b, la somme des débits alloués aux trois stations (2, 2 et 1 Mbit/s) est égale à 5 Mbit/s, soit le débit maximal utile d'une cellule. Cette réservation, c'est-à-dire la classification des flux IP entrants et sortants du réseau Wi-Fi, ne peut donc se faire qu'à l'extérieur du réseau Wi-Fi par l'utilisation d'un classificateur. Une telle solution ne garantit toutefois que le débit et pas le délai, un paramètre important des trafics voix et vidéo.

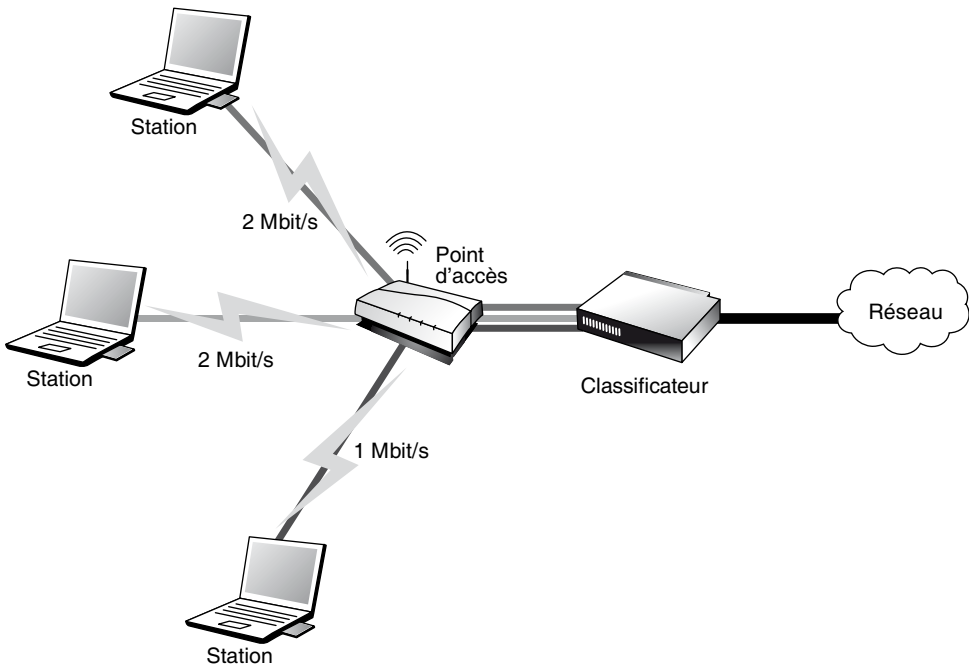


Figure P.4

Classification du trafic pour un réseau Wi-Fi 802.11b.

Cette solution est actuellement utilisée par de nombreux hotspots Wi-Fi ainsi que par certains FAI afin de garantir un débit moyen à l'utilisateur.

La téléphonie Wi-Fi, un marché en plein essor, ne peut utiliser un tel mécanisme qui ne garantit pas de délai. D'une manière générale, la téléphonie n'exige pas un débit

important. Le débit de la parole proprement dite est de 9,6 Kbit/s, ce qui donne un débit réel d'une cinquantaine de kilobits par seconde en tenant compte des éléments binaires introduits pour constituer le paquet puis la trame. Le délai et la gigue sont les paramètres principaux à prendre en compte. Ces derniers ne peuvent être assurés qu'en modifiant les paramètres d'accès définis dans 802.11, comme le propose l'amendement 802.11e.

Gestion des priorités

La norme IEEE 802.11e ajoute une nouvelle méthode, HCF (Hybrid Coordination Function), qui améliore la technique d'accès DCF. Cette méthode HCF est elle-même décomposée en deux algorithmes : l'EDCA (Enhanced Distributed Channel Access) et le HCCA (HCF Controlled Channel Access). Elles correspondent à l'introduction de classes, la première dans le DCF, la seconde dans le PCF. Comme l'EDCA est la seule utilisée, nous allons la décrire en détails.

L'EDCA est une évolution du DCF, qui ajoute un système de gestion de priorités lors de l'accès au support. Toujours à la manière du DCF, l'accès au support se fait selon le niveau de priorité de la trame. Les trames de même priorité ont la même probabilité d'accéder au support, tandis que celles de priorité supérieure ont une probabilité plus grande d'accéder au support.

Aujourd'hui, dans les réseaux Wi-Fi, les priorités sont les mêmes pour toutes les stations. Comme les trames de plus haute priorité ne peuvent interrompre le transfert des trames de plus faible priorité, il n'existe aucun moyen d'avoir une garantie sur la qualité de service d'une communication Wi-Fi.

L'EDCA fournit des accès différenciés pour différents types de trafic. Il définit huit niveaux de priorités par l'intermédiaire de catégories de trafic, ou TC (Traffic Categories). Chacune de ces catégories de trafic correspond à une file d'attente ayant, d'une part, un niveau de priorité et, d'autre part, des paramètres spécifiques, en fonction de ce niveau de priorité. Une station en mode EDCA équivaut à huit stations virtuelles traitant chacune différentes catégories de trafic.

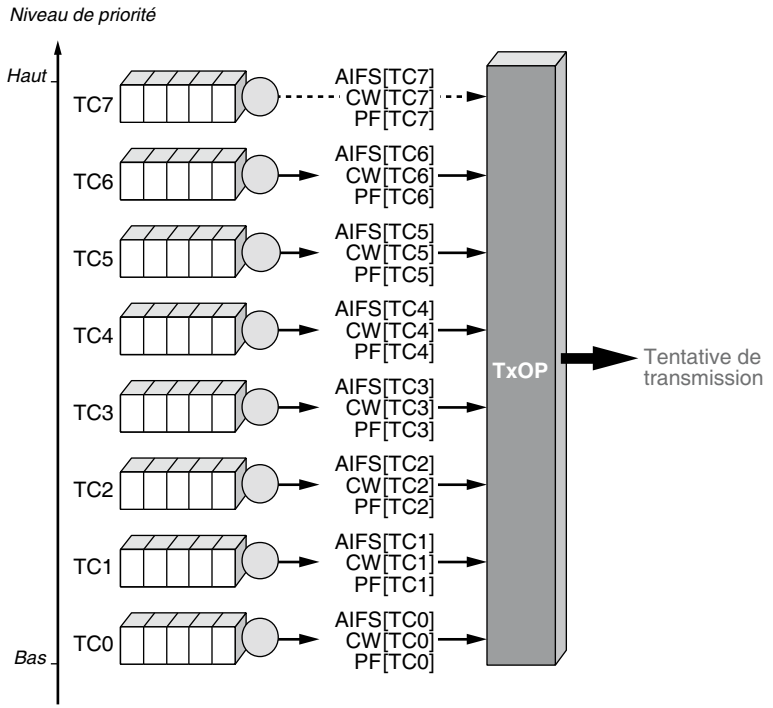
Chaque catégorie de trafic comporte des paramètres qui lui sont propres. Ces paramètres correspondent aux valeurs des différents temporisateurs utilisés (IFS, back-off), ainsi qu'aux paramètres utilisés dans le calcul de ces temporisateurs. La catégorie de trafic ayant la plus haute priorité est celle dont les valeurs de ces paramètres sont les plus faibles.

Les valeurs des temporisateurs ne sont pas fixes, comme dans le DCF. L'EDCA utilise toujours les IFS mais ajoute un nouveau temporisateur, l'AIFS (Arbitration IFS), qui joue le même rôle que le DIFS mais avec une valeur dynamique. De même, l'algorithme de back-off est toujours utilisé, mais la valeur de son temporisateur n'est plus fixe.

Le dernier apport de l'EDCA est l'ordonnanceur TxOP (Transmission Opportunities). Le TxOP détermine un temps, cette fois fixe, qui définit quand la station a le droit d'accéder au support et pendant quelle durée. Si plusieurs catégories de trafic veulent accéder au support au même instant, le TxOP encourage le TC de plus haute priorité.

Le fonctionnement de l'ECDF est illustré à la figure P.5.

Figure P.5
Les huit classes de trafics dans l'EDCA



L'EDCA fonctionne de la même manière que le DCF, les stations attendant en utilisant divers temporisateurs que le support soit libre avant toute transmission. La différence avec le DCF est que l'EDCA ne définit pas de valeurs fixes pour ces temporisateurs.

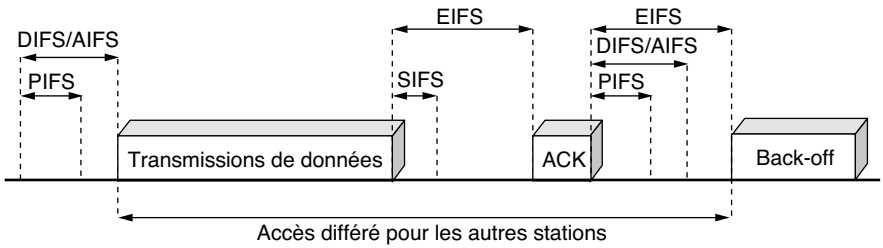
AIFS (Arbitration IFS)

Le DIFS est une durée d'attente utilisée par toutes les stations en mode DCF pour accéder au support. La valeur du DIFS est fixe et dépend de la couche physique utilisée. Seule la station arrivée la première sur le support — en supposant qu'il était auparavant libre — transmet ses données.

L'EDCA introduit un nouveau temporisateur, l'AIFS (Arbitration IFS), qui est utilisé de la même manière que le DIFS. Chaque station en mode EDCA attend un AIFS. Comme l'EDCA peut gérer jusqu'à huit niveaux de priorité, la valeur de l'AIFS n'est plus fixe mais dynamique. Elle varie en fonction du niveau de priorité requis par la station émettrice pour la transmission de sa trame. Cette valeur de l'AIFS est supérieure ou égale à celle du DIFS. Ainsi, la catégorie de trafic de priorité supérieure a une valeur d'AIFS égale à DIFS.

L'utilisation d'un tel système de priorité d'accès au support diminue le risque de collision. La figure P.6 illustre les différents temporisateurs utilisés lors de l'introduction de la qualité de service.

Figure P.6
Les relations entre les différents temporisateurs



L'algorithme de back-off

Dans le DCF, toute station accédant à un support occupé calcule un temporisateur grâce à l'algorithme de back-off. L'EDCA utilise toujours l'algorithme de back-off, mais, comme pour les temporisateurs IFS, son calcul est dynamique.

Le temporisateur de back-off est utilisé lorsqu'une ou plusieurs stations tente d'accéder au support alors que celui-ci est occupé ou qu'il y a eu des collisions. Pour accéder au support, ces stations attendent d'abord un DIFS. Si le support est toujours libre, elles attendent que le temporisateur de back-off expire. Ce temporisateur est calculé grâce à l'algorithme du même nom.

Cette variation opère sur la taille de la fenêtre de contention. Si cette taille est petite, la station virtuelle attend moins longtemps pour accéder au support par rapport à une station dont la taille de la fenêtre de contention est plus grande.

Pour chaque catégorie de trafic, la taille de la fenêtre de contention varie entre CWmin [TCi] et CWmax [TCi]. La formule permettant le calcul du temporisateur de back-off reste inchangée.

Lors d'une collision, un nouveau temporisateur est calculé. Cette fois, avec l'EDCA, on ne double pas la taille de la fenêtre de contention à chaque collision. La taille de la fenêtre de contention est calculée selon la formule suivante :

$CW_{new}\,[TCi] \geq (PF \times (CW_{old}\,[TCi] + 1)) - 1$

où PF (Persistent Factor) est le facteur persistant. Le paramètre PF est dépendant de la catégorie de trafic.

Si PF = 2, on retourne dans le mode DCF, où la fenêtre de contention est doublée après chaque collision, et l'on revient à l'algorithme de back-off exponentiel. Si PF = 1, la taille de la fenêtre de contention ne change pas. Ainsi, les catégories de trafic de priorités les plus hautes ont une valeur de PF plus petite comparées aux catégories de trafic de priorités les plus basses.

TxOP (Transmission Opportunities)

Une fois qu'une station accède au support et que son temporisateur de back-off expire, elle doit à nouveau retarder sa transmission. Comme expliqué précédemment, l'EDCA introduit un ordonnanceur de trafic, appelé TxOP (Transmission Opportunities), qui correspond à un temps fini dont la valeur est fonction de la classe de trafic utilisée.

Dans le cas où différentes catégories de trafic accèdent au support en même temps, c'est le TxOP qui détermine celle qui accède réellement au support en fonction de son niveau de priorité. Si deux classes de trafic voient leur temporisateur de back-off expirer au même instant, la valeur du TxOP détermine la classe de trafic qui peut émettre les données prioritairement. Étant donné que la classe de trafic de priorité la plus haute possède le TxOP le plus petit, c'est cette classe qui peut émettre en premier, respectant ainsi l'ordre des priorités.

Si une classe de trafic de priorité la plus haute (TC7) accède en même temps qu'une classe de trafic de priorité la plus faible (TC1) au TxOP, celui-ci favorise TC7, qui peut dès lors transmettre sur le support, et signifie à TC1 qu'une collision s'est produite. TC1 doit retransmettre ses informations en initiant l'algorithme de back-off avec ses paramètres caractéristiques : AIFS [TC1], CW[TC1] et PF[TC1].

En résumé, l'EDCA est la seule méthode d'accès qui permette d'affecter une certaine QoS au réseau Wi-Fi, même s'il n'empêche pas les collisions, obstacle majeur à la fourniture de services garantis. Par ailleurs, la classe de trafic de plus haute priorité utilise un AIFS égal au DIFS. Une classe de trafic TC7 ayant la même probabilité d'accéder au support qu'une station ne possédant pas ce mécanisme de QoS, certains paramètres de QoS ne peuvent donc être garantis. C'est pourquoi il est nécessaire de limiter l'accès au réseau aux stations 802.11e afin d'obtenir un vrai réseau Wi-Fi avec QoS.

802.11e ne spécifie pas non plus la manière dont sont choisies les applications qui ont la plus forte priorité et laisse cette tâche aux constructeurs. Le mapping le plus simple consisterait à affecter une des classes de trafic à un ou plusieurs numéros de port particulier. Chaque application possède un numéro de port permettant de le reconnaître au sein d'un flux de données. Malheureusement, cette notion de port est devenue assez obsolète depuis l'arrivée des réseaux peer-to-peer, qui utilisent des numéros de port dynamiques, voire des numéros de port déjà alloués, comme le port 80 pour HTTP, afin de passer outre les protections de type pare-feu des réseaux. On peut donc imaginer qu'un utilisateur puisse changer le numéro de port de son application afin que cette dernière passe en priorité sur un réseau Wi-Fi 802.11e.

IEEE 802.11f

La mobilité est une caractéristique essentielle d'un réseau sans fil. Elle permet aux utilisateurs du réseau de se déplacer à leur guise tout en maintenant leur communication en cours.

À l'origine, le standard 802.11 ne permettait pas de maintenir la communication lors d'un déplacement intercellulaire. Lucent, comme d'autres constructeurs, a développé un mécanisme apportant la mobilité au monde Wi-Fi. Ce protocole, appelé IAPP (Inter-Access Point Protocol), est déjà implémenté dans des équipements. Le groupe de travail IEEE 802.11f l'a désigné comme protocole de référence pour la gestion de la mobilité dans 802.11.

L'avenir de 802.11f

Le rôle premier de 802.11f est de permettre une interopérabilité entre points d'accès par le biais d'un mécanisme de gestion des handovers. Cet amendement n'est guère apprécié par les constructeurs du fait qu'il permettra l'utilisation de points d'accès hétérogènes dans un même réseau Wi-Fi. Les équipementiers proposent en effet des mécanismes de gestion des handovers propriétaires, qui nécessitent les mêmes points d'accès pour pouvoir fonctionner.

Dans Wi-Fi, une certaine mobilité n'est possible que si le réseau est en mode infrastructure. Dans le cas d'un réseau formé d'un seul BSS, c'est-à-dire d'une cellule unique contrôlée par un seul point d'accès, le point d'accès permet aux différentes stations d'avoir un service de mobilité restreint à la zone de couverture. Une fois la zone de couverture dépassée, aucune communication n'est possible. Pour un réseau en mode ad-hoc, la mobilité n'est possible que si les stations se voient.

Si le réseau est un ESS (Extended Service Set), c'est-à-dire un réseau composé d'un ensemble de BSS, les stations du réseau ont accès à une zone plus vaste. L'utilisation de certains mécanismes permet aux utilisateurs de se déplacer d'une cellule à une autre sans perte de communication.

Le standard 802.11 ne détaille pas ce mécanisme mais définit certaines règles de base, comme la synchronisation, l'écoute passive et active ou encore l'association et la réassociation, qui permettent aux stations de choisir le point d'accès le plus approprié pour communiquer.

Le groupe de travail 802.11f vise à standardiser un protocole permettant la gestion de la mobilité tout en apportant une certaine interopérabilité entre les points d'accès.

Synchronisation

Lorsque les stations se déplacent, c'est-à-dire lorsqu'elles changent de cellule ou qu'elles sont en mode économie d'énergie, elles doivent rester synchronisées pour pouvoir communiquer. Au niveau d'un BSS, les stations synchronisent leur horloge avec l'horloge du point d'accès.

Pour garder la synchronisation, le point d'accès envoie périodiquement une trame balise, ou Beacon Frame, qui contient la valeur d'horloge du point d'accès lorsque la transmission de cette trame a réellement lieu. Dès réception de cette trame, les stations mettent à jour leur horloge pour rester synchronisées avec le point d'accès. Les trames balises sont envoyés toutes les 32 µs. Cette période peut être toutefois configurable selon le matériel utilisé.

Association-réassociation

Lorsqu'une station entre dans un BSS ou un ESS, soit après une mise sous tension ou en mode veille, soit lorsqu'elle entre directement dans une cellule, elle doit choisir un point d'accès auquel s'associer. Le choix du point d'accès s'effectue selon différents critères,

tels que la puissance du signal, le taux d'erreur des paquets ou la charge du réseau. Si les caractéristiques du signal du point d'accès sont trop faibles, la station cherche un point d'accès plus approprié.

L'association, tout comme la réassociation, comporte les différentes étapes suivantes :

1. La station écoute le support.
2. Après avoir trouvé le meilleur point d'accès, elle s'authentifie.
3. Si cette phase réussit, la station s'associe avec le point d'accès et transmet ses données.

Le processus de réassociation est utilisé par une station qui veut changer de point d'accès. Bien qu'elle soit déjà associée à un point d'accès, la station essaye d'écouter le support afin de trouver un point d'accès ayant de meilleures caractéristiques. Si elle en trouve, la station se désassocie du point d'accès d'origine et se réassocie au nouveau point d'accès après s'être réauthentifiée.

L'écoute du support

Avant toute association avec un point d'accès, la station écoute le support sur tous les canaux radio inoccupés selon la réglementation en vigueur afin de découvrir les points d'accès disponibles.

Cette écoute peut se faire de deux manières différentes, active ou passive :

- **Écoute passive.** La station écoute sur tous les canaux de transmission et attend de recevoir une trame balise du point d'accès.
- **Écoute active.** Sur chaque canal de transmission, la station envoie une trame de requête (Probe Request Frame) et attend une réponse. Dès qu'un ou plusieurs points d'accès lui répond, elle enregistre les caractéristiques de ce dernier.

Une fois l'écoute terminée, la station trie les informations récupérées sur les points d'accès et choisit le plus approprié, essentiellement en fonction de la qualité du lien (rapport signal sur bruit).

L'authentification

Une fois le point d'accès choisi, la station doit s'authentifier auprès de lui.

Les deux mécanismes d'authentification suivants peuvent être utilisés pour cela :

- **Open System Authentication.** C'est le mode par défaut. Il ne fournit toutefois pas de réelle authentification car toutes les stations qui l'utilisent sont automatiquement authentifiées.
- **Shared Key Authentication.** Ce mécanisme d'authentification véritable n'est utilisé que si le protocole de sécurité WEP est implémenté sur le point d'accès et la station. Il s'appuie sur une clé secrète partagée, connue à la fois de la station et du point d'accès. Si la clé utilisée par la station est différente de celle du point d'accès, l'authentification échoue.

L'association

Dès qu'une station est authentifiée, elle peut s'associer avec le point d'accès. Elle envoie pour cela une trame de requête d'association, ou Association Request Frame, et attend que le point d'accès lui réponde pour s'associer.

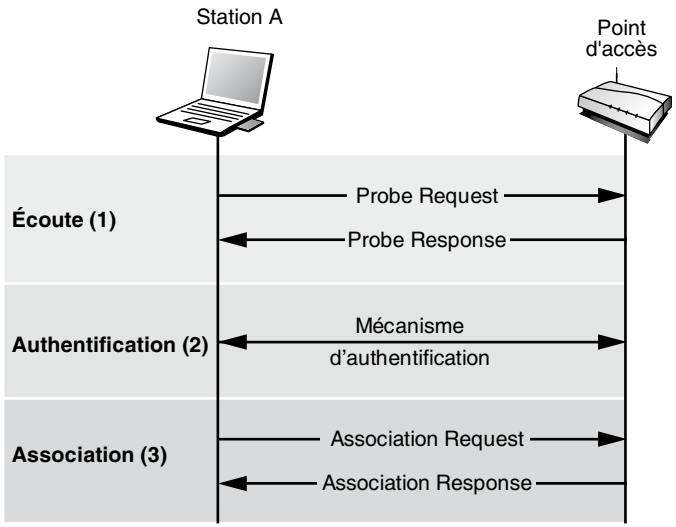
L'association se fait par le biais d'un identifiant, le SSID (Service Set ID). Cet identifiant est défini à la fois au niveau du point d'accès et des stations lorsqu'elles sont en mode infrastructure ou seulement au niveau des stations lorsqu'elles sont en mode ad-hoc. Le SSID définit en réalité le réseau lui-même, puisque c'est le nom du réseau. Il est périodiquement envoyé en clair par le point d'accès dans des trames balises dans toute la zone de couverture du réseau, ce qui permet aux stations en phase d'écoute de le récupérer.

Malheureusement, cette méthode présente une faille de sécurité, qui autorise n'importe qui à accéder au réseau. Une option permet cependant, au niveau du point d'accès, d'interdire la transmission du SSID dans les trames balises. Si la station n'est pas configurée correctement, avec le même SSID que le point d'accès, elle ne peut pas s'associer.

La figure P.7 illustre les étapes nécessaires que doit suivre une station pour s'associer à un point d'accès.

Figure P.7

Mécanisme d'association d'une station avec un point d'accès



Une fois la station associée avec le point d'accès, elle se règle sur le canal radio de ce dernier et peut commencer à transmettre et recevoir des données.

Périodiquement, la station surveille tous les canaux du réseau afin d'évaluer si un autre point d'accès ne possède pas de meilleures caractéristiques.

La réassociation

Le mécanisme de réassociation est similaire à celui décrit précédemment. Les réassociations s'effectuent lorsqu'une station se déplace physiquement par rapport au point d'accès d'origine, engendrant une diminution de la puissance du signal et entraînant une déconnexion.

Dans certains cas, les réassociations sont dues à des changements de caractéristiques de l'environnement radio ou à un trafic réseau trop élevé sur le point d'accès d'origine. Dans ce dernier cas, le standard fournit une fonction d'équilibrage de charge, ou load-balancing, qui répartit la charge de manière efficace au sein du BSS ou de l'ESS et évite les réassociations.

Les handovers

L'architecture d'un réseau sans fil peut comporter différentes cellules susceptibles de se recouvrir ou d'être disjointes. Dans un tel réseau, les utilisateurs sont généralement mobiles et doivent avoir la possibilité de se déplacer de cellule en cellule. Le déplacement intercellulaire, ou handover, ou encore handoff, est le mécanisme qui permet à tout utilisateur de se déplacer d'une cellule à une autre sans que la communication soit interrompue.

Cette technique est largement utilisée dans la téléphonie mobile. Lorsqu'on se déplace à pied, en voiture ou en train, la communication mobile n'est presque jamais coupée quand on passe d'une cellule à une autre.

La figure P.8 illustre un handover dans un réseau Wi-Fi. La station mobile connectée au point d'accès 1 doit, à un moment donné, s'associer au point d'accès 2. En d'autres termes, la communication qui passait par le point d'accès 1 doit, à un instant donné, passer par le nouveau point d'accès. La gestion du handover recouvre les mécanismes à mettre en œuvre pour réaliser la continuité de la communication, de sorte que le récepteur ne s'aperçoive pas que l'émetteur a changé de cellule.

Le standard d'origine ne supporte pas les handovers. Si une station se déplace dans un environnement couvert par de multiples points d'accès, et donc de multiples cellules, elle essaye de se connecter au point d'accès qui possède le meilleur signal. Cela assure à la station une bonne qualité du lien radio mais ne permet pas d'offrir la continuité de la communication dans un environnement cellulaire. Chaque fois qu'une station trouve un meilleur point d'accès, elle s'associe avec lui, toute communication en cours étant interrompue et non reprise par le nouveau point d'accès.

Le fait qu'il n'y ait pas de handover dans 802.11 est un facteur négatif pour le déploiement de ces réseaux et la vente des matériels correspondants. Certains constructeurs l'ont compris et n'ont pas attendu une éventuelle standardisation pour développer des protocoles de handover propriétaires. Pour en bénéficier, il faut que le réseau soit constitué d'équipements du même constructeur, ce qui présente d'autres contraintes. En l'absence de standard, il ne peut y avoir interopérabilité entre équipements de différents constructeurs.

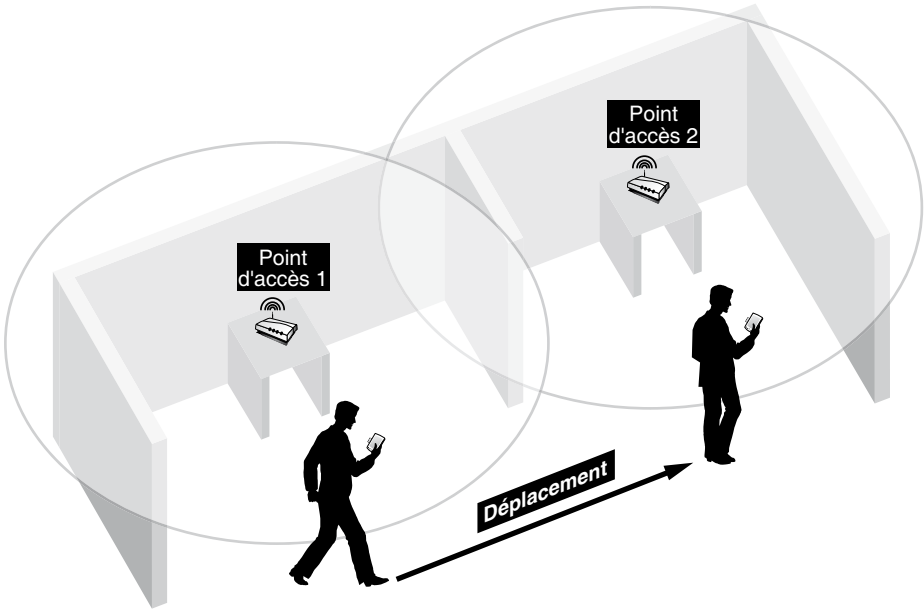


Figure P.8
Handover dans un réseau sans fil

IAPP (Inter-Access Point Protocol)

Comme expliqué précédemment, le groupe de travail 802.11f vise à la standardisation d'un protocole permettant de gérer les handovers et d'apporter ainsi l'interopérabilité entre des points d'accès de différents constructeurs. Le protocole retenu est l'IAPP (Inter-Access Point Protocol), développé à l'origine par Lucent.

IAPP fait communiquer les différents points d'accès d'un même réseau de façon à permettre à un utilisateur mobile de passer d'une cellule à une autre sans perte de connexion. Le seul lien entre les points d'accès du réseau étant le système de distribution (DS), c'est à ce niveau qu'est utilisé IAPP.

IAPP est un protocole de niveau transport (couche 4 du modèle OSI) qui se place au-dessus d'UDP (User Datagram Protocol). L'avantage d'utiliser UDP est que ce protocole de transport est sans connexion, à la différence de TCP (Transmission Control Protocol), les données étant envoyées directement.

Optionnel, IAPP ne fonctionne qu'avec les points d'accès qui l'implémentent. Il peut être désactivé à tout moment. Par ailleurs, aucun mécanisme de sécurité n'étant implémenté dans IAPP, cette tâche incombe au gestionnaire du système de distribution.

Le fonctionnement d'IAPP est illustré à la figure P.9.

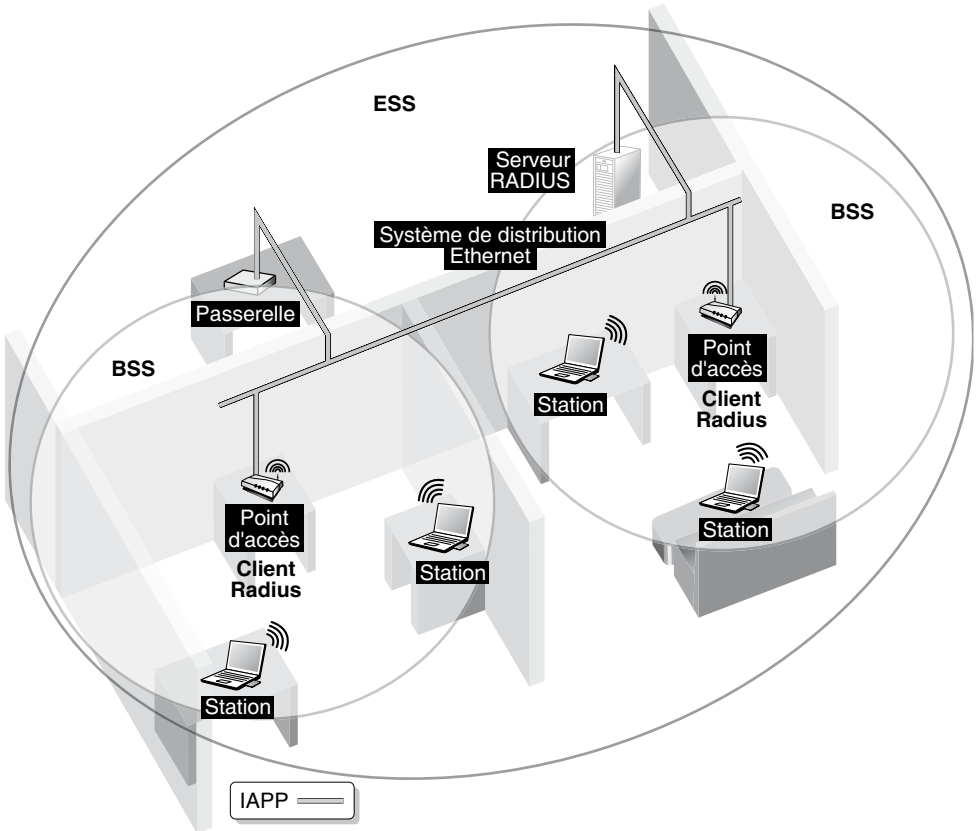


Figure P.9

Fonctionnement d'IAPP (Inter-Access Point Protocol)

Une caractéristique d'IAPP est qu'il définit l'utilisation du protocole client-serveur d'authentification RADIUS (Remote Authentication Dial-In User Server) afin d'offrir des handovers sécurisés. L'utilisation de ce protocole demande la présence d'un serveur centralisé ayant une vue globale du réseau. Le serveur RADIUS connaît la correspondance d'adresse entre l'adresse MAC des points d'accès et leur adresse IP. Par ailleurs, ce protocole permet de distribuer des clés de chiffrement entre points d'accès.

RADIUS est un protocole client-serveur, dans lequel le serveur est une entité se trouvant sur le système de distribution. Les clients ne sont pas les stations, mais les différents points d'accès du réseau. L'utilisation de RADIUS est optionnelle mais fortement conseillée, ne serait-ce que pour des raisons de sécurité.

IAPP ne résout pas la gestion de l'adressage des stations dans le réseau. L'utilisation de protocoles de niveau système de distribution, tels que DHCP (Dynamic Host Configuration Protocol) ou IP Mobile, est donc fortement recommandée.

Le protocole IAPP définit deux types de mécanismes, la configuration des points d'accès et les handovers proprement dits.

Configuration des points d'accès

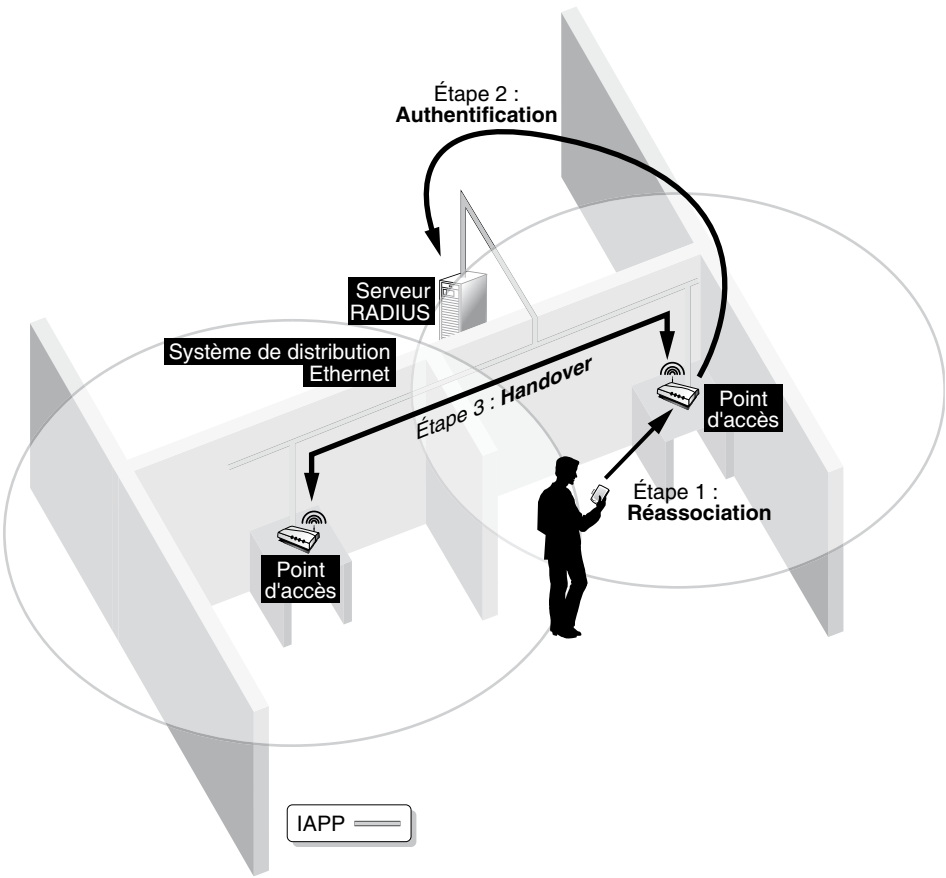
Le mécanisme de configuration permet d'instaurer un certain dialogue avec les points d'accès du réseau. Lorsqu'un nouveau point d'accès est installé, il informe les autres de sa présence et leur envoie des informations concernant sa configuration. De la sorte, tous les points d'accès se connaissent et peuvent s'échanger des attributs de configuration, voire les négocier.

Le mécanisme de handover

Un handover se produit chaque fois qu'une station passe d'une cellule à une autre. Pour cela, elle doit se réassocier avec le point d'accès contrôlant cette cellule. C'est la réassociation qui initie le mécanisme de handover.

La figure P.10 illustre le mécanisme de handover d'IAPP.

Figure P.10
Le mécanisme de handover d'IAPP



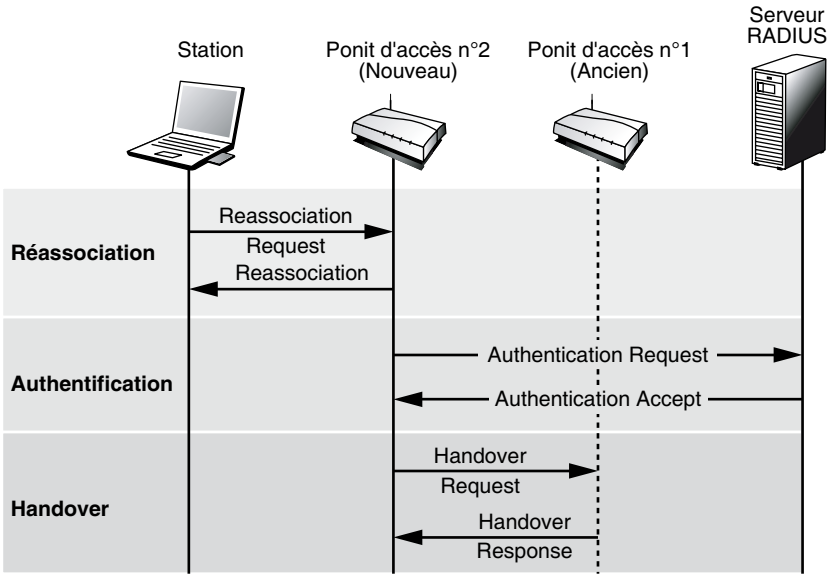
Dans les échanges d'informations entre le nouveau point d'accès et la station, le nouveau point d'accès connaît l'adresse de l'ancien. Il peut dès lors commencer à dialoguer avec celui-ci.

Avant tout handover, une authentification est nécessaire. L'utilisation de RADIUS entraîne une nouvelle phase d'authentification, qui se produit après chaque réassociation avec un nouveau point d'accès. La station envoie des informations au serveur par l'intermédiaire du point d'accès. Le serveur les vérifie, et, si les données sont correctes, authentifie la station auprès de ce point d'accès. Une fois authentifié, le nouveau point d'accès entre dans la phase de handover.

Pendant cette phase, le nouveau point d'accès envoie une requête à l'ancien par l'intermédiaire du système de distribution. L'ancien point d'accès lui répond et lui transmet toutes les informations nécessaires concernant la station. Ce processus est illustré à la figure P.11.

Figure P.11

Phase de négociation du handover



Une fois cette phase terminée, la station possède les paramètres réseau corrects et peut de la sorte soit continuer une communication, soit en commencer une nouvelle.

Économies d'énergie

Les réseaux sans fil peuvent être composés de stations fixes ou mobiles. Les stations fixes n'ont aucun problème d'économie d'énergie puisqu'elles sont directement reliées au réseau électrique. Les stations mobiles sont alimentées par des batteries, qui n'ont généralement qu'une faible autonomie (quelques heures selon l'utilisation).

Pour utiliser au mieux ces stations mobiles, le standard définit deux modes d'énergie, Continuous Aware Mode et Power Save Polling Mode :

- **Continuous Aware Mode.** C'est le mode de fonctionnement par défaut. L'interface Wi-Fi est tout le temps allumée et écoute constamment le support. Il ne s'agit donc pas d'un mode d'économie d'énergie.
- **Power Save Polling Mode.** C'est le mode d'économie d'énergie. Dans ce mode, le point d'accès tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie et stocke les données qui leur sont adressées dans un élément appelé TIM (Traffic Information Map).

Comme expliqué à la section précédente, les stations d'un BSS sont toutes synchronisées. Cette synchronisation, qui s'effectue par le biais des trames balises, permet d'établir le mécanisme d'économie d'énergie.

Les stations en veille s'activent à des périodes de temps régulières pour recevoir une trame balise contenant le TIM envoyé en broadcast par le point d'accès. Entre les trames balises, les stations retournent en mode veille. Du fait de la synchronisation, une trame balise est envoyée toutes les 32 µs. Toutes les stations partagent le même intervalle de temps pour recevoir les TIM et s'activent de la sorte au même moment pour les recevoir.

Les TIM indiquent aux stations si elles ont ou non des données stockées dans le point d'accès. Lorsqu'une station s'active pour recevoir un TIM et qu'elle s'aperçoit que le point d'accès contient des données qui lui sont destinées, elle lui envoie une trame de requête (PS-Poll) pour mettre en place le transfert des données. Une fois le transfert terminé, la station retourne en mode veille jusqu'à réception de la prochaine trame balise contenant un nouveau TIM.

Le mécanisme d'économie d'énergie ne peut être utilisé qu'au niveau des stations, lesquelles choisissent de l'utiliser ou non. Le fait d'utiliser ce mécanisme peut faire chuter les performances globales de débit du réseau de 20 à 30 %.

Annexe Q

23. Réseaux hertziens avec relais

Cette annexe s'intéresse à l'environnement satellite dans les réseaux hertziens avec relais. Elle commence par introduire les fréquences radio qui sont utilisées dans ces réseaux puis détaille les politiques d'accès au canal satellite et donne quelques exemples de constellations.

Les fréquences radio

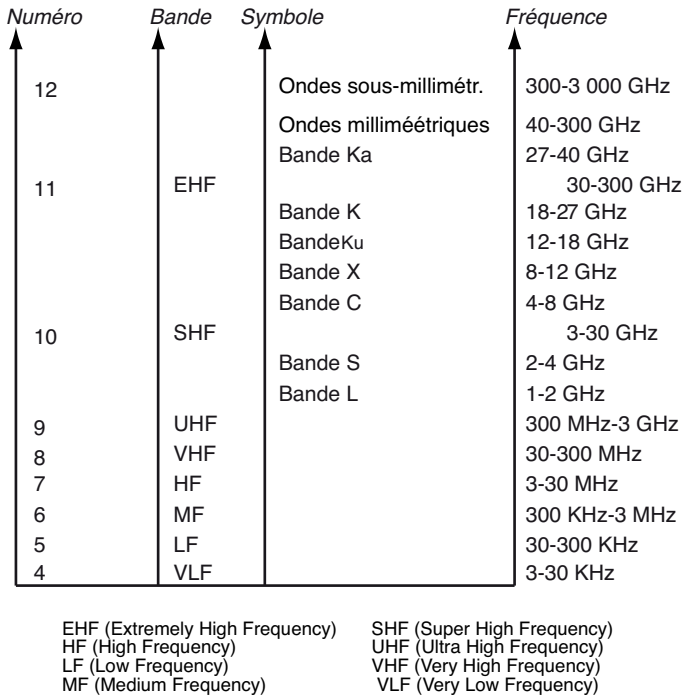
Les fréquences radio sont divisées en bandes, déterminées par un groupe de travail IEEE, le SRD (Standard Radar Definitions). Les numéros de bandes et les noms sont donnés par l'organisme international de régulation des bandes de fréquences. La figure Q.1 illustre les bandes de fréquences allouées aux systèmes satellitaires.

La bande C est la première à avoir été utilisée pour les applications commerciales. La bande Ku accepte des antennes beaucoup plus petites, dites VSAT (Very Small Aperture Terminal), de 45 cm de diamètre seulement. La bande Ka autorise des antennes encore plus petites, et c'est pourquoi la plupart des constellations de satellites l'utilisent. De ce fait, les terminaux peuvent devenir mobiles, grâce à une antenne presque aussi petite que celle des terminaux de type GSM. On qualifie ces terminaux de USAT (Ultra Small Aperture Terminal). En revanche, l'utilisation de la bande S permet d'entrer dans le cadre de l'UMTS et des réseaux de mobiles terrestres.

Les fréquences classiquement utilisées pour la transmission par satellite concernent les bandes 4-6 GHz, 11-14 GHz et 20-30 GHz. Les bandes passantes vont jusqu'à 500 MHz et parfois 3 500 MHz. Elles permettent des débits très élevés, jusqu'à plusieurs dizaines de mégabits par seconde. Un satellite comprend des répéteurs, de 5 à 50 actuellement.

Chaque répéteur est accordé sur une fréquence différente. Par exemple, pour la bande des 4-6 GHz, il reçoit des signaux modulés dans la bande des 6 GHz, les amplifie et les transpose dans la bande des 4 GHz. S'il existe n stations terrestres à raccorder par le canal satellite, le nombre de liaisons bipoint est égal à $n \times (n - 1)$. Ce nombre est toujours supérieur à celui des répéteurs. Il faut donc, là aussi, avoir des politiques d'allocation des bandes de fréquences et des répéteurs.

Figure Q.1
Fréquences radio des systèmes satellite



Les très grands projets qui ont été finalisés juste avant les années 2000 ne visent que la téléphonie, par suite d'un manque flagrant de bande passante des systèmes satellitaires non militaires. Cette limitation est cependant partiellement compensée par le grand nombre de satellites défilant à basse altitude, qui permet une bonne réutilisation des fréquences. Plusieurs grands projets techniquement aboutis se sont effondrés ces dernières années pour des raisons financières, et l'environnement satellite doit se trouver des niches de marché correspondant aux zones non couvertes par les réseaux cellulaires terrestres ou la diffusion massive.

Les techniques d'accès au satellite

Les canaux satellite, comme tous les systèmes à canaux partagés, demandent une technique d'accès. La différence essentielle avec les interfaces radio des réseaux de mobiles

provient du long délai de propagation entre l'émetteur et le récepteur. Dans les réseaux cellulaires ou les réseaux locaux, le délai de propagation très court permet de gérer simplement les instants de transmission. Dans le cas de satellites géostationnaires, les stations terrestres ne découvrent qu'il y a eu chevauchement des signaux que 0,27 s après leur émission — elles peuvent s'écouter grâce à la propriété de diffusion —, ce qui représente une perte importante sur un canal d'une capacité de plusieurs mégabits par seconde.

Les techniques d'accès pour les réseaux satellite sont généralement classées en quatre catégories :

- les méthodes de réservation fixe, ou FAMA (Fixed-Assignment Multiple Access) ;
- les méthodes d'accès aléatoires, ou RA (Random Access) ;
- les méthodes de réservation par paquet, ou PR (Packet Reservation) ;
- les méthodes de réservation dynamique, ou DAMA (Demand Assignment Multiple Access).

Les protocoles de réservation fixe réalisent des accès non dynamiques aux ressources et ne dépendent donc pas de l'activité des stations. Les procédures FDMA, TDMA et CDMA forment les principales techniques de cette catégorie. Ces solutions offrent une qualité de service garantie puisque les ressources sont affectées une fois pour toutes. En revanche, l'utilisation des ressources est mauvaise, comme dans le cas d'un circuit affecté au transport de paquets. Lorsque le flux est variable, les ressources doivent permettre le passage du débit crête.

Les techniques d'accès aléatoires donnent aux utilisateurs la possibilité de transmettre leurs données dans un ordre sans corrélation. En revanche, ces techniques ne se prêtent à aucune qualité de service. Leur point fort réside dans une implémentation simple et un coût de mise en œuvre assez bas.

Les méthodes de réservation par paquet évitent les collisions par l'utilisation d'un schéma de réservation de niveau paquet. Comme les utilisateurs sont distribués dans l'espace, il doit exister un sous-canal de signalisation à même de mettre les utilisateurs en communication pour gérer la réservation. Les méthodes de réservation dynamique ont pour fonction d'optimiser l'utilisation du canal. Ces techniques essaient de multiplexer un maximum d'utilisateurs sur le même canal en demandant aux utilisateurs d'effectuer une réservation pour un temps relativement court. Une fois la réservation acceptée, l'utilisateur vide ses mémoires tampons jusqu'à la fin de la réservation puis relâche le canal.

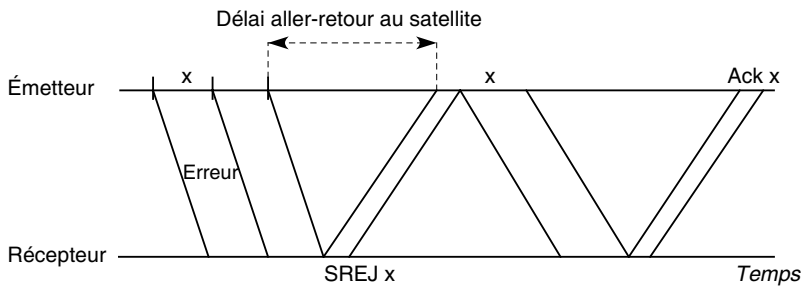
Les communications par l'intermédiaire d'un satellite montrent des propriétés légèrement différentes de celles d'un réseau terrestre. Les erreurs, en particulier, se produisent de façon fortement groupée, en raison de phénomènes physiques survenant sur les antennes d'émission ou de réception. Au contraire des réseaux locaux, aucun protocole de niveau liaison n'est normalisé pour les réseaux satellite. Plusieurs procédures ont été proposées, mais aucune ne fait l'unanimité. Le délai d'accès au satellite constitue le problème principal, puisque, pour recevoir un acquittement, un temps égal à deux fois l'aller-retour est nécessaire. À ce délai aller-retour, il faut encore ajouter le passage dans les éléments extrémité, qui est loin d'être négligeable. Ce délai dépend bien sûr de la position de l'orbite sur laquelle se trouve le satellite. Lorsque les capacités des liaisons sont importantes,

les techniques utilisant des reprises explicites à partir de la trame en erreur ne sont pas efficaces, la quantité d'information à retransmettre devenant très grande. Les techniques sélectives posent également des questions de dimensionnement des mémoires permettant d'attendre l'information qui n'est pas parvenue au récepteur.

Contrairement aux réseaux locaux, les réseaux satellite n'ont pas donné lieu à une normalisation spécifique. Plusieurs protocoles ont été proposés, mais aucun ne s'est vraiment imposé.

Un réseau utilisant un satellite géostationnaire ou un satellite situé sur une orbite moyenne se caractérise par un très long temps de propagation, comparativement au temps d'émission d'une trame. Pour cette raison, il existe des extensions aux procédures classiques, qui permettent l'émission d'un grand nombre de trames sans interruption. Si le débit est très élevé et qu'une procédure HDLC (High-level Data Link Control) avec une méthode SREJ (Selective REJect) soit adoptée, l'anticipation doit être très importante ou bien la longueur des trames très grande. Par exemple, si le débit de la liaison satellite est de 10 Mbit/s, sachant qu'il faut au moins prévoir d'émettre sans interruption pendant un temps égal à deux allers-retours (*voir figure Q.2*), la valeur minimale de la trame est de 20 Ko. Cette quantité est très importante, et la qualité de la ligne doit être excellente pour qu'un tel bloc de données (160 000 bits) arrive avec un taux d'erreur bit inférieur à 10^{-10}.

Figure Q.2
Reprise sur une liaison satellite



Les politiques de réservation fixe

Les politiques de réservation fixe, ou FAMA (Fixed-Assignment Multiple Access), utilisées dans les systèmes satellite sont les mêmes que celles utilisées dans les réseaux de mobiles : FDMA, TDMA et CDMA. Pour le moment la technique CDMA n'est pas employée dans les réseaux satellite, mais elle devrait venir en complément des techniques terrestres de troisième génération, telles que l'UMTS, le cdma2000, etc.

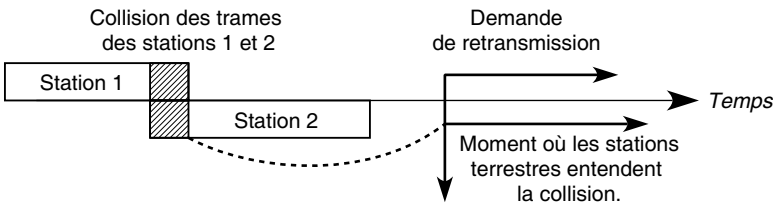
Les politiques d'accès aléatoire

Les techniques d'accès aléatoire ont été introduites dans les réseaux locaux. Dans un réseau satellite, où le délai de propagation est très important par rapport aux réseaux locaux, les stations terrestres qui émettent des signaux ne sont informées d'une éventuelle collision de leur paquet que 270 ms après l'émission. L'accès aléatoire consiste donc, pour

les stations terrestres, à émettre dès qu'elles ont un paquet de données en leur possession. S'il y a collision, les stations terrestres concernées s'en aperçoivent puisqu'elles écoutent les signaux émis sur le canal. Les paquets perdus sont retransmis ultérieurement, après un temps aléatoire, de façon à réduire au maximum le risque de nouvelles collisions.

La figure Q.3 illustre la collision entre deux paquets sur un canal satellite.

Figure Q.3
Collision entre deux paquets sur un canal satellite



Les deux techniques d'accès aléatoire

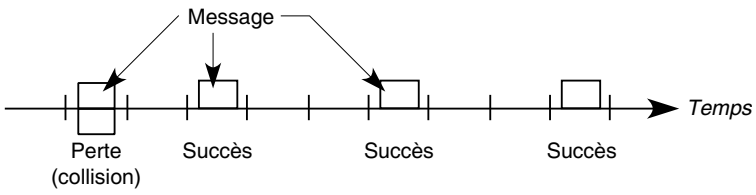
Les deux grandes catégories de politiques d'accès aléatoires sont l'aloha et l'aloha discrétisé.

La technique aloha tire son nom d'un mot hawaïen, car elle a pour origine des expériences réalisées à l'Université de Hawaï pour relier les centres informatiques dispersés sur de nombreuses îles. Dans le système aloha, la propriété de diffusion et les codes détecteurs d'erreur permettent aux stations terrestres de savoir si leurs émissions de paquets se sont effectuées correctement. Si ce n'est pas le cas, les paquets sont retransmis après un délai aléatoire. Ce délai est un paramètre essentiel, qui détermine les performances du système.

Des méthodes d'évaluation de performance montrent que, si le nombre de stations terrestres est très grand et tend mathématiquement vers l'infini et qu'aucune politique précise ne soit suivie pour la retransmission des messages perdus dans les collisions, l'utilisation du canal tend vers 0, et le débit devient nul. Les deux grandes politiques de contrôle consistent à allonger les temps avant retransmission en fonction du nombre de paquets en attente de réémission ou bien à stopper les nouvelles émissions dès que le nombre de paquets en attente de retransmission dépasse une valeur fixée à l'avance. Malgré tout, le débit maximal correspond à une utilisation du canal satellite égale à $\frac{1}{2}\,e = 0{,}184$.

Le concept d'aloha discrétisé repose sur la division du temps en tranches de longueur égale correspondant au temps de transmission d'un paquet, qui, de ce fait, doit avoir une longueur constante. Les collisions se produisent dans ce cas sur l'ensemble de la tranche, et non plus, comme avant, sur des parties de paquets seulement (*voir figure Q.4*). Les émissions doivent être synchronisées en début de tranche de temps.

Figure Q.4
Aloha en tranches



Calculons le taux d'utilisation maximal du canal satellite dans ce dernier cas, en supposant que les demandes d'émission de messages arrivent suivant un processus de Poisson, et que le nombre de stations terrestres est grand. Si S est le débit du canal et G le trafic total en comptabilisant aussi bien les réussites que les échecs, la proportion de réussite S/G est égale à la probabilité de réussite sur une tranche de temps, c'est-à-dire e^{-G}, ce qui correspond à la probabilité qu'un seul paquet à la fois soit émis sur une tranche. Nous obtenons :

$$S = G\, e^{-G}$$

où le débit S est optimisé pour G = 1. Cela permet d'obtenir le taux d'utilisation maximal : 1/e = 0,368. On voit que, en découpant le temps en tranches, on peut doubler le débit du canal. Cependant, ce débit reste faible, et des techniques de réservation peuvent parfois être utilisées pour améliorer les performances du système.

Les protocoles avec réservation par paquet

Les politiques de réservation par paquet sont très nombreuses. Les sections qui suivent en décrivent trois avec plusieurs variantes. Le dénominateur commun de ces méthodes réside dans la faculté de réserver à l'avance des tranches de temps pour les stations qui ont des paquets à émettre.

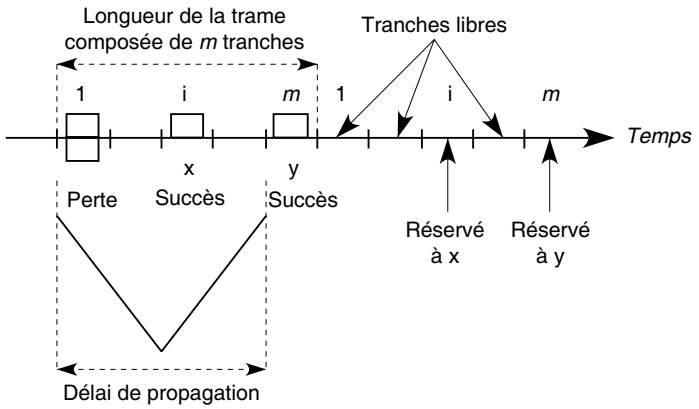
R-aloha

Les protocoles de réservation par paquets utilisent généralement une partition du temps en tranches fixes. Ces tranches sont regroupées pour former des trames. Une station ne peut émettre dans une tranche que si elle a effectué une réservation. La réservation peut être explicite ou implicite. Par exemple, dans la technique R-aloha, une transmission réussie signifie automatiquement une réservation dans la même tranche de la trame suivante. En effet, en informatique, les messages sont très souvent subdivisés en plusieurs paquets, ce qui signifie qu'une station terrestre qui vient d'émettre un paquet a toutes les chances d'en émettre un autre immédiatement derrière, d'où l'idée de lui réserver des tranches de temps.

La technique aloha avec réservation utilise le principe précédent : les tranches de temps sont réunies en trames d'une longueur supérieure au temps aller-retour, de telle sorte que toutes les stations au début d'une tranche sont au courant de ce qui s'est passé dans la même tranche de la trame précédente. Si une tranche est libre ou reflète une superposition de plusieurs paquets, la tranche correspondante dans la trame suivante est libre d'accès.

Au contraire, si une station *x* réussit une transmission, la tranche correspondante dans la trame suivante lui est réservée, comme l'illustre la figure Q.5. Dès qu'une tranche réservée est inoccupée, elle redevient libre d'accès. Le débit permis par cette technique dépend du nombre de paquets par message. Des débits correspondant à des taux d'utilisation du canal de l'ordre de 1 peuvent être obtenus pour de très longs messages.

Figure Q.5
Aloha avec réservation



PODA (Priority-Oriented Demand Assignment)

La procédure PODA utilise également une réservation par paquets. Dans ce cas, la trame est divisée en une première partie, qui permet de réaliser des réservations, et une seconde pour le transport des paquets des émetteurs ayant réussi leur réservation. Toutes les stations écoutent la partie réservation et utilisent le même algorithme pour classer les réservations. La frontière entre les deux parties dépend du nombre de stations et de la charge globale.

Dans le cas le plus classique, le temps est découpé en tranches, supposées de longueur égale, correspondant à la durée de transmission d'un paquet. Les tranches sont regroupées en trames, dont la durée est supérieure au temps de propagation aller-retour. Chaque trame débute par une première partie contenant des minitranches de réservation, suivie d'une deuxième partie contenant les tranches d'émission effective des paquets (*voir figure Q.6*).

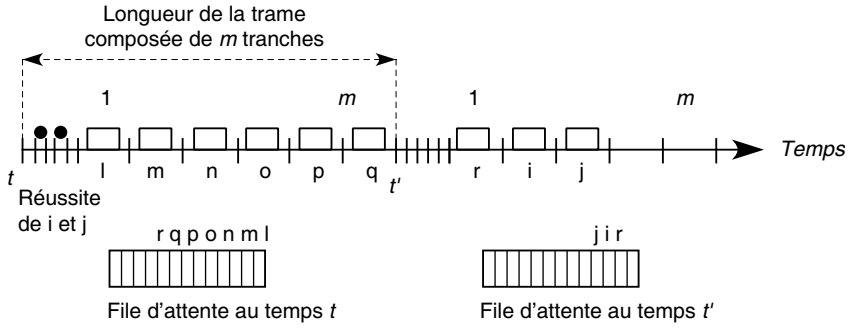


Figure Q.6
Fonctionnement de PODA

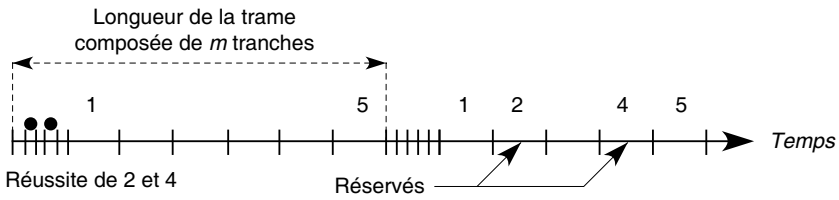
La méthode aloha permet d'accéder aux minitranches de réservation. Les réussites déterminent une file d'attente fictive dans l'ordre premier arrivé, premier servi. Cette file se vide en servant les clients un par un dans les tranches de temps.

La principale lacune de cette méthode provient du manque d'information qu'elle génère, qui ne permet pas de connaître à l'avance le nombre optimal de tranches ni de minitranches dans une trame. Un manque de réussite sur les minitranches peut engendrer un relatif effondrement du débit du système. En revanche, une trop grande réussite peut allonger la file jusqu'à provoquer des débordements.

Réservation ordonnée

Dans la réservation ordonnée, la structure de la trame est la même que dans le cas précédent, mais il y a autant de minitranches dans l'en-tête que de tranches dans la trame et que de stations terrestres. Chaque minitranche est dédiée à une station terrestre. Cela permet à une station terrestre d'avertir les autres émetteurs qu'elle va occuper la tranche qui lui appartient. Dans le cas contraire, la tranche correspondante devient libre, et tous les utilisateurs peuvent y accéder dans un mode d'accès aléatoire. La technique de réservation ordonnée est illustrée à la figure Q.7.

Figure Q.7
Réservation ordonnée



Réservation à tour de rôle

Dans la politique de réservation dite à tour de rôle, le temps est toujours découpé en tranches. Une trame est formée de *m* tranches, *m* étant supérieur à *n,* qui est le nombre de stations terrestres. Les *n* premières tranches sont réservées aux stations correspondantes. Elles permettent de transporter la valeur d'un compteur indiquant la longueur de la file d'attente de ces stations. Plus précisément, cette valeur indique le nombre de paquets en attente de transmission.

Une file d'attente commune est construite à partir des valeurs transportées dans les *n* premières minitranches indiquant le nombre de paquets en attente pour chaque station. Les $m - n$ dernières tranches de la trame sont occupées à tour de rôle par les stations d'émission en attente, suivant la file d'attente commune, comme illustré à la figure Q.8.

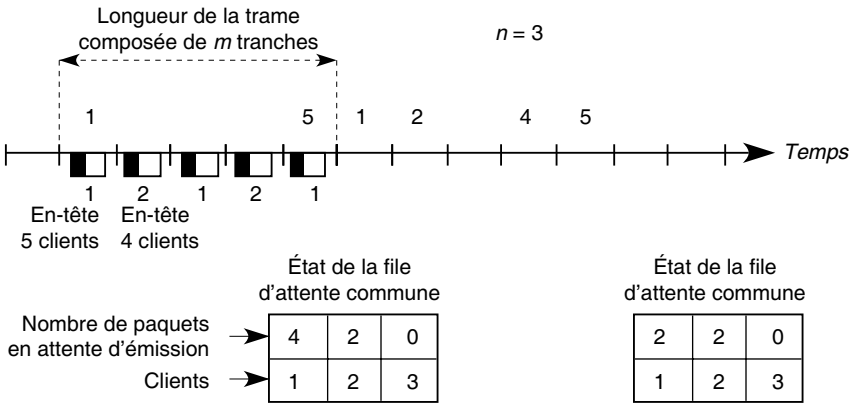


Figure Q.8

Réservation à tour de rôle

Les protocoles de réservation dynamique et les méthodes hybrides

Les protocoles de réservation dynamique allouent les ressources en fonction de la demande des utilisateurs. Des priorités peuvent être attribuées aux différents utilisateurs. Le séquenceur, qui peut se trouver dans le satellite, organise les réservations suivant les niveaux de priorité. Les garanties de service dépendent de l'allocation des ressources. Par exemple, CF-DAMA (Combined Free DAMA) garantit une qualité de service pour les priorités hautes et une distribution équitable des ressources restantes pour les basses priorités.

Techniques hybrides

Un grand nombre de techniques hybrides ont été proposées, parmi lesquelles les trois suivantes :

- L'association d'un protocole FAMA, qui assure une qualité de service pour quelques classes de clients à haute priorité, et d'une politique DAMA, pour partager le reste de la bande passante. Un exemple d'une telle solution est offert par la politique FBA/DAMA, qui fournit une garantie minimale de bande passante sur une partie, le reste de la bande passante étant répartie par une technique DAMA.
- Le schéma RRR (Round-Robin Reservation), qui requiert un nombre de stations inférieur au nombre de tranches nécessaires à la discipline TDMA. Chaque station possède une tranche dédiée. Les tranches restantes sont accédées par les stations suivantes selon un accès aléatoire de type aloha.
- La technique IFFO (Interleaved Frame Flush-Out), dans laquelle la trame est divisée en trois parties, une pour le contrôle, une pour les tranches réservées et une en accès

aléatoire. La partie contrôle, qui est subdivisée en minitranches, une pour chaque station, permet d'effectuer des réservations. Tous les émetteurs qui deviennent actifs après le passage de la partie réservation de la trame peuvent accéder aux tranches en libre-service. Si une collision se produit, les stations concernées utilisent leur tranche réservée. Les tranches appartenant à la partie réservée mais qui n'ont pas fait l'objet d'une réservation peuvent être utilisées pour l'accès aléatoire.

Dans les techniques de réservation par paquet, on peut accéder aux minitranches soit nominalement, soit par accès aléatoire. On essaie également d'utiliser au maximum les tranches qui n'ont pas été réservées, et ce par une file d'attente commune, avec une discipline de service déterminée à l'avance ou par un accès aléatoire.

Le temps de réponse en fonction du débit lorsque 50 stations terrestres émettent des messages relativement courts peut fournir un critère de performance des techniques d'accès. Les temps de réponse les meilleurs sont obtenus par l'aloha pour de faibles débits, par la méthode de réservation par paquet pour des débits moyens et par la méthode TDMA pour les taux d'utilisation du canal de l'ordre de 1.

Les satellites de deuxième génération peuvent embarquer du matériel de commutation et de mémorisation. De ce fait, les signaux sont démodulés à bord, et les erreurs en ligne peuvent être détectées, donnant naissance à une nouvelle génération de protocoles.

De nouvelles possibilités d'accès au canal sont également permises pour ces satellites de deuxième génération. L'intelligence introduite dans le satellite permet de ne retransmettre vers la Terre que les paquets corrects. Par exemple, si une politique d'accès aléatoire est utilisée dans le sens montant, les paquets ayant réussi leur transmission sans collision sont placés dans une file d'attente et retransmis vers la Terre dans l'ordre premier arrivé, premier servi. La largeur de bande dans le sens descendant peut de la sorte être beaucoup plus petite que dans le sens montant.

Les systèmes satellite bande étroite

Les satellites bande étroite correspondent à la première génération. Ils ont été construits essentiellement pour les services de téléphonie et la diffusion de canaux de télévision. Du fait de la baisse des coûts de mise en orbite d'un satellite et de l'augmentation des performances des stations terrestres, de nombreux services nouveaux se sont ouverts sur les satellites bande étroite, surtout dans le domaine de la transmission de données.

Ces services peuvent être monodirectionnels, ou monovoies, une station terrestre émettant vers une ou plusieurs stations simultanément, sans voie de retour. Si une voie de retour est nécessaire, elle peut être terrestre. Ce type de communication correspond à la diffusion d'informations sans acquittement. Il est également possible de prévoir des voies de retour spécifiques par le satellite. Malheureusement, ces voies de retour ne sont utilisées que par les acquittements et les informations de contrôle et de gestion, procurant ainsi une très mauvaise utilisation de la liaison de retour.

La transmission de données dans les systèmes bande étroite s'effectue dans les spectres 12-14 GHz en TDMA, avec un ajout de canaux de télévision.

Les services mobiles correspondent à des stations terrestres pouvant se déplacer, c'est-à-dire munies d'antennes mobiles, mais à des vitesses très faibles comparées à celles des satellites défilants. Le développement de ces services mobiles est relativement lent du fait de la difficulté d'obtenir des antennes mobiles suffisamment puissantes à des coûts acceptables pour l'utilisateur. Le début des services mobiles s'est effectué dans le cadre des liaisons entre bateaux. Ces développements ont mené à la constitution d'Inmarsat (International Marine Satellite Organization), qui est aujourd'hui, et de très loin, l'organisation la plus importante dans les services mobiles par satellite. Elle compte 66 membres et s'occupe depuis 1989 des services de communications mobiles pour l'aéronautique. Cette association dépend des opérateurs, comme expliqué précédemment, qui revendent les services d'Inmarsat aux utilisateurs.

Les satellites bande étroite

Les fréquences suivantes, concernant l'utilisation de satellites bande étroite, ont été définies en 1987 par la WARC (World Administrative Radio Conference) :

- 1,530-1,544 GHz pour les communications du satellite vers les mobiles terrestres et les bateaux ;
- 1,544-1,545 GHz pour les communications du satellite vers les mobiles en détresse ;
- 1,545-1,599 GHz pour les communications du satellite vers les mobiles aéronautiques ;
- 1,626-1,645 GHz pour les communications des mobiles terrestres et des bateaux vers le satellite ;
- 1,645-1,646 GHz pour les communications des mobiles en détresse vers le satellite ;
- 1,646-1,660 GHz pour les communications des mobiles aéronautiques vers le satellite.

Les antennes dépendent du type de service recherché. Trois grandes possibilités ont été développées :

- antennes Inmarsat A, d'un mètre de diamètre ;
- antennes Inmarsat C, d'un diamètre largement inférieur à 1 m, mais fixes, c'est-à-dire non repliables, pour des communications de données pouvant atteindre 600 Kbit/s ;
- antennes Inmarsat M, d'un diamètre inférieur à 1 m, permettant la téléphonie avec une compression à 6,4 Kbit/s et des données jusqu'à 2,4 Kbit/s.

Les communications d'affaires entre les différents points d'une même société ont commencé à se développer au début des années 1980. Il fallait pour cela des antennes de petit diamètre à des coûts acceptables pour les utilisateurs. Le vrai démarrage a eu lieu avec l'utilisation des VSAT (Very Small Aperture Terminal), dont le début des années 1990 a connu l'essor, aussi bien en Europe qu'aux États-Unis.

Intelsat et Eutelsat

Deux organisations internationales se consacrent aux services entre stations fixes : Intelsat et Eutelsat. Intelsat a été lancée en 1964 et regroupe aujourd'hui plus de cent vingt

pays membres. Son objectif est d'organiser, de coordonner et d'offrir une très grande bande passante à ses membres, dans le but de réaliser des communications téléphoniques, des diffusions de canaux de télévision et des services intégrés pour les grandes entreprises. Intelsat a été fondée par les opérateurs de télécommunications et a installé à leur intention tout un réseau de satellites. Pendant de nombreuses années, Intelsat a eu la complète maîtrise de toutes les communications par satellite. Il a commencé à perdre ce monopole dans les années 1980, lorsque les Européens ont lancé Eutelsat pour coordonner les communications par satellite en Europe et que d'autres organisations nationales ou internationales, telles que Panamsat, ont commencé à offrir des services similaires avec des techniques légèrement différentes.

Intelsat a défini plusieurs standards de stations terrestres. Le premier, le standard A, définit une antenne de 15 à 18 m de diamètre, dans la fréquence des 4-6 GHz. Les derniers standards, D, E, F, définissent des antennes entre 3,5 et 10 m de diamètre, dans des fréquences élargies à 4-6 ou aux bandes 11-12/14 GHz.

Bien que constituée en 1977, Eutelsat n'est une organisation à part entière que depuis 1985, du fait de l'opposition d'Intelsat, craignant pour son monopole. Plus d'une trentaine de membres sont aujourd'hui dénombrés. Le rôle d'Eutelsat est semblable à celui d'Intelsat mais centré sur l'Europe. Eutelsat a élargi son champ de compétences en proposant aux petites entreprises des services de diffusion et de communication intégrés. Une société possédant un grand nombre de succursales peut, d'une seule émission, toucher toutes les succursales et en même temps émettre un message particulier à l'une des succursales. Par exemple, les numéros de cartes Visa volées peuvent être envoyés simultanément à toutes les billetteries et, en même temps, un message particulier peut être adressé à telle ou telle billetterie.

Le champ des VSAT, présentés ultérieurement dans ce chapitre, fait en outre partie des prérogatives d'Eutelsat.

Annexe R

25. VLAN et VPN

Cette annexe introduit les VPN IP en commençant par les VPN personnels et les VPN de groupe avec identification du trafic. Elle examine ensuite les VPN des réseaux en mode avec connexion, c'est-à-dire les réseaux dans lesquels un paquet ne peut être envoyé qu'après une négociation avec le terminal distant. Les VPN des réseaux ATM et MPLS sont étudiés plus en détail à la section suivante.

Les VPN IP

Les VPN peuvent être implémentés selon six modèles différents. La figure R.1 illustre ces différents modèles. Parmi les nœuds, on trouve les équipements terminaux (End ou End Systems), les CE (Customer Edge) et les PE (Provider Edge). CE et PE sont généralement des routeurs qui se trouvent chez le client ou l'opérateur.

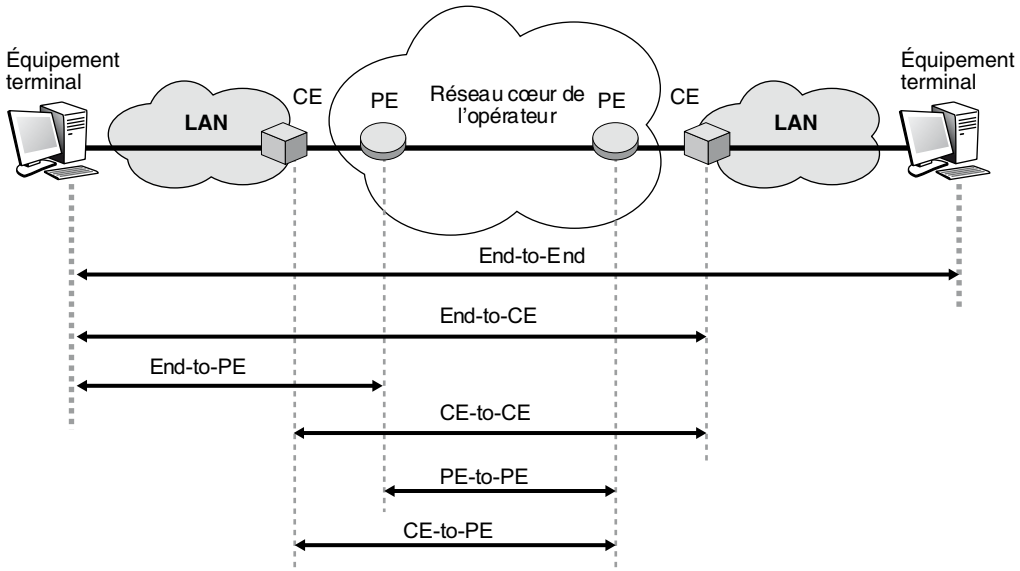


Figure R.1
Les six modèles de VPN

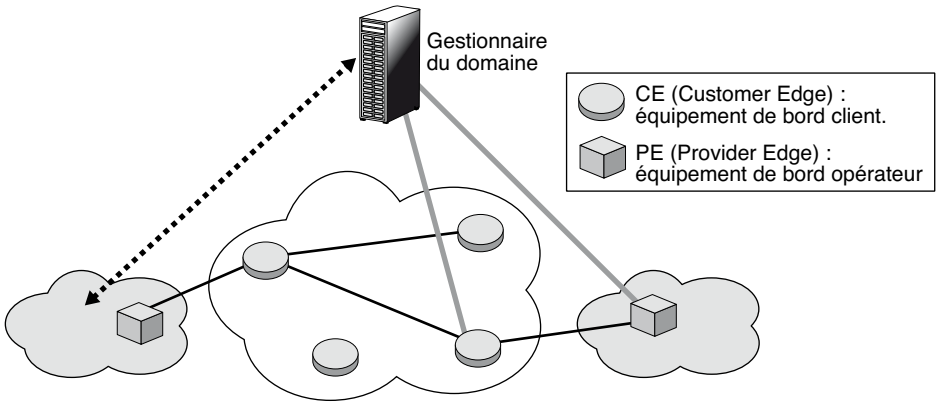
Parmi ces modèles, le cas du bout-en-bout (End-to-End) n'est pas applicable dans le cadre de la négociation de SLS avec un opérateur. Dans la suite de cette section, nous avons regroupé les modèles End-to-CE et End-to-PE dans la partie VPN personnels. Les modèles CE-to-CE, CE-to-PE et PE-to-PE sont regroupés dans la partie VPN de groupe.

VPN personnel (End-to-CE ou End-to-PE)

Le VPN personnel commence au niveau d'un terminal et prend fin au CE du LAN distant, dans lequel se trouvent les équipements terminaux, ou au PE, qui peut se situer dans un PoP (Point of Presence) de l'opérateur. Un équipement de VPN, associé à des fonctionnalités de VPN, disponible dans un CE ou dans un PE est responsable de l'application de services de sécurité entre lui et les équipements terminaux. L'approche End-to-PE peut éviter le besoin de déployer des matériels de VPN ou des fonctionnalités identiques dans le réseau du client. La plupart des VPN personnels sont implémentés selon le modèle End-to-CE.

Considérons un utilisateur distant qui demande la mise en place d'un VPN d'accès distant selon un certain niveau de service auprès du CE ou de l'opérateur du PE. Une négociation peut être mise en place entre le terminal et l'opérateur. Si cette négociation se finalise par un accord d'un certain niveau de service, l'activation du service n'est effective qu'après configuration de l'équipement terminal et du CE ou du PE. Ce schéma de fonctionnement est décrit à la figure R.2.

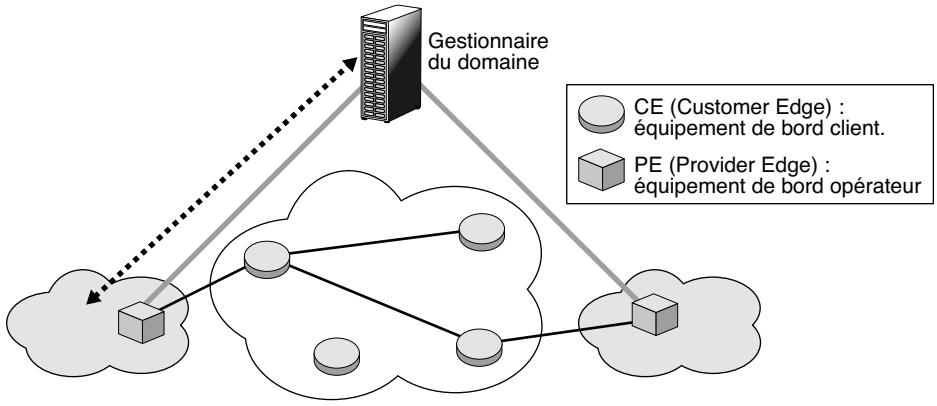
Figure R.2
Schéma de fonctionnement d'un VPN personnel



VPN:de groupe (CE-to-CE, CE-to-PE, PE-to-PE)

Avec un VPN de groupe, pour appliquer des services de sécurité, les équipements terminaux utilisent les équipements de VPN situés dans le périmètre du réseau d'entreprise (CE-to-CE ou CE-to-PE) ou dans le réseau de l'opérateur (CE-to-PE ou PE-to-PE). De cette façon, aucune fonction de sécurité n'a besoin d'être implémentée sur les terminaux. L'implémentation de services de sécurité leur est complètement transparente.

Figure R.3
Schéma de fonctionnement d'un VPN de groupe



Dans le cas d'une négociation intradomaine, par exemple CE-to-CE, les CE sont gérés par un même opérateur. La négociation du SLS a lieu entre un client situé au niveau d'un réseau d'entreprise et l'opérateur. Si nous prenons l'exemple d'un client situé dans le réseau d'entreprise de gauche de la figure R.3, le trait en pointillé indique la négociation du SLS pour un VPN à mettre en place entre le CE du réseau de gauche et le CE du réseau de droite.

Une fois la négociation terminée avec succès, l'opérateur peut mettre en place le service demandé en appliquant directement les politiques de sécurité adéquates sur les deux CE. Ce cas s'applique de façon similaire aux modèles CE-to-PE et PE-to-PE.

Le cas d'une négociation interdomaine, par exemple CE-to-CE, est illustré à la figure R.4. Les CE étant gérés par deux opérateurs différents, la négociation a lieu en plusieurs phases. La première phase de négociation se passe entre le client situé au niveau d'un réseau d'entreprise et l'opérateur qui gère son CE.

Prenons l'exemple d'un client situé dans le réseau d'entreprise de gauche. Le trait en pointillé sur la gauche de la figure indique la négociation du SLS pour un VPN à mettre en place entre le CE du réseau de gauche et le CE du réseau de droite. Une fois cette demande de négociation reçue, l'opérateur de gauche s'aperçoit qu'il ne gère pas le CE distant. Dès lors, il retransmet la demande de négociation du SLS à l'opérateur qui gère le CE distant (les pointillés du centre de la figure). Ce dernier traite la demande de négociation de service.

Deux situations se présentent alors :

- Si l'opérateur de droite l'accepte, une réponse favorable est transmise à l'opérateur de gauche puis au client initiateur de la demande. Les deux opérateurs transmettent les politiques adéquates à leur CE respectif, et ces derniers appliquent les politiques de sécurité.
- Si l'opérateur de droite refuse la négociation, deux possibilités se présentent :
  - L'opérateur distant (de droite) refuse catégoriquement la demande de négociation de service. Une réponse négative est transmise à l'opérateur de gauche puis au client. Le SLS ne peut être appliqué.
  - Le niveau de service demandé n'est pas applicable. Une renégociation du niveau du service de sécurité se met en place.

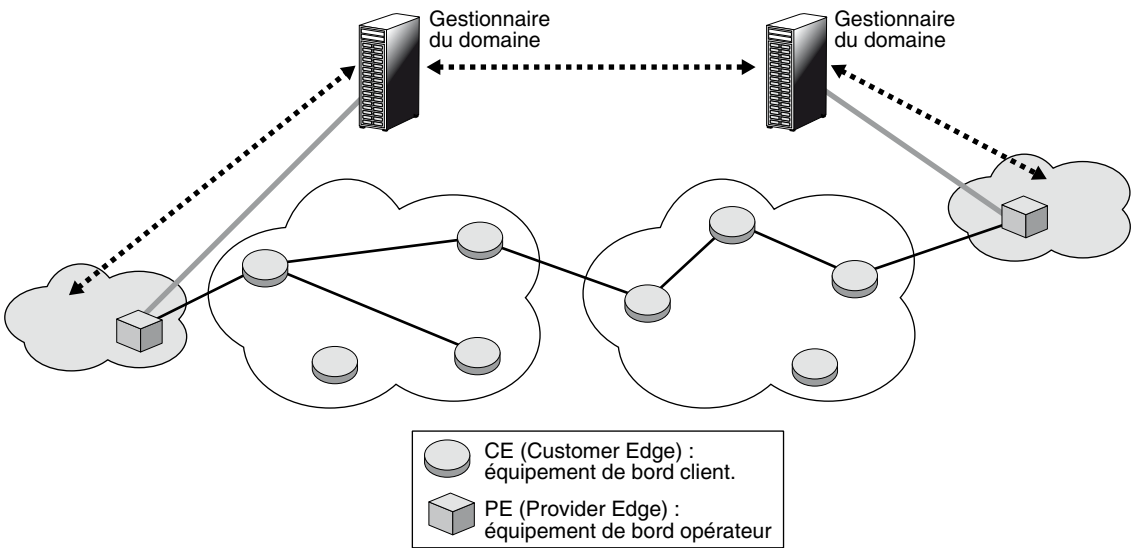


Figure R.4

Cas d'une négociation interdomaine

Identification du trafic

L'identification du trafic à sécuriser a lieu au point d'entrée de l'association de sécurité, ou SA (Security Association), IPsec. Cette information est stockée dans la base de données des politiques de sécurité SPD (Security Policy Database). À l'émission, une fois identifié, le trafic est encapsulé dans l'association de sécurité SA associée. Une SA est une connexion unidirectionnelle, ou simplex, qui apporte les services de sécurité au trafic qu'elle transporte. Deux SA sont nécessaires pour sécuriser une communication bidirectionnelle traditionnelle, une pour chaque direction. Dans ce cas, une identification du trafic à sécuriser a lieu au niveau des deux nœuds entre lesquels les SA sont mises en place.

Dans la réalité, le trafic à sécuriser entre deux points peut ne concerner que le trafic dans un sens, c'est-à-dire le trafic entrant ou sortant. On peut citer l'exemple d'un sous-réseau commercial dont la politique de sécurité est d'assurer le cryptage d'images en haute résolution à destination de ses clients. Dans ce cas, seuls les paquets IP sortants sont concernés. Les paquets IP entrants ne demandent aucune forme de cryptage. Dans ce cas, le client négocie auprès de son opérateur un niveau de service de sécurité pour le SA sortant. Aucun SA entrant n'est mis en place.

Les paramètres qui identifient le trafic à sécuriser, en unidirectionnel comme en bidirectionnel, sont les suivants :

- Adresse IP source (IPv4 ou IPv6) : peut être une adresse unique unicast, anycast ou broadcast (pour IPv4), un groupe multicast, une gamme d'adresses (valeurs inférieure et supérieure, adresse + masque de l'adresse) ou encore une adresse wildcard, c'est-à-dire une adresse réservée pour un invité.
- Adresse IP destination (IPv4 ou IPv6) : peut être une adresse unique unicast, anycast ou broadcast (pour IPv4), un groupe multicast, une gamme d'adresses (valeurs inférieure et supérieure, adresse + masque) ou une adresse wildcard.
- Nom : peut être un identifiant d'utilisateur ou un nom de système en fonction de la nature du nœud qui supporte IPsec. Le nom de système doit être applicable dans tout type de nœud IPsec. On peut se contenter d'un identifiant d'utilisateur au niveau des équipements terminaux, ainsi qu'au niveau des routeurs supportant IPsec pour le traitement du trafic entrant.

L'identifiant d'utilisateur et le nom de système peuvent être des noms d'utilisateur DNS ou des noms X.500.

Les réseaux en mode avec connexion

Les réseaux d'opérateurs sont généralement en mode avec connexion, la mise en place d'un chemin permettant de contrôler au mieux les ressources et de garantir la qualité de service. Au cours des années 1980, les opérateurs de télécommunications ont beaucoup utilisé les circuits, non seulement pour la téléphonie mais également pour les données. La première évolution après la commutation de circuits pure a été le RNIS (Réseau numérique à intégration de services), qui utilise le circuit aussi bien pour la parole téléphonique que pour le transfert de paquets.

Les opérateurs sont ensuite passés à la commutation de paquets sur des circuits virtuels. Les réseaux X.25 comme Transpac ont connu un grand succès dans les années 1980 et 1990. Ils étaient les premiers réseaux en mode avec connexion à permettre un partage des ressources entre tous les paquets acheminés dans le réseau. Les réseaux en relais de trames ont pris le relais. Ces réseaux ont à peu près les mêmes propriétés que les réseaux X.25, si ce n'est qu'au lieu de se servir de circuits virtuels au niveau 3, ils ouvrent des liaisons virtuelles de niveau 2, beaucoup plus simples et moins onéreuses. Ces liaisons virtuelles de niveau 2 permettent en outre de ne pas décapsuler les trames lors des traversées des nœuds de commutation, au contraire des réseaux X.25.

Après le relais de trames, les opérateurs ont choisi la technique de transfert ATM pour proposer des services avec garantie aux utilisateurs. Les réseaux ATM étant des réseaux de commutation de niveau trame, ils sont puissants et peuvent prétendre à des débits importants. Cette technologie a connu un grand succès sans toutefois réussir à s'imposer en raison de son système de signalisation, à la fois spécifique et relativement complexe. Cette complexité provient du choix qui a été fait d'étendre les signalisations précédentes, en particulier celle provenant du RNIS. De surcroît, l'UIT-T s'est trouvée dans l'incapacité de normaliser une interface standard que les équipementiers auraient pu intégrer dans les équipements de réseau. De ce fait, la technologie ATM n'a jamais pu s'imposer sur l'interface utilisateur, où elle a été supplantée par Ethernet et son allié de toujours IP. N'ayant pu s'imposer complètement, la technologie ATM a été remplacée par MPLS. La raison essentielle de cette nouvelle donne est l'introduction d'une signalisation permettant de mettre en place les chemins simplement avec une signalisation IP, puisque IP est un réseau de routage aux adresses universelles.

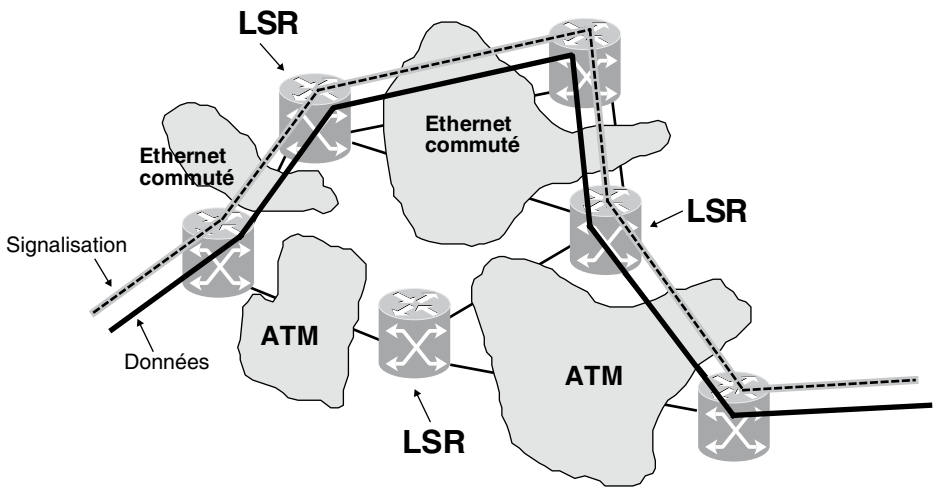
La technologie MPLS permet d'utiliser les anciens réseaux introduisant de la qualité de service, comme ATM. Le passage d'ATM à MPLS ne pose donc pas vraiment de problème. L'avantage de cette solution MPLS est l'utilisation d'un réseau de signalisation fondé sur IP, assez simple à mettre en œuvre. MPLS peut également utiliser des réseaux Ethernet à partir du moment où Ethernet emploie le mode commuté introduit avec le shim-label.

La figure R.5 illustre la traversée de plusieurs réseaux spécifiques formant un réseau MPLS afin d'illustrer la transition entre les réseaux de génération ATM et MPLS. La signalisation IP met en place un chemin de la façon suivante :

1. Lorsque le paquet de signalisation arrive au premier nœud, la technique de routage permet de déterminer le routeur suivant à atteindre après la traversée du réseau ATM. La traversée du réseau ATM par la signalisation est classique : un circuit virtuel ATM est ouvert en indiquant l'adresse ATM du routeur suivant, qui est obtenue par une traduction de l'adresse IP en une adresse ATM.
2. Une fois ouvert, le circuit virtuel ATM permet de transporter les différents fragments du paquet de signalisation, qui est reformé au nœud suivant.
3. Les fragments sont réassemblés au routeur suivant grâce à la couche AAL.
4. De nouveau, une fois déterminé le routeur suivant, il faut ouvrir un circuit virtuel ATM pour y transporter le paquet de signalisation IP.

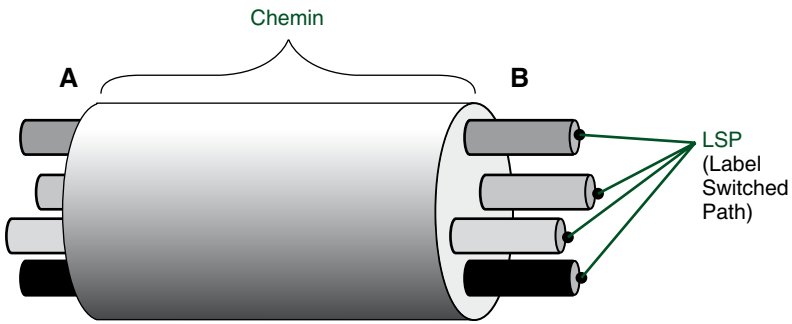
5. De même, pour traverser le réseau Ethernet, un chemin est mis en place, sur lequel les trames Ethernet sont commutées grâce aux références de type shim-label.

Figure R.5
Réseau MPLS de transition



La figure R.6 représente un réseau MPLS de façon conceptuelle. Les opérateurs n'attendent pas l'arrivée d'un client pour ouvrir un LSP mais l'ouvrent dès l'initialisation du réseau. De la sorte, lorsqu'un client se présente, il suffit de regarder l'adresse de sortie du réseau à partir de son adresse IP de destination et d'affecter le client au LSP approprié. Par exemple, entre les deux interfaces A et B, quatre circuits virtuels peuvent proposer un service EF, deux services AF, comme Gold et Bronze, et un service best-effort. Bien d'autres solutions peuvent être mises en œuvre pour affecter les chemins à des services particuliers. Par exemple, à chaque LSP pourrait correspondre une application particulière.

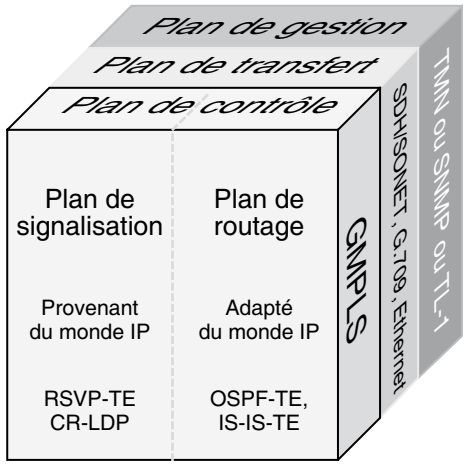
Figure R.6
Représentation conceptuelle d'un réseau MPLS



La figure R.7 représente un cas simple. Dans la réalité, MPLS fait appel à une solution de signalisation formant des FEC (Forwarding Equivalence Class). Toutes les communications qui ont une même destination se rassemblent sur un même circuit virtuel. Au

lieu d'être point-à-point, le chemin se présente sous la forme d'un arbre, dont la racine se trouve chez le destinataire et les feuilles chez les émetteurs.

Figure R.7
Architecture de GMPLS



Les réseaux MPLS seront eux-mêmes remplacés peu à peu par des réseaux GMPLS (Generalized MPLS), qui forment un surensemble de MPLS introduisant des techniques de commutation supplémentaires. L'architecture de GMPSL est illustrée à la figure R.7. Le plan de gestion utilise des standards classiques, comme SNMP ou le TMN de l'UIT-T. Le plan de transfert est issu principalement de l'UIT-T et de l'IEEE, avec SONET/SDH, G.709 et la commutation Ethernet. Le plan de contrôle provient quant à lui de l'IETF et comporte deux parties, le plan de signalisation, avec pour principaux protocoles RSVP-TE (Traffic Engineering) et CR-LDP (Constraint-based Routing/Label Distribution Protocol), et le plan de routage, avec pour principaux algorithmes de routage OSPF-TE (Traffic Engineering) et IS-IS-TE.

Les réseaux partagés

Les réseaux des opérateurs doivent être partagés entre les clients de telle sorte que chaque client puisse croire qu'il est seul à utiliser les ressources mises à sa disposition par l'opérateur et puisse avoir confiance dans la capacité de l'opérateur à sécuriser ses communications.

De ces principes sont nés les réseaux privés virtuels. Un réseau privé virtuel, ou VPN, est, du point de vue de l'entreprise cliente, un ensemble de réseaux de site reliés par un réseau d'opérateur garantissant une forte sécurité des communications. En particulier, aucun autre client que le personnel de l'entreprise ne peut y accéder de l'extérieur.

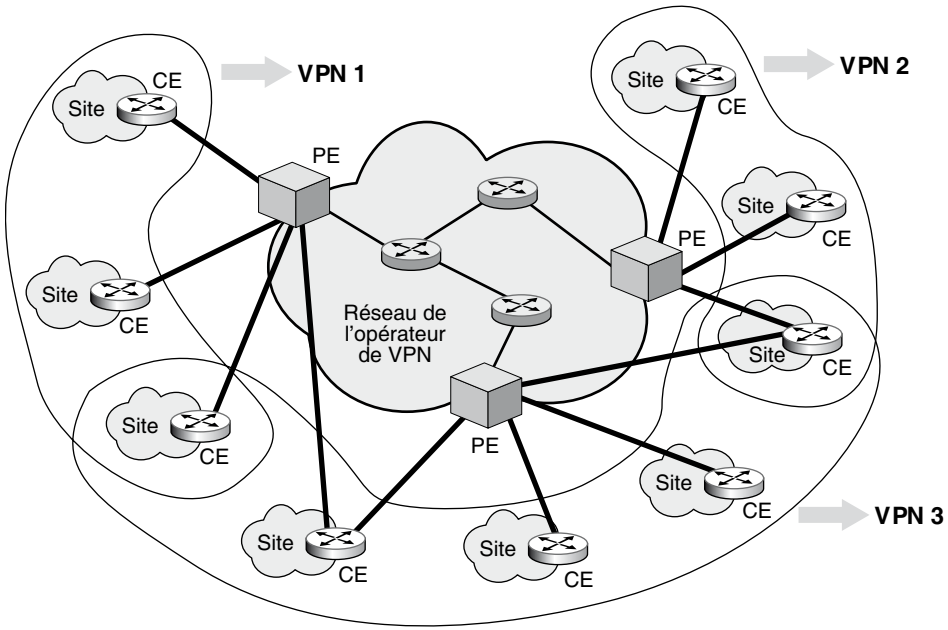
Du point de vue de l'opérateur, un VPN est un réseau dont les ressources sont partagées entre les différentes entreprises clientes de telle sorte que chaque client ait l'impression d'avoir un réseau dédié et non partagé. Pour l'opérateur, l'avantage de cette solution est énorme. Lorsque les entreprises n'utilisent les ressources qui leur sont affectées que

pendant un temps restreint, l'opérateur peut les réaffecter au fur et à mesure des besoins réels des autres entreprises clientes. En d'autres termes, nous avons un multiplexage statistique des équipements logiciels et matériels. Si la probabilité de manquer de ressources est parfaitement calculée, de façon à demeurer infime, le gain financier pour l'opérateur est très important.

Pour garantir le partage, il faut que le réseau se prête à une ingénierie simple, d'où le choix de MPLS et GMPLS.

Une structure de réseau VPN MPLS est illustrée à la figure R.8, dans laquelle trois VPN d'entreprise sont représentés. Un VPN MPLS est un ensemble de chemins, ou LSP, d'un réseau MPLS dédiés aux entreprises se connectant en VPN. Ces VPN d'entreprise sont connectés au réseau de l'opérateur par des points d'accès, ou PE (Provider Edge), appartenant à l'opérateur. Les réseaux d'entreprise sont raccordés au PE par un équipement CE (Customer Edge). Nous avons examiné ces éléments à la section précédente. Sur la figure R.8, on voit que certains sites peuvent appartenir à plusieurs VPN simultanément.

Figure R.8
Trois VPN d'entreprise sur un réseau d'opérateur

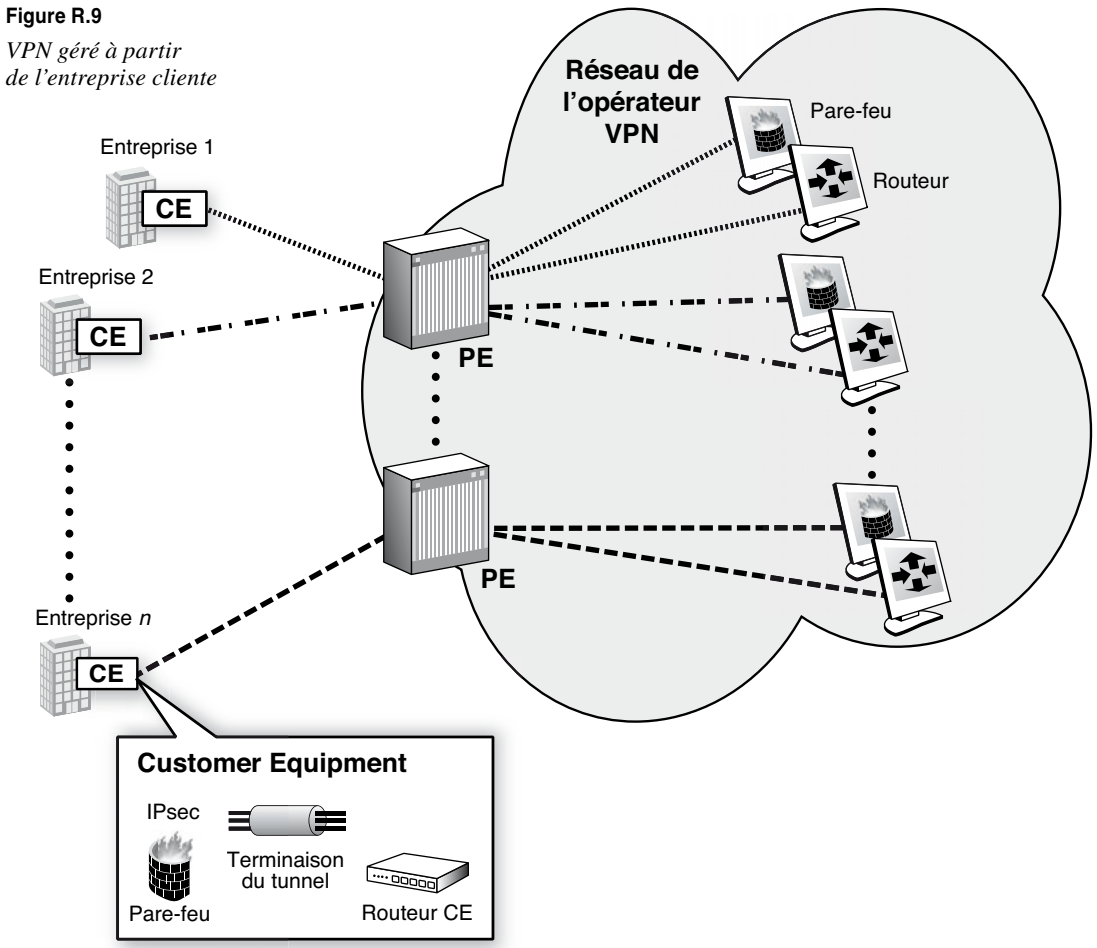


Les routeurs extrémité PE et CE peuvent gérer différents types de services. Le plus important pour les entreprises est la sécurité. Le VPN peut être sécurisé en chiffrant les paquets entrants dans le réseau de l'opérateur. Ce chiffrement peut s'effectuer dans le routeur extrémité de l'opérateur ou de l'entreprise. Bien que les opérateurs présentent cette solution comme une valeur ajoutée à leur offre de VPN, beaucoup d'entreprises préfèrent gérer elles-mêmes leur sécurité et chiffrer les données à l'entrée et à la sortie de leurs sites, en dépit du coût induit.

D'autres fonctionnalités peuvent être prises en charge par l'opérateur, notamment la qualité de service, la gestion de la mobilité ou d'autres types de services de sécurité que la simple confidentialité. Pour cela, la structure du VPN peut avoir son importance.

Deux structures de VPN MPLS peuvent être mises en place : un VPN selon le modèle overlay et un VPN selon le modèle peer. Dans le modèle overlay, les LSP sont ouverts directement de site à site, tandis que, dans le modèle peer, le routeur de bord se trouve chez l'opérateur. Dans le premier cas, les LSP sont ouverts directement entre CE, de telle sorte que le VPN de l'opérateur ne fasse que multiplexer les LSP sur son propre réseau. Le réseau de l'opérateur ne peut apporter de forte valeur ajoutée puisque l'information est chiffrée chez l'utilisateur. Dans le second cas, l'opérateur a à sa charge la gestion des extrémités des LSP et peut effectuer un multiplexage de plusieurs flots d'entreprise dans des LSP communs, garantissant au réseau de l'opérateur la scalabilité, ou passage à l'échelle.

Figure R.9
VPN géré à partir de l'entreprise cliente



La figure R.9 illustre le premier cas de figure, où le VPN démarre dans l'équipement extrémité, ou CE, de l'entreprise. Ce dernier gère les fonctionnalités de routeur, de sécurité IPsec, de terminaison de tunnel IPsec et de pare-feu mais peut aussi gérer des logiciels antivirus, antispam, etc. Le routeur PE de l'opérateur peut également jouer le rôle de pare-feu mais en proportion très limitée puisque les flots du client sont chiffrés. Seuls les paquets de gestion et de contrôle peuvent être vérifiés à ce niveau.

Cette solution revient relativement chère à l'entreprise, car elle doit gérer elle-même toutes les fonctionnalités de l'interconnexion de réseau.

La figure R.10 illustre un VPN géré par l'opérateur. Cette solution est beaucoup plus flexible puisque les équipements de routage, de pare-feu, de gestion d'IPsec, etc., sont partagés par les clients connectés au routeur PE.

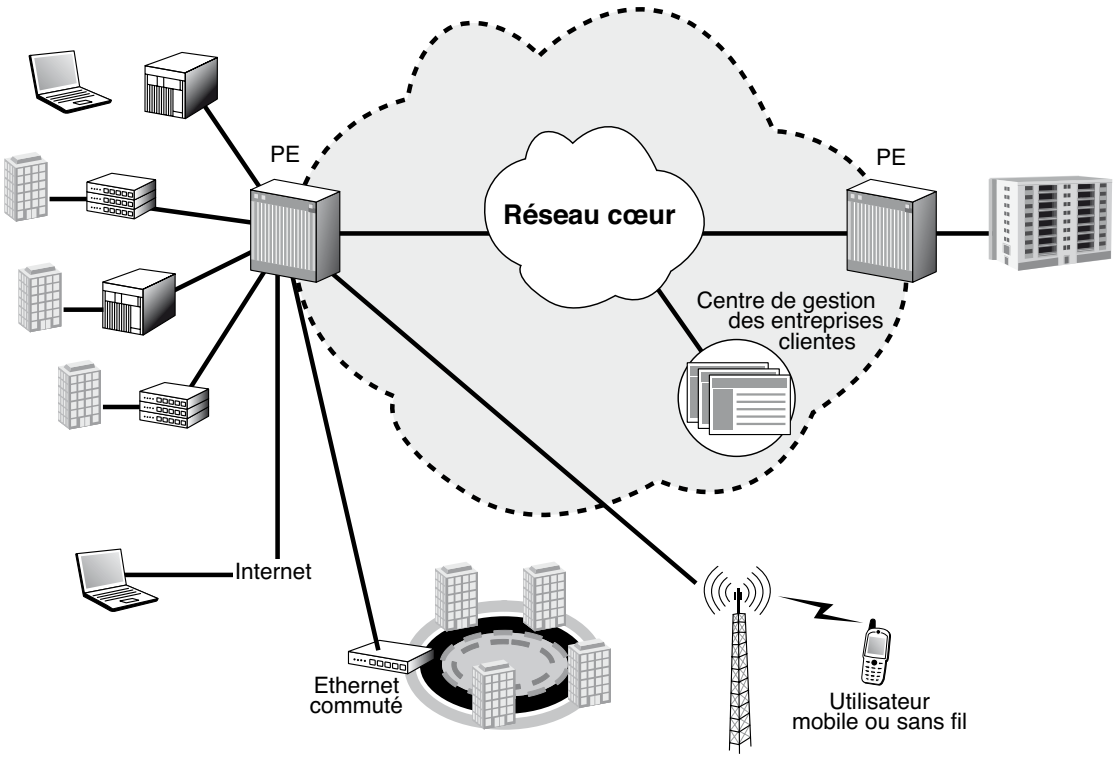


Figure R.10
VPN géré par l'opérateur

On voit que les machines de l'entreprise peuvent être connectées au routeur extrémité PE par un très grand nombre de solutions, alors que, dans la technique de raccordement au routeur CE, il faut que les matériels de l'entreprise soient connectés directement à l'entreprise. Dans la solution de gestion opérateur, les connexions peuvent s'effectuer par des

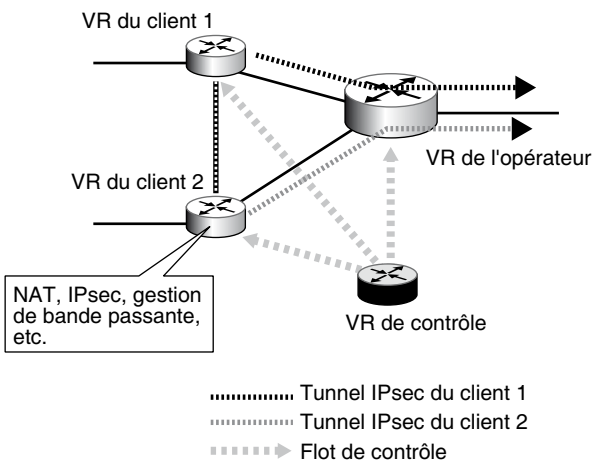
lignes *x*DSL, des liaisons spécialisées, des réseaux en relais de trames ou ATM ou même par des accès *via* des FAI permettant la connexion de terminaux mobiles ou sans fil. Des connexions Ethernet directes sont également possibles.

L'opérateur peut offrir des services supplémentaires, comme la gestion des équipements de l'entreprise cliente à partir de serveurs situés dans son réseau. Des services de gestion de messagerie électronique, d'impression, de gestion de logiciels ou de programmes métier peuvent être proposés à partir du réseau de l'opérateur. Cette solution apporte un gain à la fois au client et à l'opérateur. Le client n'a plus à gérer de façon privée un ensemble d'équipements. Il a de surcroît la possibilité de se connecter beaucoup plus facilement à ses sites par le biais de FAI intermédiaires et d'ajouter des clients mobiles ou nomades. Pour l'opérateur, le gain statistique est toujours le maître mot. Il est obtenu en partageant des équipements entre plusieurs clients.

Une autre solution qui se développe consiste, pour l'opérateur, à faire appel à des routeurs virtuels, ou VR (Virtual Router). Cette solution est illustrée à la figure R.11. Un routeur virtuel est l'équivalent d'un routeur matériel, mais avec ses propres algorithmes de routage et la possibilité de mettre en œuvre des fonctionnalités telles que NAT ou DHCP, des gestionnaires de bande passante, etc. Un routeur virtuel est donc un logiciel en technologie objet susceptible d'être implémenté sur une machine de sortie de l'entreprise ou plus généralement sur l'équipement PE de connexion de l'opérateur. Les fonctionnalités supplémentaires se présentent sous la forme d'objets spécifiques, qui peuvent être mis en route ou non. Plusieurs routeurs virtuels peuvent être créés à l'intérieur d'un même équipement. Si le routeur virtuel est situé sur le PE de l'opérateur, chaque client peut disposer de son propre routeur, avec ses propres fonctionnalités, même si, physiquement, l'équipement de réseau PE est unique.

L'opérateur peut agréger les flots sortant des différents routeurs virtuels sur des LSP uniques de façon à permettre la scalabilité de son réseau. L'opérateur possède un contrôleur de routeurs virtuels pour effectuer les modifications de configuration et la gestion du logiciel.

Figure R.11
Réseau d'opérateur à routeurs virtuels



Annexe S

26. La gestion de réseau

Cette annexe apporte des précisions supplémentaires sur la gestion ISO et plus particulièrement sur la gestion système CMIS/CMIP. Elle aborde ensuite la gestion de réseaux à base de politiques, qui a été très à la mode dans les années 2000, mais qui perd de son intérêt avec les réseaux autonomiques. L'annexe s'achève par des compléments sur les SLA (Service Level Agreement).

La gestion système CMIS/CMIP

La gestion système est au cœur du modèle de gestion ISO. C'est là que se prennent les décisions de gestion et que sont élaborées les demandes d'information nécessaires à la réalisation de cette gestion. Comme nous l'avons vu, la gestion système est effectuée par l'entité d'application SMAE, qui regroupe généralement quatre ASE.

Les services rendus par ces quatre ASE sont les suivants :

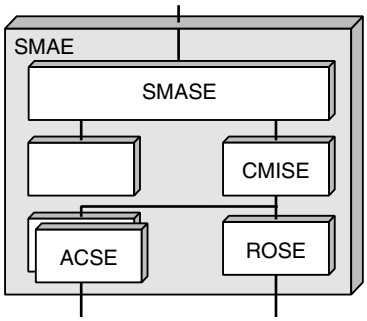
- SMAS (System Management Application Service), ou services d'application de la gestion système ;
- CMIS (Common Management Information Service), ou services communs à toutes les fonctions de gestion ;
- ACSE (Association Control Service Element), ou éléments de services de contrôle d'association ;
- ROSE (Remote Operation Service Element), ou éléments de services d'opération à distance.

Chacun de ces services repose sur un protocole spécifique :

- SMASE s'appuie sur le protocole MAP (Management Application Protocol), qui transporte des MAPDU.
- CMIS s'appuie sur le protocole CMIP (Common Management Information Protocol), qui transporte des CMIPDU.
- Le service rendu par ACSE, utilisant les quatre primitives A-ASSOCIATE, A-RELEASE, A-ABORT et A-P-ABORT, est réalisé par le protocole ACSE, qui transporte des ACSE-PDU.
- Le service rendu par ROSE, utilisant les cinq primitives RO-INVOKE, RO-RESULT, RO-ERROR, RO-REJECT-U et RO-REJECT-P, est réalisé par le protocole ROSE, qui transporte des ROSE PDU.

La figure S.1 illustre l'architecture de l'entité d'application SMAE avec ses quatre ASE.

Figure S.1
Architecture de l'entité SMAE



Les normes ISO 9595 et ISO 9596 spécifient respectivement le service commun (CMIS) et le protocole commun (CMIP). L'ensemble des services communs situés dans la couche application fournit les moyens d'échanger des données de gestion entre entités CMISE.

En résumé, une entité d'application SMAE est constituée d'un élément de service de gestion de système SMASE (System Management Application Service Element), d'un élément de service d'information de gestion commune CMISE (Common Management Information Service Element) et d'un élément de service de contrôle d'association ACSE (Association Control Service Element). Le SMASE définit la syntaxe et la sémantique de l'information de gestion transférée par des MAPDU. Les services de l'élément ACSE sont utilisés pour initialiser et terminer les associations.

Par abus de langage, le protocole de gestion d'un réseau OSI est identifié à CMIP/CMIS. En réalité, la gestion du modèle de référence est réalisée par l'entité d'application SMAE. Le service de communication utilisé par le SMASE peut être fourni par un CMISE (CMIS Element) ou tout autre ASE, comme FTAM (File Transfer and Access Management) ou TP (Transaction Processing).

L'utilisation de CMIS requiert la présence d'un ROSE, élément de service pour les opérations distribuées, qui permet de véhiculer de manière asynchrone des échanges de type question-réponse entre sites distants.

Pour compléter cette architecture de gestion du modèle de référence de l'ISO, indiquons que le processus de gestion SMAP travaille sur treize fonctions administratives qui ont été regroupées dans cinq domaines fonctionnels, ou SMFA (Specific Management Functional Area) : la configuration (Configuration Management), la sécurité (Security Management), les pannes (Fault Management), l'audit de performances (Performance Management) et la comptabilité (Accounting Management). Ces fonctions sont détaillées à la section suivante, et les cinq domaines de gestion dans une section spécifique.

Dernier point important, le processus de gestion SMAP peut être soit un processus gérant (Managing Process), soit un processus agent (Agent Process). Les utilisateurs des processus SMAP, que l'on appelle MIS-users (Management Information Service-users), peuvent donc être soit des agents, soit des gérants. Les rôles d'agent et de gérant ne sont pas assignés définitivement. Certains MIS-users peuvent, selon les opérations, être agent ou gérant.

Le service SM

Le service rendu par l'entité SMASE au processus SMAP à travers l'interface SMI (System Management Interface) s'effectue par l'intermédiaire des treize fonctions suivantes :

- Object Management Function
- State Management Function
- Relationship Management Function
- Alarm Reporting Function
- Event Report Management Function
- Log Control Function
- Security Alarm Reporting Function
- Security Audit Trail Function
- Access Control Function
- Accounting Meter Function
- Workload Monitoring Function
- Test Management Function
- Summarization Function

Les services associés à ces fonctions sont parfois appelés SMIS (Specific Management Information Service), mais ce terme trompeur est peu utilisé.

À titre d'exemple, les primitives de service de la fonction Object Management Function sont au nombre de six :

- pt-create
- pt-delete
- pt-event-report
- pt-get

- pt-set
- pt-action

Comme nous allons le voir, elles correspondent aux primitives du service CMIS.

Le service commun CMIS

CMIS (Common Management Information Service) est le service rendu par l'élément de service d'application CMISE. Six éléments de service ont été retenus dans CMIS pour les services de notification de gestion :

- M-CREATE, qui permet à un gérant de demander à un agent la création d'informations concernant des objets de gestion.
- M-DELETE, qui permet à un gérant de demander à un agent la destruction d'informations concernant des objets de gestion.
- M-EVENT-REPORT, qui permet à un agent de signaler à un gérant les changements d'état d'un objet de gestion sans y être sollicité.
- M-GET, qui permet à un gérant de demander à un agent la valeur des attributs d'un objet de gestion.
- M-SET, qui permet à un gérant de demander à un agent de positionner les valeurs des attributs d'un objet de gestion.
- M-ACTION, qui permet à un gérant de demander à un agent d'entreprendre une action trop complexe pour pouvoir être exprimée à l'aide des services précédents.

Trois autres éléments de service concernent les associations :

- M-INITIALIZE, qui permet l'association entre deux utilisateurs.
- M-TERMINATE, qui permet l'achèvement normal de l'association.
- M-ABORT, qui permet la rupture brutale de l'association par un utilisateur.

Un additif autorise l'ajout d'un service d'annulation :

- M-CANCEL-GET, qui permet à un utilisateur de demander à ne pas recevoir les résultats du GET précédent.

Grâce aux unités fonctionnelles supplémentaires, il est possible de disposer d'autres services. On trouve, par exemple :

- Le service de réponses multiples (Multiple Replies), qui permet à un système d'indiquer à un système distant qu'il peut recevoir plusieurs réponses concernant sa demande de service.
- Le service de filtre (Filter) et de profondeur de sélection (Scope), qui permet à un système d'indiquer à un système distant que l'opération demandée s'applique à plus d'un objet de gestion.

Le protocole CMIP (Common Management Information Protocol) permet à des utilisateurs du service commun CMIS d'effectuer leurs échanges. C'est un protocole de niveau 7, qui spécifie les procédures d'échange d'informations administratives entre

ASE. La syntaxe abstraite normalisée ASN.1 (Abstract Syntax Notation 1) est utilisée pour spécifier les éléments de protocole CMIP.

La gestion et le contrôle par politique

Les opérateurs de télécommunications et les gestionnaires de réseau ont besoin d'automatiser le processus de configuration des nœuds et des équipements réseau. Cette automatisation vise à la fois à contrôler les flux d'information qui transitent dans ces nœuds et à gérer plus facilement les équipements réseau. De là est née la gestion par politique, à laquelle on peut ajouter le contrôle, qui en fait partie de façon intrinsèque. La terminologie anglo-saxonne correspondante est PBM (Policy-Based Management). Le mot *policy* est traduit dans ce livre par politique, mais on aurait aussi bien pu choisir règle.

Le propos de ce chapitre est de présenter ce nouveau paradigme, consistant à gérer et contrôler les réseaux par l'intermédiaire de politiques. Nous commencerons par introduire les politiques puis détaillerons l'architecture associée au protocole de signalisation utilisé dans cet environnement.

Les politiques

Une politique s'exprime sous la forme « si condition alors action ». Par exemple, « si l'application est de type parole téléphonique, alors mettre les paquets en priorité Premium ». Cette section s'intéresse à la définition syntaxique et sémantique d'une politique puis examine en détail les politiques et leur utilisation pour le contrôle, ainsi que le protocole de signalisation permettant de transporter les paramètres des politiques et les différentes solutions pour mettre en œuvre le contrôle par politique.

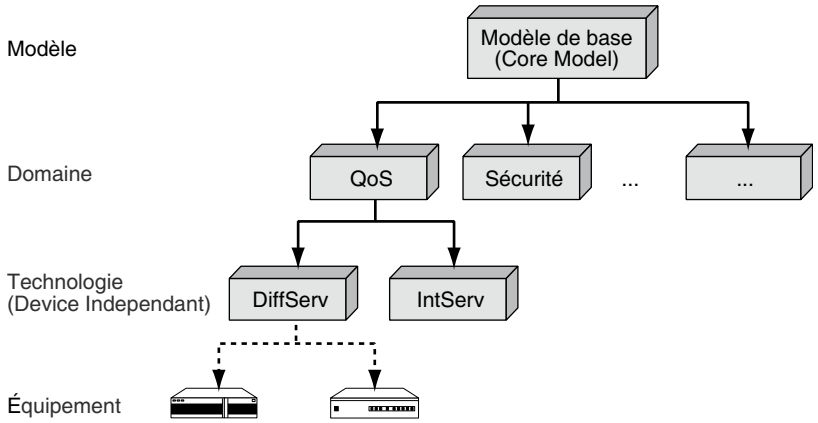
Une politique peut se définir à différents niveaux. Le niveau le plus haut correspond à celui de l'utilisateur, la détermination d'une politique s'effectuant par une discussion entre l'utilisateur et l'opérateur. On utilise pour cette discussion soit le langage naturel, soit des règles déjà préparées par l'opérateur du réseau. Dans ce dernier cas, l'utilisateur ne peut que choisir parmi ces règles la politique qu'il souhaite voir appliquer. On parle alors de politique définie au niveau business. Cette politique doit être traduite dans un langage de niveau réseau permettant de déterminer le protocole réseau de gestion de la qualité de service et son paramétrage. Enfin, il faut traduire ce langage de niveau réseau en un langage de bas niveau correspondant à la programmation des nœuds du réseau, ce que l'on peut appeler la configuration du nœud.

Ces différents niveaux de langage, business, réseau et configuration, sont pris en charge par un groupe de travail de l'IETF appelé Policy. Le modèle retenu provient d'un autre groupe de travail, le DMTF (Distributed Management Task Force) et porte le nom de CIM (Common Information Model). Les extensions sont aujourd'hui développées conjointement par les deux groupes de travail.

L'objectif de ce travail de normalisation des modèles d'information liés aux différents niveaux de langage est d'obtenir un modèle général qui puisse se décliner en modèles

d'information par domaine, ainsi qu'une représentation indépendante des équipements et des implémentations. La figure S.2 illustre le modèle le plus général possible à partir du modèle de base.

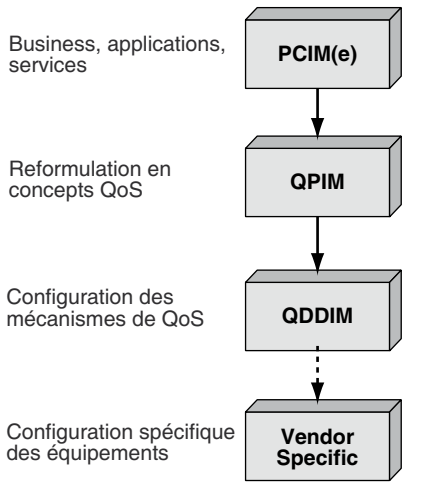
Figure S.2
Structure du modèle CIM



Si l'on ne se préoccupe que de la branche QoS, ou qualité de service, la structure des modèles successifs permet de passer de la définition générale d'une politique de qualité de service à la configuration d'un routeur.

La figure S.3 illustre la succession de modèles allant vers de moins en moins d'abstraction et s'approchant de la description d'une configuration.

Figure S.3
Structure des modèles associés à la QOS



PCIM (Policy Core Information Model)
QPIM (QOS Policy Information Model)
QDDIM (QoS Device Datapath Information Model)

PCIM (Policy Core Information Model)

PCIM définit le modèle de description des politiques, quel que soit leur domaine d'application. Le réseau est considéré comme une machine à états, c'est-à-dire un système qui ne peut prendre que des états définis à l'avance. Les politiques servent dès lors à contrôler les changements d'état en identifiant l'état courant et en définissant les transitions possibles.

Le modèle est fondé sur deux hiérarchies de classes, les classes structurelles, qui forment les éléments de base des politiques, et les classes d'association, qui déterminent les relations entre les éléments. Les politiques forment un ensemble de conditions vraies ou fausses qui peuvent être composées pour réaliser une politique plus complexe. Ces politiques forment à leur tour un ensemble d'actions associées aux conditions qui modifient la configuration d'un ou plusieurs éléments et qui introduisent des ordres d'exécution, comme la priorité des flots ou l'ordonnancement des paquets dans le réseau.

PCIMe (PCIM extension) a pour fonction de rendre le modèle PCIM plus flexible en permettant aux différents domaines d'homogénéiser leurs concepts. Les principales extensions concernent une meilleure gestion des priorités, l'ajout de variables et de valeurs, la définition de variables générales, l'ajout de règles simplifiées fondées sur les variables, la possibilité d'avoir des règles conditionnées par d'autres règles, la condition de filtrage de paquets IP à base de conditions, etc.

QPIM (QoS Policy Information Model)

Le rôle de QPIM est de fournir un format standard pour les politiques de QoS en intégrant les environnements IntServ et DiffServ, tout en restant indépendant des protocoles d'accès, des méthodes de stockage et des techniques de contrôle de QoS (files d'attente, etc.). QPIM doit en outre faciliter une représentation formelle de règles abstraites humaines.

Les actions possibles sur la définition de la QoS sont le classement par catégorie, l'adéquation par rapport aux fonctionnalités de RSVP, comme la modification de certains paramètres de RSVP, l'acceptation ou non d'une requête et la conformité au modèle COPS-RSVP et enfin les actions liées aux politiques de provisioning, comme le marquage, le lissage, la perte de paquets, l'ordonnancement, etc. D'autres extensions ont été ajoutées, notamment dix-sept variables liées à RSVP, ainsi que la définition formelle de profils de trafic pour DiffServ et IntServ.

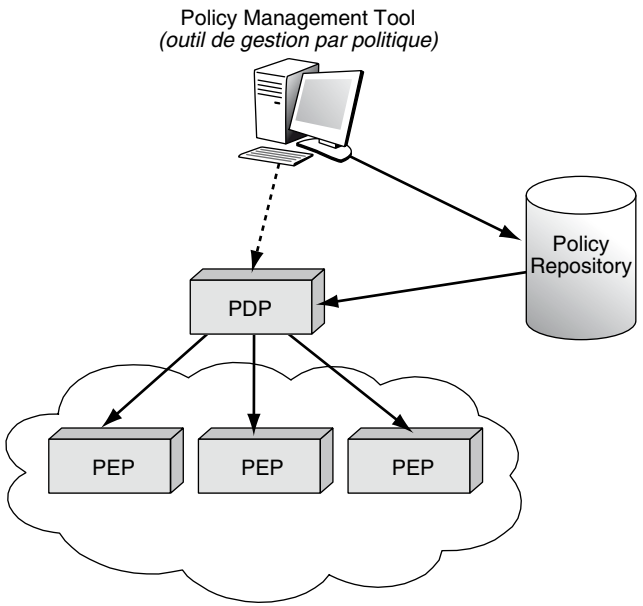
QDDIM (QoS Device Datapath Information Model)

Le modèle QDDIM permet de s'approcher de la configuration des routeurs en étendant QPIM, qui définit des actions sur les paquets, par le biais d'actions sur les équipements tout en restant indépendant des implémentations. Le rôle de QDDIM est de permettre de programmer un routeur ou un équipement réseau, indépendamment de l'équipementier qui le commercialise. Pour cela, QDDIM utilise une syntaxe générale permettant de décrire précisément l'action que doit apporter la politique à appliquer sur les composants de l'équipement réseau.

Architecture d'un contrôle par politique

Le contrôle par politique implique plusieurs composants (*voir figure S.4*). Les nœuds du réseau prennent le nom de PEP (Policy Enforcement Point). Les politiques y sont appliquées pour gérer les flux des utilisateurs. Le PDP (Policy Decision Point) est le point qui prend les décisions et choisit les politiques à appliquer aux PEP. La communication entre le PEP et le PDP s'effectue par le biais du protocole COPS (Common Open Policy Service). Le système comporte également une console utilisateur, qui contient des outils de gestion des politiques. Ces derniers permettent notamment d'entrer les politiques dans une base de données, nommée Policy Repository, qui entrepose les règles de politique que le PDP vient rechercher pour les appliquer aux nœuds du réseau.

Figure S.4
Architecture d'un système géré par politique



Des variantes de ce schéma de base peuvent inclure plusieurs PDP susceptibles de gérer un même nœud de transfert du réseau. Dans ce cas, les PDP ont des rôles différents, comme nous le verrons par la suite. Une autre variante correspond à une décentralisation des fonctions du PDP dans des PDP locaux, appelés LPDP (Local Policy Decision Point). En règle générale, un PDP gère un seul domaine administratif, et les règles de politique sont communes à la configuration de l'ensemble des nœuds du domaine.

Un problème de cohérence se pose lorsque le client émetteur et le client récepteur ne se trouvent pas dans le même domaine administratif. Dans ce cas, les PDP des deux domaines doivent négocier pour se mettre d'accord sur les règles de politique à adopter pour que la communication se déroule de bout en bout avec la qualité voulue. Ce cas est illustré à la figure S.5.

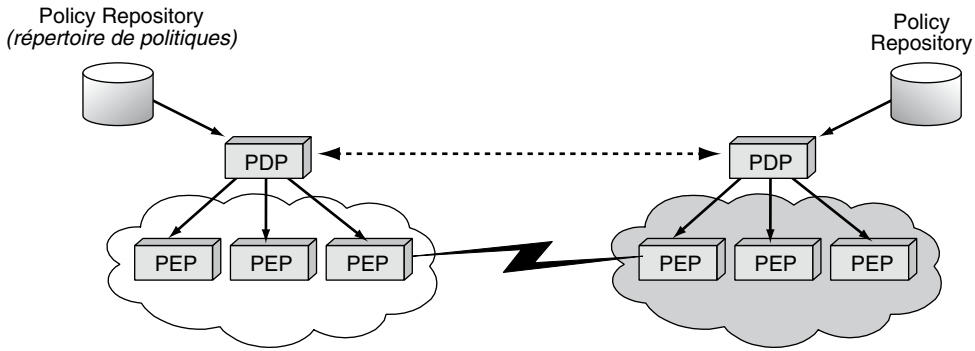


Figure S.5

Architecture de gestion par politique sur une interconnexion de deux domaines administratifs

Le PDP (Policy Decision Point)

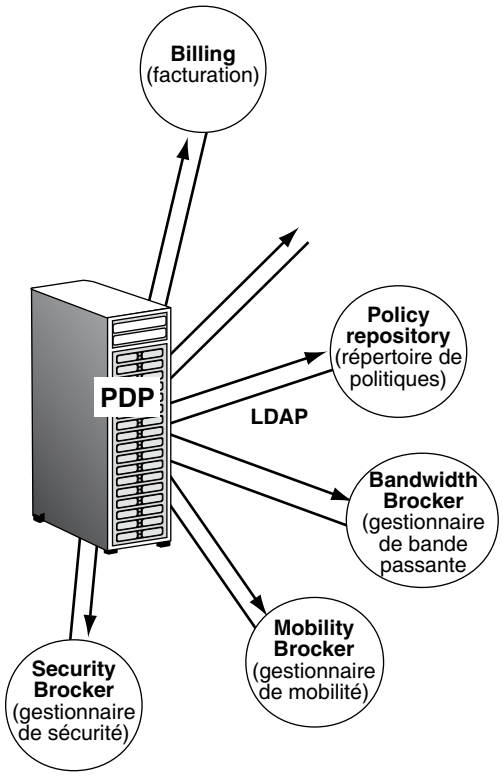
Le PDP est défini comme une entité logique prenant des décisions politiques pour elle-même ou pour d'autres éléments réseau qui demandent ses décisions. Le PDP, que l'on peut aussi appeler serveur de politiques, est donc le point central qui doit décider des politiques à appliquer dans le réseau. Il s'agit en quelque sorte d'un organe de décision, qui recherche les informations dont il a besoin dans de nombreux serveurs communiquant directement avec lui de façon à prendre une décision. Ces serveurs peuvent être locaux, ce qui est le cas le plus général, mais ils peuvent aussi être distants.

La figure S.6 illustre un PDP et ses serveurs principaux.

Les principaux serveurs sont, dans l'ordre :

- Le Policy Repository, dans lequel le PDP vient rechercher les règles de politique. Cette mémoire communique avec le PDP par le biais du protocole LDAP, ce qui explique son nom de serveur LDAP.
- Un Bandwidth Broker, qui gère la bande passante disponible dans le réseau. Ce serveur de bande passante connaît la topologie et les caractéristiques du réseau, ce qui lui permet de distribuer les ressources du réseau à bon escient.
- Un Security Broker, ou serveur de gestion de la sécurité au moment de la connexion, qui est généralement un serveur AAA (Authentication, Authorization, Accounting). Ce serveur peut également gérer la sécurité du transport de l'information sur les supports physiques.
- Un Mobility Broker, ou serveur de mobilité, qui peut être apte à gérer la continuité de la qualité de service.
- Un serveur de facturation (Billing), qui se révélera essentiel dans les prochains réseaux Internet qui délivreront de la qualité de service.

Figure S.6
Un PDP et ses serveurs



Il peut exister des serveurs complémentaires, comme la PIB (Policy Information Base), qui garde en mémoire les modèles informationnels pouvant être utilisés pour représenter une politique sous une syntaxe particulière. D'autres serveurs se révéleront sûrement très importants à l'avenir, comme le serveur de métrologie et de tuning, qui doit être capable de vérifier que les ressources mises à la disposition d'un utilisateur le sont effectivement.

Le rôle du PDP consiste à identifier les règles de politique qui sont applicables aux différents PEP et à déterminer les règles à appliquer stratégiquement à ces PEP. Le PDP doit également se préoccuper de la traduction des règles de politique dans des formats compréhensibles des nœuds comme les PIB. De plus, il doit pouvoir communiquer avec d'autres serveurs internes pour prendre ses décisions. Enfin, le PDP assure la distribution des configurations. En résumé, le PDP décide des règles à appliquer et envoie les ordres de configuration aux nœuds du réseau.

Les PEP (Policy Enforcement Point)

Les PEP sont des entités logiques qui appliquent les décisions politiques prises par le PDP dont elles dépendent. Les PEP sont généralement les nœuds du réseau, qui peuvent être de différents types : routeur, commutateur ou LSR (Label Switched Router). Un

PEP peut également être un pare-feu ou un équipement intermédiaire entre le client et le réseau. Le client peut lui-même posséder un client PEP sur son terminal. Dans les réseaux de mobiles à carte à puce, il est fréquent de considérer qu'un PEP d'accès se trouve sur la carte à puce. Son rôle est essentiellement réduit à la gestion de la sécurité et non de la qualité de service, mais il est imaginable d'implémenter la gestion de QoS dans les cartes à puce dès que celles-ci seront assez puissantes pour effectuer cette gestion.

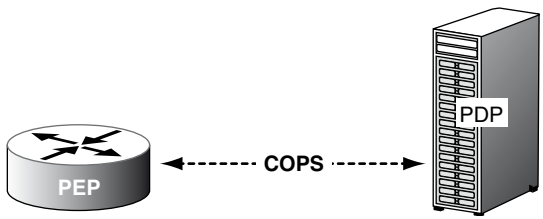
Un PEP doit être facilement accessible et paramétrable par le PDP de sorte qu'il soit possible de le configurer sans problème. Il peut être configuré par un message COPS mais aussi par une requête SNMP ou une commande CLI (Command Line Interface), qui est la commande la plus simple pour configurer manuellement un équipement de réseau. Le PEP fait le lien entre la représentation externe (PIB ou MIB) et la configuration interne de l'équipement et doit être capable de recevoir des requêtes de différents types provenant de l'utilisateur. En particulier, le PEP doit être apte à comprendre les requêtes RSVP. Le PEP s'assure de la cohérence des politiques locales et surveille leur bonne application. Enfin, il peut intégrer des fonctions d'ingénierie ou de facturation.

COPS (Common Open Policy Service)

COPS est le protocole de signalisation développé par l'IETF pour transporter les demandes de configuration et retourner les politiques à appliquer. Au départ, le protocole COPS devait permettre de prolonger RSVP vers le PDP et assurer les fonctions de contrôle d'admission au réseau en les fondant sur des politiques.

C'est un protocole requête-réponse simple pour l'échange d'informations de politiques entre un serveur de politique, ou PDP, et un client, ou PEP. La figure S.7 illustre ce schéma de base.

Figure S.7
Fonctionnement du protocole COPS



Le PEP peut être un routeur supportant RSVP ou un routeur supportant un service de gestion de la qualité de service, comme DiffServ, ou encore un nœud appliquant un contrôle quelconque. Le PEP fournit des informations au PDP concernant les décisions prises et les politiques installées. COPS transporte les messages d'erreur faisant suite à la détection d'un problème lors de l'installation d'une politique ou à un échec détecté lors de l'installation de la configuration sur le PEP.

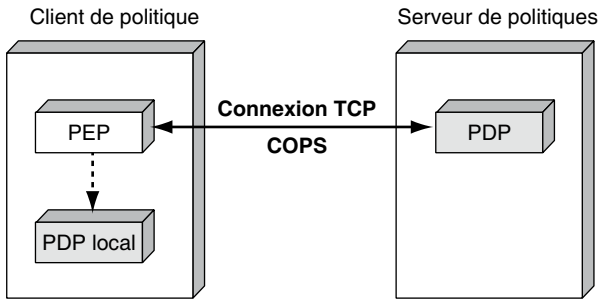
Le PEP est responsable de la mise en place d'une connexion TCP avec le PDP. Il utilise cette connexion TCP pour envoyer des requêtes et recevoir les décisions du PDP. Le PEP

doit rendre compte au PDP de l'exécution de ces décisions. De même, le PEP est responsable de la notification au PDP des modifications du PEP. Le PEP est en outre responsable de la suppression d'un état devenu inacceptable à la suite d'une modification demandée par le client ou d'une décision prise et envoyée par le PDP.

Le PEP peut être configuré et commandé par une décision locale *via* son LPDP (Local Policy Decision Point). Le PEP doit faire parvenir les caractéristiques de cette décision locale au PDP, lequel prend la décision finale. Si cette décision est différente de celle définie en local, le PDP l'envoie au PEP pour application.

La figure S.8 décrit le système de communication entre un PDP et un PEP.

Figure S.8
Architecture de base d'un environnement contrôlé par politique



PDP (Policy DecisionPoint) PEP (Policy EnforcementPoint) LPDP (Local PDP)

Le PDP est la composante de l'environnement PBN (Policy-Based Networking), qui contrôle directement le PEP. Le PDP choisit parmi les politiques disponibles dans la base, ou Policy Repository, contenant les informations de politique, la politique adaptée pour configurer le routeur.

Les règles de politique utilisées par le PDP sont saisies par la console de gestion de l'opérateur puis mises à disposition du PDP par le Policy Repository où elles sont déposées. À l'intérieur des nœuds, le PEP peut être accompagné d'un LPDP (Local PDP), dont le rôle est de remplacer le PDP en cas de besoin. La présence du LPDP est facultative. Ce point de contrôle local est utilisé pour prendre une décision locale en l'absence du PDP.

Le PDP peut utiliser différents mécanismes et protocoles de communication avec des serveurs qui lui sont attachés pour réaliser des fonctions spécifiques, comme l'authentification, la facturation ou le stockage d'informations de politique.

Le fonctionnement général du modèle de gestion par politique est illustré à la figure S.9.

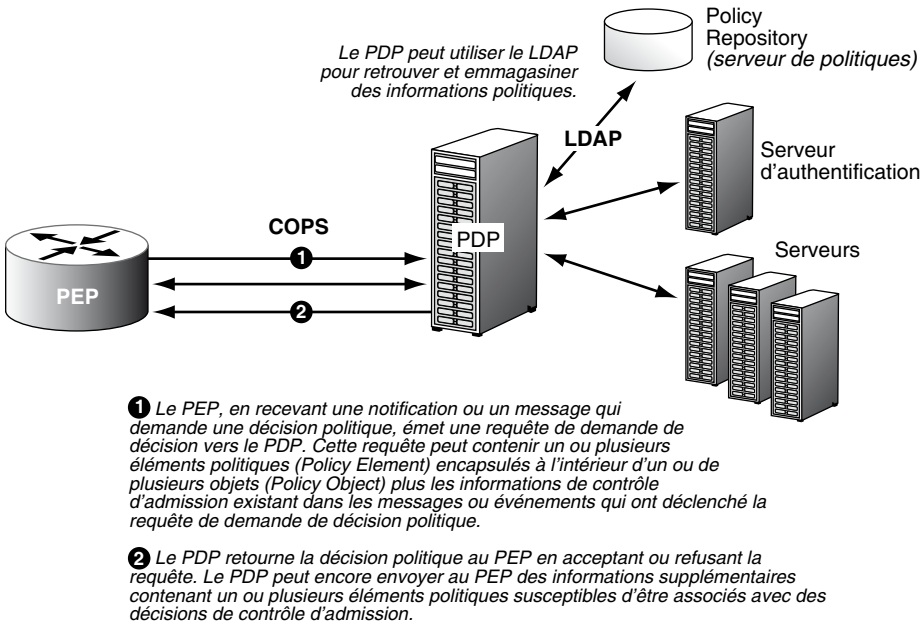


Figure S.9

Fonctionnement global d'un environnement de contrôle par politique

Caractéristiques principales du protocole COPS

Le protocole COPS emploie un modèle client-serveur, dans lequel le PEP envoie des messages de requête (Request), de mise à jour (Update) et de suppression (Delete) au PDP. Le PDP retourne des messages contenant les décisions prises.

TCP est utilisé comme protocole de transport pour fiabiliser l'échange des messages entre le PEP et le PDP. Aucun mécanisme supplémentaire n'est à mettre en œuvre pour réaliser une communication fiable entre un PDP et un PEP. Le protocole est extensible, la communication pouvant prendre en charge plusieurs types d'information (Client Specific Information) sans exiger de modification de la part du protocole COPS.

Le protocole fournit les éléments de sécurité nécessaires pour l'authentification, la protection contre les attaques malveillantes et l'intégrité du message. COPS peut aussi utiliser d'autres protocoles spécifiques pour gérer les problèmes de sécurité. Ainsi, IPsec ou TLS (Transaction Layer Security) peuvent être mis en œuvre pour authentifier et sécuriser la connexion entre le PEP et le PDP.

Les états des configurations mises en place par la communication sous forme de requêtes-décisions sont partagés entre le PEP et le PDP. Les décisions du PDP peuvent être émises d'une manière asynchrone, c'est-à-dire à tout instant, pour modifier l'état du système installé. Le protocole permet au PDP d'envoyer l'information de configuration au PEP et permet au PDP de supprimer les états du PEP lorsqu'ils ne sont plus valides.

La figure S.10 illustre un message COPS comprenant un en-tête avec différents champs de contrôle, suivi des champs objet. Chaque champ objet est composé de la même façon, en commençant par la longueur de l'objet, la définition de l'objet, le type d'objet et enfin le contenu et les valeurs associées de l'objet. La figure S.11 décrit l'échange des messages dans une communication COPS.

Figure S.10
Message COPS

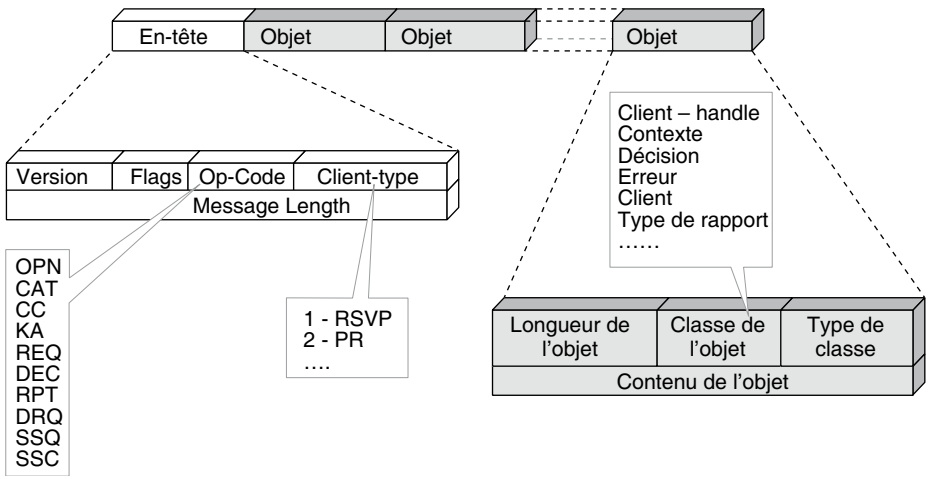
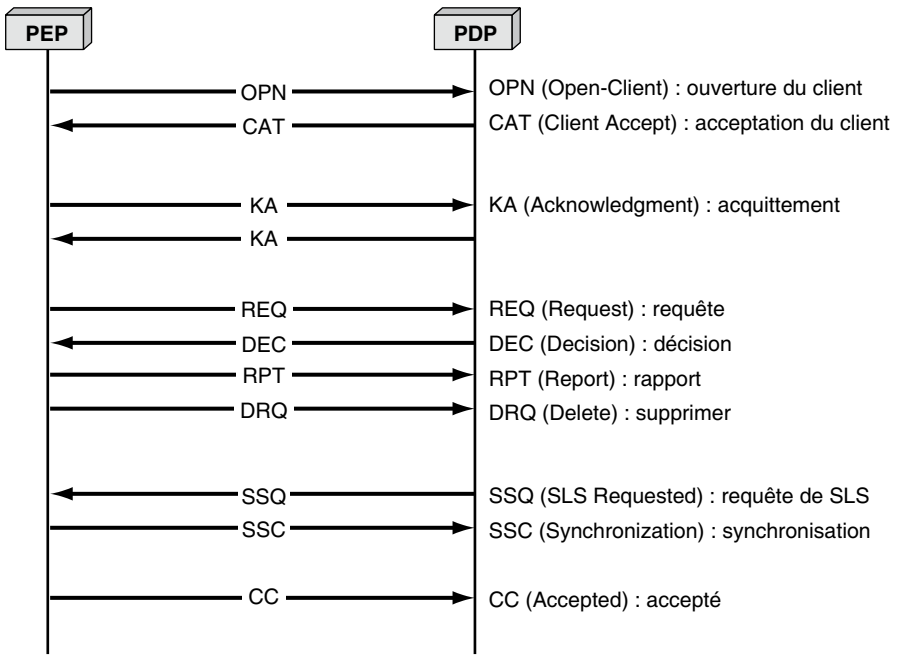


Figure S.11
Échange de messages dans une communication COPS



COPS et les modèles de gestion par politique

Les deux modèles principaux de gestion et de contrôle par politique sont le provisioning et l'outsourcing.

Dans le cas de l'outsourcing (Outsourcing Policy Model), le PDP reçoit les requêtes (Policy Requests) de demande de configuration de la part des PEP et décide ou non d'autoriser la connexion en temps réel sans qu'un lien préalable soit tissé entre l'utilisateur et l'opérateur du réseau. Si la demande d'accès est acceptée, le PDP envoie la configuration proposée au nœud d'accès, qui la propose à son tour au client demandeur.

Le fonctionnement général de l'outsourcing est le suivant :

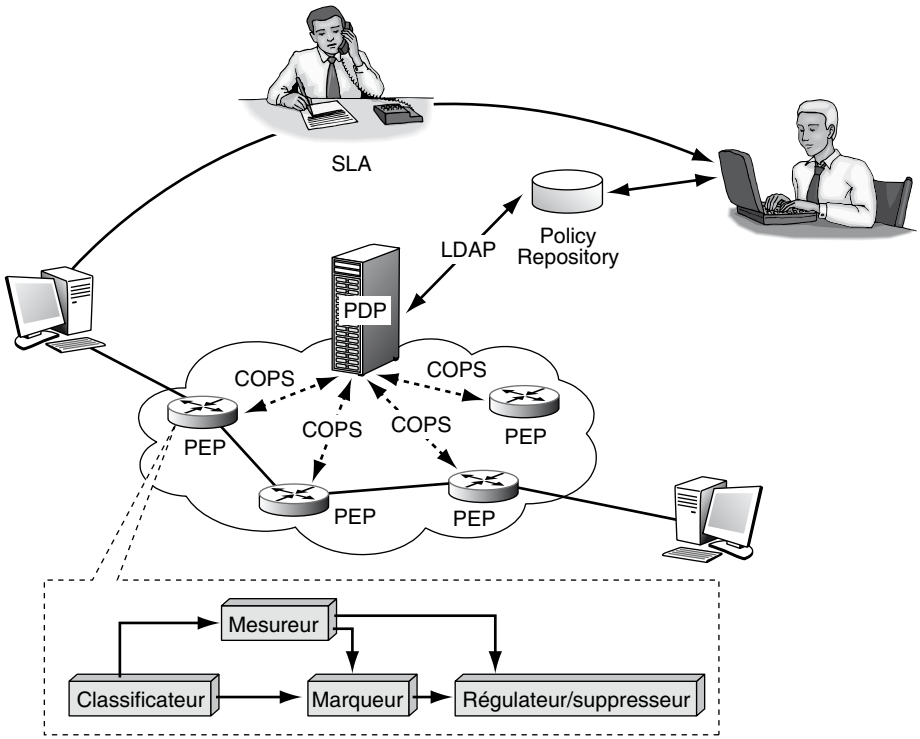
1. Le client effectue une demande de connexion à un réseau auquel il n'est pas abonné.
2. Cette demande appelle une décision concernant l'accès au réseau : l'opérateur accepte ou non la connexion du client.
3. Le client doit donc faire une requête au réseau. Le protocole RSVP est le vecteur le plus classique pour effectuer cette demande.
4. Celle-ci arrive au nœud d'entrée du réseau, ou edge router, qui la dirige vers le PDP grâce à une requête COPS.
5. Une fois la décision prise par le PDP, une réponse transitant par le protocole COPS indique au nœud d'entrée si la demande RSVP est acceptée ou non.
6. En cas d'acceptation, la requête RSVP peut continuer son chemin pour ouvrir une route satisfaisant la demande de l'émetteur.

Nous détaillons cette solution un peu plus loin dans ce chapitre.

Dans le cas du provisioning (Provisioning Policy Model), les politiques sont entrées à la console de gestion de l'opérateur à la suite d'une discussion entre le client et l'opérateur. Cette discussion débouche sur un SLA (Service Level Agreement), qui correspond à un contrat entre l'utilisateur et le gestionnaire du réseau détaillant les caractéristiques du service qui doit être rendu par l'opérateur et les dispositions administratives en cas de problème. La partie technique du SLA s'appelle le SLS (Service Level Specification). Le SLS donne lieu à l'introduction de politiques dans la base de données de l'opérateur, politiques qui devront être appliquées dès que le client présentera un flux à l'entrée du réseau.

Les politiques sont distribuées en temps réel par le PDP. Le PDP décide si la politique doit être installée en permanence dans les PEP traversés par le client ou non, suivant les caractéristiques techniques de la demande du client. Si les politiques sont implémentées directement dans les nœuds, le PDP les envoie au travers d'une commande COPS. Les nœuds d'accès sont alors prêts à recevoir les demandes d'accès des flots négociés dans le SLA-SLS. Les nœuds d'accès sont capables de traiter en temps réel ces demandes. Le provisioning est souvent associé à la technique DiffServ, dans laquelle les flots peuvent être classifiés suivant diverses classes. Dans ce cas, les paquets des clients entrants sont marqués avec la priorité négociée dans le SLS et transmis aux routeurs par la politique correspondante. La figure S.12 illustre le fonctionnement d'une politique de provisioning associée à DiffServ.

Figure S.12
Fonctionnement d'une solution de provisioning



La figure S.13 présente les requêtes échangées entre le PDP et le PEP pour une communication de provisioning (PR) avec un protocole COPS qui prend alors le nom de COPS-PR. Cette communication s'effectue par l'émission d'une requête REQ du PEP vers le PDP. Le PDP répond par une commande DEC précisant la configuration à mettre en œuvre dans le PEP.

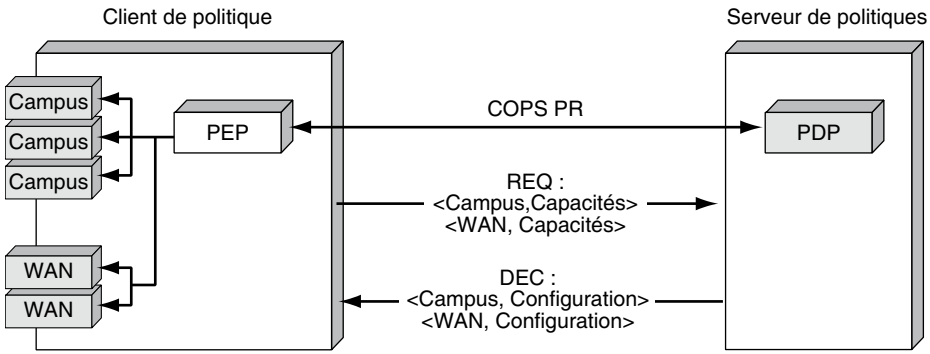


Figure S.13
Fonctionnement de COPS-PR sous DiffServ

La pile du protocole COPS peut être divisée en trois couches conceptuelles distinctes : le protocole de base, les directives dépendant du type de client (client-type) et la représentation des données de politique (Policy Data Représentation).

L'IETF a proposé COPS comme protocole de communication pour faciliter l'échange des informations de politique entre le PDP et les PEP. Avant d'effectuer un échange de données de politique, le PEP doit initialiser la communication en ouvrant une connexion TCP avec le PDP. C'est là une des différences les plus importantes par rapport aux systèmes de gestion classiques de réseau, comme SNMP, dans lesquels le serveur initialise la communication avec le client avant d'envoyer l'information de configuration en utilisant une connexion UDP. L'utilisation d'une connexion TCP augmente la fiabilité du protocole COPS.

COPS-RSVP et le modèle d'outsourcing

RSVP a été choisi comme protocole de signalisation entre le client et le réseau pour gérer la QoS dans le modèle d'outsourcing. À la suite de l'arrivée d'un message RSVP dans le nœud d'accès, un protocole COPS spécifique, COPS-RSVP, est mis en jeu afin d'utiliser les objets de RSVP.

Quand le PEP reçoit un message RSVP sollicitant une décision pour la configuration des nœuds que son flot va traverser, les objets de RSVP sont encapsulés à l'intérieur de l'objet Signaled Client SI dans un message de requête COPS envoyé au PDP. Le PDP décide alors si ce message RSVP doit être accepté ou non puis envoie sa décision au PEP par un message de réponse. D'autres informations de supervision peuvent être envoyées par le PDP, suite à la même requête, si le PDP s'aperçoit que la décision politique originale a besoin d'être modifiée ou supprimée.

Dans le cas où le PDP détecte l'absence d'un objet RSVP essentiel dans la requête, il retourne un message d'erreur <Error> dans le message de décision, qui doit indiquer MANDATORY CLIENT-SPECIFIC INFO MISSING. Dans le cas où le PDP détecte l'absence d'un objet RSVP optionnel dans la requête, il retourne une décision négative.

Pour chaque message de décision reçu, le PEP envoie un rapport au PDP, qui inclut les actions prises pour assurer que les politiques décidées par le PDP ont été convenablement installées et pour détecter d'éventuelles anomalies. De la sorte, le PDP reste bien informé de la politique installée dans le PEP.

Dans le protocole RSVP, l'objet Policy Data joue le rôle d'un conteneur de transport des messages RSVP qui arrivent au PEP, le PEP communiquant l'objet Policy Data au PDP. Le PDP prend alors une décision fondée sur le contenu de l'objet Policy Data. Le PDP peut aussi modifier ou remplacer le Policy Data par un message Outgoing RSVP, qui permet à RSVP de se propager dans le réseau.

COPS-PR et le modèle de provisioning

Le provisioning n'inclut pas de mécanisme de signalisation de QoS mais comporte un modèle de type push. La configuration des routeurs est effectuée par le PDP en poussant l'information de configuration dans les nœuds une fois le SLA négocié avec l'utilisateur.

Le mot *provisioning* (approvisionnement) provient de cette solution dans laquelle on réserve des ressources à l'avance, l'utilisateur les trouvant mises à sa disposition dans les nœuds du réseau lorsqu'il se connecte.

Au départ, le PDP choisit les règles de politique qu'il appliquera à un utilisateur en considérant les informations du SLA-SLS négocié au départ avec l'utilisateur. Ces décisions sont ensuite envoyées d'une manière asynchrone du PDP au PEP pour réaliser la configuration décidée par le PDP. Le PDP effectue un calcul de probabilité en fonction de tous les SLA-SLS des clients abonnés puis envoie l'information de configuration au PEP, telle que le changement de politique demandé directement par l'utilisateur en modifiant son abonnement, à une heure prédéterminée, à l'expiration d'un compte, etc. Le PEP confirme que l'installation de configuration est réussie à la suite du message de configuration.

Le protocole COPS-PR peut être utilisé pour mettre en place différentes configurations de gestion de la qualité de service, comme DiffServ, MPLS, etc. Les données transportées par COPS-PR forment un ensemble de données de politique. Ces données prennent le nom de PIB (Policy Information Base), ou base de données des informations de politique. La PIB est utilisée avec le protocole COPS et, dans le cas du provisioning, avec COPS-PR. Le modèle de description de l'information de politique décrit le format des informations de politique échangées entre le PEP et le PDP. La PIB contient des informations décrivant le service associé aux politiques et les techniques de classification des paquets. Elle est extensible, de sorte à permettre l'adjonction de nouveaux types de paramètres.

Interactions entre les PEP et le PDP

Au démarrage d'un PEP, celui-ci ouvre une connexion COPS avec son PDP. Une fois la connexion établie, le PEP envoie au PDP des informations à propos de lui-même sous la forme d'une requête de configuration. La requête inclut toutes les informations spécifiant le client, telles que les types de matériel et de logiciel utilisés, qui sont nécessaires à une configuration. Durant cette phase, le client peut spécifier la taille maximale du message COPS-PR.

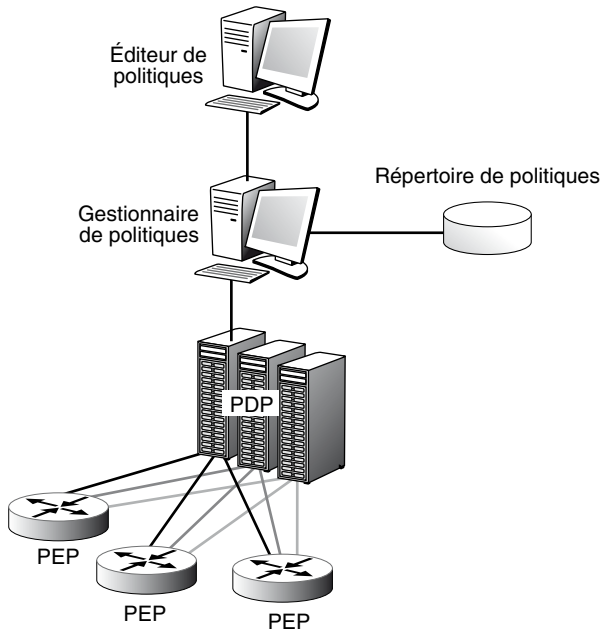
Le PDP répond à la requête de configuration en transmettant l'ensemble des politiques acceptées par le PDP concernant ce PEP. À réception de ces politiques de configuration, le PEP les organise et les installe. Si le PDP change son comportement ou est averti par le PEP d'un changement de contexte, suite, par exemple, à une panne, le PDP envoie une nouvelle configuration avec les primitives INSTALL, UPDATE et DELETE pour modifier la configuration du PEP. Si la configuration du PEP doit changer de manière radicale, suite à une demande de configuration non disponible dans le nœud, le PEP envoie de façon asynchrone de nouvelles informations au PDP dans un message UPDATE REQUEST CONFIGURATION. À réception de cette requête, le PDP fait parvenir au PEP les informations nécessaires à la gestion de l'implantation de la nouvelle politique et, bien sûr, à l'effacement des politiques qui ne sont plus nécessaires.

Nous avons vu que COPS utilisait une connexion TCP entre le PEP et le PDP. La connexion TCP est initialisée par le PEP. Chaque serveur PDP écoute la connexion sur

le port 3288. Il existe au moins un PDP par domaine administratif. Le PEP peut obtenir l'adresse du PDP par le service de gestion du réseau ou par le mécanisme de localisation de service, ou SRVLOC (Service Location). Un PEP peut supporter plusieurs types de clients. Dans ce cas, il doit envoyer plusieurs messages CLIENT-OPEN, de façon que chaque connexion spécifie un type de client particulier.

Le PEP effectue sa requête à un ou plusieurs PDP au travers d'une ou de plusieurs connexions TCP. Un PDP qui a une adresse et un numéro de port peut supporter plusieurs types de clients. Il est donc possible qu'un PEP ouvre plusieurs connexions avec plusieurs PDP. C'est le cas lorsque plusieurs PDP physiques séparés, et non logique dans un seul PDP, supportent différents types de clients. Il est important de noter que, pour une classe de clients donnée (client type), il ne peut exister qu'un PDP par domaine administratif. La figure S.14 illustre ce type d'architecture. L'éditeur de politique est généralement un ordinateur personnel qui permet d'entrer les politiques par l'intermédiaire d'un clavier.

Figure S.14
Architecture à plusieurs PDP



Pour distinguer les différents types de clients, le client est identifié dans chaque message. Les classes de clients peuvent se servir de données propres à leur classe et réclamer l'application de politiques spécifiques.

Le PEP doit passer par les étapes suivantes pour arriver à une décision politique :

1. Un événement local ou un message demande au PEP de se configurer suivant une politique particulière.
2. Le PEP créé une requête COPS contenant les informations provenant du message de demande d'admission et les éléments de politique à appliquer.

3. Le PEP peut consulter une base de données de configuration locale (Local Configuration Database) pour identifier un ensemble d'éléments de politique (Policy Element) qui peuvent être évalués localement. Le PEP passe alors la requête au LPDP (au cas où il en possède un), lequel, à son tour, renvoie une décision, appelée résultat partiel.
4. Le PEP émet une requête contenant tous les éléments de politique, accompagnés du résultat partiel du LPDP, vers le PDP, lequel prend la décision finale.
5. Le PDP retourne la décision finale au PEP et indique la politique à implémenter dans le nœud.

Le PDP doit éventuellement être informé de l'échec du LPDP en ce qui concerne la décision locale à prendre ainsi que de l'échec de l'admission, par manque de ressources, par exemple. Le PDP peut à tout moment envoyer des notifications au PEP pour demander une modification concernant une décision, générer une erreur de politique (Policy Error) ou envoyer un message d'avertissement (Warning Message).

La sécurité dans COPS

La sécurité dans COPS est négociée une fois pour toutes au début de la connexion et couvre ainsi toutes les communications utilisant cette connexion. Si une sécurité particulière est demandée pour une connexion, elle doit être négociée durant l'échange initial, pendant la phase CLIENT-OPEN/CLIENT-ACCEPT, en spécifiant un CLIENT-TYPE égal à zéro (CLIENT-TYPE = 0 est réservé à la négociation de la sécurité).

Si un PEP n'est pas configuré pour utiliser la version COPS Security avec un PDP, le PEP envoie tout simplement au PDP un message CLIENT-OPEN pour un CLIENT-TYPE disponible. Le PEP envoie sa demande de sécurité au PDP à l'aide d'un message CLIENT-OPEN possédant un CLIENT-TYPE = 0 avant même d'ouvrir un autre CLIENT-TYPE. Si le PDP reçoit un message CLIENT-OPEN avec un CLIENT-TYPE = 0 après qu'un autre CLIENT-TYPE a été ouvert avec succès, le PDP retourne un message CLIENT-CLOSE avec CLIENT-TYPE = 0 pour ce PEP.

Le premier message CLIENT-OPEN doit spécifier un CLIENT-TYPE = 0 et indiquer le PEP ID (identité du PEP) et l'objet d'intégrité de COPS. Cet objet d'intégrité contient un numéro de séquence initialisé par le PEP, que le PDP incrémente durant la communication suivant l'échange du message initial CLIENT-OPEN/CLIENT-ACCEPT. La valeur de l'ID identifie l'algorithme et la clé utilisés pour sécuriser la communication. Le PDP accepte l'algorithme et la clé de sécurité du PEP en validant le message reçu par le biais de la clé identifiée par la valeur de l'ID. Le PDP envoie alors au PEP un message CLIENT-ACCEPT avec un CLIENT-TYPE = 0 en portant un champ d'intégrité pour vérifier la correction de l'information. Cet objet d'intégrité contient le numéro de séquence initialisé par le PDP, numéro que le PEP doit incrémenter durant toute la communication avec le PDP. Ce numéro permet de bien séquencer les différents messages que s'échangent le PEP et le PDP.

Disponibilité d'un réseau d'opérateur

Dans un réseau d'opérateur, la fiabilité est une qualité essentielle. Nous avons représenté au tableau S.1 les temps d'indisponibilité d'un réseau en fonction du taux de disponibilité, c'est-à-dire la proportion du temps pendant lequel le réseau est disponible. La première colonne indique le taux de disponibilité et les colonnes suivantes le temps d'indisponibilité du réseau par mois et par an.

Les réseaux de télécommunications pour la téléphonie sont actuellement des réseaux « cinq neuf », c'est-à-dire avec un taux de disponibilité de 99,999. Ce taux représente des coupures du service téléphonique égales au total à 5 minutes par an. Actuellement, les réseaux des FAI n'offrent que « trois neuf » et donc un temps de panne de l'ordre de 9 heures par an, un temps beaucoup trop important pour un service téléphonique de qualité. Les opérateurs de télécommunications en mode IP doivent donc faire un énorme effort pour atteindre des taux de deux ordres supérieurs.

Plusieurs solutions pour atteindre des taux de disponibilité acceptables pour les applications utilisateur sont envisageables et même déjà en grande partie implémentées dans les grands réseaux d'opérateurs. La solution la plus utilisée est la réservation de chemins supplémentaires, ou chemins de back-up. Les chemins supplémentaires peuvent être soit réservés et disponibles en permanence, soit réservés mais utilisés par des flots qui cèdent leur place aux flots à sauvegarder.

Tableau S.1 • Taux d'indisponibilité d'une ligne ou d'un réseau

1	90 %	36,5 j/an	3 j/m	
2	99 %	3,65 j/an	7,3 h/m	
3	99,9 %	8,8 h/an	44 min/m	Bon ISP
4	99,99 %	53 min/an	4,4 min/m	
5	99,999 %	5 min/an	25 s/m	Téléphone
6	99,9999 %	32 s/an	3 s/m	

Une protection 1:*N* indique qu'une ligne en back-up est réservée pour *N* lignes en cours d'utilisation, la ligne en back-up pouvant elle-même être utilisée. Une protection 1+*N* indique qu'une ligne en back-up est réservée pour *N* lignes en cours d'utilisation, la ligne en back-up ne pouvant être utilisée que par les lignes à protéger. Plus généralement, une protection *M*:*N* ou *M*+*N* indique que *M* lignes en back-up sont réservées pour *N* lignes actives.

Pour arriver au « cinq neuf » dans un grand réseau où les paquets doivent passer par plusieurs routeurs, il faut protéger très fortement les chemins. En effet, le taux de panne pour une liaison en fibre optique de 1 000 kilomètres est de l'ordre de 0,3 p. 1000. Les pannes peuvent avoir de nombreuses raisons, dont la plus importante est la coupure pour travaux de génie civil. Si l'on compte un temps de réparation de 12 heures par panne, qui est déjà une valeur excellente, une redondance de 1:1 ne suffit pas à atteindre les « cinq neuf » car la probabilité que les chemins primaire et secondaire soient tous deux en panne est supérieure à 5 minutes par an. Il faut donc que la ligne de protection soit elle-même protégée.

Dans les réseaux traditionnels, la boucle locale est protégée dans le cadre de SONET par une reconfiguration qui s'effectue en 50 ms. Dans le réseau cœur, il y a toujours un chemin de rechange pour un chemin en panne. Quant à la partie entre le réseau métropolitain et l'utilisateur, sa fiabilisation s'effectue comme pour la téléphonie classique par le biais d'une alimentation indépendante du réseau électrique. Dans ce cas, il est facile d'atteindre les 99,999 %. Cependant, le prix de revient de cette fiabilisation du réseau est assez important, et les opérateurs IP hésitent du fait de la concurrence acharnée sur les prix.

SLA/SLS

Les opérateurs ont pour objectif de satisfaire les besoins de leurs clients en matière de réseau. C'est la raison pour laquelle leur première tâche est de connaître le plus précisément possible les demandes des clients. Ces demandes s'effectuent par le biais de SLA (Service Level Agreement).

Les réseaux d'opérateurs doivent en outre être en mesure de transformer ces demandes en une configuration des équipements et des lignes de transmission. Afin d'adapter leur réseau à la demande, les opérateurs ont presque tous opté pour des architectures avec signalisation. Cela consiste, avant d'envoyer le moindre paquet d'un utilisateur, à mettre en place des chemins, éventuellement avec réservation explicite de ressources. Parmi les différentes techniques de signalisation, MPLS est la plus populaire.

Une autre caractéristique importante de ces réseaux concerne l'interconnexion avec les autres opérateurs pour desservir tous les points du globe. C'est normalement le rôle de la normalisation de l'UIT-T. Cependant, cette normalisation est moins bien respectée aujourd'hui, compte tenu de la suprématie de l'IETF, qui ne spécifie pas toujours parfaitement certaines options, rendant les interconnexions entre opérateurs plus délicates.

L'objectif des opérateurs est de vendre un maximum de services à leurs clients. Les premiers d'entre eux sont évidemment la bande passante et les temps de réponse, ainsi que, de plus en plus, la sécurité, la gestion de la mobilité, l'optimisation, etc. Les réseaux privés virtuels, ou VPN (Virtual Private Network), font partie de la panoplie de solutions proposées par les opérateurs. Ce chapitre se penche sur la mise en place de ces réseaux et sur l'apparition de routeurs virtuels. Les opérateurs doivent rendre ces services de façon fiable. Le taux de disponibilité est donc un facteur important.

Le rôle d'un SLS de sécurité est de fournir les paramètres techniques du SLA pour la négociation de services de sécurité liés à la protection des données de l'utilisateur.

Comme pour le SLS de QoS, le temps de service (schedule) correspond à la durée en seconde pendant laquelle le service est assuré. Ici, le schedule peut aussi être défini en termes de quantité de trafic bénéficiant du service. Il s'exprime sous la forme de la durée divisée par la quantité d'information transportée.

Ce paramètre détermine les nœuds dans le réseau où l'opérateur peut appliquer le service de sécurité. La mise en place d'une association de sécurité, ou SA (Security Association), entre deux nœuds nécessite la configuration d'un service de sécurité sur ces deux nœuds.

Annexe T

27. Le contrôle de réseau

Cette annexe est consacrée à la qualité de service, dont il vise à donner une définition exacte. Elle détaille en outre les contrôles de flux dans le relais de trames et la commutation ATM, ainsi que la signalisation H.323, qui a été la principale signalisation de niveau application, avec une focalisation sur la parole téléphonique. La signalisation des « appliances » intermédiaires est ensuite abordée, avec le protocole MGCP, puis les signalisations COPS (Common Open Policy Service), qui permet de configurer un réseau de façon automatique, et CCITT n° 7.

La qualité de service (QoS)

Selon ces définitions, le contrôle de flux peut être considéré comme un cas particulier du contrôle de congestion. Tous deux permettent d'assurer une qualité de service, ou QoS (Quality of Service).

La qualité de service est définie par la recommandation E.800 de l'UIT-T de la façon suivante : « Effet collectif du service de performance qui détermine le degré de satisfaction d'un utilisateur du système. » Cette définition très générale est précisée dans la recommandation I.350, qui définit la QoS et la performance de réseau, ou NP (Network Performance).

La performance de réseau NP s'évalue en fonction de paramètres qui ont une signification pour l'opérateur du réseau et qui sont utilisés pour jauger le système, sa configuration, son fonctionnement et sa maintenance. La NP est définie indépendamment des performances du terminal et des actions de l'utilisateur. La qualité de service se mesure à l'aide de variables d'état, qui peuvent être directement observées et mesurées à l'endroit où l'utilisateur accède au service.

La figure T.1 illustre comment les concepts de QoS et de NP peuvent être appliqués dans un environnement réseau. De son côté, le tableau T.1 établit les distinctions entre QoS et NP.

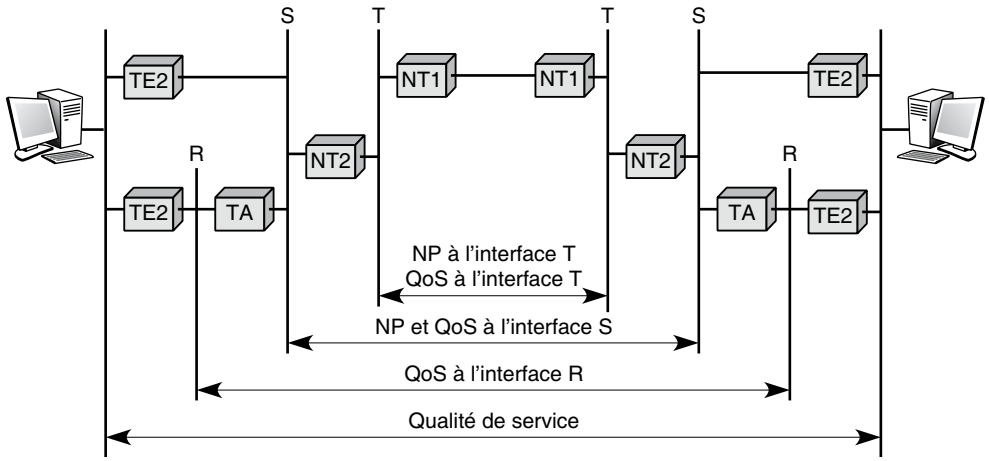


Figure T.1

Qualité de service (QoS) et performance du réseau (NP)

Tableau T.1 • Distinction entre QoS et NP

Qualité de service (QoS)	Performance du réseau (NP)
Orientée client	Orientée réseau
Attribut du service	Attribut de l'élément de connexion
Effet observable par l'utilisateur	Influe sur la planification, la gestion de performance et la maintenance.
Entre les points d'accès	Entre les deux points de la connexion réseau

Une matrice 3×3 a été développée par l'UIT-T dans l'annexe à la recommandation I.350 pour déterminer les paramètres à prendre en compte dans la valeur de la QoS et de la performance de réseau. Cette matrice est illustrée à la figure T.2. Elle détermine six zones, qui doivent être définies explicitement. Par exemple, si l'on examine la première colonne, il faut déterminer la capacité des accès, celle du transfert d'informations utilisateur et enfin la capacité maximale susceptible d'être gérée lors du désengagement d'un utilisateur. La deuxième colonne correspond aux paramètres qui permettent d'assurer la validité des actions d'accès, de transfert et de désengagement. La dernière colonne se préoccupe des paramètres qui assurent le fonctionnement sécurisé de l'accès, du transfert et du désengagement.

Figure T.2
Matrice 3×3 définissant QoS et NP

	Capacité	Validité	Sécurité de fonctionnement
Accès			
Transfert d'informations utilisateur			
Désengagement			

Le contrôle de flux est une des fonctionnalités essentielles du transfert de trames ou de paquets. Il s'agit de gérer les paquets de façon qu'ils arrivent au récepteur dans le laps de temps le plus court et surtout en évitant les pertes, en cas de surcharge, par écrasement dans les mémoires tampons des nœuds intermédiaires.

Le contrôle de congestion a pour objectif de sortir d'une congestion lorsque le contrôle de flux n'a pas permis de l'empêcher.

Le contrôle de flux s'effectue par une contrainte sur le nombre de paquets qui circulent dans le réseau. Cette limitation s'exerce soit sur le nombre de paquets en transit d'une entrée à une sortie ou sur l'ensemble du réseau, soit sur le nombre de paquets ayant le droit d'entrer à l'intérieur du réseau par unité de temps. À ces contrôles peuvent s'ajouter des techniques d'allocation des ressources, de façon à garantir qu'il n'y aura pas de congestion. Les sections qui suivent détaillent quelques-uns de ces contrôles de flux.

Le contrôle de flux dans le relais de trames

Le contrôle de flux dans le relais de trames est assuré par un contrat de trafic qui détermine en premier lieu un débit moyen à respecter par l'utilisateur, le CIR (Committed Information Rate). Ce contrôle très simple consiste à demander à l'utilisateur d'émettre un flux de débit constant, ou presque. Ainsi, l'opérateur connaît les flux qui transitent dans les nœuds de commutation et peut planifier l'ouverture ou le refus de nouvelles demandes de liaisons virtuelles. Précisons que le CIR doit être garanti pour des périodes de longueur *T.* Si *T* est relativement long, le trafic peut excéder le CIR pendant une partie de ce temps *T* et être en dessous dans une autre partie. Pour respecter cette moyenne, la quantité maximale d'informations que l'émetteur peut envoyer pendant le temps *T* est indiquée par $T \times \text{CIR} = \text{CBS}$ (Committed Burst Size).

Il est toutefois possible d'émettre des trames au-delà de la moyenne déterminée dans le contrat. Pendant une courte période de temps, le débit peut être supérieur à celui précisé dans le CIR. Cependant, le débit ne peut pas dépasser la valeur EIR (Excess Information Rate). Les trames engendrant un débit supérieur sont automatiquement détruites à l'entrée du réseau. Sur la période *T,* le trafic supplémentaire peut atteindre en moyenne la valeur EBS (Excess Burst Size), qui est égale à $T \times (\text{EIR} - \text{CIR}) = \text{EBS}$. En résumé, sur la période de longueur *T,* la quantité totale d'informations peut atteindre $T \times \text{EIR}$.

Comme nous venons de le voir, durant cette période *T,* l'utilisateur peut dépasser le trafic négocié dans le CIR, mais, à chaque dépassement de la valeur CIR, l'utilisateur se sert

du bit DE (Discard Eligibility) pour indiquer les trames supplémentaires qui forment la quantité EBS. L'utilisateur qui dépasse son contrat de trafic a intérêt à marquer les trames qui ne sont pas très importantes par rapport à la qualité de service, de façon que l'opérateur puisse les détruire dans le réseau en cas de surcharge. Le bit DE = 1 indique que la trame peut être détruite.

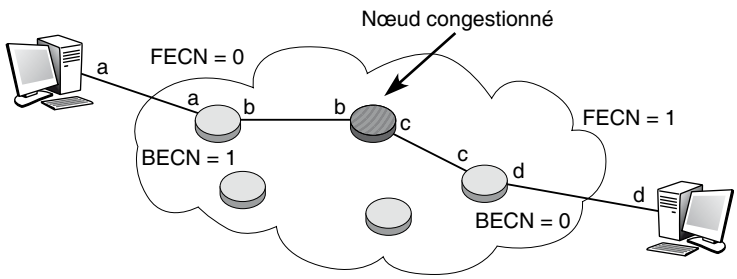
Deux bits supplémentaires ont été introduits dans la structure de trames pour permettre la mise en place d'un contrôle de flux :

- le bit FECN (Forward Explicit Congestion Notification) ;
- le bit BECN (Backward Explicit Congestion Notification).

Le premier de ces bits permet à un nœud congestionné de faire connaître son état au récepteur. Quant au second, il a pour fonction de faire remonter la connaissance de l'état de congestion d'un nœud à l'émetteur. La figure 27.14 illustre l'utilisation de ces deux bits. Le bit FECN est mis à 0 en sortant de l'émetteur avec la référence a. Lorsqu'il transite dans le nœud congestionné, il passe à la valeur 1 et arrive au récepteur avec la référence d en portant la valeur FECN = 1, qui indique au récepteur qu'un des nœuds traversés dans le circuit virtuel est congestionné. Dans l'autre sens, un processus analogue se produit : le bit BECN est mis à 0 en sortant de la station terminale. Ce bit est modifié par le nœud congestionné, qui le transforme en la valeur 1. À l'arrivée au récepteur, celui-ci prend conscience que la route sur lequel il envoie des trames possède un nœud congestionné.

Figure T.3

Contrôle de congestion dans le relais de trames



Les bits FECN et BECN sont toujours mis à 0, respectivement par l'émetteur et le récepteur, dans la structure de la trame émise sur la liaison virtuelle. Lorsque ces bits passent par un nœud congestionné, ils sont automatiquement mis à 1. Le récepteur et l'émetteur sont donc informés de l'état de congestion d'un nœud par la réception de ces deux bits à 1.

L'information concernant une congestion sur la liaison virtuelle est assez sommaire, puisque la seule chose qu'on sache est qu'un nœud a dépassé un certain seuil de trafic ou un nombre de mémoires tampons utilisées sur la liaison virtuelle. Les actions que doivent entreprendre l'émetteur et le récepteur sont totalement laissées à l'initiative de l'opérateur ou de l'utilisateur.

Il existe des intervalles de temps pendant lesquels aucune trame ne transite du récepteur vers l'émetteur. Dans ce cas, une trame de supervision, appelée CLLM (Consolidated Link Layer Management), est utilisée pour transporter des informations de supervision.

Cette trame permet à un nœud congestionné de diffuser vers ses voisins son état de congestion. Les nœuds voisins peuvent à leur tour avertir leurs voisins, et ainsi de suite. Cette trame de supervision est émise sur un circuit virtuel de numéro 1023 lorsque le DLCI est sur 2 octets.

Le contrôle de flux dans les réseaux ATM

Les réseaux ATM doivent pouvoir prendre en charge toutes les catégories de demandes de service possibles. Les récents progrès dans les domaines techniques de la commutation, du multiplexage et de la transmission par fibre optique ont rendu possible l'intégration de tous les types de services de communication, tels les services à haut débit et haute qualité, comme la TVHD ou le transfert de grands volumes de données à haute vitesse, mais aussi les services à faible débit et sans contrainte au niveau des erreurs, comme la parole téléphonique.

Les difficultés du contrôle de flux ATM proviennent des différentes qualités de service requises par tous ces services. L'efficacité de la gestion de la bande passante réalisée par le multiplexage statistique des services constitue l'un des avantages des réseaux ATM. Cependant, ce multiplexage à débit irrégulier peut créer des congestions internes.

Le multiplexage statistique et le contrôle des réseaux ATM

Dans un multiplexage statistique, une ligne du réseau peut être partagée par plusieurs circuits virtuels. L'allocation des ressources est réalisée de façon statistique. Le total des débits crêtes (Σp_i) des connexions se partageant la même liaison peut dépasser la bande passante (B) de la ligne :

- B : bande passante disponible ;
- p_i : débit crête de la connexion i ;
- n : nombre de connexions simultanées sur la ligne.

Le total des débits moyens (Σa_i) ne doit pas dépasser la bande passante de la source :

a_i = débit moyen de la connexion i.

Le gain réalisé par le multiplexage statistique peut être défini de la façon suivante :

L'augmentation du SMG est réalisée au prix d'une réduction de la qualité de service, exprimée sous la forme d'un délai de transit, d'un taux de perte ou d'une gigue (variation du délai de transfert par cellule). En règle générale, le SMG dépend du nombre de connexions et de la bande passante du conduit virtuel.

Prenons comme exemple les résultats de statistiques sur le comportement de la vidéoconférence, où le débit moyen est de 5 Mbit/s et le débit crête de 15 Mbit/s. Quand 16 connexions de vidéoconférence sont établies sur une ligne à 155 Mbit/s, le taux de perte est négligeable si 10 Mbit/s sont alloués à chaque connexion au lieu de 15 Mbit/s. Dans ce cas, la valeur du SMG est 1,5. Dans le cas d'un multiplexage de 30 sources, la bande passante requise s'approche de la somme des débits moyens, et la valeur du SMG atteint 3, mais avec un taux de perte de paquets important et des images projetées

sérieusement endommagées. Le contrôle d'admission de connexion, ou CAC (Connection Admission Control), doit décider si une nouvelle demande de connexion est acceptable ou non en considérant la charge du réseau, la bande passante disponible, les descripteurs de trafic de la nouvelle connexion et la QoS requise.

De très grands débits sont possibles dans les réseaux ATM grâce aux fonctions simplifiées des nœuds intermédiaires. En fait, il n'y a pas de contrôle de flux au niveau de la couche ATM, ce qui nécessite l'application de certaines stratégies de contrôle pour limiter des trafics entrants dans le réseau. On peut dire que les stratégies de contrôle de congestion pour les réseaux ATM sont plutôt préventives que réactives.

Pour certains types de données sensibles aux pertes mais peu exigeants en délais de propagation (données de types 3/4 ou 5 de la couche AAL), on peut utiliser un mécanisme de contrôle de flux au niveau de la couche AAL ou d'une couche supérieure. Ce mécanisme peut être utilisé soit comme une méthode de reprise des cellules erronées ou perdues, soit comme une méthode de contrôle de flux réactive sur une congestion, soit encore comme une méthode de synchronisation entre l'émetteur et le récepteur. Dans le cas où une méthode de contrôle de flux réactive est utilisée, un nombre suffisant de tampon est exigé pour les services de données dans les nœuds intermédiaires. Ainsi, les cellules éventuellement bloquées lors des débordements peuvent être reçues. Pour les services temps réel, un nombre trop important de tampons peut dégrader le temps de réponse. Même pour ce type de service, le contrôle de flux de bout en bout peut améliorer l'utilisation des ressources et le taux de perte des cellules.

La mise en œuvre des techniques de contrôle de congestion dépend des types de commutateurs utilisés. Par exemple, l'ordonnancement des priorités dans un commutateur est inutile si ce dernier ne dispose pas de mémoire tampon. Même s'il existe des mémoires tampons dans le commutateur, les performances sont influencées par plusieurs facteurs, tels que la taille de la mémoire, l'architecture du commutateur, le type de mémoire, etc.

Un développement réussi des méthodes de contrôle du réseau ATM exige des interactions douces entre les méthodes de contrôle de congestion, les fonctions OAM (Operations And Maintenance), les mécanismes de transport VC/VP, les commutateurs ATM, etc.

La qualité de service et le contrôle d'admission

Le groupe d'étude XVIII de l'UIT-T a énormément travaillé sur le problème du contrôle de flux dans les réseaux ATM, car c'était un élément stratégique pour le succès de cette technique de transfert.

Rappelons que le mode de transfert temporel asynchrone ATM (Asynchronous Transfer Mode) est le mode de transfert cible pour le RNIS large bande. L'information est transmise dans des blocs de taille fixe (53 octets), appelés cellules, chacune d'elles étant constituée d'un en-tête de 5 octets et d'un champ d'information de 48 octets. Les cellules sont transmises dans un circuit virtuel, et le routage se fonde sur l'identificateur de voie virtuelle VCI (Virtual Channel Identifier) et l'identificateur de conduit virtuel VPI (Virtual Path Identifier) de l'en-tête de la cellule. Le réseau ATM adopte une architecture simplifiée, fondée sur une commutation de cellules en mode avec connexion. Il n'y a ni

contrôle d'erreur, ni contrôle de flux au niveau de la couche ATM. L'acheminement des cellules n'est pas dynamique. Les cellules appartenant à une même connexion sont transportées en séquence à travers le réseau, le long d'un circuit virtuel.

L'ATM a été choisi comme mode de transfert pour le RNIS large bande au détriment de son concurrent, le mode de transfert temporel synchrone, ou STM (Synchronous Transfer Mode), en raison du gain économique qu'il apporte grâce au multiplexage statistique. Cependant, le multiplexage statistique de trafic en rafale peut provoquer des problèmes de congestion. Les travaux de l'UIT-T visent à minimiser cette congestion et à maximiser le taux d'utilisation du réseau, tout en garantissant la qualité de service spécifiée par l'utilisateur. Ces efforts ont abouti à la définition d'un contrat de trafic dépendant de la qualité de service requise par l'utilisateur et à la normalisation des fonctions de gestion de trafic.

Avant d'examiner plus avant ces fonctions, définissons la qualité de service. Une classe de qualité de service peut préciser des paramètres de performance (QoS spécifiée) ou non (QoS non spécifiée). Dans ce dernier cas, on parle de service best-effort, c'est-à-dire du meilleur effort possible de la part du réseau pour satisfaire la demande de l'utilisateur.

L'utilisateur et l'opérateur du réseau ATM négocient, *via* l'interface UNI, un contrat de trafic. Ce contrat de trafic doit contenir une classe de QoS, un descripteur de trafic sur la connexion demandée et une définition de la conformité.

Le descripteur de trafic est un sous-ensemble des paramètres de trafic qui servent à décrire les caractéristiques du trafic des cellules sur la connexion. Ce descripteur contient un nombre de variable qui diffère selon qu'il s'agit des recommandations de l'UIT-T ou des propositions de l'ATM Forum.

Les variables UITT sont les suivantes :

- Descripteur du trafic source, qui peut lui-même contenir :
  - le débit crête PCR (Peak Cell Rate) ;
  - le débit projeté SCR (Sustainable Cell Rate).
- Durée des rafales tolérées BT (Burst Tolerance).
- Tolérance de gigue CDV (Cell Delay Variation).
- Algorithme du taux de génération des cellules GCRA (Generic Cell Rate Algorithm), qui définit la conformité du trafic. Deux paramètres sont utilisés : le temps minimal entre deux émissions de cellule et une capacité de mémorisation maximale. Lorsqu'une cellule se présente et que la capacité maximale est atteinte (cellule non conforme), soit cette cellule est détruite, soit elle est émise en surplus, soit elle prend la place d'une autre cellule, qui, elle-même, peut être détruite ou envoyée en surplus. C'est là que le bit CLP devient opérationnel : si la cellule est envoyée en surplus, elle est marquée par le bit CLP = 1, qui permet à un nœud interne du réseau de la détruire en cas de congestion. Il y a donc deux classes de priorité : CLP = 0, qui correspond aux cellules les plus prioritaires, et CLP = 1, pour les cellules pouvant être détruites dans le réseau.
- Paramètres expérimentaux, qui permettent de faire passer dans la demande des caractéristiques spécifiques, correspondant le plus souvent à des propriétés propres à des constructeurs.

L'ATM Forum a déterminé un ensemble de combinaisons de paramètres de trafic pour simplifier les demandes. Le bit CLP est égal soit à 0, soit à 0 ou 1, ce que nous indiquons respectivement par CLP = 0 et CLP = 0 + 1 :

- PCR pour CLP = 0 et PCR pour CLP = 0 + 1 ;
- PCR pour CLP = 0 et PCR pour CLP = 0 + 1 avec un marquage demandé par le réseau en cas de cellule non conforme ;
- SCR pour CLP = 0 et PCR et BT pour CLP = 0 + 1 ;
- SCR pour CLP = 0 et PCR et BT pour CLP = 0 + 1 avec marquage ;
- PCR pour toutes les cellules CLP = 0 + 1 ;
- PCR, SCR et BT pour toutes les cellules CLP = 0 + 1 ;
- Best-effort service, PRC pour toutes les cellules CLP = 0 + 1.

Le contrôle d'admission de connexion

On désigne par contrôle d'admission de connexion, ou CAC, l'ensemble des actions exécutées par le réseau au cours de la mise en place de la connexion pour déterminer si cette demande de connexion doit être acceptée ou refusée. La demande d'ouverture de la connexion fait partie de la demande CAC. C'est la principale méthode de contrôle de congestion préventive dans les réseaux ATM.

Cette méthode permet d'accepter ou de rejeter une nouvelle demande de connexion en considérant la bande passante disponible, le descripteur de trafic de la nouvelle connexion et son exigence en terme de qualité de service. L'objectif du CAC est d'accepter une nouvelle connexion si les ressources sont suffisantes et d'assurer la qualité de service demandée pour les connexions déjà ouvertes.

Dans les réseaux de type STM, la décision est simple. Si la somme des débits crête, comprenant le débit crête de la nouvelle demande de connexion sur un VP ou sur une liaison donnée, ne dépasse pas la bande passante disponible comme l'indique la formule suivante :

la demande d'une nouvelle connexion est acceptée.

Cette approche simple peut être adoptée pour toutes les sources de trafic de VBR, ou débit binaire variable, et de CBR, ou débit binaire constant. Cependant, il est possible d'obtenir une utilisation optimisée des ressources par le multiplexage statistique de sources de trafic VBR.

Puisque le réseau ATM doit supporter des VC avec des exigences diverses de QoS (délai d'établissement d'une connexion, taux de perte des cellules, délai de transmission, etc.), la conception de méthodes CAC efficaces est complexe. La méthode la plus simple pour s'attaquer à ce problème, tout en satisfaisant les diverses demandes de QoS, consiste à classer les sources de trafic en fonction de leurs caractéristiques, des exigences de QoS, etc. Ensuite, la bande passante d'une liaison ou d'un VP est allouée pour chaque classe et contrôlée indépendamment.

Les techniques de contrôle de flux ATM

De nombreuses techniques de contrôle de flux ont été définies par l'UIT-T pour l'ATM :

- Le contrôle des paramètres de l'utilisateur et du réseau UPC/NPC (Usage Parameter Control/Network Parameter Control) regroupe l'ensemble des actions exécutées par le réseau pour surveiller et gérer le trafic offert à l'accès utilisateur et à la conformité de la connexion ouverte à l'accès réseau. Le principal objet de cette technique est de protéger le réseau contre des violations du contrat de trafic pouvant conduire à une dégradation de la qualité de service sur des connexions d'autres utilisateurs.
- La gestion de priorité par l'utilisateur peut employer deux classes de services pour la perte des cellules. Si le bit CLP est à 0, la cellule est prioritaire. Si cet élément binaire est 1, la cellule est moins prioritaire et peut être détruite dans un nœud congestionné.
- La gestion des ressources du réseau NRM (Network Resource Management) regroupe les prévisions d'attribution des ressources du réseau pour optimiser la séparation des trafics en fonction des caractéristiques du service.
- Les techniques de rétroaction (feed-back) forment l'ensemble des actions exécutées par les usagers et le réseau pour réguler le trafic sur les connexions ATM.

Parmi les méthodes de gestion de trafic permettant d'éviter les surcharges du réseau, on trouve les mécanismes de contrôle de trafic visant à rendre le trafic conforme au contrat de trafic (traffic shaper), les protocoles de réservation rapide FRP (Fast Reservation Protocol) et EFCI/BCN (Explicit Forward Congestion Indication/Backward Congestion Notification).

Le défi est toujours de concevoir des mécanismes de contrôle de flux qui permettent d'utiliser efficacement les ressources du réseau et de satisfaire la qualité de service requise. Dans les réseaux traditionnels, c'est le mécanisme de contrôle de flux par fenêtre qui est surtout utilisé. Dans les réseaux ATM, en revanche, du fait que le délai de propagation est très long par rapport au temps d'émission, les protocoles de type « envoyer et attendre » ne sont pas performants. Plusieurs autres méthodes de contrôle de flux adaptatif peuvent également être implémentées au niveau de la couche AAL ou à un niveau supérieur. En règle générale, ces contrôles travaillent sur la taille de la fenêtre, ou sur le débit, la valeur des paramètres étant décidée par le nœud destinataire en fonction de l'état du réseau.

Les hypothèses implicites à ce système, telles que la connaissance de l'état du réseau ou le temps de propagation suffisamment court pour faire un aller-retour de l'information sur l'état du réseau, posent toutefois problème. Même si une congestion dans le réseau est détectée, il est difficile de prévoir sa durée, de localiser à temps le nœud congestionné, de mesurer l'importance de la congestion et donc d'en déduire la taille de la fenêtre.

Plusieurs contrôles d'accès et de trafic ont été définis par l'UIT-T. Le rôle du contrôle des paramètres de l'utilisateur et du réseau UPC/NPC est de protéger les ressources réseau contre des utilisateurs malveillants et des fonctionnements involontaires susceptibles de dégrader la qualité de service des connexions établies auparavant. L'UPC/NPC a pour fonction de détecter les violations des contrats et d'exécuter les fonctions appropriées.

Pour éviter les pertes de cellules causées au niveau UPC/NPC, l'émulation de l'UPC/NPC peut être réalisée au niveau de l'émetteur. Cette fonction est appelée STS (Source Traffic Smoothing) pour la distinguer de l'UPC/NPC. Du point de vue de l'utilisateur, la fonction STS présente des inconvénients puisqu'elle introduit un délai supplémentaire et nécessite des mémoires tampons supplémentaires.

L'algorithme VSA (Virtual Scheduling Algorithm) recommandé dans la norme I.371 représente une première possibilité pour détecter les situations irrégulières et redonner un flux acceptable par le contrat de trafic. Il a pour rôle de surveiller le débit crête d'une connexion ATM tout en garantissant une limite sur la gigue. En termes simplifiés, si une cellule arrive plus tôt que prévu, elle est mise en attente jusqu'à l'instant où elle aurait dû arriver. À ce moment seulement, elle est émise sur le réseau et est conforme. Si la cellule arrive plus tard que prévu, soit elle arrive dans un intervalle suffisamment court pour rester conforme à la gigue — elle est alors conforme —, soit elle arrive trop tard pour rester dans la limite acceptable et est jugée non conforme. Les cellules conformes sont indiquées par CLP = 0, et les cellules non conformes par CLP = 1.

Le leaky-bucket est un autre mécanisme de l'UPC/NPC et du STS. Il est composé d'un compteur (*c*), d'un seuil (*t*) et d'un taux de vidage, le leaky-rate (*l*). Le compteur est incrémenté chaque fois qu'une cellule arrive dans le tampon et décrémenté par le leaky-rate. Si une cellule arrive au moment où la valeur du compteur est égale au seuil, elle n'est pas mémorisée dans le tampon. En d'autres termes, quand le tampon est plein, la cellule qui arrive est rejetée.

Si le débit crête de la source est *p* et la durée de la rafale *b,* le compteur est augmenté à la fin de la rafale de la façon suivante :

$c = c + b\ (p - 1)$ si cette valeur est inférieure à *t,* sinon $c = t$.

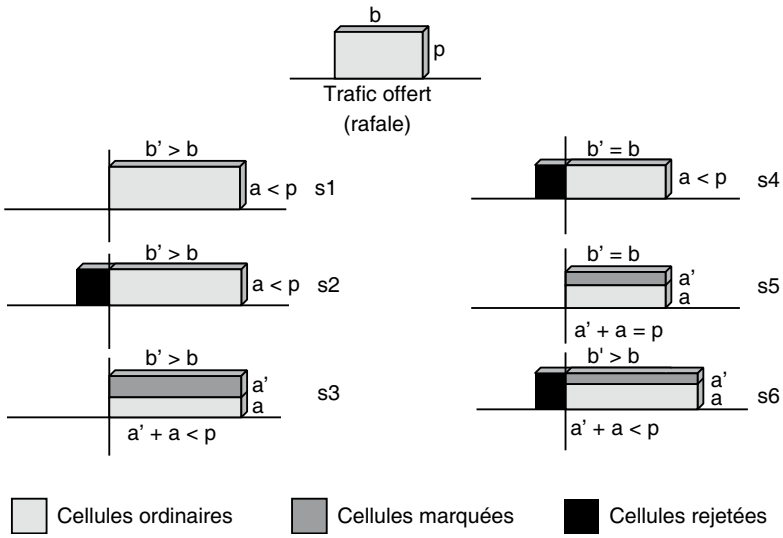
Pendant la durée d'un silence de longueur *s,* le compteur est diminué comme suit :

$c = c - sl$ si cette valeur est supérieure à 0, sinon c = 0.

Un trafic en avalanche peut être transformé en l'une des formes illustrées à la figure T.4. Ces formes sont dessinées sans qu'il soit tenu compte de la séquence réelle des cellules détruites ou marquées. Les hauteurs a et a' correspondent respectivement au débit conforme (cellules ordinaires) et au débit non conforme (cellules marquées). La longueur b' correspond à la durée de la rafale après la mise en forme par le leaky-bucket. Les paramètres b et p représentent respectivement la longueur de la rafale et le débit crête du trafic offert au leaky-bucket. Un choix approprié des valeurs des paramètres l et b permet de redonner au trafic la forme désirée. Par exemple : un service de données sensible aux pertes mais qui tolère des délais peut être remis en forme (*s*1 sur la figure). Cette fonction peut être exécutée dans un terminal afin de respecter le contrat de trafic. Dans ce cas, un tampon suffisamment grand est nécessaire pour le terminal. Si l'état du réseau est connu à temps, la perte des cellules peut être évitée grâce au contrôle dynamique du débit du leaky-bucket (leaky-rate).

Un délai inacceptable peut provenir d'une attente trop longue dans une grande mémoire tampon. Pour les services sensibles au délai, comme la vidéo ou la parole téléphonique, le choix des formes s2, s3, s4 ou s5 est préférable.

Figure T.4
Effet de contrôle du leaky-bucket



Le contrôle de flux des classes de services ATM étant détaillé au chapitre 13, nous ne le reprenons pas ici.

La signalisation H.323

En 1996, l'UIT (Union Internationale des Télécommunications) proposa la famille de protocoles H.32x, très fortement soutenue par Microsoft et Intel. L'UIT parvint rapidement à convaincre les différents équipementiers et fournisseurs de services de la nécessité d'adopter pour norme commune ces protocoles H.32x.

Sans être précurseurs ni de la téléphonie, ni de la vidéo, ni même de la conférence, ces protocoles constituent l'initiative la plus aboutie et la plus marquante des débuts de la signalisation multimédia. La généralisation progressive et systématique de H.323 a fini par faire céder les plus récalcitrants des acteurs du multimédia, qui ont abandonné leurs solutions propriétaires, pourtant très évoluées. La ToIP (Telephony over IP) trouvait là son protocole fédérateur et pouvait prendre son envol.

Les premiers travaux sur H.323 ont débuté en mai 1995. Depuis lors, six versions standardisées se sont succédé, apportant leurs lots de nouveautés et d'améliorations.

Initialement prévue dans le cadre très restreint des réseaux locaux n'apportant aucune garantie de qualité de service, la version 1 de la recommandation H.323 de l'IUT-T prit le nom de « Systèmes et équipements visiophoniques pour réseaux locaux offrant une qualité de service non garantie ». Il faudra attendre les versions suivantes pour qu'elle soit renommée « Système de communication multimédia fonctionnant en mode paquet ». Tout porte à croire que ses concepteurs n'avaient pas imaginé rencontrer un tel succès auprès des industriels, et que le protocole a ensuite évolué pour adresser des réseaux plus étendus, de type Internet.

Cette version balbutiante présentait de sévères limitations, notamment des performances, illustrées, par exemple, par la lenteur de la mise en place d'une communication ou la sécurité, totalement absente. Surtout, la spécification était imprécise quant à la manière d'implémenter le protocole, ce qui entraîna d'importants problèmes d'interopérabilité entre les différents constructeurs.

Remarquable à bien des égards, la version 2 (1998) améliora considérablement un protocole encore instable et perfectible, en particulier les délais d'établissement d'une communication grâce à la procédure de FastConnect, qui permettait de paralléliser les annonces.

Une autre nouveauté fut incarnée par la procédure H.245 tunneling, qui permettait d'encapsuler des messages H.245 dans des messages H.225.0 (Q.931). De nouveaux services étaient supportés par le protocole, dont les classiques services de renvoi et de transfert d'appel, et des mécanismes de sécurité étaient rassemblés dans la spécification H.235. Cette dernière couvrait la plupart des mécanismes de sécurité, incluant l'authentification et le cryptage des flux de données.

Des paramètres de gestion de la qualité de service étaient ajoutés dans les messages de signalisation, permettant de s'intégrer dans une architecture de type DiffServ ou RSVP, par exemple. Néanmoins, la gestion elle-même de la qualité de service ne faisait pas partie du protocole, H.323 n'offrant aucune garantie de réservation de ressources. Seuls des paramètres de qualité de service pouvaient être ajoutés dans la structure des paquets et pouvaient être utilisés par les terminaux. Au niveau du réseau cœur, ces paramètres devaient être exploités et traités par des mécanismes externes au protocole.

Plus généralement, la manière d'ajouter des services supplémentaires était décrite dans le document H.450.1, qui définissait une plate-forme générique.

Les documents suivants, numérotés H.450.x ($x > 1$) décrivent de tels services :

- H.450.2 détaille le service de transfert d'appel, qui transforme une communication entre deux postes A et B en une communication entre A et un autre poste C. Elle est classiquement utilisée dans les entreprises pour mettre l'appelant en relation avec la personne souhaitée.
- H.450.2 détaille le service de redirection d'appel, qui remplace un poste appelé par un autre, avec ou sans condition.

Grâce au support du DTMF (Dual-Tone Multi-Frequency), le protocole H.323 version 2 permettait la création de nouveaux services vocaux. Au contraire de la téléphonie par impulsion, les codes DTMF correspondent à des fréquences. En assignant à chaque touche du terminal un code DTMF unique, il devenait possible à un serveur d'interpréter les saisies de l'utilisateur appelant et de lui fournir un service adéquat en retour. Auparavant, les messages de signalisation ne transmettaient qu'une partie de ces informations DTMF, ce qui ne permettait pas d'interpréter pleinement ces signaux.

Enfin, la recommandation H.323 permettait d'utiliser des alias à la place des adresses IP afin d'identifier les utilisateurs. Ces alias respectent le format des URL traditionnellement utilisées pour désigner une ressource unique sur Internet.

Globalement, la version 3 de H.323 (1999) a apporté moins de nouveautés fondamentales que la précédente. Si la version 2 corrigeait en profondeur plusieurs imperfections de la norme initiale, la 3 contribuait à l'amélioration du protocole, sans le bouleverser en profondeur.

Retenons notamment les trois améliorations suivantes de cette version :

- Gestion de nouveaux services complétant la gamme existante, tels que les suivants :
  - CLIP (Connected Line Identification Presentation), ou présentation de l'identification de l'appel, aussi connu par son appellation commerciale d'affichage du numéro, qui permet à l'appelé de connaître le numéro d'appel de l'appelant.
  - CLIR (Connected Line Identification Restriction), ou restriction de l'identification de l'appel, plus connu sous son appellation commerciale de masquage du numéro, qui permet à l'appelant de limiter les possibilités d'identification de son numéro.
- Ajout de services destinés à compléter la série H.450.x, tels que la mise en attente ou la notification d'appel ou de message en attente.
- Intégration avec la signalisation SS7, utilisée classiquement dans les réseaux téléphoniques commutés.

L'annexe E de la norme prévoyait l'utilisation du protocole de transport UDP au lieu de TCP, les deux protocoles pouvant être utilisés au choix.

La version 4 (2000) a axé ses développements sur la robustesse, à la fois en terme de passage à l'échelle (scalabilité), de flexibilité et de fiabilité. Le protocole confirmait ainsi sa suprématie par une technologie solide et véritablement en phase avec les besoins et les usages de tous types, y compris professionnels. La recommandation proposait pour cela des changements radicaux par rapport aux versions précédentes.

Afin d'offrir un cadre de développement stable à la norme, cette version 4 proposait de formaliser les améliorations sous forme d'extensions au protocole, mais sans modifier ses fondations. Autrement dit, les améliorations ne remettaient plus en cause le principe de fonctionnement du protocole mais se présentaient sous la forme de modules génériques, appelées GEF (Generic Extensibility Framework).

Le protocole H.323 devenait de la sorte stable, tout en autorisant des enrichissements progressifs. Il offrait en outre un bon niveau de souplesse puisque les équipementiers étaient libres d'implémenter certaines extensions des GEF et pas d'autres, tout en restant compatibles avec le socle du standard. De fait, le protocole atteignait une certaine maturité, et ses acteurs n'étaient plus obligés de suivre en permanence les évolutions et de mettre à jour la norme pour garantir la compatibilité.

La notion de *gatekeeper alternative,* permettant le basculement des appels en cas de panne d'un gatekeeper, ou « garde-barrière », était explicitée dans le document. À cette fin, l'annexe R proposait des mécanismes permettant de modifier dynamiquement le routage des appels en cas de panne.

Dans cette version, le protocole H.323 se rapprochait du protocole MGCP (Media Gateway Control Protocol), dont les travaux étaient menés en parallèle. Il offrait en effet une nouvelle conception architecturale, qui décomposait l'équipement de passerelle

originale, jugé trop lourd, en deux sous-parties. Cette nouvelle répartition reprenait le modèle proposé conjointement entre le groupe de travail numéro 16 de l'IUT-T et le groupe de travail MEGACO de l'IETF. L'IUT en proposera une nouvelle recommandation, numérotée H.248, que nous détaillons ultérieurement dans ce chapitre.

Le protocole RTP (Real-time Transport Protocol) permet de séparer les flux audio et vidéo, ce qui offre aux récepteurs une plus grande flexibilité en leur permettant de choisir indifféremment de recevoir l'un ou l'autre, avec un système de priorité. L'inconvénient de ce système est que le récepteur doit synchroniser les deux flux pour transmettre de façon parfaitement homogène la diffusion du son avec la vidéo en simultané. Cela suppose des capacités complémentaires, à la fois de l'émetteur, qui sépare la voix de la vidéo, et du récepteur, qui assure la synchronisation des deux flux.

Avec la version 4 de H.323, le protocole proposait une solution de rechange facultative permettant de multiplexer la voix et la vidéo dans un même flux, de manière que l'émetteur n'ait plus à se soucier de la synchronisation de la vidéo par rapport à la voix et qu'il puisse jouer les données sans que des décalages du son et de l'image soient perceptibles.

En plus de proposer la gestion de nouveaux services, la version 4 permettait la mobilité de l'utilisateur et l'intégration avec les réseaux GSM et UTMS. En outre, le concept « d'enregistrements additionnels » donnait aux utilisateurs la possibilité de s'enregistrer plusieurs fois auprès des gatekeepers avec plusieurs pseudonymes différents. Les paquets UDP étant trop courts pour permettre de spécifier dans une même requête tous les pseudonymes à enregistrer, ce mécanisme d'enregistrements additionnels permettait de générer à la suite plusieurs courtes requêtes venant compléter les précédents enregistrements.

L'adressage H.323 était fixé, et une URL H.323 pouvait désormais prendre la forme *h323:utilisateur@domaine*, où le préfixe *h323* spécifiait qu'il s'agissait d'une adresse à interpréter par le protocole H.323, la partie *utilisateur* était un identifiant de l'utilisateur (ou éventuellement d'un service) et la partie *domaine* désignait l'entité capable de traduire cette URL, classiquement le gatekeeper susceptible de prendre en charge la résolution de cette adresse. La façon de résoudre effectivement cette adresse ne sera donnée que dans la version suivante.

La version 5, de 2002, est mineure par rapport aux précédentes. On peut la considérer comme une version de maintenance, qui répondait à un certain nombre de demandes et besoins. Reprenant la philosophie de stabilité initialisée par la version 4, avec le cadre générique des GEF, cette version 5 proposait des améliorations, avec la série de recommandations H.460.x, dont le tout premier document, H.460.1, expliquait ce nouveau dispositif. La recommandation H.460.9 permettait quant à elle aux terminaux de fournir les statistiques RTCP.

L'annexe O expliquait comment utiliser les serveurs de domaines DNS (Domaine Name Server) pour effectuer les résolutions de noms des adresses (URL) utilisées dans les identifications des abonnés H.323. L'interrogation des serveurs DNS pouvait s'effectuer selon différents procédés, tel ENUM (tElephone NUmber Mapping), qui associe un nom identifiant un utilisateur (par exemple l'utilisateur dont l'identifiant est *albert@exemple.com*) avec un numéro de téléphone conventionnel (au format à dix chiffres, comme

0102030405), ou A Record (Address Record), qui associe un nom d'utilisateur avec une adresse IP (192.168.1.15 pour une adresse en réseau local, par exemple).

La version 5 gérait le protocole SCTP (Stream Control Transmission Protocol) comme solution de rechange aux protocoles de transport TCP et UDP.

Au centre de la version 6, de 2006, on retrouve une philosophie modulaire, avec de multiples perfectionnements et des procédures simplifiées et épurées, destinées à rendre H.323 encore plus accessible. Quelques améliorations sont aussi proposées, comme des supports plus larges, par exemple, de codecs (GSM, iLBC et H.264 sont pris en charge) ou de spécifications de QoS (H.361 notamment).

Le concept de *gatekeeper affectée,* imposant un gatekeeper fixe à un terminal, complète celui de *gatekeeper alternatif* offert depuis la version 4. En termes de sécurité, les mécanismes sont complètement refondus. Le document de référence H.235 est restructuré et décomposé en plusieurs recommandations, numérotées de H.235.0 à H.235.9.

Les recommandations H.460.17, H.460.18 et H.460.18 répondent au problème de la traversée des réseaux avec translation d'adresse IP, ou NAT (Network Address Translation) et des filtres pare-feu, qui pénalisaient le protocole H.323. Pendant longtemps, les communications H.323 ne pouvaient en effet être mises en place dans les entreprises utilisant un plan d'adressage privé et des solutions de pare-feu, car le protocole H.323 utilise des ports dynamiques qui ne sont généralement pas supportés par les pare-feu ordinaires.

La translation des adressages privés et logiciels des pare-feu est une solution déployée aujourd'hui presque systématiquement dans les entreprises, ainsi que bien souvent chez les particuliers. Si certains pare-feu perfectionnés et onéreux proposent des méthodes propriétaires pour permettre aux flux H.323 d'être filtrés correctement, la solution générale n'est véritablement donnée que dans ces nouvelles recommandations H.460.

Ces dernières spécifient les procédures à implémenter dans les gatekeepers et les terminaux pour passer les translations d'adresses et traverser les pare-feu. Le principe de ces procédures est de conserver une connexion persistante TCP entre les terminaux et le gatekeeper pour assurer les communications.

Une nouvelle entité est introduite pour permettre aux terminaux n'implémentant pas encore les procédures de la version 6 de H.323 de traverser quand même les réseaux nattés et filtrés. Il s'agit en ce cas d'un proxy particulier auquel s'adressent les terminaux et qui agit comme un intermédiaire pour relayer les messages de signalisation vers leur destinataire. En quelque sorte, si les terminaux n'arrivent pas à joindre leurs correspondants parce que leurs flux sont difficilement interprétés, le proxy interprète et reformate les flux avant de les envoyer vers leur destinataire. Ces derniers utilisent eux aussi le proxy afin que leurs flux soient conformes à ce qu'attendent les émetteurs.

Architecture et fonctionnalités du protocole H.323

Le protocole H.323 s'articule autour d'une architecture particulière décrite dans ce qui suit. Cette architecture concentre les fonctionnalités autour d'entités, et, pour cette raison, le protocole H.323 est considéré comme fortement centralisé. Nous allons définir et détailler chacune des entités introduites par le protocole H.323.

Les quatre entités d'une architecture H.323

Le protocole H.323 axe très fortement ses communications sur une typologie d'équipements en proposant une architecture sur laquelle se fonde son fonctionnement.

La terminologie anglaise étant couramment employée dans les documentations françaises, il convient de la connaître. Dans ce qui suit, les premiers termes donnés peuvent être considérés comme les plus courants.

Une architecture H.323 est généralement composée des quatre catégories d'entités suivantes :

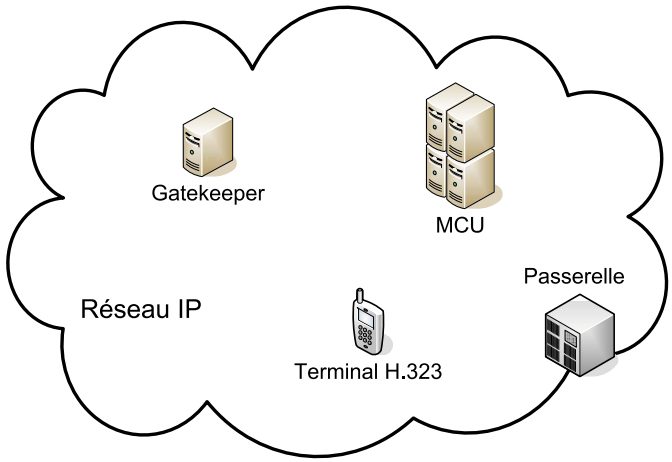
- Terminaux (au minimum deux). Ce sont les équipements de traitement destinés aux utilisateurs, leur permettant d'émettre et de recevoir des appels. Deux terminaux doivent au minimum être présents pour qu'une communication ait lieu.
- Gatekeeper, ou garde-barrière. C'est l'équipement permettant la localisation des utilisateurs. Ces derniers peuvent s'identifier entre eux par des noms, auxquels il faut attribuer l'adresse IP correspondante dans le réseau ou, si l'appelé n'est pas situé dans un réseau IP, la localisation de l'entité intermédiaire à joindre pour l'appel. Outre cette fonction primordiale, un gatekeeper remplit tout un ensemble de fonctions complémentaires de gestion et de contrôle des communications, certaines étant indispensables et d'autres facultatives.
- Passerelle, ou gateway. C'est l'équipement permettant à des utilisateurs du réseau IP de joindre les utilisateurs qui sont actifs sur d'autres types de réseaux téléphoniques, RTC, RNIS ou RTC. On peut avoir autant de passerelles différentes que nécessaire, suivant la nature des réseaux non-IP à interconnecter.
- MCU (Multipoint Control Unit), ou unité de contrôle multipoint, parfois appelée pont multipoint. C'est l'équipement permettant la gestion des conférences, c'est-à-dire les communications multimédias mettant en jeu plus de deux interlocuteurs. Ces derniers doivent préalablement se connecter à la MCU, sur laquelle s'établissent les demandes et négociations des paramètres à utiliser lors de la conférence.

Ces quatre entités sont illustrées à la figure T.5.

Avant de détailler chacune de ces entités, les deux définitions suivantes doivent être connues :

- **Points de terminaison.** Terminaux, gateway et MCU sont des entités auxquelles les émetteurs peuvent s'adresser directement pour communiquer. Contrairement au gatekeeper, qui joue un rôle intermédiaire de contrôle et de gestion, ces entités sont des points de terminaison des appels (aussi appelés endpoints).
- **Zone et système H.323.** La nomenclature H.323 définit deux notions qu'il convient de bien connaître et différencier :
  - Un système H.323 est défini comme un ensemble de deux terminaux au minimum, d'autres éléments pouvant être ajoutés.
  - Une zone H.323 est un ensemble de deux terminaux avec un gatekeeper au minimum, d'autres éléments pouvant être ajoutés.

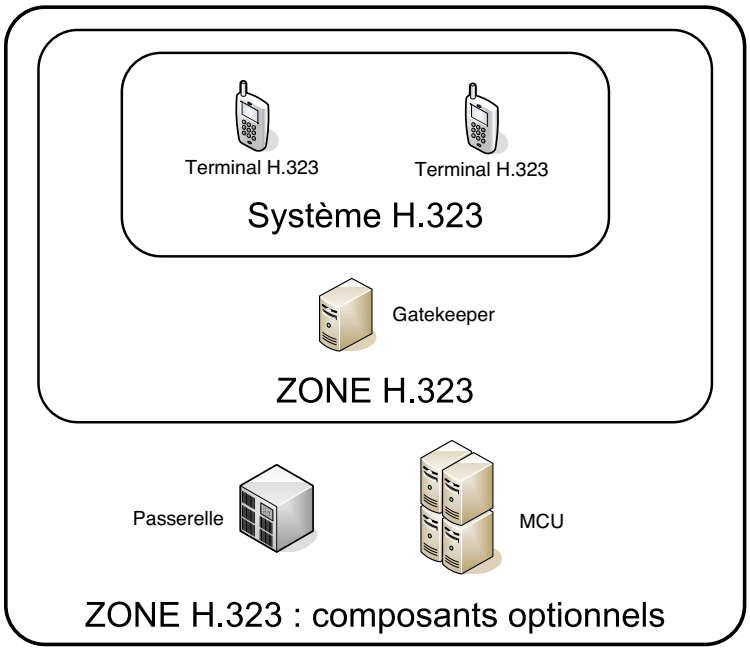
Figure T.5
Architecture de H.323



Autrement dit, une zone H.323 est un système H.323 associé à un gatekeeper et éventuellement, mais pas nécessairement, à des entités additionnelles, comme une MCU ou une gateway. Chaque entité peut être présente en grand nombre.

La figure T.6 illustre ces notions de manière hiérarchique. Système et zone correspondent à des considérations logiques. Cela signifie que plusieurs réseaux locaux peuvent être regroupés dans une même zone H.323 et dépendre d'un même gatekeeper. À l'inverse, il est possible d'avoir plusieurs zones H.323 et de les faire communiquer entre elles.

Figure T.6
Système et zones H.323



Le terminal H.323

Équipement de base des interlocuteurs, le terminal peut prendre la forme d'un téléphone IP, en apparence semblable à n'importe quel autre appareil téléphonique utilisé dans la téléphonie RTC, ou d'un logiciel téléphonique installé sur un ordinateur ou un assistant personnel de type PDA équipé d'un micro et d'une sortie audio. On parle dans ce cas de softphone.

Pour qu'un terminal soit de type H.323, il doit respecter les prérequis fonctionnels suivants :

- Support des protocoles H.225.0 et H.245 (obligatoire). Ces protocoles, dont le premier utilise des protocoles hérités du RNIS, avec Q.931 et RAS, ont à leur charge d'effectuer la partie signalisation proprement dite dans un système H.323. C'est pourquoi leur gestion est requise par les terminaux.
- Support des protocoles RTP/RTCP (obligatoire). Une fois la liaison établie entre les interlocuteurs, la session multimédia peut commencer. Le transport des données recourt au protocole RTP, auquel est associé le protocole RTCP afin que l'application téléphonique H.323 utilisée dans le terminal puisse réguler son débit selon l'état du réseau. Ces deux protocoles sont donc aussi nécessaires au terminal H.323.
- Support du codec G.711 (obligatoire). Un terminal H.323 doit être capable de gérer l'audio et, suivant les usages, les textes, images et éventuellement vidéos. Pour cela, il doit nécessairement supporter au moins le codec audio G.711, selon l'une de ces deux variantes : PCM (Pulse Code Modulation), la loi μ utilisée en Amérique du Nord et en Asie, et MIC (modulation, impulsion et codage), la loi A utilisée dans le reste du monde. Le support des autres codecs audio et de l'ensemble des codecs vidéo est laissé libre et optionnel dans la spécification du protocole H.323.
- Support de liaisons asymétriques (optionnel). Les terminaux peuvent être disposés de façon à établir des communications asymétriques, pour lesquelles la réception de données se fait avec un codec différent de celui utilisé pour l'envoi. Par exemple, un même terminal peut utiliser le codec G.222 en réception et le codec G.711 en émission. Cela permet d'affiner les débits selon les capacités des terminaux.

  À titre d'exemple, considérons deux terminaux A et B, dont le premier a un débit descendant (en réception, ou *download*) fort, mais un débit montant (envoi, ou *upload*) faible, et le second a un débit montant et descendant fort. Le terminal A peut utiliser un codec de très bonne qualité pour la réception et un codec de moins bonne qualité pour l'envoi. Parallèlement, le terminal B doit s'adapter aux capacités de son correspondant en utilisant le même codec de bonne qualité pour l'envoi et le même codec de moins bonne qualité pour la réception. Les liaisons sont de la sorte asymétriques.
- Support du multicast (optionnel). Si le terminal doit servir à la mise en place de conférences, le multicast doit être géré par le terminal. Il permet de dialoguer sans l'intervention d'une entité spécialisée, telle qu'une MCU, en diffusant ses messages dans le réseau, sous réserve que ce dernier dispose de routeurs qui autorisent la diffusion en multicast.

Comme l'illustre la figure T.7, des terminaux peuvent parfaitement communiquer entre eux en utilisant le protocole H.323 sans l'intervention d'autres éléments architecturaux.

Ils forment ainsi un système H.323 autonome, mais leurs communications ne peuvent profiter de la gamme de services fournis par les autres entités. En particulier, les utilisateurs doivent impérativement connaître l'adresse IP de leur correspondant pour pouvoir les joindre. En outre, ils restent cloisonnés dans un réseau purement IP, ce qui représente une contrainte très limitative pour H.323, qui vise à offrir une large communication entre différents types de réseaux.

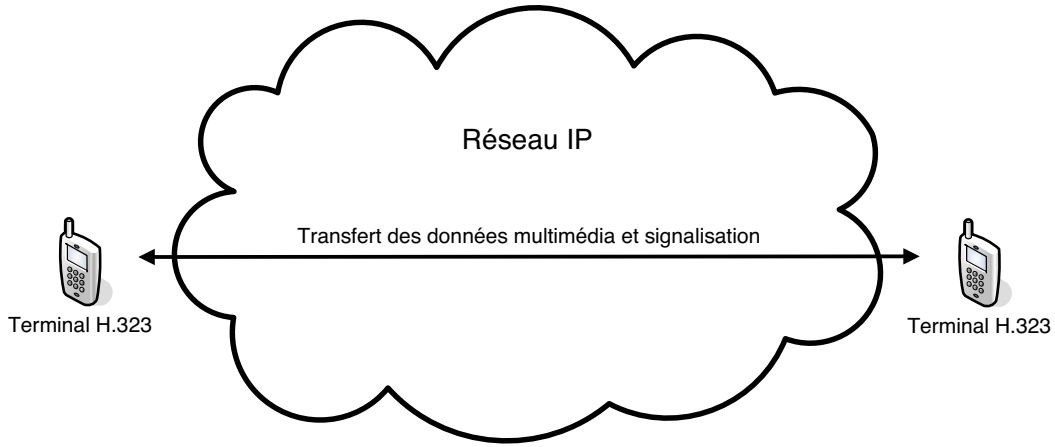


Figure T.7

Communication entre deux terminaux H.323

Le gatekeeper

Facultatif de manière générale, le gatekeeper est requis pour toutes les opérations de contrôle et de gestion des communications. Il offre de la valeur ajoutée aux communications en proposant plusieurs fonctions, dont la première consiste à assurer la localisation des abonnés. Progressivement, le gatekeeper est devenu un élément central, dans lequel se concentrent toutes les fonctionnalités additionnelles, offrant une gamme de services complémentaires. L'architecture de H.323 est donc fortement centralisée autour de lui.

Si un gatekeeper est présent dans une zone H.323, tous les terminaux doivent nécessairement s'y enregistrer et y solliciter l'autorisation d'effectuer des appels, en émission comme en réception.

Localisation des abonnés

Pour permettre la localisation des utilisateurs dans un réseau IP utilisant H.323, le gatekeeper effectue la conversion d'un alias en une adresse IP.

Un alias est un identifiant associé à un utilisateur. Chaque utilisateur est localisé dans le réseau IP par une adresse IP, mais cette adresse peut être attribuée dynamiquement. Pour être joignables, les utilisateurs ne sont pas identifiés par cette adresse IP, qui est impropre

à les qualifier pleinement et univoquement, mais par un alias qui les représente et que les utilisateurs peuvent s'échanger pour se contacter.

Le gatekeeper se charge d'effectuer la correspondance entre les alias et les adresses IP. Les utilisateurs qui ne sont pas situés dans un réseau IP doivent aussi pouvoir être joignables par les utilisateurs du réseau IP. C'est à nouveau le gatekeeper qui permet de les localiser.

Un alias peut être défini de plusieurs façons :

- une adresse de type e-mail, éventuellement préfixée de l'indication *h323:* spécifiant qu'il s'agit d'un alias H.323 ;
- une adresse de type numéro de téléphone (recommandation E.164 de l'UIT-T) ;
- une chaîne de caractères Unicode quelconque ;
- une adresse de type URL ;
- une adresse IP, éventuellement suffixée du numéro de port à utiliser.

Les adresses suivantes sont donc des alias H.323 valides : *albert@domaineH323.com, albert323, 132.227.55.155:1720, 0323323323,* etc.

La translation d'un alias vers une adresse IP est illustrée à la figure T.8. Lors de sa connexion au réseau IP, Bertrand indique au gatekeeper sa localisation dans le réseau (étape 1), comme tout utilisateur qui se connecte. Le gatekeeper a sauvegardé cette association de l'alias avec l'adresse IP correspondante dans sa base de données. Lorsqu'Alice souhaite joindre Bertrand, elle ignore sa localisation mais dispose de son alias. En sollicitant le gatekeeper (étape 2), Alice peut donc déterminer la localisation de Bertrand (étape 3) puis initialiser un appel vers ce dernier (étape 4).

Autres fonctionnalités du gatekeeper

Initialement chargé d'assurer seulement la traduction d'adresses, le gatekeeper est progressivement devenu un équipement de point de contrôle dans lequel se concentre l'ensemble des fonctionnalités complémentaires du réseau.

Parmi elles, les fonctionnalités suivantes sont spécifiées dans la norme comme indispensables et implémentées systématiquement dans tous les gatekeepers :

- Contrôle d'admission. Si la bande passante ne permet pas d'établir un nouvel appel dans une zone H.323, la gateway est habilitée à interdire de nouveaux appels et à établir une liste de priorités d'appels licites.
- AAA (Authentication, Authorization, Accounting), ou authentification, autorisation et comptabilisation. L'authentification permet de connaître l'identité de la personne connectée, tandis que l'autorisation indique quels sont les droits (et éventuellement les conditions) attribués à la personne qui s'est authentifiée.
- Gestion des flux. Le gatekeeper peut implémenter un gestionnaire de bande passante pour décider de l'allocation de bande affectée aux terminaux. Il est en outre possible de limiter le nombre d'intervenants dans une conférence et de rejeter certaines demandes de flux (par exemple en n'autorisant que la voix à un utilisateur qui réclame l'audio et la vidéo).

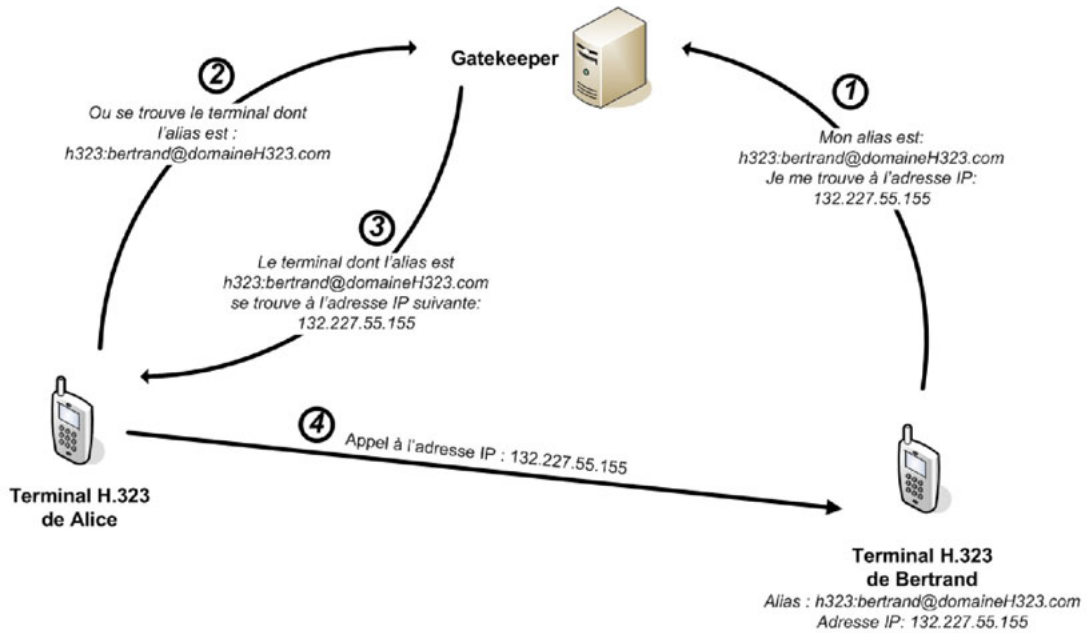


Figure T.8

Traduction d'adresses par le gatekeeper

Signalisation routée et directe

Pour mettre en relation deux utilisateurs, il est possible d'utiliser deux moyens différents pour faire transiter la signalisation dans le réseau :

- un mode indirect, ou routé, la signalisation entre les correspondants passant par le gatekeeper ;
- un mode direct, la signalisation entre les correspondants ne faisant intervenir que ces correspondants, sans entité intermédiaire.

Dans le mode indirect, toute la signalisation passe systématiquement par le gatekeeper. Ce dernier garde donc la supervision totale de la communication et peut intervenir ensuite lors des négociations entre les utilisateurs, en interdisant certains flux vidéo, par exemple, ou en sauvegardant les paramètres négociés lors de l'appel, ce qui peut être utilisé à des fins de facturation notamment.

Comme l'illustre la figure T.9, l'inconvénient immédiat de cette méthode est que le gatekeeper, déjà fortement sollicité dans une zone H.323, l'est davantage encore puisqu'il fait transiter l'ensemble des messages de signalisation.

Seule la partie signalisation de l'appel est concernée par cette redirection vers le gatekeeper, la transmission des flux multimédias eux-mêmes ne faisant pas intervenir le gatekeeper mais seulement les utilisateurs finaux.

Figure T.9
Signalisation en mode indirect

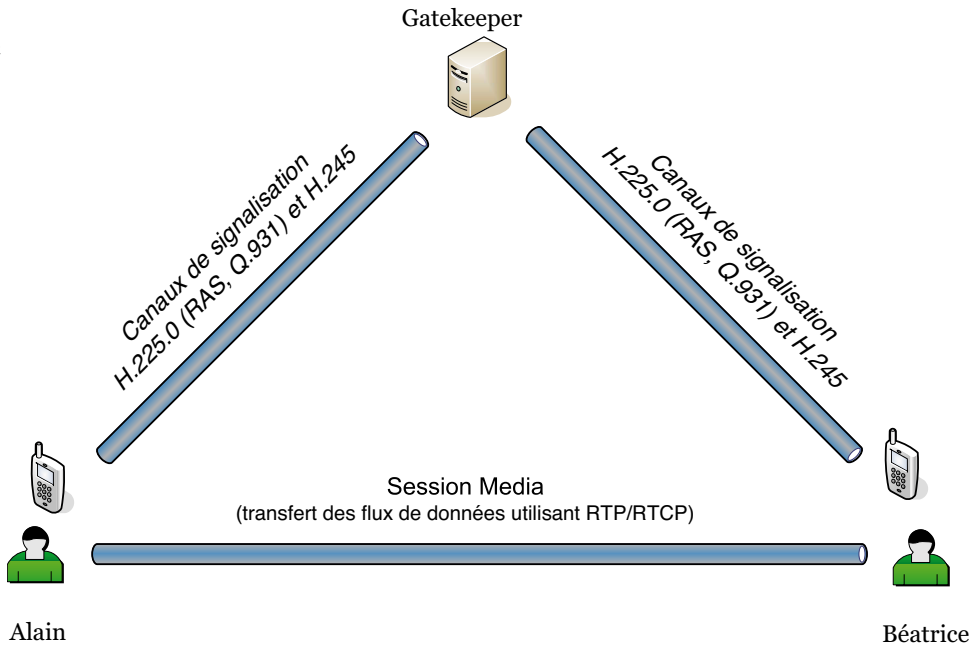
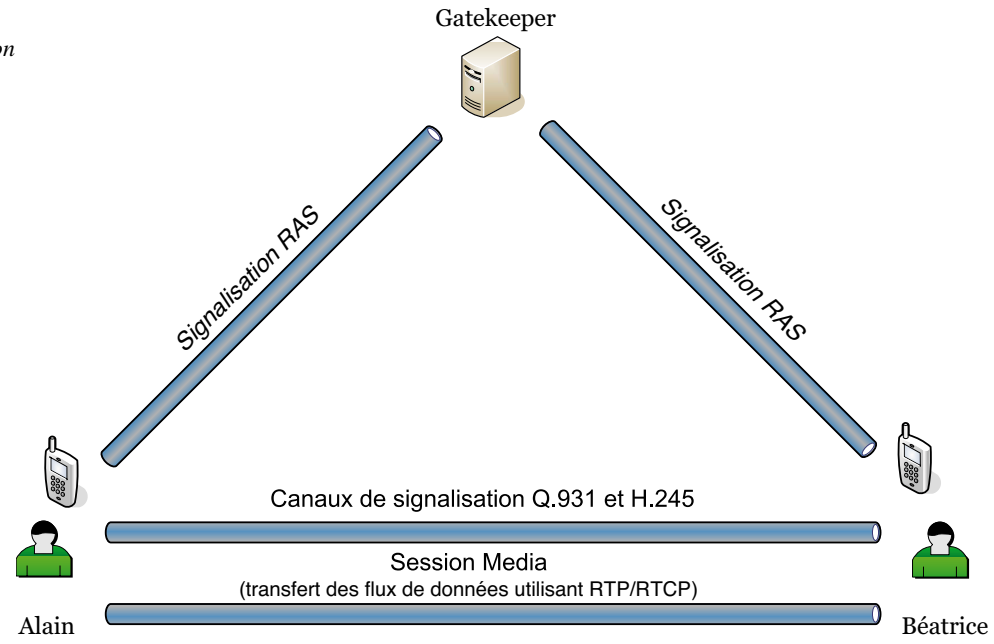


Figure T.10
Signalisation en mode direct



Dans le mode direct, les interlocuteurs s'échangent la signalisation entre eux, comme l'illustre la figure T.10. Le gatekeeper joue cependant toujours son rôle, et les intervenants l'utilisent pour effectuer préalablement à l'appel la traduction d'adresse permettant de localiser le terminal appelé puis pour s'y authentifier et être soumis au contrôle d'admission ainsi qu'à toutes les fonctionnalités dont dispose le gatekeeper. Ce n'est qu'ensuite que les informations de signalisation sont envoyées uniquement entre les correspondants, exactement comme pour un appel dans un système H.323 ne faisant pas intervenir de gatekeeper.

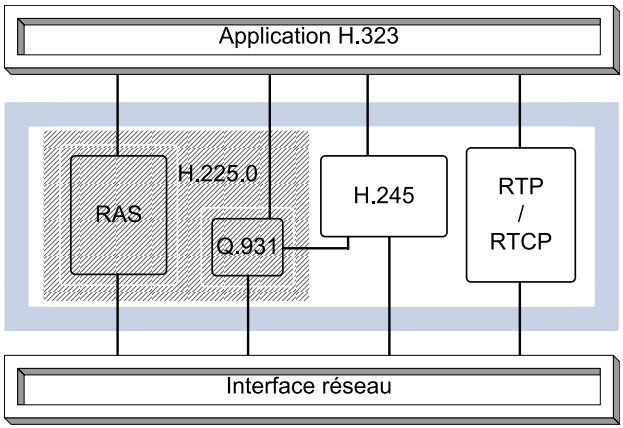
Les messages H.323

Bien plus qu'un protocole, H.323 renvoie à une plate-forme complète décrivant comment des protocoles se combinent pour assurer la signalisation. Pour être fonctionnel, H.323 doit impérativement utiliser d'autres protocoles, qui forment son ossature. Les plus importants d'entre eux sont les standards fondamentaux H.225.0, qui exploite les protocoles RAS, Q.931, hérité du RNIS, et H.245.

Le protocole H.225.0 met en place un canal de signalisation d'appel et d'enregistrement afin d'assurer la mise en relation des interlocuteurs. Le protocole H.245 permet quant à lui de créer un canal de contrôle pour la négociation des paramètres de la communication (codeur utilisé, contrôle de flux, etc.).

Les couches protocolaires de ce modèle sont illustrées à la figure T.11.

Figure T.11
Couches protocolaires de H.323



Initialement, les protocoles H.245 et Q.931 ne supportaient que le protocole de transport TCP, mais, depuis la version 3 de H.323, ils supportent indifféremment TCP et UDP.

Le protocole H.245, la signalisation de contrôle de connexion

Le protocole H.245 gère l'ouverture du canal de contrôle, l'établissement du canal de transmission, la négociation des paramètres (comme le codec utilisé) et le contrôle de flux ainsi que la fermeture du canal de contrôle. Comme pour le protocole Q.931,

tous les messages H.245 ne sont pas exploitables dans le protocole H.323, qui n'en utilise qu'une faible proportion.

Initialement, les messages H.245 ne devaient être diffusés qu'après le message Q.931 SETUP. Pour optimiser les temps d'établissement d'une communication, les versions suivantes de H.323 ont fortement suggéré que les échanges H.245 s'établissent en parallèle ou même avant le message Q.931 SETUP.

Les autres protocoles

Bien d'autres protocoles sont utilisés dans la spécification H.323. Le tableau T.2 récapitule les principaux d'entre eux.

Tableau T.2 • Principaux protocoles de H.323

Protocole	Description
RTP (Real Time Transport Protocol)	Assure l'horodatage des paquets au niveau de l'émetteur pour permettre la synchronisation au niveau du récepteur.
RTCP (Real Time Transport Control Protocol)	Retourne des informations statistiques sur la qualité de la connexion du récepteur vers l'émetteur, afin que ce dernier puisse adapter ses envois en conséquence.
H.235.x	Les protocoles de sécurité à utiliser dans un système H.323 sont décrits dans les documents H.235 sous dix sections référencées de H.235.0 à H.235.9.
H.450.x	La série H.450.x définit un ensemble de protocoles pour la mise en œuvre de services supplémentaires. Alors que la spécification H.450.1 propose simplement un cadre générique, les suivantes spécifient la fourniture de services divers, comme le transfert d'appel (H.450.2), la mise en attente d'appel (H.450.4), l'indication d'un appel pendant un autre appel (H.450.6), la présentation de l'appelant (H.450.8), le renvoi d'appel (H.450.9), etc.
H.460.x	La série H.460.x définit un ensemble d'extensions qu'il est possible d'apporter au protocole de base. Par exemple, le document H.460.9 détaille comment un point de terminaison peut envoyer des informations de qualité de service pour permettre à ce dernier d'optimiser le routage des appels.
X.680	C'est le document de référence pour la syntaxe ASN.1 qui est utilisée dans le codage des données H.323.
X.691	Ce document définit les règles d'encodage des paquets (Packet Encoding Rules) pour la transmission réseau.
T.120	Spécification pour l'échange de données lors des conférences, offrant la fiabilité des échanges et l'interopérabilité entre les constructeurs, tout en préservant une indépendance vis-à-vis du type de réseau utilisé.
T.38	Définit la manière de relayer les communications pour les fax.
V.150.1	Définit la manière de relayer les communications pour les modems.
H.26x	Ces documents détaillent les codecs normalisés pour les transmissions multimédias. Les deux plus utilisés sont H.261 pour le codage vidéo à débits multiples de 64 Kbit/s par seconde et H.263 pour le codage vidéo à faible débit.
H.510	Ce document décrit un support pour la mobilité des utilisateurs en leur fournissant des services analogues quel que soit le terminal qu'ils utilisent.

Le dispositif middle box et l'architecture MIDCOM

Une *middle box* est un dispositif de réseau intermédiaire permettant d'implémenter des services divers tels qu'un filtrage de paquets, un VPN, une détection d'intrusion, une

translation d'adresse NAT ou un pare-feu. Une middle box est donc une appliance située entre deux équipements de réseau, d'où son nom de middle box. En fait, middle box et appliance sont deux noms désignant pratiquement les mêmes équipements. Middle box est le terme utilisé par l'IETF, appliance étant surtout le terme des industriels commercialisant des boîtiers intermédiaires.

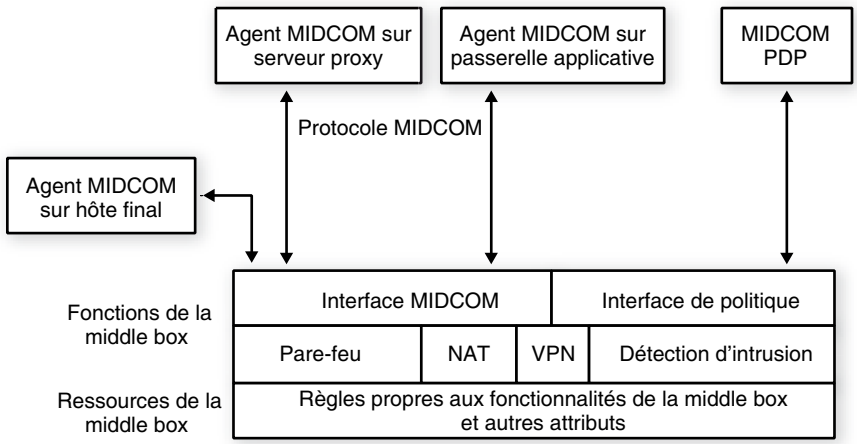
Ces boîtiers nécessitent de l'intelligence pour faciliter la traversée du flux applicatif. Cela rend leur maintenance difficile et dégrade leur performance. D'où l'idée de déplacer l'intelligence de ces boîtiers dans des agents MIDCOM communiquant avec le boîtier à l'aide du protocole MIDCOM. Les agents MIDCOM exécutent des fonctions ALG (Application Level Gateway), qui examinent le flux applicatif et aident la middle box à remplir ses fonctions.

Le protocole MIDCOM s'exécute en trois phases : établissement de la session, session et rupture de la session. La communication entre le boîtier et l'agent se déroule de façon transparente pour l'utilisateur final. Les agents peuvent résider dans les hôtes finals, des serveurs proxy des applications, des passerelles applicatives ou dans la middle box.

Seuls des agents MIDCOM autorisés peuvent influencer le fonctionnement du boîtier. L'autorisation d'un agent requiert une inscription, pendant laquelle les agents suppléent leur profil à la middle box ou au MIDCOM PDP que la middle box consulte. Ce profil détermine les opérations autorisées. L'inscription est souvent une opération manuelle.

L'architecture d'une middle box est illustrée à la figure T.12.

Figure T.12
Architecture d'une middle box



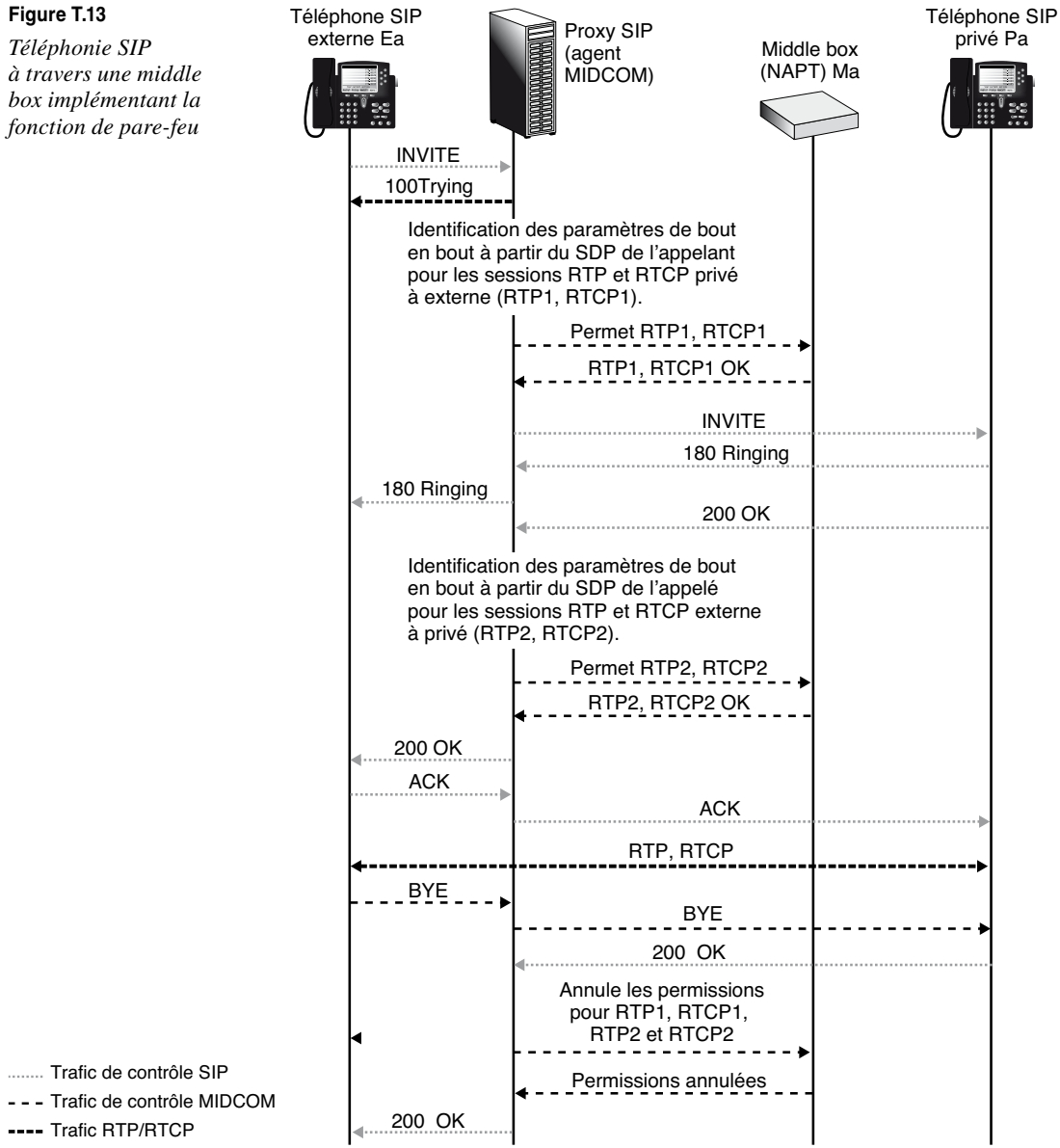
Un agent MIDCOM assistant un pare-feu, par exemple, peut lui demander d'autoriser l'accès au trafic d'une application.

Les sections suivantes illustrent le fonctionnement temporel d'une *middle box* par des exemples d'applications temps réel, notamment avec l'implémentation de fonctionnalités de pare-feu et de NAT dans une middle box pour la téléphonie SIP.

Implémentation d'une fonction de pare-feu dans une middle box

Prenons le cas d'un téléphone SIP externe au réseau qui souhaite communiquer avec un téléphone interne. L'agent MIDCOM résidant dans le SIP proxy demande à la middle box pare-feu du réseau de débloquer les ports nécessaires aux flux RTP (Real-time Transport Protocol) et RTCP (Real-Time Control Protocol) dans les deux sens. La figure T.13 en illustre le fonctionnement.

Figure T.13
Téléphonie SIP à travers une middle box implémentant la fonction de pare-feu



Implémentation de NAT dans une middle box

La middle box est configurée pour rediriger les appels SIP entrants vers l'adresse privée du téléphone SIP. La commande INVITE est destinée à l'adresse NAT externe. Les appels SIP sont des sessions TCP/UDP sur le port 5060.

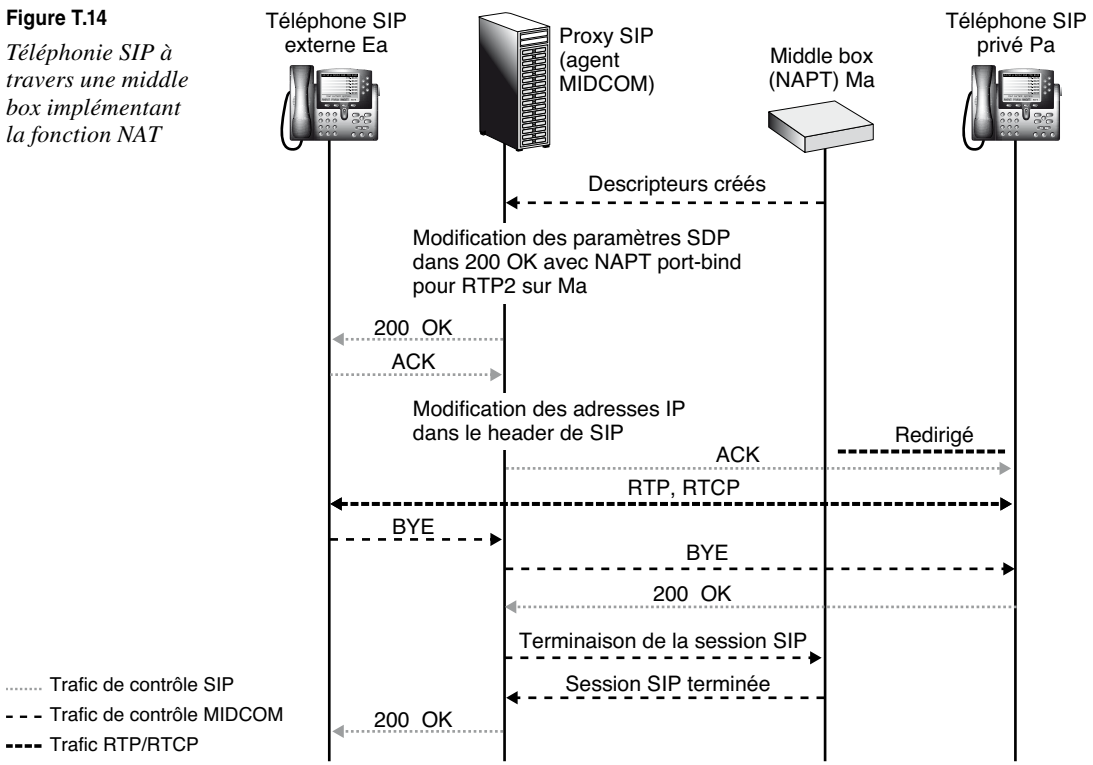
Nous utilisons la notation suivante :

- Ma : adresse externe de la middle box ;
- Pa : adresse interne du téléphone SIP ;
- Ea : adresse du téléphone SIP externe.

Le proxy SIP demande les descripteurs de la session NAT pour les deux flux entrant et sortant. Les ports dynamiques utilisés pour le flux média sont contenus dans la partie SDP du message SIP. Après le 200 OK reçu par le proxy du téléphone privé, l'agent demande à la middle box d'allouer des descripteurs de session NAT pour le trafic entrant de sorte que les ports réservés pour RTP2 et RTCP2 soient contigus. Bien que les flux média entrants et sortants soient indépendants, ils sont liés à la même session SIP. Quand le message BYE est envoyé, toutes les ressources sont libérées.

La figure T.14 illustre l'interaction entre un proxy SIP et une middle box implémentant la fonctionnalité NAT.

Figure T.14
Téléphonie SIP à travers une middle box implémentant la fonction NAT



La signalisation MGCP

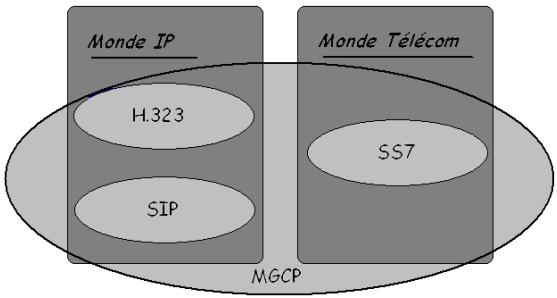
L'une des raisons ayant expliqué l'émergence et le succès du protocole H.323 est le besoin de regrouper les différents acteurs du multimédia, qu'ils soient équipementiers ou fournisseur de services, autour de normes communes. La concurrence engendrée par le protocole SIP a réduit cet effet d'universalité puisque les réseaux IP ont désormais une solide solution de rechange à H.323. Dès lors, se pose la question de la communication entre des réseaux de nature différente (ATM, RNIS, RTC ou IP) ou bien de même nature mais exploitant des protocoles de signalisation différents (H.323, SIP ou autre).

Si les passerelles ont déjà été introduites avec le protocole H.323, elles demeurent des entités complexes, onéreuses et non administrables, qui plus est fortement sollicitées alors qu'elles tiennent difficilement la montée en charge. Pour combler ce nouveau besoin, le protocole MGCP (Media Gateway Control Protocol), ou protocole de contrôle des passerelles multimédias, a été proposé.

Il fonctionne au niveau applicatif et permet d'offrir une couverture plus large en fédérant toutes les signalisations, qu'elles soient de type IP ou RTC entre autres. C'est le maître d'œuvre de l'interopérabilité entre tous les protocoles de signalisation et tous les réseaux, de quelque nature qu'ils soient.

Comme l'illustre la figure T.15, qu'il s'agisse de la signalisation CCITT n° 7 (SS7), utilisée dans un réseau commuté, H.323 ou SIP, le protocole MGCP est conçu pour relier et faire communiquer l'ensemble de ces réseaux.

Figure T.15
Rôle fédérateur du protocole MGCP



MGCP est aujourd'hui utilisé par les FAI pour assurer le contrôle et l'administration à distance des InternetBox mises à disposition de leurs abonnés.

Les travaux ont débuté après que le protocole H.323 eut été proposé par l'UIT. Très vite, il est apparu que l'initiative H.323 était insatisfaisante pour relier à grande échelle des réseaux de natures différentes. Les passerelles (gateways) proposées dans l'architecture H.323 sont des éléments complexes et coûteux, ce qui pose problème dans le monde IP. Plus le nombre de réseaux à traverser pour établir une communication est important, plus l'est aussi celui des passerelles sollicitées.

Progressivement, un certain nombre d'initiatives ont été lancées, dont l'idée-force est de disposer d'un réseau dont toutes les passerelles multimédias soient des composants simples. Ces passerelles sont reliées à un contrôleur maître concentrant toute l'intelligence

du réseau et centralisant les décisions. C'est le modèle maître-esclave. L'architecture générale qui conceptualise les entités de contrôleur et de passerelle multimédia, et plus généralement le modèle maître-esclave, fut initialement proposée dans le projet TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) de l'ETSI. La première tentative de protocole de communication entre ces entités fut SGCP (Simple Gateway Control Protocol), en 1997. Proposée par Telcordia (anciennement BellCoRe, acronyme de Bell Communications Research), elle reçut le soutien de Cisco. TIPHON est le protocole précurseur de MGCP.

En 1998, l'opérateur de télécommunications Level 3 Communications (groupe XCOM Technologies) a mis en place un comité consultatif technique, ou TAC (Technical Advisory Council), réunissant une douzaine d'industriels renommés, comme Ericsson, Lucent, Nortel, Alcatel, 3Com et Cisco. Avec ces membres fondateurs, le TAC sera à l'origine de la conception d'un protocole de contrôle des entités réseau sur Internet, nommé IDCP (Internet Device Control Protocol). Ses spécifications seront présentées à ITU, l'IETF et l'ETSI.

En octobre 1998, avec le soutien d'importants constructeurs, tels que Cisco et Alcatel, le protocole MGCP a été standardisé à l'IETF par le groupe de travail MEGACO (Media Gateway Control). Celui-ci réalisait la fusion des initiatives SGCP et IDCP. MGCP s'inscrit dans la droite ligne de la version 1.1 du protocole SGCP, qui servira de socle principal à MGCP.

En plus de dériver de SGCP, MGCP s'est enrichi de nombreuses fonctionnalités proposées dans IDCP. En octobre 1999, la RFC 2705 présentait la première version de MGCP. Elle sera rendue obsolète en janvier 2003 par la RFC 3435, qui sera complétée par la RFC 3661, en décembre 2003.

Architecture et fonctionnement de MGCP

Pour communiquer entre deux réseaux de nature différente, il est nécessaire d'utiliser une passerelle. Cette entité prend en charge à la fois la signalisation pour l'établissement, la gestion et la terminaison de la communication, mais aussi la conversion des signaux pour l'adaptation des flux d'un réseau vers un autre. MGCP sépare ces deux aspects en entités distinctes, l'une pour contrôler les appels, l'autre pour appliquer le contrôle ordonné par la première entité.

MGCP fonctionne selon une architecture centralisée permettant de faire communiquer et de contrôler différentes entités appartenant à des réseaux distincts. Il se fonde sur l'hypothèse que les terminaux des utilisateurs peuvent être des composants de base peu coûteux et sans aucune intelligence, réduits à des fonctionnalités élémentaires.

Les passerelles sont également des entités simples. En fournissant un service générique, elles restent indépendantes de leur constructeur. Pour leur donner des directives permettant le traitement des services, ces passerelles multimédias sont reliées à une entité centrale. Le protocole MGCP assure le contrôle et l'échange de messages de signalisation entre ces passerelles, réparties dans un réseau IP, et le contrôleur de passerelles, chargé de l'administration et de la gestion dynamique des passerelles.

MGCP fait éclater le modèle architectural proposé avec H.323 en décomposant le rôle des passerelles et en externalisant toute leur intelligence sur une entité centrale.

Pour réaliser cette distinction, MGCP définit les entités suivantes :

- Le Call Agent, qui sert à piloter et administrer les passerelles de manière centralisée.
- Les passerelles, qui maintiennent la connectivité entre réseaux de nature différente.

Le Call Agent

Le Call Agent, également appelé contrôleur de passerelles multimédias ou encore SoftSwitch, selon une terminologie non officielle mais courante, a pour fonction de contrôler les passerelles et de concentrer toute l'intelligence ainsi que la prise de décision dans le réseau.

Entité logique, pouvant être localisée n'importe où sur le réseau, le Call Agent est spécifiquement responsable de l'établissement, de la maintenance et de la terminaison des appels établis entre des terminaux appartenant à des réseaux de nature différente.

Comme ces opérations sont initialisées au niveau des passerelles multimédias, le Call Agent intervient pour contrôler l'activité de ces dernières et leur donner les directives de traitement de ces opérations. Il est en quelque sorte le maître d'œuvre et d'opération des communications entre les réseaux.

Dans la mesure où il contribue à centraliser le réseau autour de lui, le Call Agent est une entité fortement sollicitée. De ce fait, il devient un élément sensible dans le réseau, particulièrement en cas de panne. Néanmoins, cette centralisation n'intervient que pour arbitrer et assurer la maintenance et la gestion des échanges de signalisation. Elle n'entre pas en jeu dans les communications intra-réseau. En outre, pour gérer les pannes, il est plus simple de mettre en place des doublures, sous forme de Call Agents redondants, que de rendre toutes les passerelles multimédias redondantes.

Il est possible d'avoir plusieurs Call Agents, chacun ayant en charge un parc de passerelles multimédias. Par exemple, chaque opérateur peut gérer ses propres passerelles par un Call Agent propriétaire. Le protocole MGCP ne définissant pas de mécanisme de synchronisation entre Call Agents, on doit considérer indépendamment chaque Call Agent et les passerelles qu'il contrôle.

Fondamentalement, MGCP repose sur un modèle maître-esclave, et il n'est pas dans son objectif de fournir des mécanismes de communication entre les agents de contrôle, qui sont des entités de même nature, auxquelles le modèle maître-esclave ne convient pas. Pour faire communiquer entre eux plusieurs Call Agents, un protocole tel que SIP peut être utilisé afin de négocier les paramètres de communication.

Les passerelles multimédias

Selon le protocole MGCP, la notion de passerelle est assez floue et couvre un vaste ensemble de définitions, notamment les suivantes :

- Passerelle d'opérateur téléphonique, pour faire le lien entre un réseau téléphonique et un réseau IP. Les opérateurs de téléphonie alternatifs, par exemple, utilisent souvent le réseau RTC de l'abonné comme réseau de base puis basculent les flux de l'abonné

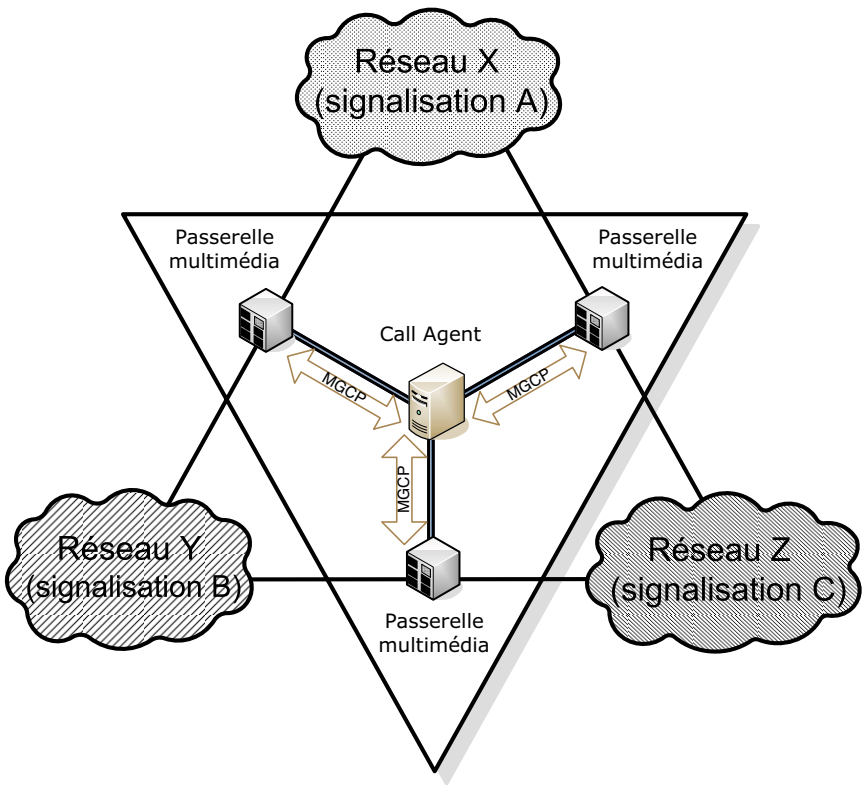
vers un réseau IP (lequel présente l'avantage d'être à commutation de paquets, donc sans réservation de ressources, et ainsi moins coûteux qu'un réseau à commutation de circuits) sur de longues distances internationales, avant de basculer à nouveau les flux de l'appelant vers le réseau RTC auquel le terminal du destinataire est connecté.

- Passerelle résidentielle de type box (boîtier exploitant le modem, le câble ou les technologies xDSL), généralement mise à disposition par le FAI. Ce boîtier fait la liaison entre le réseau IP des utilisateurs et le réseau d'accès téléphonique de l'opérateur. Nous en verrons une illustration un peu plus loin dans ce chapitre.
- PBX d'entreprise faisant la liaison entre le réseau IP de l'entreprise et le réseau téléphonique RTC de l'opérateur. Au sein de l'entreprise, des téléphones IP ou des softphones peuvent être utilisés en interne pour exploiter les services complémentaires qu'offre le réseau IP et permettre la convergence des flux sur un support unique. Comme le réseau de l'entreprise est connecté à une liaison RTC, une passerelle est toutefois nécessaire.

Par rapport aux passerelles initialement prévues dans le protocole H.323, les passerelles multimédias sont simplement dépourvues de la fonctionnalité de traitement des appels. Elles s'en remettent pour cela au Call Agent. Néanmoins, elles conservent intact leur emplacement physique, à la frontière entre les deux réseaux de nature distincte, alors que le Call Agent peut être situé n'importe où, comme l'illustre la figure T.16.

Figure T.16

Places des passerelles et du Call Agent dans l'architecture MGCP



X, Y ou Z représentent des réseaux quelconques (RNIS, ATM, IP, RTC, etc.). Sur chacun de ces réseaux, le protocole de signalisation intra-réseau de son choix peut être utilisé, par exemple SIP ou H.323 dans un réseau IP, ou SS7 dans un réseau RTC. MGCP ne peut s'appliquer au sein de ces réseaux, mais seulement à leur périphérie afin d'assurer la gestion et le traitement des communications inter-réseau.

On observe deux niveaux de communications : l'un qui fait intervenir les réseaux et les passerelles multimédias et l'autre les passerelles multimédias et le Call Agent. Le protocole MGCP s'applique exclusivement à transmettre de la signalisation entre le Call Agent et les passerelles. Les flux de données multimédias (voix, vidéo, données) entre deux terminaux appartenant à des réseaux différents ne transitent jamais par le Call Agent. Une fois que le Call Agent en a donné l'autorisation, ces flux sont véhiculés de poste terminal à poste terminal, en passant uniquement par la passerelle.

Le rôle de la passerelle multimédia est donc réduit à l'acheminement cohérent des données, ce qui implique qu'elle accomplisse les tâches suivantes :

- conversion du signal ;
- adaptation au support ;
- compression des données ;
- conversion de la signalisation ;
- multiplexage ;
- mise en paquets.

Les passerelles multimédias se retrouvent ainsi réduites à leur fonctionnalité première et fondamentale de transmission : elles travaillent au niveau du média lui-même et assurent les traitements des données, sans la logique de traitement. Toutefois, ces actions ne sont réalisables qu'en accord avec le Call Agent, dont les passerelles sont les exécutants.

Globalement, le mode de fonctionnement des passerelles est donc allégé par rapport à H.323 et le réseau devient constitué d'éléments simples et configurables.

Les communications MGCP passent systématiquement par le protocole UDP, choisi pour optimiser les délais de traitement des envois.

S'il n'est pas mentionné, le Call Agent utilise par défaut le port 2727 pour ses communications, tandis que les passerelles utilisent le port 2427.

Principes d'établissement d'une communication

On appelle *endpoint* un équipement dit de terminaison, qui représente soit la source soit la destination d'un message multimédia.

Un routeur réseau n'est pas un endpoint puisqu'il se contente d'acheminer des données, sans être à l'origine de l'envoi. Le Call Agent n'est pas non plus un endpoint, puisqu'il ne traite pas des messages multimédias.

Dès lors qu'une entité participe aux échanges de médias et se place comme source ou destinataire de ces échanges, même si elle n'est pas la source initiale ou le destinataire

final et qu'elle ne joue qu'un rôle d'intermédiaire dans ces échanges, elle est considérée comme en endpoint. Les terminaux des utilisateurs sont des endpoints de référence.

Supposons que nous souhaitions connecter deux terminaux, appelés des endpoints. Chacun d'eux se trouve localisé derrière une passerelle multimédia. Ces deux passerelles sont elles-mêmes contrôlées par un Call Agent, comme l'illustre la figure T.17.

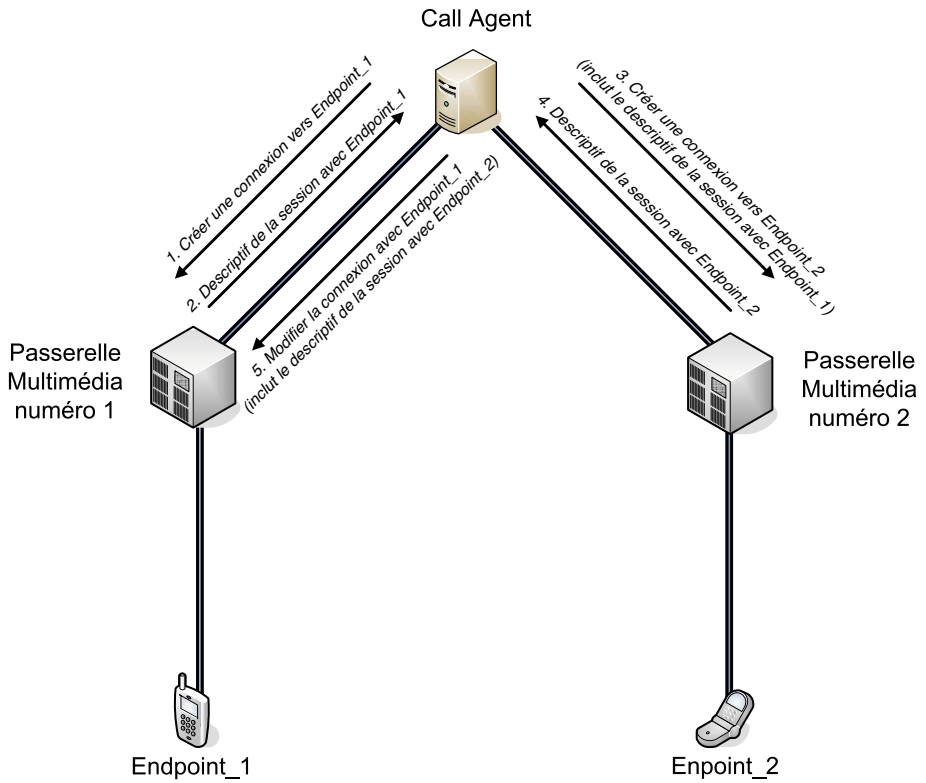


Figure T.17

Mise en relation de deux endpoints

Pour mettre en relation les deux endpoints, les cinq étapes suivantes sont nécessaires :

1. **Requête de création de connexion vers la première passerelle.** Le Call Agent sollicite la création d'une connexion avec un endpoint auprès de la passerelle concernée.
2. **Réponse de la première passerelle.** Celle-ci se charge de joindre le endpoint et lui attribue les ressources nécessaires à la communication : une session est créée entre la passerelle et le endpoint. En retour, la passerelle envoie au Call Agent un descriptif de la session créée. Ce descriptif contient l'ensemble des paramètres permettant de joindre le endpoint, incluant l'adresse IP de ce dernier, le port UDP sur lequel la communication est en attente et les codecs supportés.

3. **Requête de création de connexion vers la seconde passerelle.** Le Call Agent procède de la même façon pour le second endpoint et sa passerelle : il sollicite cette dernière en lui envoyant un message pour la création d'une connexion avec le second endpoint. En plus, et dans le même message, le Call Agent lui fait parvenir le descriptif de session que lui a retourné la première passerelle.
4. **Réponse de la seconde passerelle.** La seconde passerelle joint le endpoint concerné et alloue les ressources nécessaires à cette communication. En retour, elle transmet au Call Agent un descriptif de session contenant les paramètres permettant de joindre le second endpoint.
5. **Mise en relation des deux endpoints.** Le Call Agent contacte la première passerelle et lui transmet le descriptif de la session retournée par la seconde passerelle. Comme une connexion existe déjà avec le endpoint, il n'est pas nécessaire de créer une nouvelle connexion. Il suffit de modifier celle qui existe et de la compléter. C'est donc une commande de modification qui est effectuée par le Call Agent.

Une fois ces étapes achevées, la communication débute dans les deux sens. Elle peut être modifiée à tout moment par le Call Agent, qui peut imposer, par exemple, un changement de codec, d'adresse IP ou de port. De même, le Call Agent peut mettre fin à la communication à tout moment en envoyant un message aux passerelles, qui doivent alors rompre les connexions.

On peut résumer tous les états possibles d'une passerelle multimédia comme illustré à la figure T.18.

Les messages MGCP

La communication avec MGCP obéit à un modèle de type client-serveur. Un message MGCP est soit une requête soit une réponse à une requête. Il est constitué sous forme textuelle, ce qui simplifie son usage (traitement sans compilateur, donc plus rapide, et débogage immédiat), et présente plusieurs analogies avec le protocole SIP. Ainsi, une transaction MGCP est-elle constituée d'une requête et de la réponse à cette requête, éventuellement précédée de réponses temporaires. Le format d'un message MGCP est illustré à la figure T.19.

Dans ce message, on distingue trois parties :

- Ligne de requête ou de réponse : notifie la commande à exécuter (s'il s'agit d'une requête) ou le résultat de la commande (s'il s'agit d'une réponse). C'est une partie indispensable.
- En-tête : spécifie la liste des paramètres du message. C'est une partie facultative.
- Corps du message : décrit les paramètres de la session à établir. C'est une partie facultative.

Plusieurs lignes peuvent constituer chacune des parties. On sépare chaque ligne par des retours chariot, ou CR (Carriage Return), et des sauts de ligne, ou LF (Line Feed), ou par des retours chariot seulement.

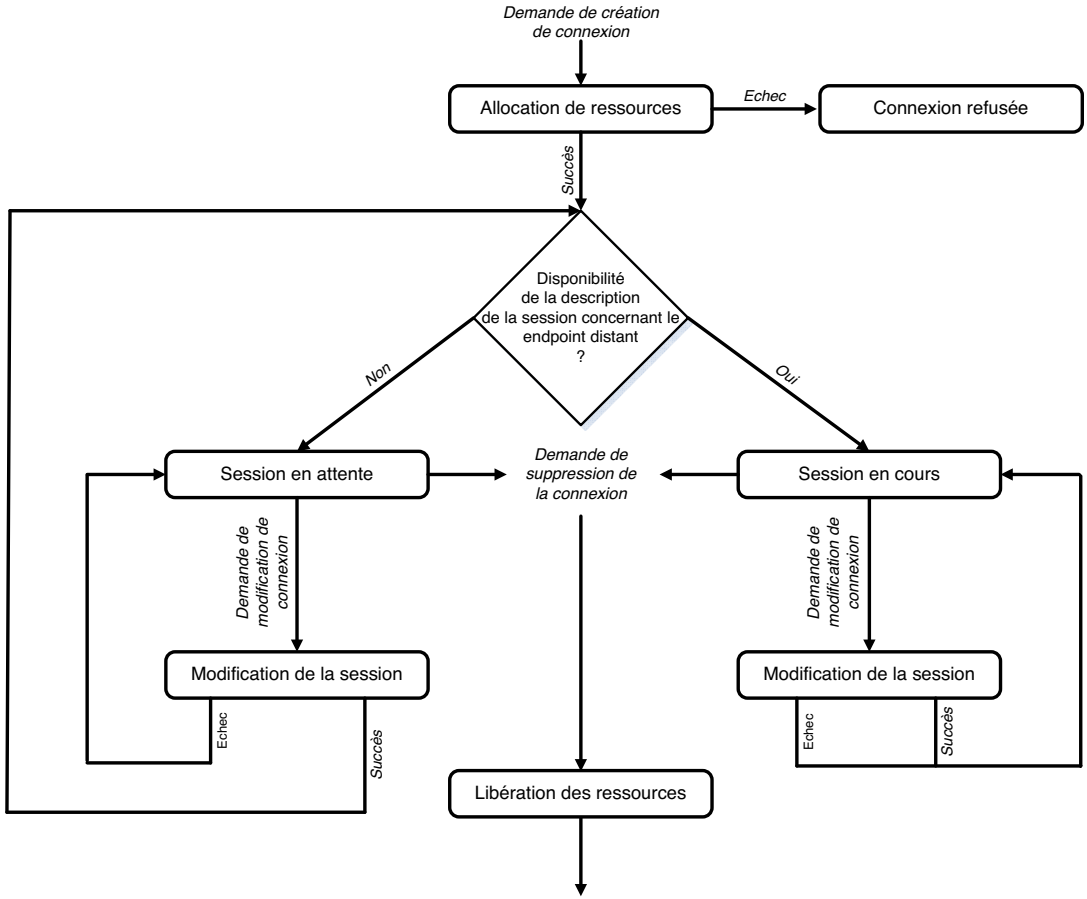


Figure T.18
Diagramme d'états d'une passerelle

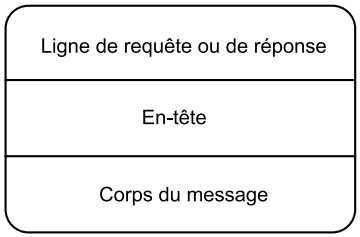


Figure T.19
Format d'un message MGCP

Notons que, dans la RFC 3435, la partie spécifiant la ligne de requête ou de réponse et celle spécifiant l'en-tête sont regroupées.

Les requêtes

Le protocole MGCP définit neuf requêtes permettant de spécifier l'action à entreprendre. Les commandes sont lancées entre le Call Agent et les passerelles (Media Gateway). Comme MGCP est un protocole de type maître-esclave, toutes les entités n'ont pas des possibilités comparables, et ces commandes ne peuvent être lancées qu'à l'initiative de l'une de ces entités, soit le Call Agent, soit la Media Gateway.

On distingue donc deux catégories de commandes : celles qui sont lancées par le Call Agent vers une ou plusieurs passerelles et celle qui vont dans l'autre sens, de la passerelle vers le Call Agent.

À chaque requête correspond un code en quatre lettres de caractères ASCII, qui permet de condenser la taille de la requête. Les neuf requêtes et leur code respectif sont récapitulés au tableau T.3.

Tableau T.3 • Les 9 requêtes MGCP et leur format abrégé

Format complet	Format abrégé
AuditConnection	AUCX
AuditEndpoint	AUEP
CreateConnection	CRCX
DeleteConnection	DLCX
EndpointConfiguration	EPCF
ModifyConnection	MDCX
NotificationRequest	RQNT
Notify	NTFY
RestartInProgress	RSIP

La signalisation COPS (Common Open Policy Service)

COPS est un protocole d'échange de politiques. Il a été introduit au chapitre précédent en même temps que l'architecture globale du contrôle par politique. Cependant, nous ne sommes pas entrés dans le détail du protocole COPS en tant que signalisation, et c'est ce que nous allons faire ici.

Le protocole COPS est issu de travaux démarrés en 1996 dans le contexte de la réservation de ressources. COPS a été étendu en 1999 dans un contexte plus large dans le groupe de travail RAP (Resource Allocation Protocol) de l'IETF et normalisé par la RFC 2748 de janvier 2000.

Dans sa version actuelle, COPS a pour objectif l'échange d'informations de politiques réseau entre un PDP (Policy Decision Point) et un PEP (Policy Enforcement Point). Le PDP et le PEP font partie de l'architecture de gestion de réseau à base de politique définie par les groupes PFWG (Policy Framework Working Group) et DMTF (Distributed Management Task Force) de l'IETF. Le rôle du PDP est de prendre des décisions sur les politiques réseau, tandis que celui du PEP est d'appliquer les décisions que lui a communiquées le PEP.

Deux modes de signalisation sont actuellement standardisés au sein de l'IETF :

- COPS-Outsourcing, issu des premiers travaux, intègre COPS dans un réseau où existe un protocole de signalisation tel que RSVP. Les événements déclencheurs d'échanges COPS sont les messages de signalisation arrivant au PEP. Le PDP est alors sollicité pour prendre la décision sur la politique à appliquer. La première RFC qui se réfère à ce mode est COPS-RSVP (COPS usage for Resource ReserVation Protocol), que nous examinons un peu plus loin.
- COPS-Configuration, aussi appelé COPS-Provisioning, permet l'intégration de COPS dans un réseau où les politiques sont transmises au préalable par le PDP au PEP et engendrent la configuration du PEP. La RFC qui se réfère à ce mode est COPS-PR (COPS usage for Policy Provisioning), que nous étudions également plus loin.

Le mode d'échange de COPS est de type client-serveur, avec une relation maître à esclave. Le PDP est le maître et le PEP l'esclave. Il n'y a pas de classification de message de type requête/réponse. COPS ne peut fonctionner qu'au-dessus de TCP. Une connexion persistante TCP est établie entre le PEP et le PDP. La fiabilité est donc assurée par TCP.

COPS définit un fonctionnement général, qui peut être étendu pour générer des fonctionnements plus spécifiques, propres à la politique ou au mode de gestion de la politique. Ces fonctionnements spécifiques sont définis hors de COPS dans des extensions que nous verrons ultérieurement.

Dans le protocole COPS, le mode de communication est unique et direct entre le PEP et le PDP, et il n'y a pas d'entités intermédiaires. Dans COPS et ses deux extensions COPS-RSVP et COPS-PR, le PEP est une entité logique, qui représente un équipement actif du réseau. Le PDP est une entité logique qui représente un équipement de management du réseau. En retour des requêtes du client, il envoie des décisions. C'est le fonctionnement naturel dans le mode outsourcing. Le PEP et le PDP conservent l'état des requêtes/décisions échangées, selon un fonctionnement « stateful ». L'architecture complète dans laquelle s'insère COPS est illustrée à la figure T.20.

Les messages COPS

Les messages COPS ont tous la même structure générale : un en-tête commun donnant les informations sur le type du message et un corps transportant les objets spécifiques. Cette structure est représentée à la figure T.21.

Figure T.20
Architecture de gestion de réseau par politique

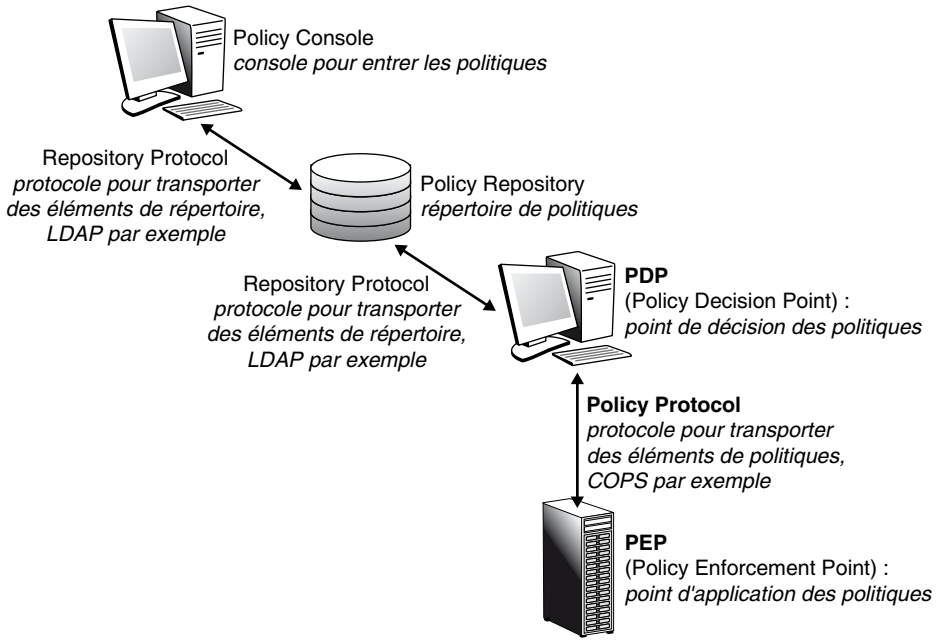
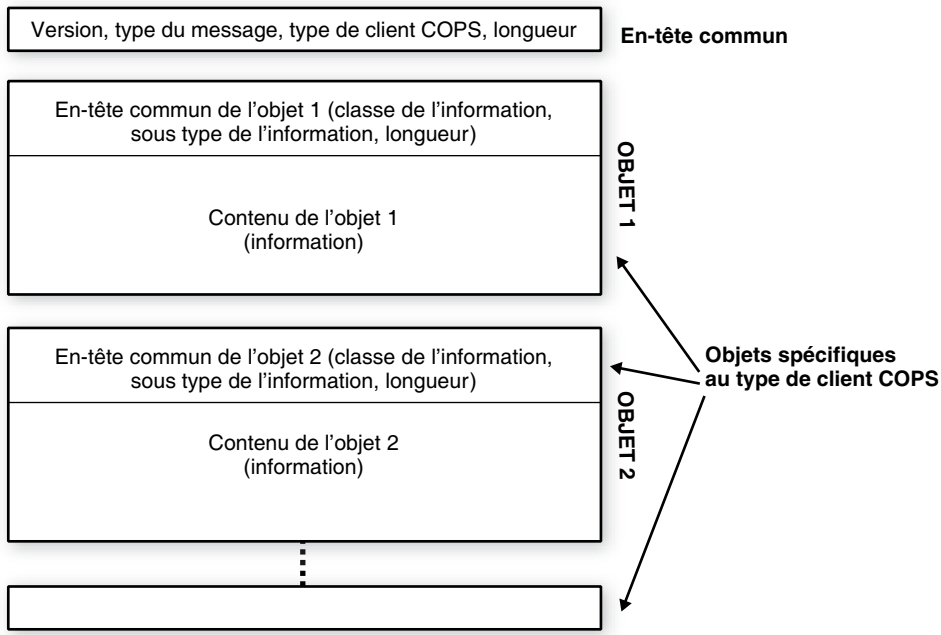


Figure T.21
Format général des messages COPS



COPS comporte les 16 classes d'objets, ou plutôt classes d'information de contenu d'objets, récapitulées au tableau T.4. La structure des objets est soit précisée dans la RFC, soit étendue et définie dans les extensions du protocole.

Tableau T.4 • Classes d'objets de COPS

C-Num	Classe de l'objet	C-Type	Objet
1	Handle (Handle)	1	Client – Handle
2	Context (Context)	1	Context
3	In Interface (IN-Int)	1 2	IPv4 address + Interface IPv6 address + Interface
4	Out Interface (OUT-Int)	1 2	IPv4 address + Interface IPv6 address + Interface
5	Reason Code (Reason)	1	Reason Code
6	Decision (Decision)	1 2 3 4 5	Decision Flags Stateless Data Replacement Data Client Specific Decision Data Named Decision Data
7	LPDP Decision (LPDPDecision)	1 2 3 4 5	Decision Flags Stateless Data Replacement Data Client Specific Decision Data Named Decision Data
8	Error (Error)	1	Error
9	Client Specific Info (ClientSI)	1 2	Signaled ClientSI Named ClientSI
10	Keep-Alive Timer (KATimer)	1	Keep-alive Timer value
11	PEP Identification (PEPID)	1	PEP Identification
12	Report Type (Report-Type)	1	Report Type
13	PDP Redirect Address (PDPRedirAddr)	1 2	IPv4 + TCP port IPv6 + TCP port
14	Last PDP Address (LastPDPAddr)	1 2	IPv4 Address IPv6 Address
15	Accounting Timer	1	Accounting timer value
16	Message Integrity	1	HMAC digest

Dans COPS-RSVP, la classe d'objets Context object est utilisée pour transporter le type de message RSVP et la classe Client specific information pour transporter les objets RSVP.

Dans COPS-PR, de nouveaux objets sont encapsulés dans les sous-types Named Client-Specific Information object et Named Decision Data Object. Les objets spécifiques sont issus d'une base d'information de politiques, ou PIB (Policy Information Base), relative à chaque type de client COPS. L'ensemble de ces PIB réunies compose la PIB générale. Cette PIB suit la même convention que la MIB SNMP. Les formats d'encodage actuellement définis pour le stockage des informations et leur transport sont ASN.1 (Abstract Syntax Notation 1) et BER (Basic Encoding Rule).

Les messages sont définis d'une manière générale dans la RFC COPS, leur utilisation spécifique étant précisée dans les RFC d'extension. Le tableau T.5 récapitule les 10 messages COPS regroupés par sens de circulation.

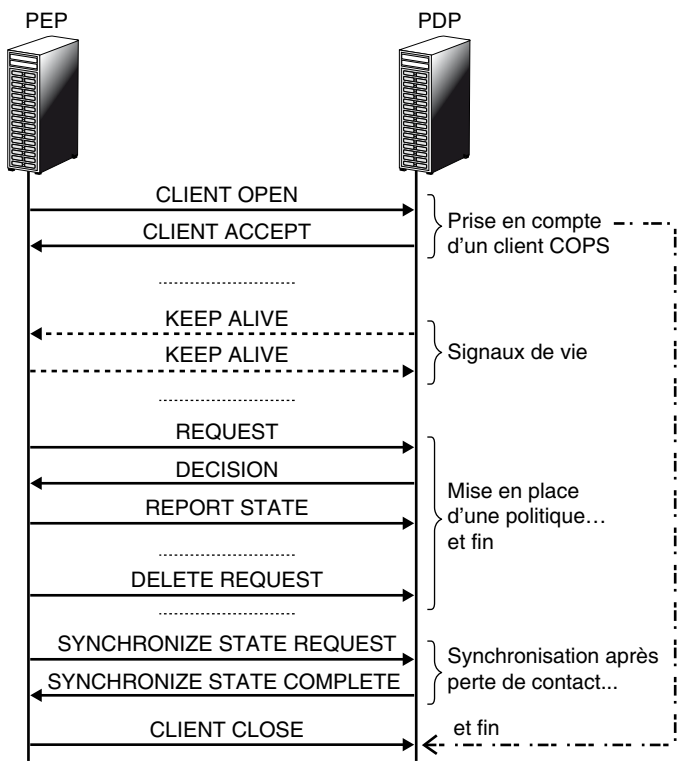
Tableau T.5 • Messages COPS

Message PEP → PDP	Message PDP → PEP	Message PDP ↔ PEP
REQUEST (demande de politique)	DECISION (envoi de politique)	CLIENT CLOSE (fin de prise en compte de client COPS)
REPORT STATE (résultat d'installation de politique)	SYNCHRONIZE STATE REQUEST (demande de synchronisation)	KEEP ALIVE (Signal d'existence)
DELETE REQUEST STATE (fin d'application de politique)	CLIENT ACCEPT (prise en compte de client COPS)	
CLIENT OPEN (demande de prise en compte de client COPS)		
SYNCHRONIZE STATE COMPLETE (fin de synchronisation)		

Scénarios de contrôle de politique

Les scénarios de contrôle de politique COPS dépendent du mode de contrôle de politique. Cependant, on peut illustrer les échanges de messages COPS par la décomposition en étapes de la figure T.22.

Figure T.22
Échanges COPS



Les extensions de COPS

Le protocole COPS peut être étendu en introduisant de nouveaux types de clients. Nous ne décrivons ici que les deux extensions les plus répandues, COPS-RSVP et COPS-PR.

COPS-RSVP (COPS usage for RSVP)

La RFC 2749 de janvier 2000 précise les directives d'usage pour le support de COPS dans un environnement RSVP. C'est dans cette première optique que COPS a été développé par le groupe de travail RAP (Resource Allocation Protocol) afin de fournir un mécanisme de contrôle d'admission à partir de requêtes sur les ressources réseau. Cela a donné lieu à la création d'une extension pour RSVP permettant de prendre en charge le contrôle d'admission par politique, qui spécifie notamment l'objet POLICY-DATA transporté par les messages RSVP et utilisé pour le contrôle par politique par les PEP et le PDP. La RFC 2750 décrit cette extension.

Comme expliqué précédemment, le mode de fonctionnement de COPS-RSVP est l'outsourcing, dans lequel les événements déclencheurs sont les messages RSVP.

Les détails de l'architecture COPS-RSVP sont peu développés dans les RFC 2749 et 2750. On peut cependant déduire les informations suivantes :

- Un PEP est un client RSVP.
- Un client RSVP n'est pas forcément un PEP.
- Un client RSVP sur un routeur extrémité du domaine est forcément un PEP.

L'architecture COPS-RSVP est illustrée à la figure T.23.

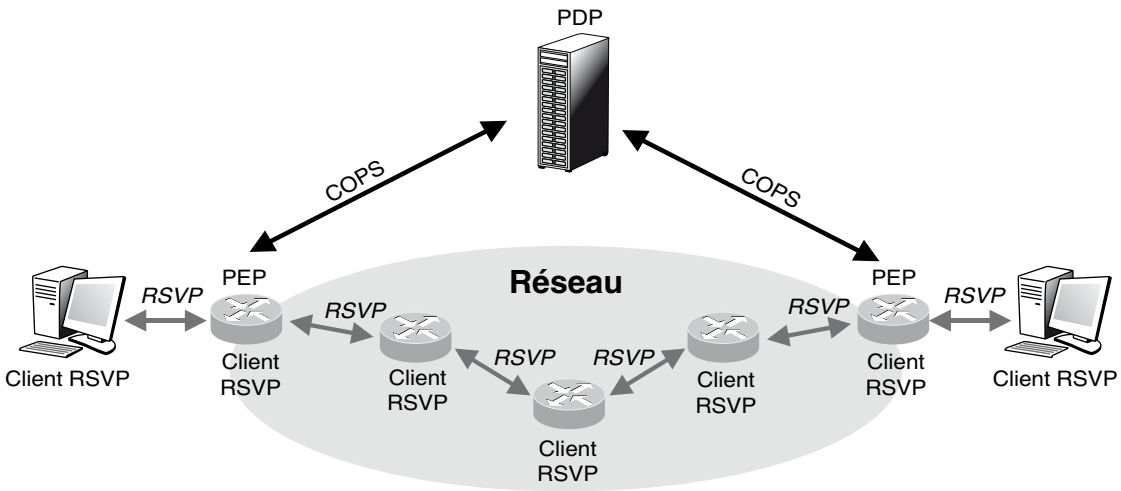


Figure T.23
Architecture COPS-RSVP

Les types de messages RSVP générant des requêtes COPS sont Path, Resv, PathErr et ResvErr. Tous les objets reçus dans ces messages sont encapsulés dans les requêtes COPS. Trois contextes objet sont définis pour la génération de requêtes COPS du PEP vers le PDP en fonction des événements/actions RSVP :

- Incoming-Message request : lors de l'arrivée d'un message RSVP, une sollicitation pour l'accepter ou le rejeter est envoyée du PEP au PDP.
- Resource-Allocation request : lors de l'arrivée d'un message RSVP Resv, une sollicitation pour injecter (commit) les ressources dans le flux RSVP est envoyée du PEP au PDP.
- Outgoing-Message request : lorsque le PEP doit faire suivre un message RSVP sortant, il sollicite le PDP, qui accepte ou refuse cette sortie et fournit l'objet POLICY-DATA qui sera encapsulé dans le message RSVP.

Lors de l'établissement d'une réservation RSVP, plusieurs sollicitations sont déclenchées. Le nombre de messages COPS engendrés dépend de nombreux paramètres. Dans un fonctionnement normal d'une réservation pour une session point-à-point (unicast), le nombre de ces messages peut être minimisé par regroupement de plusieurs contextes objet dans une même requête COPS. C'est le cas avec le contexte objet combiné In & Allocation & Out pour traiter l'arrivée d'un message Resv et l'affectation des ressources associées et pour le faire suivre.

COPS-PR (COPS usage for Policy Provisioning)

La RFC 3084 de mars 2001 précise les directives d'usage pour la prise en charge de COPS dans un environnement à base d'approvisionnement de politiques. Cette prise en charge est indépendante du type de la politique devant être approvisionnée (QoS, sécurité, etc.) et développe les mécanismes et conventions utilisés pour l'échange d'information en mode provisioning entre des PEP et des PDP.

Le mode provisioning se différencie du mode outsourcing par le fait qu'il n'y a plus de corrélation entre un événement se produisant dans un PEP et la décision relative du PDP. Le PDP peut envoyer directement des informations de provisionnement au PEP suite à une sollicitation externe ou à un ensemble d'événements s'étant produits dans le PEP ou encore à toute autre combinaison.

Le provisionnement des ressources dans un réseau est souvent fondé sur les SLA et s'opère aux frontières du réseau. Cela confère un aspect statique au modèle COPS-PR, où les échanges entre PEP et PDP sont espacés par des temps longs comparativement au modèle dynamique du mode outsourcing.

Les événements externes susceptibles de déclencher des décisions directes du PDP vers le PEP peuvent être les suivants :

- Utilisateur sollicitant des services réseau *via* une interface Web de l'application centrale de gestion.
- Serveur H.323 sollicitant des ressources pour le compte d'un utilisateur voulant établir une visioconférence.

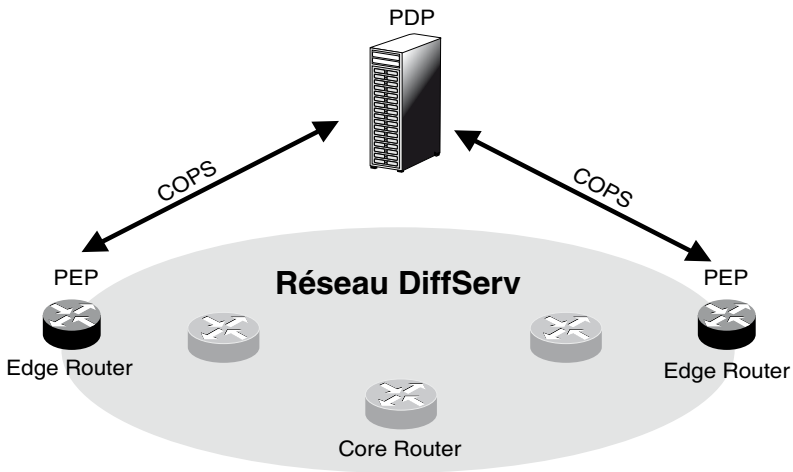
Ces sollicitations externes arrivent directement au PDP. Cependant, la RFC ne décrit pas le mode de communication entre le serveur H.323 et le PDP. D'un autre côté, le PEP peut lui aussi solliciter directement le PDP. Dès l'ouverture de la connexion globale entre PEP et PDP, c'est-à-dire juste après l'échange Client Open ↔ Client Accept, le PEP sollicite le PDP pour obtenir l'ensemble des politiques à approvisionner en son sein. Il peut ensuite le faire à chaque modification de sa configuration, telle que le retrait d'une carte d'interface.

Pour représenter les informations de politique approvisionnée à échanger entre les PEP et le PDP, une base d'information de politiques PIB (Policy Information Base) est introduite. La PIB est représentée par un arbre, dans lequel les branches identifient les classes de politiques, ou PRC (Provisioning Class), et les feuilles les instances de ces PRC, ou PRI (Provisioning Instance), qui sont échangées entre PEP et PDP. Ces PIB sont stockées à la fois dans les PEP et le PDP.

Si l'on regarde l'application du modèle provisioning à la gestion des politiques de QoS, on voit tout de suite son adéquation avec le modèle DiffServ. Dans le modèle DiffServ, les équipements du réseau sont configurés au préalable pour appliquer des mécanismes de qualité de service à l'ensemble des flux du réseau. L'architecture DiffServ définit deux catégories d'équipements, les routeurs extrémité (edge routers) et les routeurs internes. Les premiers doivent classifier les flux et leur affecter un DSCP (DiffServ Code Points), qui sera utilisé dans la suite par tous les seconds pour traiter les paquets avec le comportement associé à ce DSCP particulier. La mise en place de politiques de contrôle de QoS dans cette architecture se fait par l'implantation d'un PEP COPS-PR au niveau de chaque routeur extrémité.

L'architecture de l'environnement COPS-PR pour un réseau DiffServ est décrite à la figure T.24.

Figure T.24
Architecture COPS-PR pour un réseau DiffServ

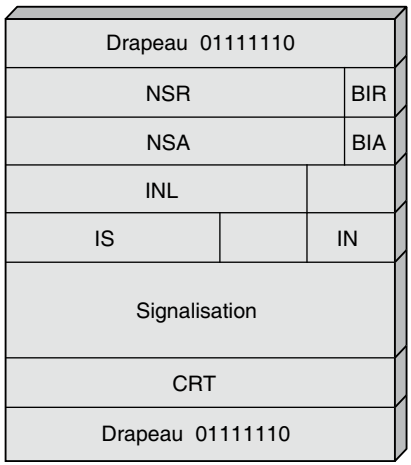


La signalisation CCITT n° 7 (SS7)

Le protocole CCITT n° 7 (SS7 en anglais) a été mis au point par l'UIT-T dans le cadre de la transmission de la signalisation sur les réseaux publics. Le protocole LAP-D, que nous verrons par la suite, véhicule la signalisation sur la terminaison d'abonnés. Au moment de leur passage dans le réseau public proprement dit, les informations de supervision sont prises en charge par un réseau spécifique de type datagramme, le réseau sémaphore, qui suit la recommandation CCITT n° 7 décrivant les couches du protocole. Cette architecture est compatible avec le modèle de référence.

Le protocole de niveau 2 est de type HDLC. Il a été légèrement modifié pour prendre en compte les contraintes temps réel de la signalisation. Tous les algorithmes sont semblables à ceux de HDLC, excepté celui des reprises sur erreur. La détection se fait toujours par la zone de contrôle. La structure de la trame CCITT n° 7 est illustrée à la figure T.25.

Figure T.25
La trame CCITT n° 7



Trois types de trames sont disponibles dans la procédure :

- Les PDU de signalisation sans champ d'information.
- Les PDU avec un champ d'information, qui servent aux contrôles de la procédure elle-même. C'est par ce type de trame que le contrôle de flux de la liaison est effectué. Lorsque la procédure n'a pas de signalisation utilisateur à transmettre, elle émet en continu des trames de ce type, en acquittant la dernière trame bien reçue. On a ainsi une duplication des acquittements, ce qui est très utile en cas de perte d'acquittement. Un autre avantage de ces trames est qu'elles détectent presque instantanément une rupture de la liaison.
- Les PDU avec un champ d'information, qui transportent la signalisation de bout en bout. Pour cette catégorie, on trouve un numéro de trame sur 7 bits situé dans le deuxième octet de la trame, juste derrière le drapeau, ainsi qu'un deuxième numéro de séquence dans le troisième octet de la trame. Ces deux numéros, associés aux bits BIR

(indicateur de bit arrière) et BIA (indicateur de bit avant), permettent un contrôle avant et arrière de la procédure.

Les trames contiennent encore un indicateur de longueur sur 6 bits, le champ INL, un indicateur de service dans le champ IS sur 4 bits et un indicateur national IN sur 2 bits.

Deux techniques de reprise sur erreur sont disponibles. La première est conforme à la procédure HDLC. La seconde permet une récupération plus rapide et une duplication des réémissions. Cette seconde technique est particulièrement appréciable dans les réseaux où le temps de propagation est très long, comme les réseaux satellite. À chaque réémission, si le support est libre, on retransmet toutes les trames depuis la trame en erreur, et l'on recommence jusqu'à ce qu'il y ait une nouvelle signalisation à émettre. Cette politique permet de dupliquer ou tripliquer, c'est-à-dire faire trois copies, les reprises et de prévoir, le cas échéant, plusieurs trames successives erronées.

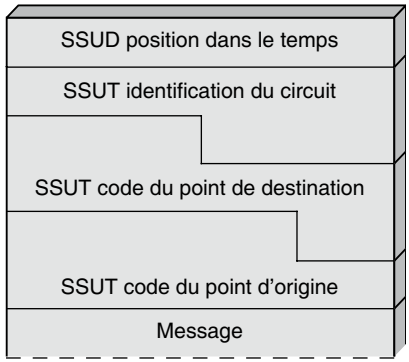
Pour compléter les caractéristiques de la procédure CCITT n° 7, indiquons que les coupleurs extrémité possèdent des compteurs d'erreur, qui comptabilisent le nombre de trames erronées par unité de temps. Si le compteur dépasse une valeur déterminée par le gestionnaire du réseau, la liaison est fermée.

Le niveau réseau de la recommandation CCITT n° 7 spécifie un réseau datagramme puisque les données à transmettre sont extrêmement courtes, de l'ordre de quelques octets. Nous allons décrire brièvement le protocole de niveau réseau.

Les avis Q.702 à Q.704 de l'UIT-T décrivent le protocole CCITT n° 7. Le niveau 3 prend surtout en charge le problème de l'adressage. Celui-ci est décrit dans les recommandations Q.711 à Q.714. En particulier, la norme 84 définit le sous-système de commande des connexions sémaphore SCCP (Signaling Connection Control Part). Le paquet de niveau 3 est illustré à la figure T.26.

Figure T.26

Paquet de niveau 3 du protocole CCITT n° 7



SSUT (sous-système utilisateur téléphonique)
SSUD (sous-système utilisateur informatique)

Deux sous-systèmes ont été normalisés : le sous-système correspondant aux applications téléphoniques, dans les avis Q.721 à Q.725, et celui correspondant aux applications infor-

matiques. Ils sont appelés respectivement TUP (Telephone User Part) et DUP (Data User Part).

Le service de transport de la recommandation CCITT n° 7 assure pour le compte du niveau session un transport de bout en bout des TSDU. Il offre cinq classes de services spécifiques suivant le type de relation entre les deux extrémités.

Annexe U

29. La sécurité dans l'environnement IP

Cette annexe passe en revue des exemples de protocoles EAP utilisés part divers grands équipementiers des réseaux. Elle aborde ensuite la sécurité de la messagerie électronique.

Exemples de protocoles EAP (Extensible Authentication Protocol)

Cette section présente les protocoles LEAP, EAP-FAST, EAP-SIM et PEAP.

LEAP (Lightweight Extensible Authentication Protocol)

L'architecture LEAP s'appuie sur la procédure d'authentification disponible sur les plates-formes Windows.

L'authentification LEAP fonctionne de la façon suivante (*voir figure U.1*) :

1. À partir du mot de passe utilisateur, on calcule une empreinte MD4 de 16 octets. Cette dernière est complétée par cinq octets nuls. On obtient ainsi une suite de 21 octets interprétée sous la forme de trois clés DES de 7 octets, soit 56 bits. Le mécanisme d'authentification, de type CHAP, consiste à chiffrer un nombre aléatoire de 8 octets à l'aide des trois clés DES associées à un utilisateur, ce qui produit une réponse de 24 octets. LEAP est associé au type EAP 17 (0x11) pour réaliser une double authentification, entre le serveur d'authentification et le supplicant (utilisateur du réseau), d'une part, et entre l'authenticator (point d'accès) et le serveur d'authentification, d'autre part.

2. Au terme d'un scénario d'authentification réussi entre supplicant et serveur RADIUS (correspondant aux phases 1 à 5 de la figure U.1), les deux entités déduisent une clé de session SK (unicast), qui est transportée à l'aide d'un attribut propriétaire (CISCO-AVPAIR, LEAP SESSION-KEY) du protocole RADIUS. LEAP supporte également des mécanismes de mise à jour de clés WEP, soit par la négociation d'une session RADIUS limitée (Session Timeout), soit par des demandes périodiques de réauthentification par le supplicant à l'aide des trames EAP LOGOFF et EAP START.

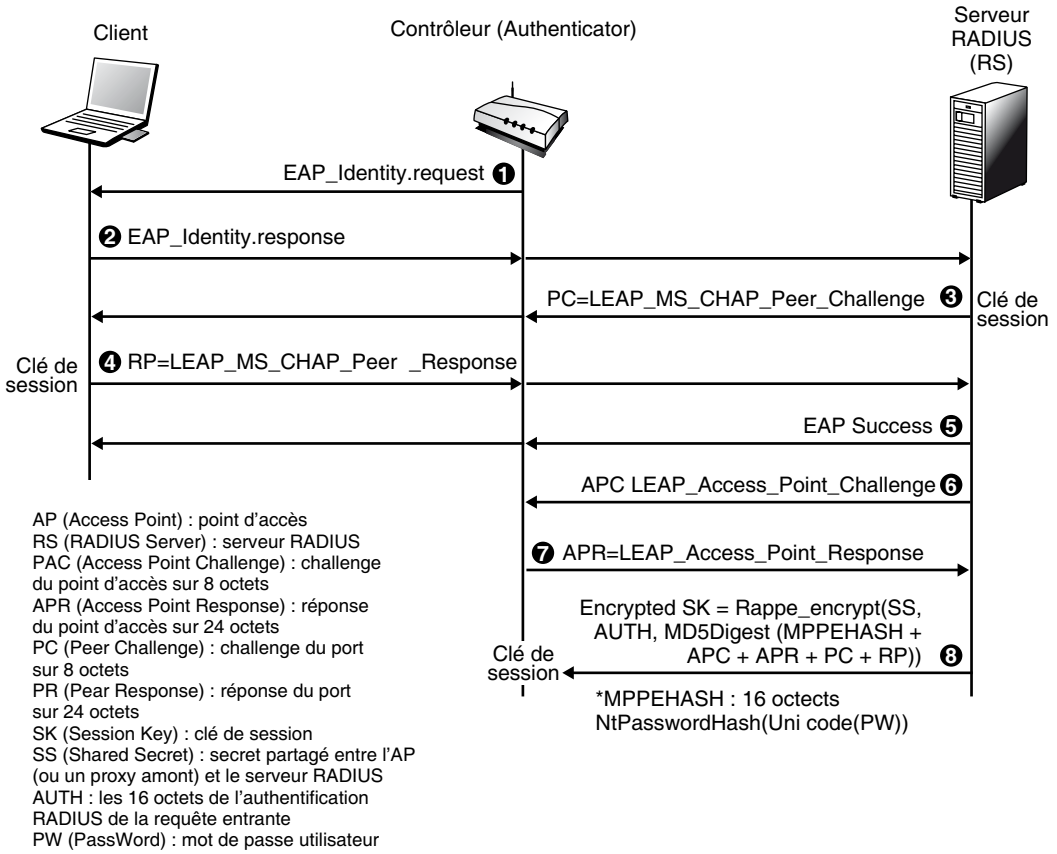
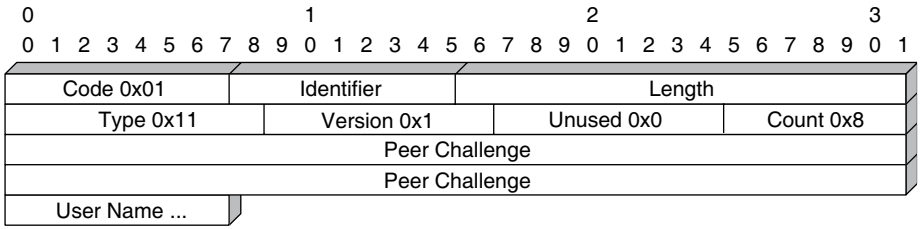


Figure U.1

Processus d'authentification LEAP

Le format du paquet LEAP est illustré à la figure U.2.

Figure U.2
Paquet LEAP



EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)

EAP-FAST a été développé par Cisco Systems pour résoudre une faille de sécurité de son protocole propriétaire LEAP (Lightweight EAP), que nous venons d'examiner, lorsque les mots de passe ne sont pas assez sophistiqués.

Ce protocole vise notamment à contrer les attaques par dictionnaire utilisées avec succès contre LEAP. Contrairement à PEAP, que nous verrons un peu plus loin dans ce chapitre, qui est le fruit d'une alliance entre Cisco, Microsoft et RSA Security, EAP Fast ne requiert pas la mise en place d'une infrastructure complexe de distribution de certificats pour l'établissement de tunnels sécurisés entre machines terminales.

EAP FAST est intégré dans l'ensemble des produits Aironet de Cisco ainsi que dans son serveur VPN Cisco Secure ACS. Les partenaires de Cisco auront aussi accès au standard dans le cadre de la spécification Cisco Compatibility Extensions 3.0.

De façon plus précise, EAP-FAST est une architecture de sécurité de type client-serveur, qui chiffre les transactions EAP au moyen d'un tunnel TLS. Cette solution est assez semblable à PEAP, à la différence essentielle près que le tunnel EAP-FAST est établi à l'aide de secrets forts, qui appartiennent aux utilisateurs. Ces secrets sont appelés PAC (Protected Access Credentials). Ils sont générés par le serveur Cisco Secure ACS à l'aide d'une clé maître connue uniquement du serveur Cisco Secure ACS. Les handshakes réalisés par des secrets partagés étant beaucoup plus rapides à mettre en œuvre qu'une PKI, EAP-FAST est plus simple à mettre en place que les solutions qui chiffrent les transactions EAP, comme EAP-TLS ou PEAP.

EAT-FAST s'exécute en trois phases :

- La phase 0, spécifique d'EAP-FAST, consiste à ouvrir un tunnel sécurisé entre les machines terminales en utilisant les certificats PAC. Le tunnel est établi par un échange de clés au moyen d'une procédure de type Diffie-Hellman. Si l'authentification EAP-MSCHAPv2 réussit, le serveur Cisco Secure ACS donne un certificat PAC à chaque client. Cette phase 0 est optionnelle si les certificats sont introduits par une autre méthode assurant le secret des certificats.
- En phase 1, le serveur Cisco Secure ACS et les machines terminales établissent des tunnels TLS grâce aux PAC présents dans les machines terminales. La façon dont le PAC a été introduit dans la machine terminale est indépendante de la phase 1.

- En phase 2, le serveur Cisco Secure ACS authentifie les certificats des machines terminales par l'intermédiaire d'un EAP-GTC, qui est protégé par le tunnel TLS créé à la phase 1. Le protocole EAP-FAST ne supporte pas d'autre type d'EAP. Cisco Secure ACS autorise un service réseau au travers du point d'accès si la phase 2 s'est déroulée avec succès.

Cette solution est présentée par Cisco comme étant aussi simple que LEAP et aussi sécurisée que PEAP. En fait, EAP-FAST est un compromis entre les deux. Le fait de ne pas utiliser de PKI semble plus simple mais est en réalité aussi difficile à mettre en œuvre pour obtenir une bonne sécurité. De plus, la sécurité n'est pas aussi bonne qu'avec PEAP car la phase 0 peut conduire à des attaques décisives si elle n'est pas aussi sécurisée que peut l'être une PKI.

EAP-SIM (Subscriber Identity Module)

Une solution classique d'authentification est proposée par les opérateurs de téléphones mobiles de deuxième génération, ou GSM, selon une procédure d'authentification réalisée entre le serveur de l'opérateur et la carte SIM (Subscriber Identity Module) située dans le terminal de l'utilisateur. Cette authentification utilise non pas le protocole EAP mais des protocoles provenant de l'ETSI effectuant un travail comparable.

Les sections qui suivent décrivent ce mécanisme avant de présenter EAP-SIM, une extension normalisée d'EAP pour le monde IP que les opérateurs peuvent, par exemple, utiliser dans les hotspots.

L'authentification du GSM

Le GSM est un standard de téléphonie mobile défini par l'ETSI (European Telecommunications Standards Institute). Il supporte des opérations de sécurité telles que l'authentification de l'utilisateur et le chiffrement entre le réseau nominal, où l'abonné est inscrit, et la carte SIM de l'abonné.

Les éléments du réseau GSM intervenant dans ces fonctions de sécurité sont les suivants :

- AuC (Authentication Center), ou centre d'authentification du réseau de l'opérateur.
- HLR (Home Location Register), ou base de données des abonnés de l'opérateur, qui mémorise les données de chaque abonné, telles que son identité internationale, ou IMSI (International Mobile Subscriber Identity), son numéro de téléphone, son profil d'abonnement, etc. Il stocke aussi pour chaque abonné le numéro de VLR courant.
- VLR (Visitor Location Register), ou base de données des seuls abonnés localisés dans la zone géographique gérée.

Les données d'authentification sont stockées dans la carte SIM et ne sont pas chargées dans le terminal mobile. La procédure d'authentification consiste donc en un échange de messages entre la carte SIM et le réseau.

Lors de l'inscription d'un nouvel abonné, une clé Ki (jusqu'à 128 bits) lui est attribuée. Cette clé est secrète et n'est stockée que sur sa carte SIM et sur l'AuC de l'opérateur.

La procédure d'authentification se déroule de la façon suivante :

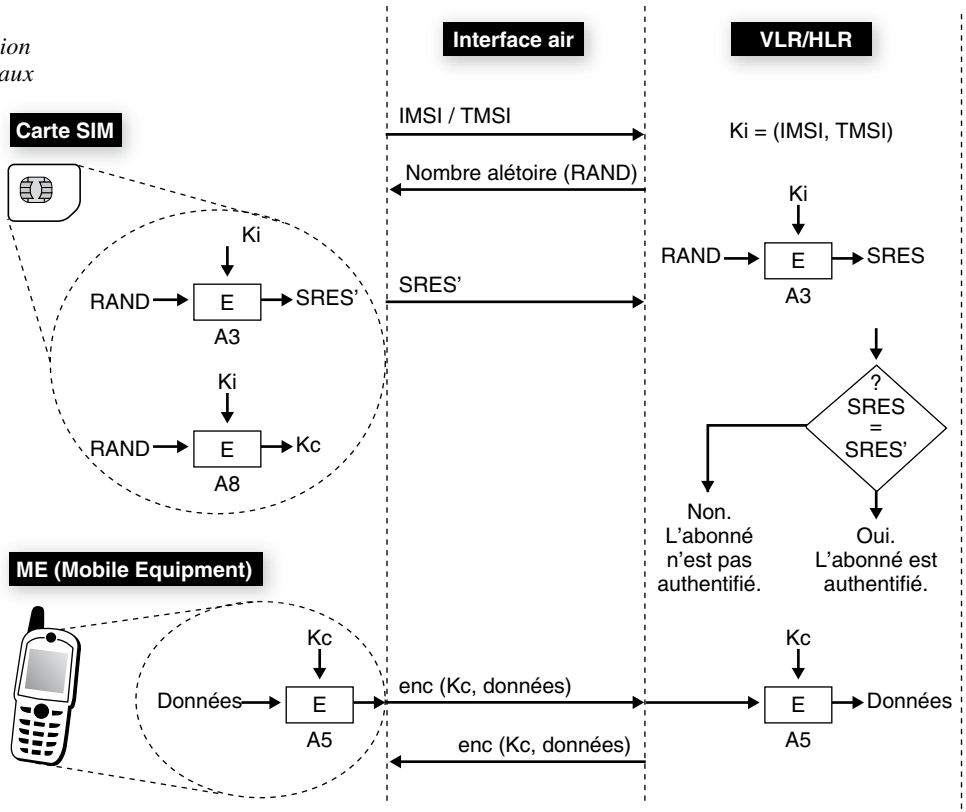
1. Le réseau transmet au mobile un nombre aléatoire RAND, codé sur 128 bits.
2. La carte SIM du mobile calcule la signature de RAND grâce à l'algorithme d'authentification A3 et sa clé Ki. Le résultat, SRES (32 bits), est envoyé par le mobile au réseau.
3. Le réseau compare SRES avec le résultat calculé de son côté. Si les deux coïncident, l'abonné est authentifié.

Une fois l'abonné authentifié, le chiffrement est effectué selon l'algorithme A5. Il utilise la clé Kc, de 64 bits, calculée à partir de la clé secrète Ki et du nombre aléatoire RAND, selon l'algorithme A8.

Il suffit au réseau de disposer d'un triplé (RAND, SRES, Kc) pour authentifier un abonné et activer le chiffrement de ses communications. Cependant, le réseau ne calcule pas ces données en temps réel. L'AuC prépare des triplés pour chaque abonné et les transmet à l'avance au HLR, qui les stocke. Le VLR qui a besoin d'un triplé en effectue la demande le moment venu.

La procédure d'authentification entre l'équipement mobile et le VLR/HLR est illustrée à la figure U.3.

Figure U.3
Authentification dans les réseaux GSM



L'algorithme A5 est implémenté dans chaque terminal et dans le réseau. Les implémentations des algorithmes A3 et A8, aussi appelés COMP128, existent sur Internet, mais aucun standard n'a encore été publié.

L'authentification EAP-SIM

Les hotspots, ou zones publiques à forte densité de population, telles que gares, aéroports, etc., peuvent être vus par les opérateurs de mobiles comme une extension possible de leur réseau. Il existe pour ces hotspots un mécanisme d'authentification mutuelle fondé sur le module SIM, appelé EAP-SIM. Ce protocole complète les procédures d'authentification utilisées par le GSM en fournissant une authentification entre le centre d'authentification de l'opérateur mobile et chaque module SIM. Les algorithmes d'authentification sont présents à la fois dans le réseau et dans toutes les cartes à puce SIM.

La solution EAP-SIM interagit directement avec les cartes à puce existantes. Sur le terminal, le composant logiciel qui implémente le protocole EAP-SIM peut utiliser PC/SC (Personal Computer/Smart Card), un environnement défini par un groupe d'industriels mené par Microsoft, pour communiquer directement avec la carte à puce de l'abonné. Une telle configuration ne nécessite aucune modification du réseau cœur GSM pour implémenter EAP-SIM. Par contre, il est nécessaire d'implémenter les communications entre le serveur d'authentification et le HLR/AuC, côté serveur, et entre le logiciel EAP-SIM et la carte SIM, côté client.

Une solution innovante a également été mise en place par un des fabricants majeurs de téléphones portables, permettant à une carte réseau 802.11 de communiquer directement avec un module SIM intégré, sans passer par le terminal, renforçant ainsi la sécurité.

L'identité (EAP-ID) est obtenue par la concaténation du caractère 1 de la valeur, exprimée en une suite de chiffres ASCII, de l'IMSI, du caractère @ et du nom de domaine de l'opérateur (EAP-ID = 1IMSI@operator.com).

L'authentification EAP-SIM se déroule de la manière suivante (*voir figure U.4*) :

1. Soit C le client et A le point d'accès. Dans ce processus, A utilise trois triplés d'authentification (RAND, Kc, SRES) :

   $$C \rightarrow A: RC$$

   Lors de cette première étape, le client C envoie au point d'accès A un défi aléatoire Rc.

2. A répond au client par la liste des trois nombres aléatoires RAND1, RAND2 et RAND3 provenant de trois triplés. Il envoie aussi le MAC calculé sur ces 3 nombres et sur Rc (MACk) :

   $$A \rightarrow C: RAND1, RAND2, RAND3, MACk[\ldots, RAND1, RAND2, RAND3, Rc]$$

3. La clé K, permettant le calcul de MACk, a été préalablement calculée par le point d'accès par dérivation d'une clé maître MK=SHA[…,Kc1,Kc2,Kc3,Rc,…], où Kc1, Kc2 et Kc3 sont les clés Kc des 3 triplés.

   $$C \rightarrow A: MACk[\ldots, SRES1, SRES2, SRES3]$$

4. Quand C reçoit MACk et la liste de nombres aléatoires RAND, il vérifie le MACk. Pour ce faire, C utilise Ki (présente sur la carte à puce de l'utilisateur et partagée avec le serveur d'authentification) pour retrouver les clés Kc1, Kc2 et Kc3. Ces dernières lui permettent de générer MK, qu'il utilise pour calculer K par dérivation.
5. Avec cette même clé K, C calcule le MAC sur les trois valeurs SRES des triplés et envoie le résultat au point d'accès. À son tour, A vérifie le MAC et la liste de SRES qu'il a reçus du réseau GSM. Si les résultats obtenus sont identiques, C est authentifié.

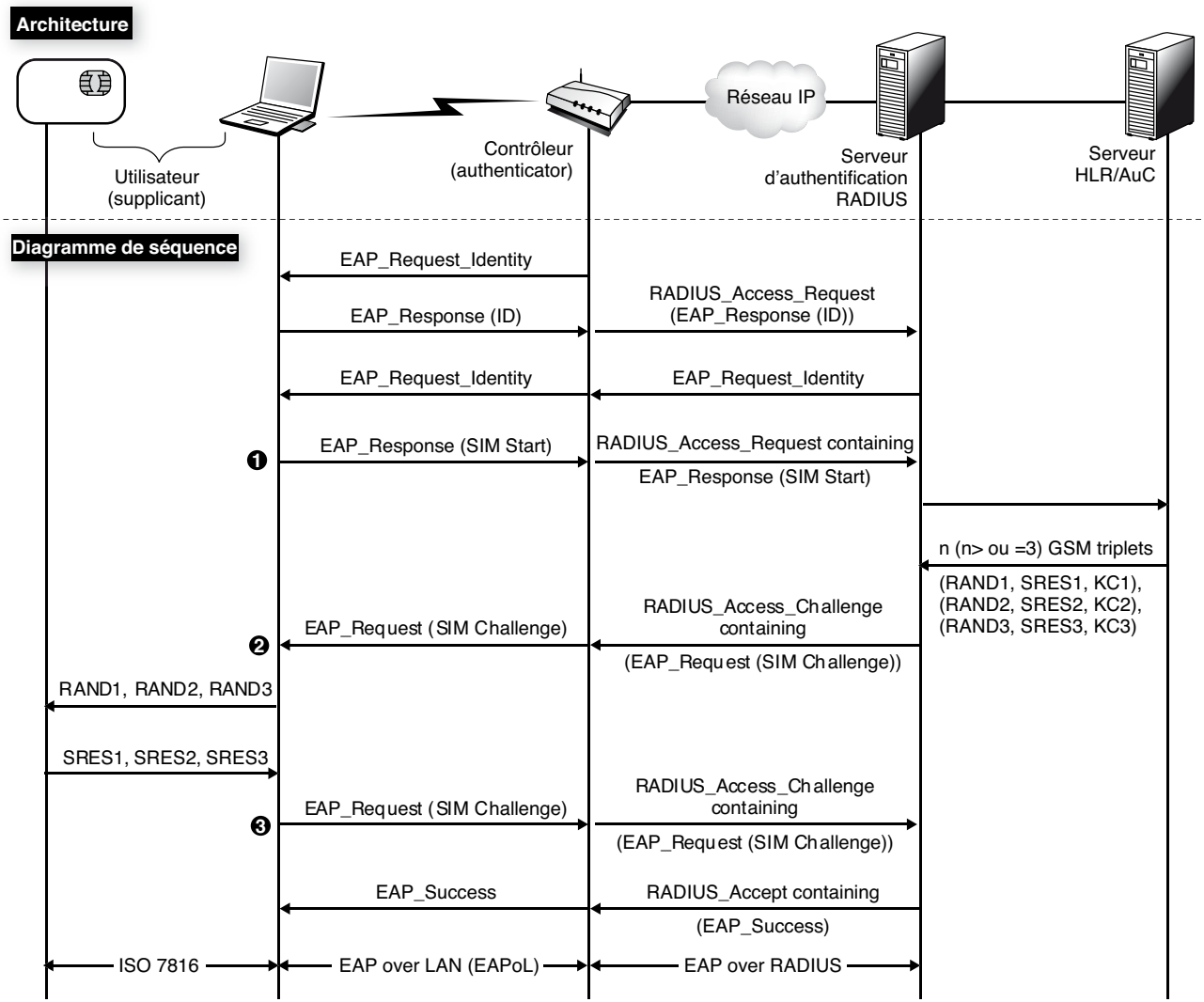


Figure U.4
Authentification EAP-SIM

Grâce à la technologie EAP-SIM, les opérateurs de téléphonie peuvent utiliser leur base de données client (HLR) pour assurer la facturation des services sans fil.

PEAP (Protected Extensible Authentication Protocol)

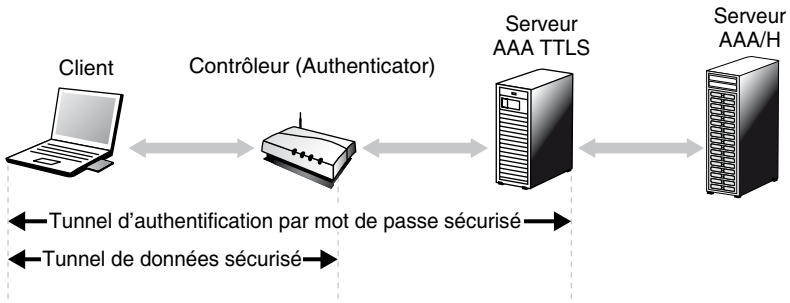
Les installations sans fil actuellement déployées utilisent des protocoles d'authentification hétérogènes. De ce fait, la mobilité du client est difficile à gérer. Pour une entreprise, EAP offre l'avantage de réutiliser dans son environnement sans fil des mécanismes déjà adoptés dans l'environnement filaire.

La sélection d'une méthode d'authentification est une décision stratégique pour le déploiement sécurisé d'un réseau. La méthode d'authentification conduit au choix du serveur d'authentification, qui, à son tour, conduit au choix du logiciel client. Dans le cas où une infrastructure PKI n'est pas déjà déployée, il existe d'autres méthodes d'authentification, présentant un niveau de sécurité équivalent à celui obtenu avec les certificats numériques et permettant de s'affranchir des barrières liées à la mise en place d'une infrastructure PKI. Ces méthodes permettent aussi de protéger les procédures d'authentification du client fondées sur des mots de passe.

Par exemple, EAP-TTLS (Tunneled Transport Layer Security) et PEAP conservent les fortes fondations cryptographiques de TLS et d'EAP mais utilisent d'autres mécanismes pour authentifier le client.

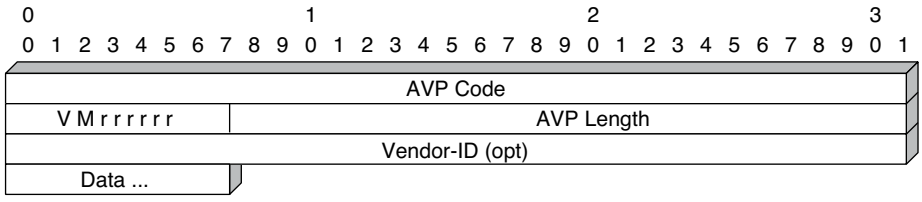
Ces protocoles établissent d'abord un tunnel sécurisé TLS, après quoi le client authentifie le serveur (*voir figure U.5*).

Figure U.5
Tunnels PEAP et EAP-TTLS



Dans une seconde étape, des paquets d'authentification sont échangés. TTLS échange des AVP (Attribute-Value Pairs) avec un serveur, qui les valide pour tout type d'authentification. Le format des paires de valeurs d'attributs est illustré à la figure U.6.

Figure U.6
Format des paires de valeurs d'attributs



PEAP utilise le canal TLS pour protéger un second échange EAP. MS-CHAP-V2 peut être utilisé pour les clients n'ayant pas de PKI. Pour les clients ayant une PKI, EAP-TLS peut être utilisé. L'avantage de PEAP par rapport à l'EAP-TLS classique est que l'identité du client est protégée lors de l'échange.

La figure U.7 illustre le principe de fonctionnement de PEAP.

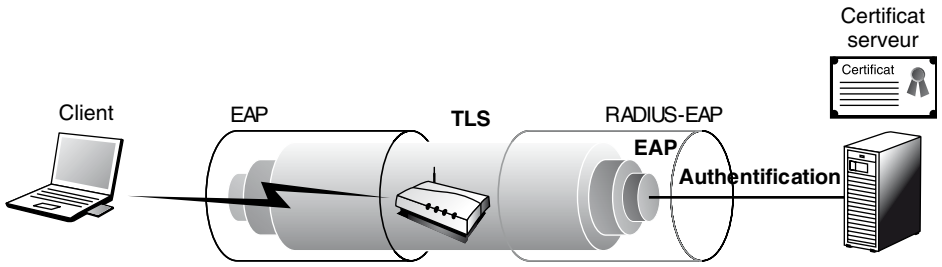


Figure U.7

Principe de fonctionnement de PEAP

La sécurité dans les protocoles

Conçus avant les années 2000, les protocoles du monde IP n'ont pas intégré de fonctions de sécurité. De nombreuses failles de sécurité existent donc, qui sont comblées régulièrement par des RFC spécifiques.

Les attaques sur les protocoles de gestion ou de contrôle peuvent facilement arrêter le fonctionnement d'un réseau. Il suffit, par exemple, de faire croire aux accès que le réseau est saturé ou que les nœuds sont en panne pour que les performances du réseau s'effondrent totalement.

La sécurité dans SNMP

La RFC 2274 définit le modèle USM (User-based Security Model) de sécurité de SNMP, qui offre à la fois une authentification et un service de sécurité.

Les principales attaques dont SNMP peut être l'objet sont les suivantes :

- Modification de l'information : une entité peut altérer un message en transit généré par une entité autorisée pour modifier une opération de type comptabilité, configuration ou opération.
- Mascarade : une entité prend l'identité d'une entité autorisée.
- Modification à l'intérieur d'un flot de messages : SNMP est construit pour gérer un protocole de transport en mode sans connexion. Les messages peuvent être réordonnés d'une façon différente de celle d'origine et détruits ou rejoués d'une autre manière. Par exemple, un message qui redémarre une machine peut être copié puis rejoué ultérieurement.

- Ordre de secret : une entité peut observer les échanges entre un manager et son agent et apprendre les valeurs des objets gérés. Par exemple, l'observation d'un ensemble de commandes capables de modifier un mot de passe permettrait à un utilisateur de modifier le mot de passe et d'attaquer le site.

Le modèle de sécurité USM ne prend pas en compte les deux fonctionnalités suivantes :

- Refus de service : un attaquant interdit l'échange d'informations entre un manager et son agent. Nous avons vu au chapitre 34, consacré à la gestion de réseau, que les échanges d'information de gestion s'effectuaient entre un manager de gestion et ses agents. Si le manager ne reçoit plus les informations du réseau et *vice versa,* les agents ne reçoivent plus les commandes du manager, et le processus de gestion du réseau ne peut plus s'effectuer. On appelle cette attaque un refus de service, puisque le service de gestion refuse de travailler.
- Analyse de trafic : un attaquant observe le type de trafic qui s'effectue entre un manager et son agent. L'analyse permet de détecter les ordres qui sont passés et les remontées d'information. Après analyse du trafic, le pirate peut faire croire au manager que le trafic est totalement différent de ce qu'il est effectivement dans le réseau.

Pour contrer ces différentes attaques, deux fonctions cryptographiques ont été définies dans USM : l'authentification et le chiffrement. Pour les réaliser, le moteur SNMP requiert deux valeurs : une clé privée et une clé d'authentification. Ces valeurs sont des attributs de l'utilisateur qui ne sont pas accessibles par des primitives SNMP.

Deux algorithmes d'authentification sont disponibles : HMAC-MD5-96 et HMAC-SHA-96. L'algorithme HMAC utilise une fonction de hachage sécurisée et une clé secrète pour produire un code d'authentification du message. Ce protocole fortement utilisé dans Internet est décrit en détail dans la RFC 2104.

Annexe V

30. ToIP et IPTV

Cette annexe détaille la téléphonie sur ATM et le relais de trames. En particulier, elle se penche sur la technologie AAL2, utilisée sur le RAN (Radio Accès Network) de l'UMTS, et examine l'évolution des PABX et l'intégration téléphonie-informatique.

La téléphonie sur ATM et le relais de trames

La technique de transfert ATM a été conçue pour transporter de la parole téléphonique de type G.711 à 64 Kbit/s. La raison de la petite taille de la cellule se trouve dans cette fonctionnalité. Les 48 octets de données de la trame sont remplis en 48 fois 125 µs, c'est-à-dire 6 ms, ce qui reste acceptable, même lorsqu'il y a des échos et que le temps de transit doit rester inférieur à 28 ms. Si la parole téléphonique est compressée par un codeur G.729 à 8 Kbit/s, il faut un temps de 48 ms de remplissage des 48 octets de données puisque le signal donne naissance à 1 octet toutes les 1 ms. Cette section examine la technique AAL-2 introduite dans la commutation ATM pour réaliser le transport de la voix téléphonique et plus particulièrement la téléphonie UMTS. Avant d'aborder l'AAL-2, introduisons les techniques préalables, qui sont encore utilisées dans les réseaux ATM.

L'émulation de circuit CES (Circuit Emulation Service) a été la première solution pour transporter de la téléphonie en paquet. Cette émulation de circuit utilise l'AAL-1 de l'environnement ATM, et plus précisément le service CBR (Constant Bit Rate), présenté au chapitre 15. Les PABX interconnectés par cette solution utilisent des interfaces E1 normalisées (G.703 et G.704). Le service ATM est de type circuit virtuel permanent. La signalisation sur l'interface est portée dans l'IT16 de l'interface E1.

Une autre solution, VTOA (Voice and Telephony Over ATM), ne privilégie pas de protocole AAL spécifique mais demande le support du service VBR-rt (Variable Bit Rate-real-time). Le PABX est relié au nœud d'accès du réseau de l'opérateur par un canal de type E1 structuré. La signalisation utilise encore l'IT16 de l'interface ou un circuit virtuel permanent dédié. Des normes classiques, comme le CCITT n° 7 ou Q-SIG (Q-Interface Signaling Protocol), une signalisation développée par l'UIT-T, sont utilisées. La parole elle-même est transportée par des liaisons permanentes ou commutées.

AAL-2

L'AAL-2 (ATM Adaptation Layer de type 2) correspond à la troisième couche du modèle ATM. C'est la couche qui s'occupe de la fragmentation et du réassemblage des messages pour obtenir des blocs à la dimension des cellules ATM. Comme nous allons le voir, l'AAL-2 détermine des fragments qui peuvent être tout petits de façon à ne pas perdre de temps à attendre des octets téléphoniques et à envoyer les fragments aussi vite que possible.

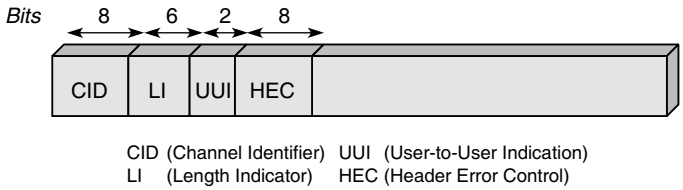
Les solutions précédentes concernent essentiellement la parole numérique sous forme de flux à 64 Kbit/s. En réalité, la parole est de plus en plus souvent compressée, comme nous l'avons vu au début de ce chapitre. Lorsque la compression est forte, comme lors de l'utilisation du codeur G.723.1, qui diminue le débit du flot à 6,3 Kbit/s, le temps de remplissage d'un paquet ATM devient très long, même pour une petite cellule.

Un calcul simple montre que, pour remplir une cellule de 48 octets à la vitesse de 6,3 Kbit/s, il faut plus de 60 ms. Ce temps est inacceptable si la communication génère des échos ou si d'autres temps d'attente incompressibles s'ajoutent. C'est notamment le cas de la parole numérique dans les réseaux de mobiles, où, au temps de remplissage de la cellule, s'ajoute un temps d'accès important sur l'interface air. Une solution possible, mais guère enthousiasmante, à ce problème est de ne remplir que partiellement les cellules. En supposant, par exemple, une compression de 50 %, amenant le débit à 32 Kbit/s, si l'on veut garder les mêmes contraintes que pour des flux à 64 Kbit/s, il ne faut remplir les cellules qu'à moitié. Cette solution induit un flux à 64 Kbit/s de cellules à moitié remplies.

Le rôle de l'AAL-2 est de remplir une cellule d'octets provenant de plusieurs connexions de parole, mais avec des débits variables pour les différentes voies basse vitesse. La solution du multiplexage de voies de débit constant est simple, puisqu'il suffit de connaître le numéro de l'octet pour récupérer le numéro de la connexion. Lorsque les flux sont variables, il faut ajouter une information pour savoir à quelle voie de parole appartient le segment.

Dans l'AAL-2, ce multiplexage de plusieurs voies de parole est effectué par des minitrames, appelées paquets CSP (Common Part Sublayer). La minitrame AAL-2 est illustrée à la figure V.1.

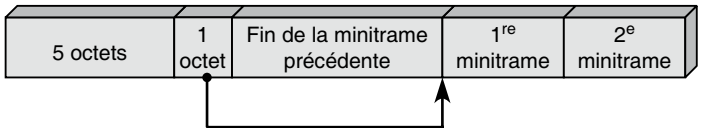
Figure V.1
Minitrame de l'AAL2



L'en-tête de la minitrame tient sur 3 octets. La zone CID (Channel IDentifier) est un identificateur de la voie de parole. Sa longueur de 1 octet permet de multiplexer jusqu'à 248 voies de parole (les valeurs 0 à 7 sont réservées). Le champ LI (Length Indicator) indique la longueur de la minitrame. Le champ UUI (User-to-User Indication) permet de transmettre de l'information d'une extrémité à l'autre de la connexion. Le champ HEC (Header Error Control) permet la détection et la correction des erreurs sur les deux octets précédents de l'en-tête. La longueur maximale d'une minitrame est de 64 octets, si bien que le transport d'une minitrame requiert parfois plus d'une seule cellule. Exactement 44 octets de longueur maximale sont nécessaires à son encapsulation dans une cellule ATM.

Les minitrames sont donc encapsulées dans les cellules ATM, et des bits de bourrage complètent la cellule pour arriver à une longueur de 47 octets, un octet étant réservé, comme dans l'AAL-1, pour transmettre des informations de contrôle. La cellule AAL-2 est illustrée à la figure V.2.

Figure V.2
Cellule AAL-2



L'octet de contrôle permet de pointer sur le début de la première minitrame encapsulée. En effet, il se peut que le début d'une minitranche ait été transporté dans une cellule précédente. Pour trouver cette valeur, il faut connaître la longueur de la dernière minitrame et compter les octets déjà envoyés dans la fin de la cellule précédente. Le pointeur est utile lorsqu'une cellule est perdue et qu'il faut retrouver le début d'une minitrame. Le pointeur requerrant 6 bits, il reste 2 bits, qui permettent d'effectuer une numérotation modulo 2 et une vérification de parité.

En conclusion, malgré la surcharge engendrée par l'en-tête des minitrames, l'AAL-2 est beaucoup plus efficace que l'utilisation d'une connexion unique pour une voie de parole.

Le relais de trames

Le problème du transport de la parole dans le relais de trames est similaire à celui que l'on trouve dans les réseaux ATM. Sur une liaison virtuelle, où les paquets peuvent atteindre plus de 4 000 octets, il est indispensable de multiplexer sur une même liaison plusieurs

voies de parole. La proposition FRF.11 du Frame Relay Forum décrit une solution de minitrame semblable à celle de l'AAL-2 pour transporter les voies de parole.

La possibilité d'avoir un commutateur occupé par la transmission d'une longue trame LAP-F crée toutefois une difficulté supplémentaire. Il faut donc un mécanisme de priorité pour laisser passer les petits paquets portant de la parole téléphonique.

Évolution des PABX

Les PABX sont les autocommutateurs téléphoniques qui gèrent les communications téléphoniques de type circuit. Leur évolution s'est accélérée au cours des quinze dernières années pour aboutir aujourd'hui à la quatrième génération. Ces différentes générations se sont enrichies d'une multitude de services et offrent désormais la possibilité de transmettre des données. Après un développement assez anarchique, la mise en place d'un réseau de communication entre PABX hétérogènes est devenue indispensable aux grandes entreprises. Cette communication entre PABX s'est concrétisée par la normalisation des échanges entre autocommutateurs.

L'environnement PABX s'est enrichi d'une extension lui permettant de prendre en charge des services évolués, comme le télémarketing ou la gestion des appels par menu grâce à l'association de processeurs informatiques. Nous présentons à la fin de ce chapitre cette intégration de la téléphonie et de l'informatique, appelée CTI (Computer Telephony Integration).

Les autocommutateurs privés

Un autocommutateur assure une liaison temporaire entre deux lignes d'abonnés (communication locale) ou entre une ligne d'abonné et une jonction allant vers un autre autocommutateur. L'autocommutateur se subdivise en deux sous-ensembles principaux : le réseau de connexion, à travers lequel s'effectue la connexion, et les organes de commande, qui effectuent les différents dialogues permettant l'établissement de la communication.

Fonctionnellement, on peut distinguer :

- les équipements individuels de ligne permettant le raccordement des postes téléphoniques ou des circuits ;
- le réseau de connexion ;
- l'unité de commande qui gère la traduction, la maintenance, les équipements de signalisation, etc. ;
- les organes de collecte et de distribution de la signalisation voie par voie ;
- les organes de collecte et de distribution de la signalisation par canal sémaphore.

Le numéro de l'appelé est la seule source d'information pour l'autocommutateur. Ce numéro doit être analysé, ou traduit, en fonction du plan de numérotation. En règle générale, un premier chiffre indique que l'appelé est sur le même PABX que l'appelant. Les

chiffres suivants désignent la ligne correspondant à l'appelé. Si le premier chiffre ne correspond pas au chiffre de l'autocommutateur, cela signifie que l'appelé est situé sur un autre autocommutateur. Dans ce cas, les premiers chiffres représentent le numéro de l'autocommutateur de l'appelé, et les derniers la ligne correspondant à l'appelé.

Cette architecture peut devenir plus complexe si l'on ajoute de nouvelles fonctionnalités, telles que des interfaces avec les réseaux locaux, des applications de messagerie vocale, etc. Un exemple de PABX IP avec des fonctionnalités de connexion à de la téléphonie classique est détaillé à la figure V.3.

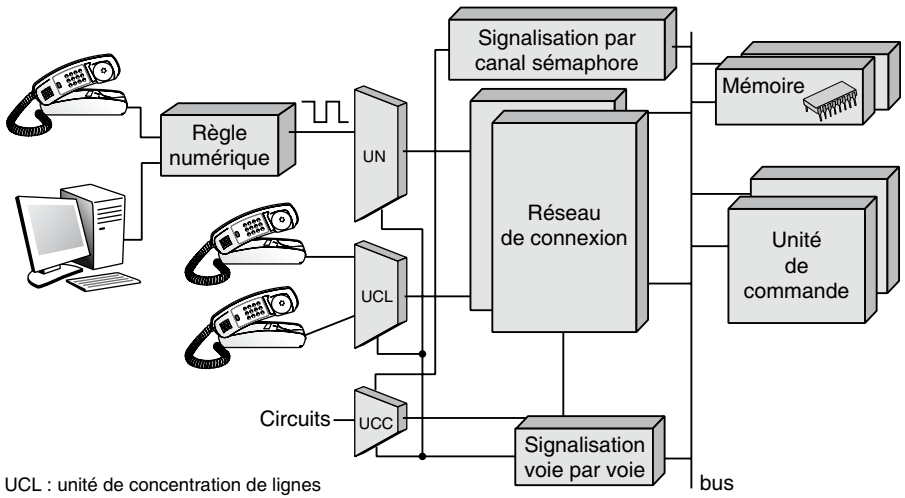


Figure V.3

Architecture générale d'un PABX

Un commutateur temporel permet d'émettre des voies entrantes dans un ordre quelconque sur les voies du multiplex de sortie. Il est constitué d'une mémoire tampon réceptionnant les IT (intervalles de temps) entrants et d'une mémoire de commande gérant la mémoire tampon. On distingue les commutateurs à commande aval et ceux à commande amont.

En mode de commande aval, les IT sont inscrits au fur et à mesure dans la mémoire tampon. La mémoire de commande contient à chaque instant l'adresse, en mémoire tampon, de l'échantillon à transmettre sur le multiplex de sortie. Si l'ITi entrant doit être connecté à l'ITj sortant, les octets de données entrant sur l'ITi doivent être envoyés sur l'ITj en sortie.

En mode de commande amont, les IT entrants sont inscrits dans la mémoire tampon, sous le contrôle de la mémoire de commande, dans l'ordre où ils sont lus avant d'être envoyés sur le multiplex de sortie. Ainsi, le mot i de la mémoire de commande contient l'adresse j où inscrire l'ITi entrant.

Les différentes générations de PABX

Issu de la technologie électromécanique, le type le plus ancien de commutateur privé a duré près de cent ans. La première génération de commutateurs électroniques est apparue dans les années 1960. La commutation est pilotée par un calculateur universel, et le réseau de connexion est de type spatial. Le raccordement au réseau public s'effectue *via* des groupements de lignes analogiques.

Dans un commutateur spatial, électronique ou électromécanique, l'établissement et la libération d'une communication se font respectivement par la mise en place et la rupture d'un certain nombre de points de connexion. Une fois un itinéraire établi, il sert de support exclusif à une seule communication.

La deuxième génération, datant du milieu des années 1970, offre la commutation de données, mais la voix et les données se trouvent sur des lignes séparées. L'interface avec les terminaux reste analogique. Si le calculateur intégré gérant la commutation offre certaines fonctionnalités nouvelles, telles que la numérotation abrégée ou l'interdiction d'appeler l'international, ces dernières restent largement sous-employées (IBM 3750 et TBX de Philips) en raison d'une ergonomie médiocre. Le réseau de connexion est temporel, et les abonnés sont reliés entre eux par l'intermédiaire d'une ligne multivoie. Un intervalle de temps est régulièrement affecté à chaque connexion, ce qui simplifie le réseau.

La troisième génération correspond à l'avènement des réseaux numériques à intégration de services, au début des années 1980. Elle est caractérisée par le multiplexage de la voix et des données sur la même porte du PABX, soit sur une même paire torsadée, soit sur deux. La transmission est généralement analogique. Le PABX étant entièrement numérique, des codecs équipent ses portes. La commutation est de type temporel, mais les voix et les données sont traitées différemment dans le PABX. Ces commutateurs offrent également des interfaces numériques à 64 Kbit/s, où peuvent se connecter divers terminaux et téléphones numériques. Le raccordement au réseau public devient lui aussi numérique grâce à des liaisons MIC (modulation par impulsion et codage) à 2 Mbit/s. Ces liaisons autorisent la sélection directe à l'arrivée et permettent aux centraux publics d'envoyer au PABX des informations relatives au coût de la communication (taxation), qui peuvent donc être retransmises à l'utilisateur au cours de la communication.

Une troisième génération et demie, de conception modulaire, est apparue au début des années 1990. Elle associe un commutateur de circuits à 64 Kbit/s et un commutateur de paquets X.25 ou relais de trames, chacun ayant son propre processeur. Ainsi, les variations du trafic de données ne pénalisent pas la qualité des services téléphoniques.

La quatrième génération est intervenue avec les PABX-IP, au milieu des années 1990, pour gérer des flux de paquets IP. Il est possible de connecter à la fois des téléphones numériques, les octets étant paquétisés dans des paquets IP, et des téléphones IP, qui envoient directement des paquets IP.

Une cinquième génération est à l'étude avec un cœur complètement IP. Cette génération ressemble à maints égards aux routeurs IP avec des signalisations SIP ou H.323.

PABX et transmission de données

Le débat en cours depuis quelques années sur les rôles respectifs des PABX et des LAN (réseaux locaux) dans la communication d'entreprise est aujourd'hui clos, les deux réseaux étant considérés comme complémentaires. Le PABX est parfaitement adapté au transport de la voix (64 Kbit/s/ligne), mais il peut également transporter des données à faible débit (jusqu'à 256 Kbit/s par ligne en interne). Le réseau local est adapté au transfert de données haut débit (10 Mbit/s pour un réseau Ethernet) mais pas à celui de la voix, du fait de contraintes temporelles trop strictes, sauf exception. Le tableau V.1 récapitule les caractéristiques comparées des PABX et des réseaux locaux.

Tableau V.1 • Comparaison des PABX et des réseaux locaux

	PABX	Réseau local
Architecture	Étoile	Étoile/bus/anneau
Support	Paire téléphonique	Paire téléphonique, coaxial, fibre
Mode de transmission	Analogique, numérique	Bande de base, large bande
Méthode d'accès	Circuit, paquet	CSMA/CD, jeton (bus/anneau)
Débit maximal	64 et 144 Kbit/s	De 50 à 1 000 Mbit/s
Capacité	10 à 6 000 terminaux	10 à 10 000 terminaux
Connexion aux réseaux publics	Multifréquence, numérique	Problèmes d'interface
Normalisation	De fait	Ethernet, Token-Ring

Pour satisfaire les besoins des utilisateurs, les deux techniques de commutation, paquet et circuit, doivent pouvoir être offertes sur les PABX. La première optimise les circuits physiques en y multiplexant plusieurs communications tandis que la seconde permet des débits élevés.

Les communications en mode circuit se font soit par modem, soit par intégration dans un raccordement numérique. L'accès d'un système informatique au service de circuits s'effectue par le biais d'un adaptateur de terminal chargé d'adapter la vitesse du terminal à celle du circuit (64 Kbit/s) et de supporter la fonction d'établissement de la communication. Les normes V.110 ou ECMA 102 sont utilisées pour l'adaptation de la vitesse et X.21 pour l'interface d'accès.

De même, les communications en mode paquet se font soit par modem, soit par intégration dans un raccordement numérique. Les relations entre terminaisons de standards différents sont automatiquement établies. Le PABX peut aussi établir en mode circuit une relation entre un terminal et un équipement de passerelle, lequel, selon les modèles, est situé dans le PABX.

Aujourd'hui, on distingue deux types d'architecture de PABX. Le premier privilégie la commutation de circuits pour le raccordement de terminaux. Les accès en transmission de données sont traités comme des communications téléphoniques, le PABX ayant alors

surtout un rôle de concentrateur de terminaux. L'optimisation du câblage est atteinte par l'utilisation des câbles téléphoniques pour le transfert des données.

Cette solution est plutôt destinée aux entreprises ayant peu de postes de travail informatiques par rapport aux téléphones ou qui emploient des applications à faible taux d'utilisation. Elle nécessite la mise en place d'un réseau local en cas de transmission de données importantes.

Certains commutateurs peuvent accéder à des réseaux locaux. C'est le cas des autocommutateurs munis d'une URM (unité de raccordement multiservice). Celle-ci peut recevoir des cartes d'interface pour permettre à un terminal asynchrone d'accéder à un réseau. De même, certains PABX sont dotés d'un interfaçage Ethernet. Chaque carte Ethernet peut supporter 24 connexions, et plusieurs cartes peuvent être installées en parallèle. Cet équipement permet le raccordement d'un système, *via* un câblage en paire torsadée, à un débit à 10 ou 100 Mbit/s.

Le second type d'architecture entraîne également la cohabitation PABX-LAN, les deux étant fournis cette fois par le même équipementier. Le LAN et le PABX sont alors reliés par une passerelle. Celle-ci permet à un utilisateur occasionnel, connecté au PABX, d'accéder à l'ensemble des ressources informatiques raccordées au LAN. De même, un utilisateur du LAN atteint les serveurs connectés au PABX et les réseaux publics raccordés à celui-ci. Ce type d'architecture profite pleinement de la complémentarité PABX-LAN et du plan de câblage unique.

La signalisation entre PABX

La signalisation entre les PABX peut se faire voie par voie ou par canal sémaphore. Jusqu'à présent, la première méthode est la plus utilisée. L'information utile et la signalisation empruntent les mêmes circuits physiques dans le réseau. Une bande de fréquences est réservée en mode spatial et 1 octet en mode temporel. Dans ce mode temporel, les paroles téléphoniques sont transportées dans des octets, et un octet particulier est réservé à la signalisation, par exemple l'octet transporté dans l'intervalle de temps Numéro 16 d'une communication en mode MIC (modulation, impulsion et codage).

La seconde méthode est caractérisée par l'utilisation d'un réseau de signalisation séparé du réseau transportant le trafic utile. Les informations relatives à chaque appel sont échangées sous forme de messages transportés par un canal annexe de transmission de données, commun à tout un groupe de circuits. Il y a quelques années, cette signalisation était propre à chaque constructeur. On compte aujourd'hui une centaine de types de signalisation privée inter-PABX, dont aucune n'est normalisée. Les organismes de normalisation ont par la suite proposé le protocole D, du nom du canal de signalisation dans lequel il est mis en œuvre, pour permettre la communication entre PABX hétérogènes et une gestion du réseau (réacheminement et reconfiguration en cas de surcharge de trafic ou de défaillance d'un commutateur, etc.). Adapté par l'ECMA (European Computer Manufacturers Association), ce protocole a été normalisé par l'ETSI sous le nom de Q-SIG (141 et 143). Cette norme s'aligne sur le protocole Q.932 de l'UIT-T utilisé pour l'interconnexion des autocommutateurs privés et des centraux publics.

Les caractéristiques principales du protocole de signalisation, que ce soit Q-SIG ou Q.932, sont les suivantes :

- Gestion des communications de type circuit ou paquet.
- Capacité à transmettre des informations de nature différente (signalisation, téléaction, maintenance, etc.).
- Fiabilité, due à l'emploi de méthodes efficaces de détection et de correction d'erreur grâce à l'utilisation d'une signalisation de type transmission de données.
- Extension du vocabulaire de la signalisation : il suffit pour toute nouvelle application d'indiquer aux logiciels des calculateurs l'élaboration et l'interprétation des nouveaux messages.

Parallèlement aux travaux de l'ECMA, un groupe de constructeurs, mené par Alcatel et Siemens, a fondé le forum IPNS (ISDN PBX Networking Standard), dont l'objectif est la normalisation des compléments de services offerts par les protocoles propriétaires. L'utilisation d'un protocole normalisé tel que Q-SIG devrait permettre de rassembler au sein d'un même réseau des PABX de constructeurs différents. Rappelons que la procédure CCITT n° 7 est le protocole choisi pour la signalisation entre commutateurs du RNIS. Ce protocole de signalisation n'est pas accessible par l'utilisateur, l'interfonctionnement avec le protocole Q-SIG se faisant dans les commutateurs d'abonnés.

L'intégration téléphonie-informatique

L'intégration de la téléphonie et de l'informatique n'est pas une nouveauté. Prévue depuis longtemps, la nécessité de cette alliance a commencé à se faire sentir dans les produits à partir de 1995. Cette intégration, qui a pris le nom de CTI, est née d'un groupe de travail sur le CSTA (Computer Supported Telephony Applications), et c'est l'ECMA qui a pris les choses en main en créant le groupe de travail TG11.

Un premier rapport a décrit les objectifs du CSTA :

- téléphonie évoluée (messagerie vocale, accès divers au réseau, téléconférence téléphonique, etc.) ;
- télémarketing ;
- service de clientèle ;
- micro-ordinateur comme centre de communication ;
- service de contrôle et d'alarme ;
- accès aux données de l'entreprise.

Ces services s'obtiennent par l'adjonction d'un équipement supplémentaire, qui s'interconnecte au PABX par une liaison CTI. Les terminaux sont connectés à ce serveur de téléphonie, tandis que les combinés téléphoniques continuent, bien sûr, à être connectés au PABX.

Éditeurs de logiciels et constructeurs de produits CTI

Les principales entreprises qui commercialisent des interfaces de programmation ou des produits de CTI sont les suivantes :

- Microsoft et Intel, avec l'interface TAPI (Telephony API) ;
- Novell, avec l'interface TSAPI (Novell Telephony Server API) ;
- Dialogic's, avec Dialogic's CT-Connect ;
- IBM Callpath ;
- Sun XTL Teleservice ;
- Hewlett Packard ACT ;
- Tandem CAM.

Tous ces produits de CTI visent à permettre au client qui téléphone d'atteindre l'agent capable de lui répondre par une synthèse vocale, par fax ou par toute autre solution viable. Ils visent également à mettre en mémoire les réponses d'un utilisateur.

Regardons d'un peu plus près l'interface de programmation TAPI de Microsoft-Intel, qui fait partie de l'architecture WOSA (Windows Open Services Architecture) de Microsoft. Plus exactement, WOSA est une plate-forme qui intègre les différents logiciels destinés aux applications du système d'information d'une entreprise. Outre l'application TAPI, WOSA contient ODBC (Open DataBase Connectivity), MAPI (Messaging Application Programming Interface), LSAPI (Licensing Server Application Program Interface), ainsi que des services de communication, comme le RPC de Microsoft.

TAPI est une interface générique d'appel de services. Trois objets ont été définis :

- L'objet ligne, qui caractérise la configuration et les numéros d'appel.
- L'objet appel, qui représente la mise en liaison avec le correspondant.
- L'objet téléphone, qui définit la configuration statique et les caractéristiques des combinés.

L'évolution de la CTI consiste en son intégration dans un environnement Internet permettant une connectivité totale de tous les éléments nécessaires à la vie d'une entreprise. Il devient dès lors possible de mettre en place des stratégies extrêmement évoluées d'utilisation des communications téléphoniques arrivant dans l'entreprise. De plus, il est relativement simple d'évoluer vers le multimédia.

Une des avancées immédiates provient des boîtes aux lettres universelles, capables de gérer toutes sortes de messages, de paroles, de fax, d'e-mail, etc. Il est possible, par exemple, d'effectuer une synthèse de parole à partir d'un e-mail ou d'un fax, de traduire une parole en fax, etc.

En résumé, l'association de la téléphonie et de l'informatique est en train de s'imposer par le biais de logiciels grand public. Cette intégration commence à faire partie de la vie de tous les jours.

Annexe W

31. Les réseaux autonomiques

Cette annexe concerne les réseaux intelligents, qui ont été définis dans les années 1990 pour permettre à de nouveaux services de télécommunications de se mettre en place en des laps de temps courts par rapport à ceux des années 1980. Ces réseaux intelligents sont aujourd'hui utilisés par les opérateurs pour introduire facilement de nouveaux services.

Les réseaux intelligents

L'expression « réseaux intelligents » concerne à une autre catégorie de réseaux, qui sont des réseaux qui peuvent s'adapter assez simplement à l'introduction d'un nouveau service. Ces réseaux sont totalement différents de ceux qui intègrent des agents intelligents.

Les architectures de réseau développées jusqu'à aujourd'hui ne permettent de prendre en compte que des services simples, ne faisant appel qu'à une seule application, tels les services de messagerie électronique, de transfert de fichiers, de traitement transactionnel, etc. Il est possible d'associer plusieurs applications pour réaliser un nouveau service en utilisant l'architecture mise en place dans la couche application. On peut ainsi transporter un document EDI (échange de données informatisé) dans un message électronique.

La complexité de la gestion et du contrôle des équipements de réseau s'accroît énormément dès lors que l'on sort du cadre du réseau et que l'on y intègre les applications. En effet, l'utilisateur désire avoir une vue globale du service qu'il demande, depuis son fonctionnement jusqu'à son coût, en passant par les problèmes de sécurité et de qualité de service. Le plus simple pour un utilisateur serait qu'il puisse définir exactement ce qu'il souhaite du réseau. Le rôle du réseau intelligent est justement de pouvoir s'adapter à la demande des utilisateurs.

Un premier exemple de service de réseau intelligent est le suivant : au début des années 1980, un grand utilisateur demande à son opérateur de mettre en place un service de renseignements téléphonique à destination de ses clients qui puisse, au moment le plus chargé, fournir un standard par département et, au moment le moins chargé, au milieu de la nuit, un seul standard répondant pour toute la France. Le client n'a aucune idée du numéro de téléphone à choisir en fonction de l'heure de la journée.

Ce service ne pouvait guère être mis en place à l'époque. Cependant, les opérateurs ont compris le message et ont lancé le numéro 800, ex-numéro vert en France. Ce numéro permet de diriger l'appel d'un client vers le standard le plus proche qui comporte une opératrice disponible. L'application 800 paraît simple. Elle a cependant demandé huit ans de développement. C'était le premier service intelligent à voir le jour. La raison de ce temps extrêmement long est due à l'impossibilité de programmer certains autocommutateurs pour leur dire que s'ils reçoivent un numéro qui commence par 800, ils doivent faire un travail très spécial, qui consiste à interroger une base de données pour trouver le numéro de téléphone à appeler.

Avec l'expérience retirée de la mise en place de ce service, les autocommutateurs sont devenus plus intelligents, et les concepts du réseau intelligent ont suivi. De nouveaux services intelligents, surtout associés à la téléphonie, sont nés, comme la facturation par carte de crédit et tous les numéros spéciaux qui existent aujourd'hui.

Le rôle d'un réseau intelligent est de mettre en place et d'adapter l'infrastructure du réseau de communication de façon à prendre en charge des fonctionnalités d'un nouveau service. Cette adaptation doit également déterminer l'environnement de contrôle et de gestion associé au réseau. De façon assez simpliste, on peut représenter le réseau intelligent comme une couche de protocoles située entre les ressources réseau et l'utilisateur, comme illustré à la figure W.1.

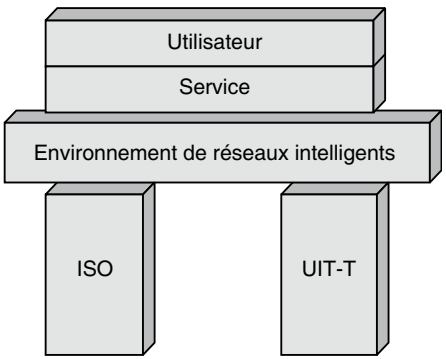


Figure W.1
Place du réseau intelligent dans l'architecture réseau

Pour introduire de façon correcte les différents composants logiciels et matériels nécessaires à la réalisation d'un réseau intelligent ou d'une architecture ayant les mêmes propriétés, il faut modéliser de façon efficace les fonctionnalités du réseau traité. Les

sections qui suivent décrivent le modèle de base du réseau intelligent avant de s'intéresser aux outils permettant de modéliser les fonctionnalités indispensables d'un tel réseau. Nous terminons par l'architecture TINA, que les opérateurs de télécommunications développent en ce sens.

INCM (Intelligent Network Conceptual Model)

Pour définir un réseau intelligent, il faut un modèle précisant l'architecture et les interfaces de référence. L'objectif d'un réseau intelligent étant de s'adapter à la demande de l'utilisateur, ces interfaces doivent permettre une adaptation simple des ressources du réseau. Un tel réseau est en fait intelligent grâce à ces interfaces.

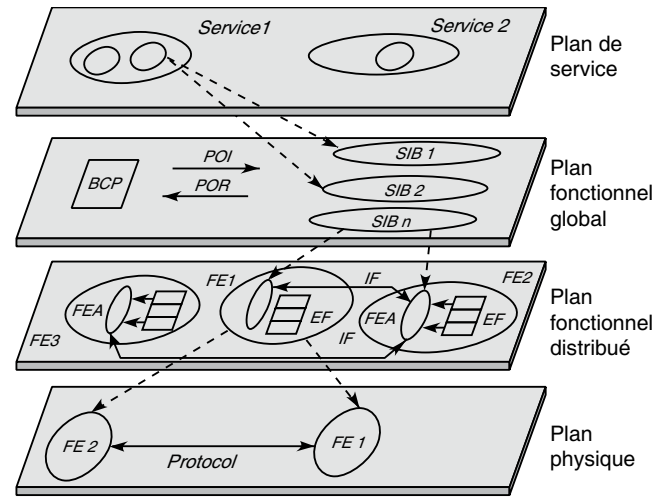
Le modèle conceptuel définissant l'architecture normalisée d'un réseau intelligent est aujourd'hui parfaitement défini. Il s'agit du modèle INCM (Intelligent Network Conceptual Model), qui peut être utilisé pour construire une architecture de réseau intelligent satisfaisant aux exigences suivantes :

- indépendance par rapport à la réalisation du service ;
- indépendance par rapport à la réalisation du réseau ;
- indépendance par rapport aux industriels ;
- indépendance par rapport à la technologie.

Le modèle INCM est illustré à la figure W.2. Il contient quatre couches, que nous allons décrire en détail.

Figure W.2

Plans de l'architecture du modèle de réseau intelligent



BCP (Basic Call Process)
SIB (Service Independent Building block)
FEA (Functional Entity Action)
POI (Point Of Initiation)
POR (Point Of Return)
EF (Elementary Function)
IF (Information Flows)
FE (Physical Entity)

Le plan de service

Le plan de service concerne la définition des services que l'utilisateur peut demander. Ces services peuvent être plus ou moins complexes, mais il s'agit généralement d'une superposition de services élémentaires. Un service élémentaire est appelé SF (Service Feature). La demande de l'utilisateur peut rassembler plusieurs services élémentaires pour former un nouveau service. Le service élémentaire SF est réalisé par un module qui se situe dans la couche sous-jacente : le plan fonctionnel global.

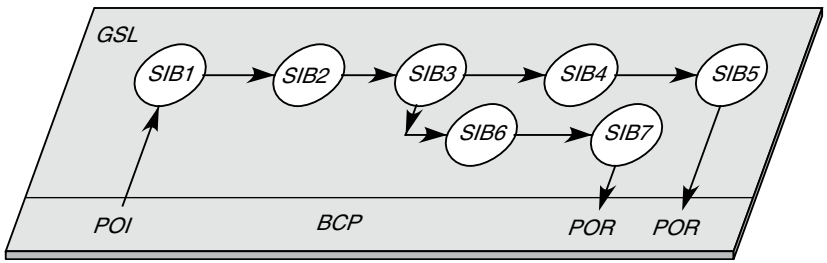
Le plan fonctionnel global

Le plan fonctionnel global contient les modules de base, ou SIB (Service-Independent Building). Ces modules doivent être considérés comme des blocs indépendants de la distribution. À ces blocs correspondent des services ou des parties de service. La distribution n'est prise en compte que dans le plan fonctionnel distribué, le réseau étant interprété comme une machine virtuelle.

Dans ce plan, le processus BCP (Basic Call Process) et les processus GSL (Global Service Logic) sont des SIB spécialisés. Les GSL permettent de chaîner les SIB entre eux pour réaliser un service. Le GSL décrit donc entièrement le service.

Le BCP est un SIB qui contient toutes les fonctionnalités permettant de gérer un appel. Cette gestion utilise deux types de points de synchronisation : les POI (Point Of Initiation) et les POR (Point Of Return). Les POI déterminent à quel moment du traitement il faut appeler le GSL et selon quels critères. Les POR définissent les points au niveau desquels le GSL peut réactiver le réseau pour continuer le processus de service. Ce processus est illustré à la figure W.3.

Figure W.3
Fonctionnement d'un processus GSL



Le GSL décrit un enchaînement linéaire d'exécution de SIB. Le parallélisme, c'est-à-dire la possibilité que plusieurs SIB soient exécutés en parallèle, ne devrait pas tarder. Ce parallélisme devrait apporter des améliorations à la définition de services futurs encore plus complexes. Enfin, dans l'exécution du GSL, plusieurs demandes de POR peuvent être engendrées entre deux POI, de façon à gérer, par exemple, divers événements lors du traitement d'appel.

Les SIB peuvent être extrêmement nombreux. En voici quelques exemples :

- Charge, qui définit les procédures de taxation.
- Compare, qui permet de comparer deux valeurs.

- Limit, qui limite le nombre d'appels à un service.
- Log Call Information, qui permet de stocker des informations sur l'appel en cours.
- Queue, qui permet de mettre un appel en attente.
- Screen, qui permet de vérifier la présence d'un identifiant.
- Service Data Management, qui permet de lire, de créer, d'ajouter ou de supprimer des données dans un fichier.
- Status Notification, qui permet de connaître l'état des ressources du réseau.
- Translate, qui traduit des données de l'utilisateur en termes accessibles au système.
- User Information, qui permet au système de correspondre avec un utilisateur.
- Verify, qui vérifie la syntaxe des informations émises par l'utilisateur.

Le plan fonctionnel distribué

Le plan fonctionnel distribué a pour rôle d'identifier les modules (et leurs relations) nécessaires à la réalisation du réseau intelligent. Ces modules possèdent des fonctions décrites dans la recommandation Q.1204 de l'UIT-T. La description de cette architecture est indépendante de sa réalisation. Celle-ci doit être très flexible, de façon à permettre l'introduction de nouvelles fonctionnalités, indispensables à l'extension des possibilités du réseau intelligent.

Une correspondance assez simple doit être réalisée entre les entités fonctionnelles du plan fonctionnel distribué et les modules SIB (Service-Independent Building) du plan fonctionnel global. Plus précisément, la réalisation de chaque SIB doit s'effectuer à l'aide d'au moins une unité fonctionnelle. Les fonctions de base de l'entité fonctionnelle sont gérées par des actions d'entité fonctionnelle, ou FEA (Functional Entity Action).

Construction d'une application intelligente

En ayant en tête cette représentation du modèle de réseau intelligent, il est possible de comprendre la construction d'une application intelligente.

Le client choisit les services élémentaires dont il a besoin pour réaliser son service global. Il définit ainsi dans le plan de service le service désiré. Une fois le service déterminé, le modèle lui indique les SIB dont il a besoin et l'ordre dans lequel il doit les mettre en œuvre. En d'autres termes, il construit, grâce aux briques de logiciel dont il dispose, le logiciel dont il a besoin pour réaliser son service. C'est le travail effectué dans le plan fonctionnel global.

Pour distribuer ce logiciel global sur le réseau, le client peut soit le distribuer dans tous les nœuds du réseau, soit le placer en un emplacement unique. Le rôle du plan fonctionnel distribué est d'effectuer la distribution du logiciel global. La dernière étape consiste à déterminer où implanter physiquement les briques logicielles.

Les entités fonctionnelles

Une entité fonctionnelle est un groupe unique de fonctions destinées à rendre un service. Une ou plusieurs entités fonctionnelles peuvent être situées sur une même entité physique. Deux entités fonctionnelles distinctes peuvent contenir des fonctions identiques. Les entités fonctionnelles communiquent entre elles par des flux d'information (Information Flow).

Les principales entités fonctionnelles sont les suivantes :

- CCAF (Call Control Agent Function), qui gère l'interface entre l'utilisateur et le réseau.
- CCF (Call Control Function), qui établit, manipule et relâche les appels des utilisateurs dans leur demande de service.
- SSF (Service Switching Function), qui est souvent associée au CCF et permet de réaliser la connexion entre un utilisateur et l'entité de contrôle du service (SCF).
- SCF (Service Control Function), qui contrôle le bon déroulement du module CCF lors de son exécution de sorte qu'il atteigne les entités fonctionnelles de service nécessaires à la réalisation du service demandé par l'utilisateur.
- SDF (Service Data Function), qui contient toutes les informations et fonctions nécessaires pour qu'une entité SCF ait accès en temps réel à un service de réseau intelligent demandé par l'utilisateur.
- SRF (Specialized Resource Function), qui contient des ressources spécifiques qui peuvent s'avérer nécessaires à un service de réseau intelligent.

Les entités fonctionnelles que nous venons de décrire servent à l'accès et à la mise en place du service dans un réseau intelligent mais n'ont pas de fonctionnalités correspondant au service. Il s'agit d'entités fonctionnelles communes, permettant de mettre en place le service.

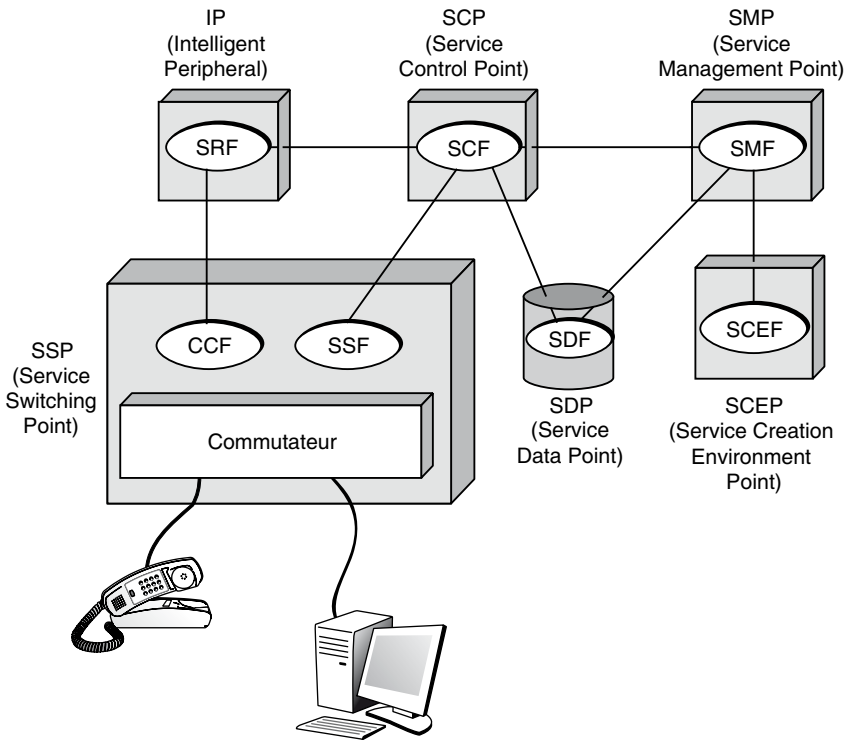
Les entités fonctionnelles suivantes servent, elles, à créer et gérer les services :

- SCEF (Service Creation Environment Function), qui permet la création de nouveaux services de réseau intelligent.
- SMAF (Service Management Agent Function), qui définit une interface entre le gestionnaire du service et la fonction de gestion SMF.
- SMF (Service Management Function), qui doit prendre en charge la gestion des services ouverts dans le cadre du réseau intelligent et coordonne les SCF et les SDF.

Les relations entre les entités fonctionnelles sont nombreuses. La figure W.4 en fournit un exemple simplifié. Elle schématise également des éléments physiques que nous allons aborder ci-après.

Figure W.4

Exemple de relations entre les entités fonctionnelles



Le plan physique

Le plan physique du modèle conceptuel de réseau intelligent identifie les différentes entités physiques et les interfaces entre ces entités. L'architecture du plan physique doit être en cohérence avec le modèle conceptuel INCM. Pour cela, cette architecture doit satisfaire aux exigences suivantes :

- À une entité fonctionnelle du plan fonctionnel distribué correspond une entité physique.
- Une entité fonctionnelle ne peut être découpée et correspondre à deux entités physiques. En d'autres termes, une entité fonctionnelle correspond à une entité physique ou à une partie d'une entité physique.
- Des copies d'une même entité fonctionnelle correspondent à des entités physiques différentes.
- Les entités physiques peuvent être regroupées pour former une architecture physique.
- Les entités physiques peuvent offrir des interfaces standards.
- Les entités physiques sont capables de développer des entités physiques fondées sur une correspondance avec des entités fonctionnelles, et ce avec des interfaces standards.
- Les industriels peuvent adapter leurs produits à de nouvelles technologies sans revoir les principes de l'architecture.

De nombreuses entités physiques ont été définies pour le réseau intelligent, notamment les suivantes :

- SSP (Service Switching Point). Ce sont les points d'accès des utilisateurs au réseau intelligent. Ils sont avant tout des points de commutation, qui se chargent des informations provenant des machines terminales. Les SSP peuvent communiquer avec les autres entités physiques, et en particulier avec les SCP. Un SSP contient une fonction de contrôle d'appel, ou CCF (Call Control Function), une fonction de service de commutation, ou SSF (Service Switching Function), et, si le SSP est un point d'accès utilisateur, une fonction d'agent de contrôle des appels, ou CCAF (Call Control Agent Function). D'autres fonctions plus spécialisées peuvent être disponibles dans un SSP, telles une fonction de ressources spécialisées, ou SRF (Specialized Resource Function), et une fonction de données de service, ou SDF (Service Data Function).
- SCP (Service Control Point). Contient les programmes de logique de service, ou SLP (Service Logic Programs), qui sont utilisés pour rendre le service demandé. Les SCP peuvent posséder des SLP identiques. Un SCP contient une fonction de contrôle de service, ou SCF (Service Control Function), et peut avoir une fonction de données de service, ou SDF (Service Data Function). Le SCP peut accéder à des données situées dans une autre entité physique, soit directement, soit par l'intermédiaire du réseau de signalisation. Le SCP est souvent connecté à des SSP pour traiter les demandes utilisateur qui nécessitent l'intervention du réseau intelligent. La connexion s'effectue par l'intermédiaire du réseau sémaphore.
- SDP (Service Data Point). Les SDP contiennent toutes les données qui seront utilisées par les programmes de logique de service (SLP). Un SDP comporte une fonction de données de service, ou SDF (Service Data Function). Il est possible d'accéder au SDP soit directement, par un SCP ou un SMP, soit par le réseau sémaphore.
- IP (Intelligent Peripheral). Les IP disposent de ressources spécifiques pour permettre une adaptation des commandes de service à la demande utilisateur. Ces ressources très générales incluent :
  - Les annonceurs, par exemple l'organe qui indique le nouveau numéro de téléphone d'un abonné qui a déménagé.
  - Des organes de synthèse de la parole.
  - Des organes de reconnaissance de la parole.
  - Des organes nécessaires à la réalisation d'une téléconférence.
  - Des organes pour intégrer des données venues de l'extérieur.
  - Des générateurs de tonalité.
  - Des tests en synthèse de la parole.
  - Des convertisseurs de protocole.

  Fonctionnellement, un IP contient une fonction de ressources spécifiques SRF (Specialized Resource Function) ou une fonction de contrôle d'appel CCF (Call Control Function). Ces deux fonctions permettent d'accéder aux ressources de l'entité physique IP à partir du SSP.

- AD (ADjunct). L'entité physique AD est fonctionnellement équivalente à celle de SCP. Elle contient les mêmes entités fonctionnelles. La spécificité de l'AD est d'être connecté directement à un SSP. L'interface entre les deux entités peut permettre de très hauts débits et générer de nouveaux services. Un AD peut être connecté à plusieurs SSP, et plusieurs AD peuvent être connectés au même SSP.
- SN (Service Node). Le SN sert à contrôler les services rendus par le réseau intelligent. Un SN communique directement avec un ou plusieurs SSP par le réseau sémaphore. Fonctionnellement, un SN peut contenir un SCF, un SDF, un SRF, un SSF et un CCF. D'une manière similaire à l'AD, la fonction de contrôle de service SCF d'un SN reçoit des messages du SSP, exécute les SLP et renvoie des messages au SSP. Les SLP peuvent être développés par l'environnement de création de nouveaux services.
- SSCP (Service Switching and Control Point). Cette entité physique est une combinaison des SCP et SSP dans un même nœud. Elle contient les fonctions SCF, SDF, CCAF et SSF.
- SMP (Service Management Point). Le SMP réalise les contrôles nécessaires à la gestion du service. Les exemples de fonctions que cette entité physique doit contrôler sont nombreux et vont de la gestion des bases de données de gestion, à la surveillance du réseau, en passant par les tests sur le réseau et la gestion du trafic, des anomalies, de la comptabilité, etc. Un SMP contient la fonction de gestion du service, ou SMF (Service Management Function), ainsi que, optionnellement, celle d'accès à la gestion du service, ou SMAF (Service Management Access Function) et celle d'environnement de création de service, ou SCEF (Service Creation Environment Function).
- SCEP (Service Creation Environment Point). Un SCEP permet de définir, de développer et de tester un nouveau service de réseau intelligent. Il peut charger le logiciel correspondant dans le SMP. Le SCEP contient la fonction d'environnement de création de services, ou SCEF. L'unité physique SCEP travaille directement avec l'unité SMP.
- SMAP (Service Management Access Point). L'unité physique SMAP permet à certains utilisateurs d'accéder directement à l'unité physique SMP. Un SMAP peut notamment constituer l'interface unique d'un utilisateur avec plusieurs SMP. Un SMAP contient une fonction d'accès à la gestion du service, ou SMAF. Les SMAP communiquent directement avec les SMP.

Modélisation des fonctionnalités

La mise en place d'un réseau intelligent requiert des outils informatiques avancés, tels que des techniques objet, des bases de données distribuées, des bases de connaissances, des techniques provenant de l'intelligence artificielle, etc. L'intelligence est presque absente des architectures que nous avons rencontrées à la section précédente. C'est là un paradoxe, même si une certaine intelligence primaire se cache dans cette adaptation.

Le temps nécessaire à l'introduction de nouveaux services intelligents a été jusqu'à présent très long et se compte en années. Par exemple, l'introduction du numéro vert ou des cartes téléphoniques a demandé de nombreuses années du fait qu'il fallait implanter de nouvelles commandes dans tous les commutateurs et points de gestion. L'introduction

des SIB et de l'infrastructure des réseaux intelligents va permettre de diviser par 10, voire par 100, ces temps de mise en œuvre.

Les techniques utilisées proviennent des architectures orientées objet, qui offrent une grande souplesse de mise en œuvre et une gestion simplifiée par la suite. Les bases de données distribuées forment également un thème clé pour le stockage des connaissances et des informations.

L'intelligence artificielle est à la base de très nombreux outils qui commencent à être utilisés dans le logiciel du réseau intelligent. En effet, les systèmes qui nous intéressent sont particulièrement complexes, et l'on ne sait plus aujourd'hui gérer cette complexité avec des machines centralisées de type séquentiel. Les corrélations entre événements sont telles que des systèmes à base de règles et de connaissances sont plus aptes à répondre aux problèmes de diagnostic et plus généralement aux demandes des systèmes de gestion. La distribution pousse vers une nouvelle direction : l'intelligence artificielle distribuée.

Par l'introduction du concept d'intelligence artificielle distribuée, on doit pouvoir parvenir à une automatisation de la mise en place de l'infrastructure associée au service. Ce type d'implémentation prend en compte la complexité due à la distribution des fonctionnalités. Des systèmes multiagents cognitifs peuvent aussi être introduits dans le plan fonctionnel global pour permettre de corréler, filtrer, diagnostiquer et prendre des décisions. Ce type d'environnement est présenté au chapitre 31.

ODP (Open Distributed Processing)

Cette section s'intéresse à la modélisation des fonctionnalités nécessaires pour réaliser un réseau distribué. À ce titre, nous examinons ODP et le modèle d'architecture G.805 de l'UIT-T.

L'architecture ODP propose un modèle très général, qui a pour objet de décrire la sémantique et l'architecture des systèmes répartis ouverts. Défini dans les normes ISO et UIT-T X.901, X.902 et X.903, ce modèle se fonde sur deux concepts de base, à savoir une distribution objet et une découpe des systèmes en « points de vue » (*voir plus loin*).

À la fin des années 1980, l'ISO s'est efforcé de dépasser la seule normalisation des protocoles de communication et a essayé d'organiser les protocoles dans un contexte plus vaste, celui d'un système distribué, mis en place dans le cadre d'une entreprise. Le rôle d'ODP est de normaliser les outils de conception et de gestion globale de la distribution des traitements dans l'univers réparti d'une entreprise.

L'ensemble des documents normatifs comprend quatre parties :

- La partie 1, non normative, regroupe les objectifs d'ODP, un aperçu d'ODP, les concepts clés et des éléments de base de l'architecture.
- La partie 2 contient le modèle descriptif. Ce modèle définit les concepts de la modélisation (objets, interfaces, états, interactions, etc.), les concepts de spécification (composition, décomposition, compatibilité, type, classe, etc.) et les concepts architecturaux (organisation, propriétés des objets, nommage, etc.).
- La partie 3 contient le modèle prescriptif. Celui-ci permet de caractériser un système ouvert à l'aide de techniques descriptives aptes à détecter si les contraintes définissant un système ODP sont satisfaites.

- La partie 4 décrit la sémantique architecturale, c'est-à-dire la manière dont les concepts de modélisation et le modèle prescriptif peuvent être représentés par une technique de description formelle.

Cinq points de vue, représentant autant d'approches d'un même problème — un point de vue apporte une description abstraite du système — ont été définis par les normalisateurs :

- Le point de vue Enterprise (entreprise) envisage la place du système distribué dans l'entreprise. Il concerne essentiellement l'utilisation du système distribué et la gestion de l'entreprise.
- Le point de vue Informational (information) concerne les informations manipulées par le système distribué et l'usage que l'on peut en faire.
- Le point de vue Computational (traitement) vise l'organisation fonctionnelle du système. En d'autres termes, il implique la définition des logiciels qui participent aux systèmes distribués.
- Le point de vue Engineering (ingénierie) est relatif à la distribution des ressources du système distribué, c'est-à-dire à la façon de construire le système distribué pour que les traitements puissent se faire dans les meilleures conditions possibles.
- Le point de vue Technology (technologie) concerne les choix d'implantation des composants physiques (matériels, logiciels, systèmes de gestion, protocoles, etc.).

L'architecture ODP s'appuie sur la notion d'objet. Un objet est caractérisé par un identificateur, un état et un comportement. L'accès à un objet s'effectue par des interfaces, qui déterminent les interactions entre l'objet et son environnement. Nous reviendrons sur la normalisation des environnements objet au chapitre suivant.

Dans ODP, on définit également les aspects d'un système. Ces aspects sont identifiés par les problèmes que doit résoudre le système de traitement réparti et existent généralement dans les différents points de vue. Deux catégories ont été définies, qui regroupent, d'une part, les aspects qui nécessitent la répartition (traitement, stockage et accès utilisateur) et, d'autre part, les aspects supportant la distribution (communication, identification, gestion et sécurité).

Des fonctions génériques ont aussi été définies pour la construction des systèmes ODP. Elles sont décrites selon les points de vue et regroupées en quatre classes : gestion, répertoire, sécurité et transparence.

Le modèle de référence ODP (RM-ODP) définit un ensemble de concepts architecturaux pour la construction d'un système ODP. Orientés objet, les systèmes ODP sont définis en terme d'interactions d'un ensemble de composants objets avec les interfaces identifiées. Des templates, ou « patrons », d'objets sont introduits pour décrire les contraintes en fonction desquelles les objets sont instanciés. Les objets résultant des templates sont organisés dans une famille de classes liées par la relation entre sous-classe et superclasse.

Le modèle G.805 et UML

Le modèle G.805 a été élaboré à la fin des années 1990 pour définir les principales fonctionnalités des réseaux. Il a pour rôle de représenter tous les types de réseaux et tous les protocoles associés.

Trois fonctions de base ont été identifiées : les fonctions de connexion, d'adaptation et de terminaison. Les fonctions de connexion concernent l'établissement de connexions entre deux points. Les fonctions d'adaptation correspondent à la mise en forme des données d'un utilisateur en vue de leur émission sur un réseau. Les fonctions de terminaison correspondent au contrôle et à la gestion effectués sur le service de transport du réseau. Outre ces principes fonctionnels, la recommandation G.805 introduit un ensemble de concepts pour modéliser les couches de protocoles, les différents niveaux d'abstraction et les entités de transport.

Les entités du processus de modélisation sont essentiellement les suivantes :

- Les sous-réseaux formés des points qui peuvent être connectés directement. Le mot sous-réseau remplace le mot réseau, trop générique.
- Les connexions de liens, qui représentent les connexions définies une fois pour toutes entre deux points.
- Les connexions de sous-réseaux, qui correspondent à des connexions pouvant être modifiées avec le temps.
- Les liens, qui correspondent à des capacités de transfert entre deux sous-réseaux.
- Les trails, qui correspondent à des connexions de bout en bout.
- Les points de connexion, qui forment les extrémités d'une connexion.
- Les points de terminaison, qui constituent les extrémités d'un trail.

Ces différentes fonctionnalités constituent un modèle complet permettant d'établir des architectures de réseau avec leurs fonctionnalités. Des extensions ont été réalisées à la fin des années 1990 pour que soit pris en compte l'aspect service, qui n'apparaît pas vraiment dans la modélisation de base. Contrairement au modèle ODP, la description n'est pas du tout orientée objet. Des sous-ensembles ont été déterminés pour la description d'architectures spécifiques, comme G.803, qui vise les architectures SDH (Synchronous Digital Hierarchy).

Décrire une architecture fonctionnelle est une chose, mais arriver à utiliser ces concepts simplement en est une autre. Pour cela, il faut unifier les notations. À cet égard, UML (Unified Modeling Language) constitue une réponse possible pour une notation unifiée acceptée par les industriels. Finalisée en 1999 par l'OMG (Object Management Group), la norme UML repose sur des concepts fondés sur un métamodèle, c'est-à-dire un modèle réalisé à partir des modèles de base, bien formalisés. UML s'appuie fortement sur C++ et non sur les nouveaux langages apportant une forte distribution, comme Java. Cependant, les outils UML offrent de nombreux moyens de génération vers les principaux langages de programmation.

TINA (Telecom Information Networking Architecture)

L'initiative TINA est plus large que le concept de réseau intelligent. Elle consiste à développer une plate-forme ouverte pour accueillir tous les types de services.

Le concept de réseau intelligent est né du besoin de développer une architecture globale capable d'appréhender l'ensemble des problèmes posés par la mise en place d'un nouveau service, depuis ceux à traiter par l'utilisateur jusqu'à ceux à traiter par le réseau. Tous les SIB doivent être les mêmes pour tous les opérateurs pour qu'un service puisse être accessible depuis tous les clients de tous les opérateurs. Il faut donc que tous les opérateurs désirant développer un réseau intelligent se mettent d'accord sur les composants divers et variés (service élémentaire, SIB, etc.) nécessaires à sa réalisation. Plusieurs initiatives ont été élaborées par différents types de groupements pour essayer de créer un consortium mondial capable d'imposer une vue uniforme du réseau intelligent.

Finalement, l'initiative qui a réellement lancé le mouvement pour développer un réseau intelligent sur la planète a été prise par des organes de normalisation, et plus particulièrement par l'UIT-T, qui a développé le modèle conceptuel du réseau intelligent INCM (Intelligent Network Conceptual Model), présenté à la première section de ce chapitre.

Une cinquantaine d'opérateurs de télécommunications ont regroupé leur force pour donner naissance à l'architecture TINA (Telecommunications Information Networking Architecture). Le groupe TINA-C (TINA Consortium) a défini une architecture très générale, la plus ouverte possible, susceptible de prendre en charge tous les types de services large bande et multimédias, y compris les grands standards du monde des télécommunications, tels ODP (Open Distributed Processing), IN (Intelligent Network), TMN (Telecommunications Management Network) et CORBA (Common Object Request Broker Architecture).

L'architecture TINA est divisée en trois sous-ensembles : une architecture de traitement, une architecture de service et une architecture de gestion. Un service TINA est déterminé par des composants de service, qui sont des unités de logiciel, appelées objets de traitement. L'exécution de ces objets est réalisée par un environnement distribué d'exécution, le DPE (Distributed Processing Environment). Cet environnement s'appuie sur un noyau, le noyau DPE, et des services DPE.

Parmi les exemples de services DPE, citons les services rendus par des intermédiaires, appelés traders, les serveurs de noms, qui permettent d'identifier et de localiser les unités de logiciels nécessaires à l'exécution, les serveurs de sécurité et les serveurs de transactions.

L'architecture de traitement suit le modèle ODP. C'est une architecture orientée objet. Dans TINA, le composant de base, l'objet, est appelé USCM (Usage, Substance, Core, Management), car il est défini par les éléments suivants : un noyau (core), décrivant la nature de l'objet indépendamment de son utilisation et de sa gestion, un usage, décrivant son apparence pour l'utilisateur, une gestion (management), décrivant les opérations de gestion et de maintenance, et une substance, représentant sa dépendance vis-à-vis des autres composants du système.

Un autre principe de l'architecture de traitement est l'indépendance des composants logiciels vis-à-vis des services et de leur environnement distribué ainsi que vis-à-vis de la technologie déployée pour réaliser le système.

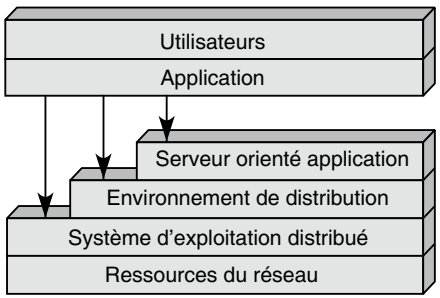
Le modèle d'interaction qui définit comment les composants peuvent interagir est décrit dans le document *TINA Computational Modeling Concepts*. Les interfaces sont spécifiées indépendamment du langage de programmation utilisé (GDMO, OMG IDL, OSF IDL). Pour réaliser les spécifications d'interface de TINA, une extension d'IDL (Interface Definition Language) a été développée sous le nom d'ODL (Object Definition Language).

L'architecture de service décrit le moyen de construire des services de tout type : accès, transport, gestion, information, etc. De nouveau, les services sont décrits indépendamment des moyens qui permettent leur mise en œuvre. L'architecture du réseau intelligent en est la base.

L'architecture de gestion décrit l'ensemble des services de gestion à mettre en œuvre pour administrer le système. L'architecture de base retenue pour la gestion est le TMN.

On peut définir TINA comme une architecture à six niveaux, comme illustré à la figure W.5.

Figure W.5
Architecture TINA

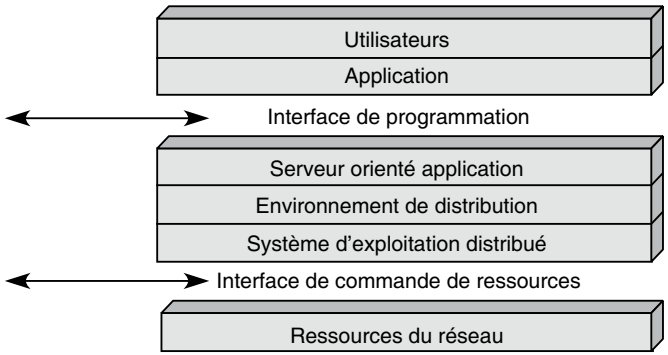


Le niveau le plus haut concerne l'utilisateur et sa vision dans l'entreprise du service qu'il souhaite obtenir. Le deuxième niveau s'intéresse au service lui-même : il en définit les objectifs. Le niveau 3, appelé Serveur orienté application (Application-Oriented Server), fournit un ensemble de ressources conceptuelles capables de répondre à la demande d'un nouveau service. Cette réponse est envisagée de façon centralisée, sans que sa réalisation effective sur un réseau entre en ligne de compte. Le niveau 4, ou Support de l'environnement distribué (Distribution Support Environment), prend le relais de la couche précédente pour réaliser de façon conceptuelle la distribution de la solution proposée par le niveau 3. Le niveau 5 doit établir avec le précédent une adéquation entre la distribution proposée au niveau conceptuel et sa prise en charge par le système d'exploitation distribué et le système d'interconnexion. Enfin, le dernier niveau se préoccupe des ressources physiques du réseau, lesquelles doivent être mises en place pour prendre en charge le nouveau service.

Entre le service et les couches sous-jacentes, les interfaces peuvent être multiples, suivant que le service demandé a déjà fait l'objet d'une réalisation partielle ou globale. Le cas le plus classique et le plus simple consiste à passer directement du service aux ressources distribuées lorsque l'infrastructure est déjà préparée à recevoir le service. À l'extrême inverse, il faut passer par le serveur orienté application lorsque le nouveau service n'est

pas répertorié dans les cas déjà réalisés. Dans cette architecture, les deux interfaces importantes sont celles illustrées à la figure W.6.

Figure W.6
Interfaces du réseau intelligent



L'interface la plus haute, ou interface de programmation, fait transiter la demande d'un nouveau service, c'est-à-dire la description de sa logique et de ses données associées. Les logiques permettront de bâtir, dans le niveau 3, des briques de base répondant aux besoins des services. Ces briques de base, ou SIB (Service-Independent Building), doivent être indépendantes les unes des autres et réutilisables. Il faut en outre que l'interface de programmation mette en place la demande de service et les SIB correspondants. Dans cette interface, on ne s'intéresse pas à la distribution. La correspondance est centralisée, ce qui facilite la relation service-logique de base.

La seconde interface, ou interface de commande de ressources, a pour fonction de mettre en correspondance la solution conceptuelle et sa réalisation au sein d'une architecture réelle distribuée. Cette réalisation s'effectue dans un environnement hétérogène. En d'autres termes, l'interface de commande de ressources doit disposer des ressources nécessaires à la réalisation du nouveau service.

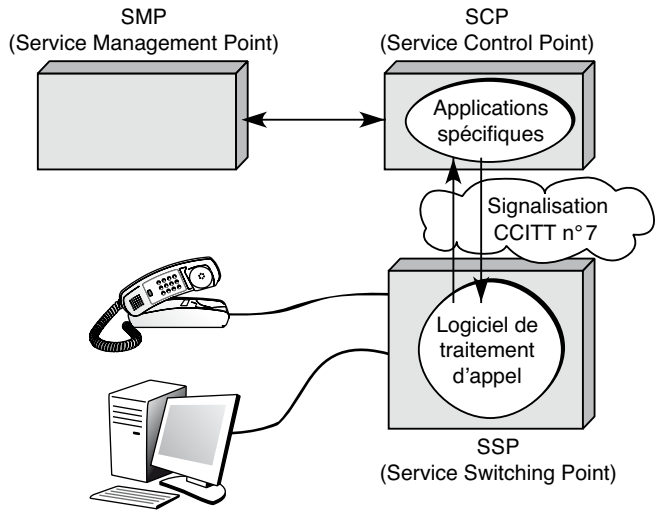
Réalisation d'un réseau intelligent

Plusieurs générations de réseaux intelligents ont été introduites pour tenir compte de la complexité croissante de l'environnement réseau.

La première génération, ou IN/1 (Intelligent Network/1), est assez simple : le client accède au point de commutation, appelé SSP (Service Switching Point), où un logiciel détecte s'il s'agit d'une demande de service dépendant du réseau intelligent. Le SSP prend également en charge le transfert de cette demande vers l'infrastructure du réseau intelligent. Si la réponse est positive, la demande est prise en compte par ce même logiciel, qui s'occupe de l'ouverture du circuit. La mise en place des ressources nécessaires s'effectue par l'intermédiaire du point de contrôle des services, ou SCP (Service Control Point). Celui-ci peut aussi s'adresser à un organe spécialisé, le système d'administration du service.

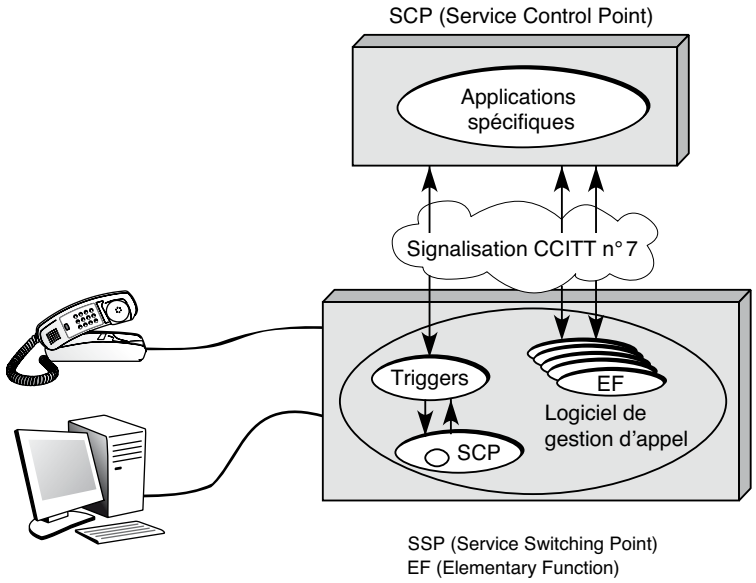
Cette première génération IN/1 est illustrée à la figure W.7.

Figure W.7
Architecture IN/1



Une première amélioration de cette architecture est illustrée à la figure W.8. Dans cette architecture, appelée IN1/+, apparaissent les fonctions élémentaires, ou EF (Elementary Function), qui forment les éléments de base dans les points d'accès au service. Ces éléments doivent être choisis ou adaptés à la prise en compte d'un nouveau service.

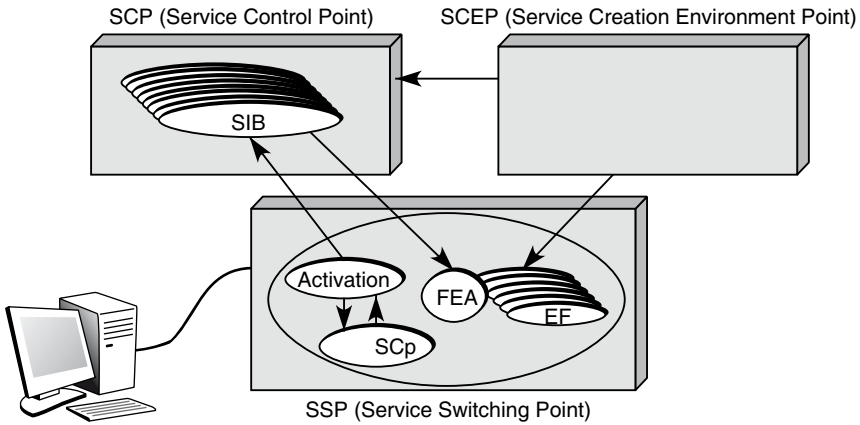
Figure W.8
Architecture IN/1+



Dans cette architecture IN1/+, à partir de la requête utilisateur de demande d'un nouveau service, la fonction trigger demande de l'aide au SCP, soit localement, soit à distance. À l'aide d'applications préspécifiées, le SCP peut renvoyer des ordres de mise en route ou d'adaptation des entités fonctionnelles. Les commandes-réponses entre le point d'accès et le point de contrôle des services s'effectuent par l'intermédiaire du réseau de signalisation. Ce réseau suit la recommandation CCITT n° 7 dans cette génération.

L'architecture IN/2, la plus évoluée aujourd'hui, est illustrée à la figure W.9.

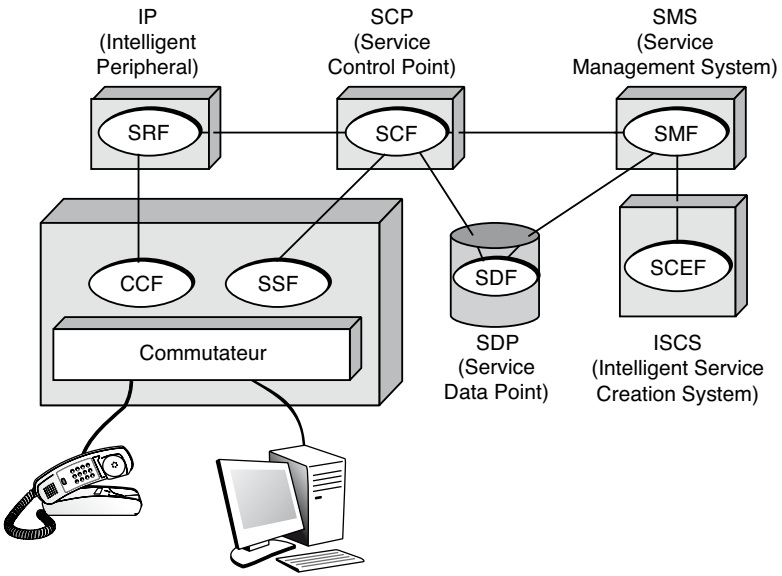
Figure W.9
Architecture IN/2



Cette architecture intègre les modules de base, ou SIB. Ce sont les modules rencontrés dans le plan fonctionnel global de l'architecture des réseaux intelligents. Les fonctions élémentaires EF sont coordonnées par des entités FEA (Functional Entity Action). Les regroupements de fonctions élémentaires permettent de mettre en place l'infrastructure physique pour desservir un nouveau service. Cette définition de l'architecture ressemble fortement à celle de la couche application du modèle de référence OSI, où les ASE (Application Service Element) sont coordonnés par des entités adaptées. Dans cette architecture IN/2, on trouve également un environnement de création de service, activé dès que le service ne peut être rendu par les SIB disponibles. Cet environnement, appelé SCE (Service Creation Environment), crée de nouveaux modules de base SIB et les fonctions élémentaires associées EF.

Les différents éléments de ces architectures peuvent être distribués de façons différentes. À la figure W.10, les différentes fonctions que nous avons rencontrées sont représentées avec les équipements physiques susceptibles de les accueillir. Les fonctions de contrôle de service sont incluses dans le point de contrôle des services (SCP).

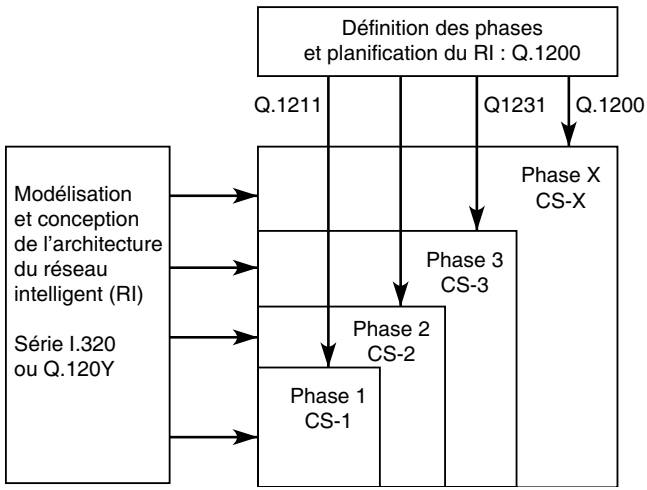
Figure W.10
Architecture matérielle de l'IN/2



Normalisation des réseaux intelligents

Les normes des réseaux intelligents sont parfaitement structurées. Elles se présentent sous la forme illustrée à la figure W.11. La série I.320/Q.120Y concerne la modélisation et les concepts de l'architecture des réseaux intelligents. Les différents niveaux sont référencés par la valeur Y. Plusieurs phases de réseaux intelligents sont prévues : les CS (Capability Set). Pour chaque ensemble, une série de normes sont introduites dans la recommandation Q.1200. Les recommandations Q.12XY concernent le niveau Y de l'ensemble X.

Figure W.11
Normalisation des réseaux intelligents



Appendices

Références bibliographiques

Les références fournies dans cette bibliographie concernent des ouvrages généraux, classés par chapitre de cette 7e édition des *Réseaux* et par ordre alphabétique d'auteur. Cette liste comporte quelques livres qui ont marqué leur époque et les principaux livres généraux couvrant le domaine des réseaux.

1. Introduction aux réseaux

Livre généraliste, avec une approche non technique, pour une introduction globale au monde des télécommunications :

T. ANTTALAINEN, *Introduction to Telecommunications Network Engineering*, Artech House, 1999

Un livre intéressant qui introduit très bien les problématiques du transport de la voix et des données dans les réseaux de télécommunications :

R. B. J. BATES, D. W. GREGORY, *Voice & Data Communications Handbook* (McGraw-Hill Communication Series), McGraw-Hill Osborne Media, 5e édition, 2006

La téléphonie numérique a été introduite il y a une vingtaine d'années. Le livre de Bellamy est le premier ouvrage complet expliquant les problèmes liés à cette numérisation :

J. BELLAMY, *Digital Telephony*, Wiley, 1982

Une excellente introduction aux techniques de routage et de commutation :

H. C. BERKOWITZ, *Network Architecture and Development Series: Designing Routing and Switching Architectures*, Macmillan, 1999

Un livre complet sur l'architecture des réseaux IP de nouvelle génération :

S. BRADNER, A. MANKIN, *IPng: Internet Protocol Next Generation*, Addison Wesley, 2000

Excellent livre de présentation du domaine des réseaux et des télécommunications :

M. P. Clark, *Networks and Telecommunications: Design and Operation*, Wiley, 1997

Un des auteurs les plus lus ces dernières années :

D. E. Comer, *Internetworking with TCP/IP Volume 1: Principles, Protocols, and Architecture*, Prentice Hall, 2000

Les transmissions sont passées de l'analogique au numérique au cours des années 1970. Le livre de L. Couch décrit bien ce processus et montre les grandes directions prises au début des années 1980 :

L. Couch, *Digital and Analog Communication Systems*, Macmillan, 1983

Davies et Barber ont été des précurseurs dans le domaine des réseaux d'ordinateurs. Ils en ont expérimenté en Angleterre un des prototypes et en ont tiré un livre :

D. W. Davies, D. L. A. Barber, *A Communication Networks for Computers*, Wiley, 1973

Très bon livre sur les réseaux optiques en général et sur la commutation optique en particulier :

T. S. El-Bawab, *Optical Switching*, Springer, 1re édition, avril 2006

Fragouli et Soljanin ont réalisé avec ce livre une excellente introduction aux techniques de codage et leur utilisation dans le cadre des réseaux terrestre et sans fil :

C. Fragouli, E. Soljanin, *Network Coding Fundamentals* (Foundations and Trends in Networking), Now Publishers Inc, 2007

Le livre suivant de Freeman propose une description très complète de la situation des télécommunications au début des années 2000 :

R. Freeman, *Fundamentals of Telecommunications*, Wiley, 1999

Une bonne introduction aux différentes catégories de réseaux en partant des réseaux personnels pour aller aux réseaux étendus en passant par les réseaux locaux et métropolitains :

L. Harte, *Introduction to Data Networks, PAN, PDN, LAN, MAN and WAN Technologies and Systems*, Althos, 2e édition, 2006

Livre qui s'intéresse aux architectures, en particulier pour le transport des données et de la parole de façon intégrée :

O. C. Ibe, *Converged Network Architectures: Delivering Voice and Data Over IP, ATM, and Frame-Relay*, Wiley, 2001

Excellent livre, qui reflète l'expérience de leurs auteurs, mais assez technique sur la partie performance :

H. Kobayashi, B. L. Mark, *High Speed Networks*, Prentice Hall, 1re édition, 2007

Ce livre traite de manière complète des réseaux haut débit et devrait, à ce titre, intéresser de nombreux lecteurs qui souhaitent se spécialiser dans les réseaux du futur :

D. Kofman, M. Gagnaire, *Réseaux haut débit*, InterÉditions, 1999

Excellent livre, très didactique, partant des couches supérieures pour aller vers les couches inférieures, introduisant les modèles architecturaux d'aujourd'hui :

J. F. KUROSE, K. W. ROSS, *Computer Networking*, Addison Wesley, 2000

—, *Analyse structurée des réseaux*, Pearson Education France, 2003

Un bon livre, pour une introduction complète aux différentes catégories de réseaux :

X. LAGRANGE, *Introduction aux réseaux*, Artech House, 1998

Le routage a toujours été un des fondamentaux des réseaux. Ce livre en explique bien les caractéristiques techniques :

J. MACFARLANE, *Network Routing Basics: Understanding IP Routing in Cisco Systems*, Wiley, avril 2006

Le Macchi-Guilbert a été un des grands livres de référence de 1980 à 2000. La première édition, datant de la fin des années 1970, dressait un tableau complet des réseaux et présentait la théorie du signal associée. Ce livre a été refondu et complété en 1988 :

C. MACCHI, J. F. GUILBERT, *Téléinformatique*, Dunod, 1988

Le cas de l'architecture IP Switching, qui travaille à la fois en routage et en commutation, est bien expliqué dans ce livre :

C. METZ, *IP Switching: Protocols and Architectures*, McGraw-Hill, 2000

Livre complet avec un bon panorama global :

N. F. MIR, *Computer and Communication Networks*, Prentice Hall PTR, 1re édition, 2006

Excellent livre qui introduit les réseaux destinés aux entreprises et fournit des compléments pratiques indispensables à une implémentation :

J.-L. MONTAGNIER, *Réseaux d'entreprise par la pratique*, Eyrolles, 2004

Livre généraliste pour une introduction globale au monde des télécommunications :

J. G. NELLIST, E. M. GILBERT, *Modern Telecommunications*, Artech House, 1999

Nora et Minc ont rendu au gouvernement, en 1978, un rapport célèbre sur la jonction des télécommunications et de l'informatique. Le mot télématique a été introduit dans ce document, qui n'est autre que le rapport lui-même :

S. NORA, A. MINC, *L'informatisation de la société*, Points Seuil, 1978

Excellent livre de base sur les architectures de réseau :

M. NORRIS, R. DAVIS, *Component-based Network System Engineering*, Artech House, 1999

Livre assez technique qui décrit bien l'ensemble des protocoles des réseaux d'aujourd'hui :

N. OLIVER, V. OLIVER, *Computer Networks: Principles, Technologies and Protocols for Network Design*, Wiley, 2006

Ce livre essaie de donner un panorama complet, en 700 pages, du domaine des réseaux et des télécommunications :

L. L. PETERSON, B. S. DAVIE, *Computer Networks. A Systems Approach*, Morgan Kaufmann, 4e édition, 2007

Ce panorama des réseaux et des télécommunications est complété de nombreux exercices :

G. PUJOLLE, *Cours réseaux et télécoms*, Eyrolles, 2008

Un des grands classiques de la fin des années 1980 :

G. PUJOLLE, D. SERET, D. DROMARD, E. HORLAIT, *Réseaux et télématique*, Eyrolles, 1985

Ce livre permet de bien comprendre la transformation technologique des réseaux ces dix dernières années :

C. RIGAULT, *Principes de commutation numérique : du téléphone au multimédia*, Hermès, 1998

Internet avec une vision nouvelle et les derniers développements :

B. VAN SCHEWICK, *Internet Architecture and Innovation*, The MIT Press, 2010

Un livre très complet avec des exercices :

C. SERVIN, *Réseaux et télécoms,* Dunod, 2003

Pour ceux qui souhaitent mieux comprendre la problématique des hauts débits :

C. SERVIN, S. GHERNAOUTI-HÉLIE, *Les Hauts Débits en télécoms*, InterÉditions, 1998

L'ouvrage suivant présente en détail l'architecture TCP/IP et la nouvelle génération de protocoles de cette architecture :

S. A. STEPHEN, *IPng and the TCP/IP Protocols*, Wiley, 1996

Le livre de Tanenbaum est certainement l'un de ceux qui s'est le plus vendu ces dix dernières années grâce à une approche très pédagogique :

A. TANENBAUM, *Computer Networks*, Prentice Hall, 1988 (trad. fr. *Réseaux, Architectures, protocoles, applications*, InterÉditions, 1996)

—, *Réseaux*, 4e édition, Pearson Education France, 2003

Excellent livre orienté vers les applications et l'utilisation des réseaux dans les entreprises :

C. WHITE, *Data Communications and Computer Networks: A Business User's Approach*, Course Technology, 4e édition, 2006

Un excellent livre, très complet, sur les architectures réseau :

R. WILLIAMS, *Computer Systems Architecture*, Addison Wesley, 2001

2. Architecture des réseaux

Livre plutôt généraliste sur les différentes architectures réseau qu'il est possible de trouver dans le monde des télécommunications :

J. ATKINS, M. NORRIS, *Total Area Networking*, Wiley, 1998

Un livre très pédagogique sur le modèle de référence :

U. Black, *OSI a Model for Computer Communications Standards*, Prentice-Hall, 1991

Un livre complet sur l'architecture des réseaux IP de nouvelle génération :

S. Bradner, A. Mankin, *IPng: Internet Protocol Next Generation*, Addison Wesley, 2000

Livre intéressant par sa présentation orientée vers la pratique des réseaux plus que par l'aspect théorique :

A. Burke, T. Tierney, *Network Practices: New Strategies in Architecture and Design*, Princeton Architectural Press, 1re édition, juin 2007

Cet article introduit parfaitement les protocoles de l'architecture TCP/IP :

V. Cerf, E. Cain, « The DOD Internet Architecture Model », *Computer Networks*, vol. VII, octobre 1983

Excellent livre pour l'introduction du monde IP orienté Cisco :

B. Chapman, *Deploying QoS fro Cisco IP and Next generation Networks*, Morgan Kaufmann, 2009

La genèse de l'architecture OSI présentée par deux de ses concepteurs :

J. Day, H. Zimmermann, « The OSI Reference Model », *Proceedings of the IEEE*, vol. LXXI, n° 12, pp. 1334-1340, décembre 1983

Le livre suivant donne une très bonne vue des protocoles et de la façon de les architecturer :

M. G. Gouda, *Elements of Network Protocol Design*, Wiley, 1998

Livre orienté vers l'accès de l'utilisateur à haut débit et du multiplexage voix, données, image sur cet accès :

C. Hellberg, D. Green, T. Boyes, *Broadband Network Architectures: Designing and Deploying Triple-Play Services*, Prentice Hall PTR, 1re édition, mai 2007

Cet ouvrage introduit parfaitement les problèmes de choix et de validation des protocoles de communication :

G. Holzmann, *Design and Validation of Computer Protocols*, Prentice-Hall, 1991

Excellente présentation de l'environnement réseau, incluant architecture, protocoles et logiciels :

J. Y. Hsu, *Computer Networks: Architecture, Protocols, and Software*, Artech House, 1996

Très bonne introductions aux protocoles de l'Internet :

C. Kozierok, *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference*, Starch Press, octobre 2005

Excellent livre, très didactique, partant des couches supérieures pour aller vers les couches inférieures, introduisant les modèles architecturaux d'aujourd'hui :

J. F. Kurose, K. W. Ross, *Computer Networking*, Addison Wesley, 2000

Très bon livre pour ceux qui veulent aller un peu plus loin dans la mise en place effective d'un réseau grâce à des outils permettant d'architecturer les réseaux :

J. D. Mccabe, *Network Analysis, Architecture and Design*, Morgan Kaufman, 4e édition, juin 2007

Excellent livre pour comprendre les technologies de base dans les réseaux :

M. Norris, *Understanding Networking Technology*, Artech House, 1999

Un article de base sur les protocoles :

L. Pouzin, H. Zimmermann, « A Tutorial on Protocols », *Proceedings of the IEEE*, vol. LXVI, n° 11, pp. 1346-1370, novembre 1978

Un livre récent focalisé sur la gestion des adresses, qui reste un problème majeur dans le monde Internet.

T. Rooney, *Introduction to IP Adress Management*, Wiley-IEEE Press, 2010

Internet avec une vision nouvelle et les derniers développements :

B. van Schewick, *Internet Architecture and Innovation*, The MIT Press, 2010

H. Zimmermann a été l'un des concepteurs du modèle de référence. L'article suivant est l'un des premiers à faire le point sur ce modèle :

H. Zimmermann, « OSI Reference Model, The ISO Model of Architecture for Open Systems Interconnection », *IEEE Transactions on Communications*, vol. XXVIII, n° 4, pp. 425-442, avril 1980

3. Le médium de transport

Un bon livre pour comprendre et maîtriser les techniques utilisées dans les réseaux locaux :

C. Anderson, M. Minasi, *Mastering Local Area Networks*, Sybex, 1999

Le câblage des réseaux locaux est parfaitement abordé dans le livre suivant :

M. Azadeh, *Fiber optic engineering*, Springer, 2009

Un bon livre pour aller plus loin sur le câblage d'une entreprise :

BICSI, *Telecommunications Cabling Installation*, McGraw-Hill, 2001

Il peut être intéressant de s'intéresser au câblage qui mène à l'entreprise. Le livre suivant en donne une bonne idée :

BICSI, *Residential Network Cabling*, McGraw-Hill, 2001

Livre qui fait le point sur un ensemble de propriétés du niveau physique :

R. Blahut, *Modem Theory: an Introduction to Telecommunications*, Cambridge University Press, 2010

Un des livres de base sur les technologies de câblage :

C. Clark, *Network Cabling Handbook*, McGraw-Hill, 2001

Un très bon livre pour débuter dans les réseaux optiques, avec de nombreux apports sur les composants optiques :

J. Crisp, B. Elliot, *Introduction to Fiber Optics*, Newnes, 3e édition, 2005

Un très bon livre dans la série Cisco sur les réseaux d'entreprise :

J. Durkin, J. Goodman, F. Posse, M. Rezek, M. Wallaca, R. Harris–*Building Multiservice Transport Networks*, Cisco Press, 1re édition, 2006

Livre très intéressant pour ceux qui s'intéressent à la sécurité des supports physiques :

D. Engenbreston, *Guide to Networking for Physical Security Systems*, Thomson Delmar Learning, 1re édition, 2007

Un livre intéressant sur un sujet difficile. Cependant, l'intérêt de l'ATM dans le domaine local a fortement baissé ces dernières années :

A. Ferrero, *Les Réseaux locaux commutés et ATM*, Masson, 1998

Un des meilleurs livres actuellement sur le câblage :

D. Groth, D. McBee, J. McBee, D. Barnett, *Cabling: The Complete Guide to Network Wiring*, Sybex, 2001

Un livre facile à lire pour une bonne introduction à Ethernet :

J. L. Harrington, *Ethernet Networking Clearly Explained*, Morgan Kaufmann Publishers, 1999

Livre assez technique sur les possibilités de boucle locale orientée transport de la télévision :

L. Harte, *Introduction to Cable Television (CATV) 2nd Edition: Analog and Digital Television and Modems*, Althos, 2e édition, 2007

Très bonne introduction aux réseaux optiques, avec de nombreux conseils plus pratiques que dans la plupart des livres sur le même sujet :

L. Harte, D. Eckard, *Fiber Optic Basics; Technology, Systems and Installation*, Althos Publishing, 2006

Excellent livre d'introduction sur les réseaux optiques :

J. Hecht, *Understanding Fiber Optics*, Prentice Hall, 5e édition, avril 2005

Un livre qui introduit bien les produits de la génération Ethernet à 100 Mbit/s :

H. W. Johnson, *Fast Ethernet: Dawn of a New Network*, Prentice Hall, 1995

Un des tout premiers livres sur le Gigabit Ethernet, avant même que la norme définitive soit sortie. Ce libre explique comment peut s'effectuer la migration des réseaux locaux actuels de l'entreprise vers les hauts débits du Gigabit Ethernet :

J. Kadambi, M. Kalkunte, I. Crayford, *Gigabit Ethernet: Migrating to High-Bandwidth Lans*, Prentice Hall, 1998

Pour aller plus loin sur les réseaux optiques :

K. Kazi, *Optical Networking Standards: A Comprehensive Guide for Professionals*, Springer, 1re édition, 2006

Un livre spécialisé sur la fibre optique et les techniques de transmission associée :

K.-P. Ho, *Phase-modulated optical communication systems*, Springer, 2010

Un livre très récent sur les réseaux optiques et les supports optiques :

G. Keiser, *Optical Fiber Communications*, McGraw-Hill Science, 2010

Les réseaux locaux ont été étendus aux réseaux métropolitains. Le livre suivant montre les différences à attendre lorsque l'on veut réaliser un tel réseau et les problèmes nouveaux posés par l'éloignement des utilisateurs :

G. C. Kessler, A. Krishna, *Metropolitan Area Networks: Concepts, Standards and Services*, McGraw-Hill, 1992

Un des livres de base pour les réseaux optiques :

L. G. Kazovsky, S. Benedatto, *Optical Fiber Communication Systems*, Artech House Publishers, 1996

Un autre livre de base pour les réseaux optiques :

A. Mendez, T. F. Morse, *Specialty Optical Fibers Handbook*, Academic Press, 2007

Un excellent livre pour mettre en place un réseau d'entreprise. Il aborde de nombreux points pratiques montrant bien la complexité de l'opération :

J.-L. Montagnier, *Pratique des réseaux d'entreprise*, Eyrolles, 1998

Un excellent livre sur les systèmes de câblage optique WDM avec leur moyen de subsistance en cas de problème :

S. Canhui, B. Mukherjee, *Survivable Optical WDM Networks*, Springer, 2010

La gestion des réseaux Token-Ring et Ethernet est abordée avec beaucoup de précision dans les deux livres suivants :

M. Nemzow, *The Token-Ring Management Guid*e, McGraw-Hill, 1993

—, *The Ethernet Management Guide*, McGraw-Hill, 1991

Un livre récent et très pratique sur le câblage universel courant faible dans les bureaux comme dans les logements à partir de la norme NF C 15-100 :

J. Nozik, *Guide du câblage universel*, Eyrolles, 2004

Les problèmes d'interconnexion sont complexes. Le livre suivant est une excellente porte d'entrée à ce domaine :

R. Perlman, *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*, Addison Wesley, 1999

Pour ceux intéressés par la fibre optique jusqu'au domicile :

J. PRAT, *Next Generation HTTH Passive Optical Networks*, Sringer, 2000

Livre technique sur la mise en place de systèmes de câblage :

J. Riddel, *Packet Cable Implementation*, Cisco Press, 1re édition, 2007

Excellent livre sur le haut de gamme Ethernet pour l'entreprise :

S. RILEY, R. A. BREYER, *Switched, Fast, and Gigabit Ethernet*, New Riders Publishing, 1999

La technologie commutée pour les réseaux locaux est rarement traitée dans la littérature. Le livre suivant en donne une description complète :

R. SEIFERT, *The Switch Book: The Complete Guide to LAN Switching Technology*, Wiley, 2000

Le câblage des réseaux locaux est parfaitement abordé dans le livre suivant :

J. TRULOVE, *LAN Wiring*, McGraw-Hill, 2000

Deux très bons livres sur les câblages disponibles au début des années 2000 et sur la montée en puissance de la fibre optique :

J. R. VACCA, *The Cabling Handbook*, Prentice Hall, 2000

—, *Optical Networking Best Practices Handbook*, Wiley-Interscience, 2006

Le câblage des réseaux locaux est parfaitement abordé dans le livre suivant :

B. WOODWARD, *Cabling: the Complete Guide to Copper and Fiber-Optic Networking*, Sybext, 2009

4. Les équipements réseau

Les nœuds MPLS ou LSR ont des architectures qui intègrent à la fois une architecture de commutateur et de routeur. Le livre suivant aborde ce sujet dans un ensemble plus vaste :

V. ALWAYN, *Advanced MPLS Design and Implementation*, Cisco Press, 2001

Excellent livre pour tout apprendre sur les modems câble :

A. A. AZZAM, *High-Speed Cable Modems*, McGraw-Hill, 1997

Un livre qui introduit toutes les techniques modernes de codage et de compression pour les images fixes et animées :

F. BARLAUD, *Compression et codage des images et des vidéos*, Hermès, 2001

Un des livres de référence depuis de nombreuses années sur la téléphonie numérique et les codages du téléphone (3e édition) :

J.-C. BELLAMY, *Digital Telephony*, Wiley-Interscience, 2000

Un des livres de base sur les techniques de codage :

R. BLAKE, J. MULLIN, *Mathematical Theory of Coding*, Academic Press, 1975

Un livre très complet sur les techniques de codage :

M. BOSSERT, *Channel Coding*, Wiley, 1999

Un livre technique pour ceux qui veulent aller plus loin dans la théorie du signal et de l'information :

P. BRÉMAUD, *Signal et communications : modulation, codage et théorie de l'information*, Ellipses Marketing, 1998

Un livre plutôt commercial, qui introduit les différentes catégories d'équipements réseau :

V. C. Bridges, V. C. Marney-Petix, *Switches, Routers, Gateways*, Numidia Press, 2002

Excellent livre, qui introduit les codages dans les communications dans les réseaux de mobiles et les réseaux sans fil :

A. Burr, *Modulation and Coding for Wireless Communications*, Prentice-Hall, 2001

Un excellent livre sur les équipements réseau et les distinctions dans leur architecture :

A. B. Caslow, V. Pavlichenko, *Cisco Certification: Bridges, Routers and Switches for CCIEs*, Prentice Hall, 2000

Excellent livre pour ceux qui veulent aller plus loin dans les architectures internes des commutateurs et des routeurs :

H. J. Chao, H. Lam, E. Oki, *Broadband Packet Switching Technologies: a Practical Guide to ATM Switches and IP Routers*, Wiley-Interscience, 2001

Très bon livre sur la commutation ATM :

T. M. Chen, S. S. Liu, *ATM Switching Systems*, Artech House, 1995

Un excellent livre, qui reste l'un des traités de base sur les techniques de correction des erreurs :

G. Cohen, J.-L. Dornstetter, P. Godlewski, *Codes correcteurs d'erreur : une introduction au codage algébrique*, Masson, 1992

Un très bon livre sur l'environnement ATM et ses commutateurs :

E. R. Coover, *ATM Switches*, Artech House, 1997

Un livre de base sur la théorie du signal et les techniques utilisées dans le domaine des télécommunications :

R. Gallager, *Information Theory and Reliable Communication*, Wiley, 1968

Un livre très technique sur la théorie du codage. Pour ceux qui veulent comprendre les mathématiques qui se cachent derrière les techniques de codage :

P. Garrett, *The Mathematics of Coding Theory*, Prentice Hall, 2003

Les codeurs-décodeurs forment l'équipement de base pour la transformation des signaux analogiques en signaux numériques. Le livre suivant en fait une très bonne synthèse :

M. Ghanbari, *An Introduction to Standard Codecs*, IEEE Press, 1999

Excellent livre de base sur les principes de la transmission de données :

R. D. Gittlin, J. F. Hayes, *Data Communications Principles*, Plenum Publishing Corporation, 1992

Un livre commercial sur les routeurs et commutateurs à très haut débit du commerce :

Global Industry Analyst, *Gigabit and Terabit Switches and Routers*, 2002

Les routeurs Cisco représentant plus des trois quarts du parc global, ce manuel est une excellente source pour la programmation de la plupart des routeurs :

D. HUCABY, S. MCQUERRY, A. Whitaker, *Cisco Router Configuration Handbook*, Cisco Press, 2010

Livre bien fait pour une introduction aux théories de l'information et du codage :

G. A. JONES, J. M. JONES, *Information and Coding Theory*, Springer Verlag, 2000

Les gros systèmes de sauvegarde utilisent fortement les commutateurs. L'objectif du livre suivant est de nous faire pénétrer dans ce domaine qui recoupe celui introduit dans ce chapitre :

J. JUDD, C. BEAUCHAMPS, B. F. KUO, *Building SANs with Brocade Fabric Switches*, Syngress Publishing, 2001

La parole téléphonique sur un réseau à transfert de paquets est devenue un élément essentiel de l'environnement réseau. Le livre suivant présente les différentes techniques de codage qui peuvent être utilisées, en particulier les techniques à très bas débit :

A. M. KONDOZ, *Digital Speech*, Wiley, 1999

Un livre spécialisé sur les commutateurs Ethernet de Cisco :

T. LAMMLE, W. SPANGENBERG, R. PADJEN, *CCNP: Cisco LAN Switch Configuration Study Guide*, Sybex, 1999

Les environnements sans fil posent des problèmes complexes étant donné leur taux d'erreur assez élevé et très aléatoire. Ce livre aborde plus particulièrement le codage dans ce contexte :

E. G. LARSSON, P. STOICA, G. GANESAN, *Space-Time Block Coding for Wireless Communications*, Cambridge University Press, 2003

Livre général, où l'essentiel des problèmes de transmission est abordé :

P. LECOY, *Technologie des télécoms*, Hermès, 1999

Une bonne introduction à la théorie du codage :

S. LING, C. XING, *Coding Theory: A First Course*, Cambridge University Press, 2004

Livre spécialisé sur la sécurité des routeurs et des commutateurs de Cisco, qui vaut également pour les autres types de routeurs :

D. LIU, *Cisco Router and Switch Forensics: Investigating and Analysing Malicious Network Activity*, Syngress, 2009

Livre complet sur la partie matérielle des réseaux sans fil :

A. LUZZATTO, G. SHIRAZI, *Wireless Transceiver Design: Mastering the Design of Modern Wireless Equipment and Systems*, Wiley, 2007

Un livre apportant un bon compromis entre la théorie et la pratique des pare-feu.

H. MANKELL, E. SEGERBERG, *Firewall*, Vintage Books, 2003

Bon livre complet sur les théories de l'information et du codage :

R. MCELIECE, *Theory of Information & Coding*, Cambridge University Press, 2002

Livre qui fait le point sur un ensemble de propriétés du niveau physique :

C. MEINERS, A. X. LIU, E. TORNG., *Hardware Based Packet Classification for High Speed Internet Routers*, Springer, 2010

Livre qui fait le point sur un ensemble de propriétés du niveau physique :

H. MEYR, *et al.*, *Digital Communication Receivers: Synchronization, Channel Estimation, and Signal Processing*, Wiley, 1997

Livre entrant dans les détails des techniques de la compression :

N. MOREAU, *Techniques de compression des signaux*, Masson, 1995

Un livre dédié aux techniques de correction des erreurs :

R. H. MORELOS-ZARAGOZA, *The Art of Error Correcting Coding*, Wiley, 2002

Livre spécialisé sur la parole téléphonique et la voix dans les réseaux sans fil :

A. PENY, *Fundamentals of Voice-Quality Engineering in Wireless Networks*, Cambridge University Press, 2006

Excellente introduction à tous les équipements réseau, dont les passerelles :

R. PERLMAN, *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*, Addison Wesley, 1999

La meilleure référence pour la technologie ATM :

H. PERROS, *An Introduction to ATM Networks*, Wiley, 2001

Excellent livre, qui pose la problématique de la convergence des techniques de commutation et de routage. On s'aperçoit que la commutation est indispensable et que, à l'intérieur, les routeurs ne sont que de commutateurs :

R. PUZMANOVA, *Routing and Switching: Time of Convergence?*, Addison Wesley, 2001

Livre assez complet sur le codage et la compression des applications que l'on peut trouver sur Internet :

K. R. RAO, J. J. HWANG, *Techniques and Standards for Image, Video, and Audio Coding*, Prentice Hall, 1996

Pour tout connaître sur les antennes et la propagation du signal dans les réseaux sans fil :

S. R. SAUNDERS, A. ARAGON- ZAVALA, *Antennas and Propagation for Wireless Communication Systems*, Wiley, 2e édition, 2007

Un très bon livre de base sur les procédures et les équipements du niveau physique :

A. SIMMONDS, *Data Communications and Transmission Principles*, Macmillan, 1997

Livre dédié aux technologies associées à l'audio :

A. SPANIAS, T. PAINTER, V. ATTI, *Audio Signal Processing and Coding*, Wiley-Interscience, 2007

Un livre très complet pour démarrer et approfondir les techniques de contrôle d'erreur :

P. SWEENEY, *Error Control Coding: From Theory to Practice*, Wiley, 2002

La vidéo peut être numérisée suivant de très nombreuses techniques. Le livre suivant fait une bonne synthèse des différentes solutions :

P. SYMES, *Video Compression*, Prentice Hall, 1998

Un très bon livre sur les fondements de la théorie du codage et de l'utilisation qui peut en être faite :

R. TOGNERI, C. J. S. DESILVA, J. J. S. SULLUM, *Fundamentals of Information Theory and Coding Design*, Chapman & Hall, 2003

Un très bon livre pour tout comprendre des pare-feu :

J. R. VACCA, *Firewalls Clearly Explained*, Academic Press, 2004

Un livre très complet sur les architectures des routeurs et des serveurs dans le monde Internet :

G. VARGHESE, *Internet Algorithmics: How To Build Fast Routers and Servers*, Pearson Education, 2004

Un livre très complet sur les techniques de numérisation :

W. N. WAGGENER, *Pulse Code Modulation Systems Design*, Artech House, 1999

Livre orienté ingénieurs, mais ayant déjà de bonnes connaissances de base, intéressés par le codage des signaux :

R. B. WELLS, *Applied Coding and Information Theory for Engineers*, Prentice Hall, 1998

Un bon livre de base sur la modulation et le codage :

S. G. WILSON, *Modulation and Coding*, Prentice Hall, 1995

Excellent document sur l'ensemble des techniques de modulation et leur application à différents types de réseaux :

F. XIONG, *Digital Modulation Techniques*, Artech House, 2000

5. Le niveau physique

Excellent livre pour tout apprendre sur les modems câble :

A. A. AZZAM, *High-Speed Cable Modems*, McGraw-Hill Companies, 1997

Un livre qui introduit toutes les techniques modernes de codage et de compression pour les images fixes et animées :

F. BARLAUD, *Compression et codage des images et des vidéos*, Hermès, 2001

Un des livres de référence depuis de nombreuses années sur la téléphonie numérique et les codages du téléphone (3e édition) :

J.-C. BELLAMY, *Digital Telephony*, Wiley-Interscience, 2000

Livre qui fait le point sur un ensemble de propriétés du niveau physique :

R. BLAHUT, *Modem Theory: an Introduction to Telecommunications*, Cambridge University Press, 2010

Un des livres de base sur les techniques de codage :

R. Blake, J. Mullin, *Mathematical Theory of Coding*, Academic Press, 1975

Un livre très complet sur les techniques de codage :

M. Bossert, *Channel Coding*, Wiley, 1999

Un livre technique pour ceux qui veulent aller plus loin dans la théorie du signal et de l'information :

P. Brémaud, *Signal et communications : modulation, codage et théorie de l'information*, Ellipses Marketing, 1998

Excellent livre, qui introduit les codages dans les communications dans les réseaux de mobiles et les réseaux sans fil :

A. Burr, *Modulation and Coding for Wireless Communications*, Prentice-Hall, 2001

Un excellent livre, qui reste l'un des traités de base sur les techniques de correction des erreurs :

G. Cohen, J.-L. Dornstetter, P. Godlewski, *Codes correcteurs d'erreur : une introduction au codage algébrique*, Masson, 1992

Ce livre fait le point sur le codage dans les réseaux optiques :

I. Djordjevic, W. Ryan, B. Vasic, *Coding for Optical Channels*, Springer, 2010

Les codages et les modulations utilisés dans la télévision numérique sont assez spécifiques. Ils sont expliqués en détail dans le livre suivant :

G. Drury, G. Markarian, K. Pickadvance, *Coding and Modulation for Digital Television*, Springer, 2010

L'OFDM est la technologie utilisée dans la 4G. Ce livre très spécialisé en détaille la technologie :

F. Adalat, *Sub-Carrier Adaptive Modulation and coding in OFDM: Real-Time Design and Performance in Wideband Wireless System*, LAP Lambert Academic Publishing, 2010

Un livre très technique sur la théorie du codage. Pour ceux qui veulent comprendre les mathématiques qui se cachent derrière les techniques de codage :

P. Garrett, *The Mathematics of Coding Theory*, Prentice Hall, 2003

Les codeurs-décodeurs forment l'équipement de base pour la transformation des signaux analogiques en signaux numériques. Le livre suivant en fait une très bonne synthèse :

M. Ghanbari, *An Introduction to Standard Codecs*, IEEE Press, 1999

Excellent livre de base sur les principes de la transmission de données :

R. D. Gittlin, J. F. Hayes, *Data Communications Principles*, Plenum Publishing Corporation, 1992

Livre bien fait pour une introduction aux théories de l'information et du codage :

G. A. Jones, J. M. Jones, *Information and Coding Theory*, Springer Verlag, 2000

Dans un réseau à transfert de paquets, la parole téléphonique est devenue un élément essentiel de l'environnement réseau. Le livre suivant présente les différentes techniques de codage qui peuvent être utilisées, en particulier les techniques à très bas débit :

A. M. Kondoz, *Digital Speech*, Wiley, 1999

Les environnements sans fil posent des problèmes complexes étant donné leur taux d'erreur assez élevé et très aléatoire. Ce livre aborde plus particulièrement le codage dans ce contexte :

E. G. Larsson, P. Stoica, G. Ganesan, *Space-Time Block Coding for Wireless Communications*, Cambridge University Press, 2003

Livre général, où l'essentiel des problèmes de transmission est abordé :

P. Lecoy, *Technologie des télécoms*, Hermès, 1999

Une bonne introduction à la théorie du codage :

S. Ling, C. Xing, *Coding Theory: A First Course*, Cambridge University Press, 2004

Livre complet sur la partie matérielle des réseaux sans fil :

A. Luzzatto, G. Shirazi, *Wireless Transceiver Design: Mastering the Design of Modern Wireless Equipment and Systems*, Wiley, 2007

Bon livre complet sur les théories de l'information et du codage :

R. McEliece, *Theory of Information & Coding*, Cambridge University Press, 2002

Ce livre fait le point sur un ensemble de propriétés du niveau physique :

H. Meyr, *et al.*, *Digital Communication Receivers: Synchronization, Channel Estimation, and Signal Processing*, Wiley, 1997

Le livre suivant entre dans le détail des techniques de compression :

N. Moreau, *Techniques de compression des signaux*, Masson, 1995

Un livre dédié aux techniques de correction des erreurs :

R. H. Morelos-Zaragoza, *The Art of Error Correcting Coding*, Wiley, 2002

Un bon livre pour s'initier aux techniques de codage dans les réseaux hertziens :

O. Osman, O. Uçan, *Contemporary Coding Techniques and Applications for Mobile Communications*, Auerbach Publications, 2009

Livre spécialisé dans la parole téléphonique et la voix en général dans les réseaux sans fil :

A. Peny, *Fundamentals of Voice-Quality Engineering in Wireless Networks*, Cambridge University Press, 2006

Ce livre sur le codage et la modulation dans les communications hertziennes contient beaucoup d'informations utiles pour ceux qui veulent aller plus loin sur les transmissions hertziennes :

R. Rafi, R. Shan, *Adaptive Coding and Modulation*, VDM Verlag, 2010

Livre assez complet sur le codage et la compression des applications que l'on peut trouver sur Internet :

K. R. Rao, J. J. Hwang, *Techniques and Standards for Image, Video, and Audio Coding*, Prentice Hall, 1996

Pour tout connaître des antennes et de la propagation du signal dans les réseaux sans fil :

S. R. Saunders, A. Aragon-Zavala, *Antennas and Propagation for Wireless Communication Systems*, Wiley, 2e édition, 2007

Un très bon livre de base sur les procédures et les équipements du niveau physique :

A. Simmonds, *Data Communications and Transmission Principles*, Macmillan, 1997

Livre dédié aux technologies associées à l'audio :

A. Spanias, T. Painter, V. Atti, *Audio Signal Processing and Coding*, Wiley-Interscience, 2007

Un livre très complet sur les techniques de contrôle d'erreur :

P. Sweeney, *Error Control Coding: From Theory to Practice*, Wiley, 2002

La vidéo peut être numérisée suivant de très nombreuses techniques. Le livre suivant propose une bonne synthèse des différentes solutions :

P. Symes, *Video Compression*, Prentice Hall, 1998

Un très bon livre sur les fondements de la théorie du codage et de l'utilisation qui peut en être faite :

R. Togneri, C. J. S. Desilva, J. J. S. Sullum, *Fundamentals of Information Theory and Coding Design*, Chapman & Hall, 2003

Un livre très complet sur les techniques de numérisation :

W. N. Waggener, *Pulse Code Modulation Systems Design*, Artech House, 1999

Livre orienté ingénieurs, mais ayant déjà de bonnes connaissances de base, intéressés par le codage des signaux :

R. B. Wells, *Applied Coding and Information Theory for Engineers*, Prentice Hall, 1998

Un bon livre de base sur la modulation et le codage :

S. G. Wilson, *Modulation and Coding*, Prentice Hall, 1995

Excellent document sur l'ensemble des techniques de modulation et leur application à différents types de réseaux :

F. Xiong, *Digital Modulation Techniques*, Artech House, 2000

6. Le niveau trame

Un livre spécialisé sur PPP pour les systèmes enfouis :

J. Bartas, *PPP for Embedded Systems*, CMP Books, 2002

Un livre pour compléter sa culture dans le domaine des architectures réseau :

H. C. Berkowitz, *Designing Addressing Architectures for Routing and Switching*, Macmillan, 1999

Les protocoles de transport des paquets IP à partir de l'utilisateur sont particulièrement nombreux. Ce livre en détaille les deux principaux, provenant du monde Internet :

U. D. Black, *PPP and L2TP: Remote Access Communications*, Prentice Hall, 1999

Le protocole PPP est certainement l'un des plus utilisés. Pour l'étudier en détail, le livre de Carlson est précieux :

J. D. Carlson, *PPP Design, Implementation, and Debugging*, Addison Wesley, 2001

Ce document permet de comprendre la façon d'architecturer un réseau :

J. DiMarzio, *Network Architecture and Design*, Sams, 2001

Un livre très complet sur les réseaux :

J. Y. Hsu, *Computer Networks: Architecture, Protocols and Software*, Prentice Hall, 1998

La commutation Ethernet dans un environnement Cisco très bien expliquée dans ce livre :

S. Mc Querry, D. Jansen, D. Hucaby, *Cisco LAN Switching Configuration Handbook*, Cisco Press, 2009

Un livre complet pour tous ceux qui se servent de la technologie ATM :

S. Kasera, *ATM Networks*, McGraw-Hill Professional, 1re édition, 2006

Un livre pour ceux qui veulent aller plus loin en matière de programmation des protocoles :

I. Lavallée, *Protocoles et programmation dans les réseaux*, Hermès, 1995

Un livre spécialisé dans les architectures de niveau 2 et plus spécifiquement dans les réseaux privés virtuels de ce même niveau :

W. Luo, C. Pignataro, A. Yhchan, D. Bokotey, *Layer 2 VPN Architecture*, Cisco Press, 2005

Un livre de base, qui permet d'entrer dans les grands principes des réseaux :

P. Rolin, *Les Réseaux. Principes fondamentaux*, Hermès, 1996

Les architectures de niveau trame sont fortement utilisées dans les réseaux locaux, particulièrement dans le monde Ethernet. Ce livre fait le tour de ces technologies :

R. Seifert, *The Switch Book: The Complete Guide to LAN Switching Technology*, Wiley, 2000

Très bonne introduction au protocole PPP, avec de nombreux détails intéressants sur sa mise en œuvre :

A. Sun, *PPP, configuration et mise en œuvre*, O'Reilly, 1999

Un livre bien fait, qui introduit les concepts d'architecture en fonction de l'environnement de l'entreprise :

E. Taylor, *The Network Architecture Design Handbook*, Taylor Networking Series, 1999

Ce livre contient de nombreuses descriptions de protocoles et permet de bien comprendre les architectures réseau :

L. Toutain, *Réseaux locaux et Internet : des protocoles à l'interconnexion*, Hermès, 1999

Un livre très complet sur les services réseau de niveau trame, en particulier Ethernet Forwarding, la commutation Ethernet et les réseaux virtuels de type VPLS :

Z. Xu, *Designing and Implementing IP/MPLS based Ethernet layer 2 VPN Services: an Advanced Guide for VPLS and VLL*, Wiley, 2009

7. Le niveau paquet

Un des nombreux livres d'Ulysse Black, qui porte essentiellement sur le niveau paquet :

U. Black, *IP Routing Protocols: RIP, OSPF, BGP, PNNI and Cisco Routing Protocols*, Prentice Hall, 2000

IP se démocratise dans les réseaux sans fil. Ce livre explique bien ses implémentations dans ce contexte :

J.-C. Chen, T. Zhang, *IP-Based Next-Generation Wireless Networks: Systems, Architectures, and Protocols*, Wiley-Interscience, 2003

Un très bon livre sur IPv6 :

G. Cizault, *IPv6 : Théorie et pratique*, O'Reilly, 1999

Un des grands classiques du domaine :

D. E. Comer, *Réseaux et Internet*, CampusPress, 2000

Un livre spécialisé dans les architectures de commutation et plus spécifiquement celles permettant d'atteindre de très hauts débits :

I. Elhanany, M. Hamdi, *High-Performance Packet Switching Architectures*, Springer, 2006.

Un livre particulièrement intéressant pour ceux qui veulent en savoir plus sur les algorithmes de construction d'une table de routage :

L. Ford, D. Fulkerson, *Flows in Networks*, Princeton University Press, 1962

Un des livres de base sur les protocoles de l'environnement TCP/IP :

B. A. Forouzan, *TCP/IP Protocol Suite*, McGraw-Hill Science/Engineering/Math, 3e édition, 2005

Livre assez général sur les environnements réseau dans lequel le niveau paquet est au centre des architectures :

M. Gallo, *Networking Explained*, Butterworth-Heinemann, 2001

Un livre qui permet d'entrer dans les détails de l'adressage dans un réseau Internet :

B. Grah, *TCP/IP Addressing*, AP Professional, 2000

Un excellent ouvrage sur les protocoles de routage Internet :

C. HUITEMA, *Le Routage dans l'Internet*, Eyrolles, 1994

Un des meilleurs livres sur la génération IPv6 :

C. HUITEMA, *IPv6 the New Internet Protocol*, Prentice Hall, 1998

Les fonctionnalités de protection et de disponibilité ne sont que rarement étudiées dans les livres techniques. Celui-ci en donne un excellent panorama technique :

K. LEE, F. LIM, B. ONG, *Building Resilient IP Networks*, Cisco Press, 2005

Un livre assez grand public et très pédagogique sur la norme IP et les protocoles associés :

P. LOSHIN, *TCP/IP Clearly Explained*, Academic Press, 1999

Le niveau paquet est parfois difficile à contrôler et à mesurer. Ce livre apporte des solutions dans l'analyse des flots :

M. LUCAS, *Network Flow Analysis*, No Start Press, 2010

Très bon livre sur les algorithmes de routage et les solutions d'implémentation et d'optimisation :

D. MEHDI, K. RAMASAMY, *Network Routing: Algorithms, Protocols, and Architectures*, Morgan Kaufmann, 2007

Un livre assez technique sur le niveau paquet et plus particulièrement sur les techniques de commutation de niveau 3 :

D. MINOLI, J. DOYLE, A. SCHMIDT, *Network Layer Switched Services*, Wiley, 1998

La qualité de service (QoS) est très généralement gérée au niveau 3 de l'architecture des réseaux. Ce livre décrit les différentes solutions pour garantir cette qualité de service :

K. PARK, *QoS in Packet Networks*, Springer, 2010

Ce livre fait le point sur les évolutions des réseaux IP :

G. PUJOLLE, *Management, Control, and Evolution of IP Networks*, ISTE Publishing Company, 2006

Pour démarrer dans l'environnement IP et plus généralement Internet, ce livre peut faire l'affaire :

W. S. RICHARD, G. R. WRIGHT, *TCP/IP : la mise en œuvre*, Vuibert, 1998

Un livre très bien fait et qui aborde les possibilités de service du protocole IP :

K. S. SIYAN, *TCP/IP*, CampusPress, 2001

Le routage des paquets IP est un domaine des plus austères et des plus complexes à expliquer. Ce livre est une réussite de ce point de vue :

M. A. SPORTACK, *IP Routing Fundamentals*, Cisco Press, 2000

Une introduction solide au protocole IPv6 et à son environnement :

O. LI, J. TATUYA, K. SHIMA, *IPv6 Core Protocols Implementation*, Morgan Kaufmann, 2007

Un très bon livre pour tout comprendre sur X.25 :

N. M. Thorpe, D. Roos, *X.25 facile*, Masson, 1997

Ce livre explique les techniques commutées de niveau 3 et les principaux protocoles de routage :

S. A. Thomas, *IP Switching and Routing Essentials: Understanding RIP, OSPF, BGP, MPLS, CR-LDP, and RSVP-TE*, Wiley, 2001

Un bon livre sur l'architecture protocolaire de l'Internet :

E. Tittel, L. Chappell, *Guide to TCP/IP*, Course Technology, 3e édition, 2006

Livre assez général sur l'introduction d'applications multimédias dans le cadre des réseaux sans fil :

M. Van Der Schaar, P. A. Chou, *Multimedia over IP and Wireless Networks: Compression, Networking, and Systems*, Academic Press, 2007

Très bon livre sur les techniques commutées de niveau 3 pour les hauts débits :

H. Wang, *Packet Broadband Network Handbook*, McGraw-Hill, 2002

Beaucoup de développements sont effectués au niveau paquet. Ce livre en dresse l'inventaire :

P.-C. Wang, *IP Packet Forwarding Research Progress*, Nova Science Publisher, 2009

L'intégration du protocole IP dans les technologies pour réseaux de mobiles 3G est bien expliquée dans ce livre :

D. Wisely, P. Eardley, L. Burness, *IP for 3G: Networking Technologies for Mobile Communications*, Wiley, 2002

8. Le niveau message

Un des nombreux livres décrivant la suite de protocoles de l'environnement TCP/IP :

A. Behrouz , S. Forouzan, *TCP/IP Protocol Suite*, McGraw 2007

Un excellent livre pour ceux qui veulent implémenter une interface vers le protocole TCP dans une application :

K. L. Calvert, M. J. Danahoo, *TCP/IP Sockets in Java: Practical Guide for Programmers*, Morgan Kaufmann Publishers, 2008

Dans la couche message, les sockets de TCP ont été les éléments les plus importants du succès du monde IP. Une socket est le point d'entrée dans les systèmes d'exploitation. Toute la réussite de TCP/IP tient à dans cette inclusion simple dans les logiciels UNIX :

M. Donahoo, K. Calvert, K. L. Calvert, M. J. Donahoo, *TCP/IP Sockets in C: Practical Guide for Programmers*, Morgan Kaufmann Publishers, 2000

Ce livre explique clairement les différents protocoles de l'architecture TCP/IP, en particulier ceux de la couche transport :

B. Forouzan, *TCP/IP Protocol Suite*, McGraw-Hill, 2010

Un livre qui détaille les protocoles de l'architecture OSI :

J. HENSHALL, *OSI Explained*, Ellis Horwood, 1990

Un très bon livre pour découvrir les fonctionnalités du protocole TCP :

C. HUNT, *TCP/IP Network Administration*, O'Reilly, 2002

Un livre très spécialisé sur la couche transport du monde Internet, et plus spécifiquement sur l'amélioration de ses performances :

S. ISLAM, *Performance Measurement and Improvement of TCP*, VDM Verlag, 2010

La gestion de la mobilité est fortement simplifiée avec IPv6. Ce livre permet d'entrer dans les moindres détails des solutions de mobilité dans le champ d'IPv6 :

R. S. KOODLI, C. E. PERKINS, *Mobile Inter-Networking with IPv6: Concepts, Principles and Practices*, Wiley-Interscience, 2007

Livre technique sur les applications multicast qui sont gérées par la couche transport :

D. B. MAKOFSKE, K. C. ALMEROTH, *Multicast Sockets: Practical Guide for Programmers*, Morgan Kaufmann Publishers, 2002

Excellent livre sur les protocoles TCP et IP ainsi que sur leur environnement :

P. MILLER, *TCP/IP Explained*, Digital Press, 1997

Un livre très pédagogique pour entrer facilement dans le monde des protocoles de l'architecture TCP/IP :

A. RODRIGUEZ, J. GATRELL, J. KARAS, R. PESCHKE, *TCP/IP Tutorial and Technical Overview*, Prentice Hall, 2001

Un des tout premiers livres consacrés à l'adressage dans le monde Internet. C'est un des fondements du monde TCP/IP qui est expliqué :

T. ROONEY, *Introduction to IP address management*, Wiley/IEEE Press, 2010

Un livre d'un format particulier qui donne des réponses claires à de nombreuses questions que l'on peut se poser sur les protocoles de la pile TCP/IP :

T. SANCHEZ-CLARK, *TCP/IP Networking Interview. Questions, Answers, and Explanations: TCP/IP Network Certification Review*, Equity Press, 2007

Un livre qui part des applications pour montrer comment les protocoles Internet s'adaptent au contexte :

B. VAN SCHEWICK, *Internet Architecture and Innovation*, MIT Press, 2010

Pour tout connaître de l'environnement TCP/IP :

R. SCRIMGER, P. LASALLE, C. LEITZKE, M. PARIHAR, *TCP/IP Bible*, Hungry Minds, 2001

Un des nombreux livres de bonne qualité sur la suite de protocoles de l'environnement Internet :

E. TITTEL, L. CHAPPELL, *Guide to TCP/IP*, Course Technology, 2006

W. Stevens a écrit une série de trois livres sur l'environnement TCP/IP. Les deux plus intéressants sont le premier et le troisième. Le premier introduit très bien l'environnement, et le troisième permet de comprendre l'utilisation de TCP du point de vue applicatif :

W. R. Stevens, *The Protocols TCP/IP Illustrated*, Addison Wesley, 1994

—, *TCP for Transactions, HTTP, NNTP, and the UNIX(R) Domain Protocols*, Addison Wesley, 1996

9. Les réseaux d'accès terrestres

Pour les accès à très haut débit avec un fort multiplexage, le protocole IPv6 apporte de nombreuses fonctionnalités. Ce livre en décrit toutes les possibilités :

A. Ahmed, *Deploying IPv6 in Broadband Access Networks*, Wiley, 2009

Livre détaillé, qui entre profondément dans la technologie DSL :

J. A. C. Bingham, *ADSL, VDSL, and Multicarrier Modulation*, Wiley, 2000

Un livre assez pointu, qui fait le tour complet des extensions du protocole PPP :

U. D. Black, *PPP and L2TP: Remote Access Communications*, Prentice Hall, 2000

Un livre technique sur le fonctionnement réseau des modems ADSL. En particulier, l'environnement ATM est étudié en détail :

M. Busby, *Demystifying ATM/ADSL*, Prentice Hall, 1998

Le livre de base sur les modems DSL :

W. Y. Chen, *DSL: Simulation Techniques and Standard Development for Digital Subscriber Lines*, Macmillan, 1998

Petit livre assez technique sur les technologies utilisées dans les réseaux d'accès :

P. France, *Local Access Network Technologies*, IEEE Press, 2004

Le livre le plus complet sur la boucle locale, avec toutes les solutions pour réaliser du haut débit :

M. Gagnaire, *Broadband Local Loops for High-Speed Internet Access*, Artech House, 2003

Pour entrer dans le détail de l'implémentation d'un modem ADSL, le livre suivant est recommandé :

D. Ginsburg, *Implementing ADSL*, Addison Wesley, 1999

Toutes les technologies DSL et en particulier ADSL sont présentées dans ces deux livres :

W. Goralski, *ADSL & DSL Technologies*, McGraw-Hill, 2001

—, V. Giry, *ADSL et xDSL : nouvelles technologies d'accès à Internet*, Osman Eyrolles Multimédia, 2000

Livre de bonne qualité sur l'ensemble des technologies de la boucle locale, en particulier en utilisant des solutions Ethernet :

A. GUMASTE, T. ANTONY, *First Mile Access Networks and Enabling Technologies*, Pearson Education, 2004

Un petit livre facile à lire et qui introduit bien les modems *x*DSL :

L. HARTE, R. KIKTA, *Delivering xDSL*, McGraw-Hill, 2001

Gilbert Held a écrit un grand nombre d'ouvrages. Celui-ci est un excellent guide pour comprendre les caractéristiques des modems à haut débit :

G. HELD, *Next-Generation Modems: A Professional Guide to DSL and Cable Modems*, Wiley, 2000

Les solutions permettant d'apporter à l'utilisateur la parole, les données et l'image animée sont décrites dans ce livre :

C. HELLBERG, D. GREENE, D. TRUMAN, *Broadband Network Architectures: Designing and Deploying Triple-Play Services*, Prentice Hall PTR, 2007

L'accès *x*DSL et le Triple-Play associant la voix, les données et l'image sont expliqués en détail dans ce livre :

F. HENS, J. CABALLERO, *Triple Play: Building the Converged Network for IP, VoIP and IPTV*, Wiley, 2008

Les accès utilisant le réseau des câblo-opérateurs sont le sujet de ce livre :

S. OVADIA, *Broadband Cable TV Access Networks: From Technologies to Applications*, Prentice Hall PTR, 2008

Un excellent livre sur les accès fibre optique de type FTTH, qui montre également les directions de recherche qui devraient permettre d'atteindre des débits de plusieurs gigabits par seconde :

J. PRAT, *Next-Generation FTTH Passive Optical Networks: Research Towards Unlimited Bandwidth Access*, Springer, 2010

Ce livre introduit bien les modems DSL de tout type :

J. REYNOLDS, *A Practical Guide to DSL: High-Speed Connections for Local Loop and Network*, CMP, 2001

Par l'utilisation de modems câble, les accès haut débit sont beaucoup utilisés dans les pays câblés comme les États-Unis. Le livre suivant décrit en détail les mécanismes mis en œuvre pour obtenir ces hauts débits :

R. SBUDD, J. BATES, *Cable TV Systems and Modem Systems and Technology*, McGraw-Hill, 2002

Un livre facile à lire et à comprendre sur les techniques *x*DSL et câble :

R. W. SMITH, *Broadband Internet Connections: A User's Guide to DSL and Cable*, Addison Wesley, 2002

Encore un excellent livre sur l'ADSL :

C. K. SUMMERS, *ADSL*, CRC Press, 1999

Les femtocells sont les petites cellules réalisées à partir de la Home Gateway pour couvrir les connexions des machines situées dans les quelques dizaines de mètres de l'antenne :

J. Zhang, *Femtocells: Technologies and Deployment*, Wiley, 2010

10. Les réseaux d'accès hertziens

Livre complet sur les réseaux de mobiles et les réseaux sans fil :

K. Al Agha, G. Pujolle, G. Vivier, *Réseaux de mobiles et réseaux sans fil*, Eyrolles, 2e édition, 2005

Un livre sur la boucle locale radio qui a été un des livres de référence du domaine :

H. R. Anderson, *Fixed Broadband Wireless System Design*, Wiley, 2003

Livre sur la boucle locale radio pour aller beaucoup plus loin dans ce domaine :

M. P. Clark, *Wireless Access Networks: Fixed Wireless Access and WLL Networks-Design and Operation*, Wiley, 2000

B. Elbert a écrit toute une série de livres sur les communications par satellite, allant de l'application jusqu'aux techniques réseau en passant par les problèmes liés au spatial. Ses livres sont clairs et de bonne qualité :

B. R. Elbert, *The Satellite Communication Applications Handbook*, Artech House, 1996

—, *Introduction to Satellite Communications*, Artech House, 1999

—, *The Satellite Communications Ground Segment and Earth Station Handbook*, Artech House, 2002

Un livre technique essentiellement centré sur les réseaux WiMAX fixes :

M. Engels, F. Petre, *Broadband Fixed Wireless Access: A System Perspective*, Springer, 2010

Le meilleur livre et le plus complet sur la boucle locale, en particulier pour ceux qui veulent aller loin dans les détails :

M. Gagnaire, *Broadband Local Loops for High-Speed Internet Access*, Artech House, 2003

Le satellite peut également participer aux réseaux d'accès. Ce livre assez technique en fait l'inventaire :

G. Giambene, *Resource Management in Satellite Networks: Optimization and Cross-Layer Design*, Springer, 1re édition, 2007

Les accès hertziens peuvent utiliser des technologies extrêmement variées, allant des réseaux de mobiles 2G, 3G et 4G à des réseaux sans fil comme Wi-Fi, WiMAX, WRAN, etc. Ce livre fait le tour de la question :

E. Hossain, *Heterogeneous Wireless Access Networks: Architectures and Protocols*, Springer, 2010

L'accès vers les réseaux cœur peut également être réalisé par des réseaux personnels, ou PAN (Personal Area Network). Ce livre donne un panorama complet de ce type de réseaux :

M. Jacobsson, I. Niemegeers, S. Heemstra de Groot, *Personal Networks: Wireless Networking for Personal Devices*, Wiley, 2010

Livre technique portant sur la boucle locale correspondant à la 3G :

C. Johnson, *Radio Access Networks for UMTS: Principles and Practice*, Wiley, 2008

Le livre de référence depuis plus de vingt ans sur les communications par satellite (existe également en anglais) :

G. Maral, M. Bousquet, J. Pares, *Les Systèmes de télécommunications par satellite*, Masson, 1982 (remis à jour régulièrement)

Les techniques d'accès pour des clients mobiles sont expliquées en détail dans ce livre bien fait :

A. Mishra, *Cellular Technologies for Emerging Markets: 2G, 3G and Beyond*, Wiley, 2010

Excellente introduction aux boucles locales radio :

R. Pandya, *Introduction to WLLs*, Wiley, 2003

Livre avancé qui fait le point sur les techniques d'accès pour les futures technologies de réseaux de mobiles :

Y. Park, F. Adachi, *Enhanced Radio Access Technologies for Next Generation Mobile Communication*, Springer, 1re édition, 2007

Excellent livre sur WiMAX qui s'intéresse non seulement aux aspects techniques mais également économiques de cette boucle locale :

R. Prasad, F. Velez, *WiMAX Networks: Techno-Economic Vision and Challenges*, Springer, 2010

Un livre complet sur les communications par satellite :

T. Pratt, C. W. Bostian, J. E. Allnutt, *Satellite Communications*, Wiley, 2002

Bon livre sur l'ensemble des problématiques liées aux satellites :

M. Richharia, *Satellite Communication Systems*, McGraw-Hill, 1999

Un bon livre complet sur les communications par satellite :

D. Roddy, *Satellite Communications*, McGraw-Hill, 2001

Ce livre est destiné à ceux qui veulent installer un réseau d'accès de mobiles avec les derniers développements. Il faut pour cela être capable de prédire le moment où le réseau va devenir congestionné et être capable de l'optimiser :

L. Song, J. Shen, *Evolved Cellular Network Planning and Optimization for UMTS and LTE*, CRC Press, 2010

Un livre technique sur la technologie LMDS fortement utilisée dans la boucle locale :

C. Smith, *LMDS: Local Multipoint Distribution Service*, McGraw-Hill, 2000

Bon livre sur les communications vers les mobiles :

R. Steele, *Mobile Radio Communications*, Pentech Press, 1992

Un livre intéressant sur les accès hertziens de type mobile de deuxième et troisième générations :

M. Taferner, E. Bonek, *Wireless Internet Access over GSM and UMTS*, Springer, 2010

Excellent livre, qui introduit surtout les réseaux de mobiles :

W. Webb, *Introduction to Wireless Local Loop*, Artech House, 2000

Une excellente introduction à la radio cognitive, qui est sûrement une des plus grandes avancées de ce début de XXIe siècle :

A. Wyglinski, M. Nekovee, T. Hou, *Cognitive Radio Communications and Networks: Principles and Practice*, Academic Press, 2009

Livre orienté vers les communications de données dans les systèmes satellitaires :

Y. Zhang, *Internetworking and Computing over Satellite Networks*, Kluwer Academic Publishers, 2003

11. Les réseaux de domicile

Un livre spécialisé dans les courants porteurs en ligne à haut débit :

J. Anatory, N Theethayi, *Broadband Powerline Communications Systems: Theory and Applications*, WIT Press, 2010

Un livre à lire éventuellement en complément sur le réseau électrique :

C. Bayliss, B. Hardy, *Transmission and Distribution Electrical Engineering*, Newnes, 3e édition, 2006

Un livre assez complet mais qui date un peu dans un domaine où tout change en un an :

BICSI, *Residential Network Cabling*, McGraw-Hill Professional, 1re édition, 2002

Un livre à lire pour ceux qui veulent savoir de très près comment fonctionne cette technologie :

X. Carcelle, *Powerline Communications in Practice*, Artech House, 2009

Livre complet sur les différentes technologies utilisées dans les réseaux de domicile :

S. Dixit, R. Prasad, *Technologies for Home Networking*, Wiley-Interscience, 2008

Deux livres de Doherty et Anderson introduisant, d'une part, les réseaux de domicile du point de vue des réseaux sans fil et, d'autre part, les principaux éléments de sécurisation de ces réseaux :

J. Doherty, N. Anderson, *Wireless Home Networking Simplified*, Cisco Press, 1re édition, 2006

—, *Home Network Security Simplified*, Cisco Press, 1re édition, 2006

Le premier livre sur les CPL en anglais, très technique et complet :

K. Dostert, *Powerline Communications*, Prentice Hall, 2000

Un bon livre sur le CPL, qui donne de nombreux détails intéressants sur cette technologie :

H. Ferreira, L. Lampe, J. Newbury, T. Swart, *Powerline Communications: Theory and Applications for Narrowband and Broadband Communications over Power Lines*, Wiley, 2010

Livre sur les technologies Ethernet utilisées dans les réseaux de domicile et les bureaux des petites sociétés :

J. L. Harrington, *Ethernet Networking for the Small Office and Professional Home Office*, Morgan Kaufmann, 2007

Un livre complet sur les technologies CPL pour les réseaux de desserte :

H. Hrasnica, A. Haidine, R. Lehnert, *Broadband Powerline Communications: Network Design*, Wiley, 2004

Une bonne introduction aux réseaux de domicile :

K. Ivens, *Home Networking For Dummies*, For Dummies, 4e édition, 2007

Un livre de référence sur la technologie HomePlug 1.0 rédigé par des chercheurs de l'Université de Floride :

M. K. Lee, R. E. Newman, H. A. Latchman, S. Katar, L. Yonge, *Home-Plug 1.0 Powerline Communication LANs, Protocol Description and Performance Results*, Wiley, 2000

Un livre généraliste qui permet de recadrer le CPL dans son environnement :

G. O'Driscoll, *Essential Guide to Home Networking Technologies*, Prentice Hall PTR, 1re édition, 2000

Description bien faite de l'environnement Wi-Fi dans les réseaux de domicile:

R. Smith, *Wi-Fi Home Networking*, McGraw-Hill, 1re édition, 2003

12. Les réseaux optiques

Un très bon livre sur le déploiement des réseaux optiques :

V. Alwayn, *Optical Network Design and Implementation*, Cisco Press, 2004

Livre très complet sur les réseaux large bande, avec des chapitres sur les architectures ATM, IP, relais de trames et SMDS :

J. Atkins, M. Norris, *Total Area Networking*, Wiley, 1998

Un livre très complet sur l'ensemble du domaine :

G. Bernstein, B. Rajagopalan, D. Saha, *Optical Network Control: Architecture, Protocols, and Standards*, Addison Wesley, 2003

Livre introduisant les réseaux optiques de façon pédagogique :

U. Black, *Optical Networks: Third Generation Transport Systems*, Prentice Hall, 2002

Un livre facile à lire pour entrer dans le sujet des réseaux de télécommunications par fibre optique :

A. Borella, G. Cancellieri, F. Chiaralucu, *Wavelength Division Multiple Access Optical Networks*, Artech House, 1998

Très bon libre pour tout connaître sur les réseaux optiques :

D. Came, *Optical Networking*, Wiley, 2001

Les réseaux IP ayant gagné la guerre des interfaces réseau, il a fallu transporter des paquets IP sur de la fibre optique. Cela a donné naissance à IP over WDM. Ce livre introduit bien ce nouveau concept et les solutions qui peuvent y être apportées pour transporter ces flots de paquets IP à très haute vitesse :

S. Dixit, *IP over WDM: Building the Next Generation Optical Internet*, Wiley, 2003

La commutation optique est décrite en détail dans ce livre : les techniques de transmission optique, les équipements, les commutateurs :

T. El-Bawab, *Optical Switching*, Springer, 2010

Une bonne synthèse en deux cents pages du monde des communications optiques :

E. Forestieri, *Optical Communication Theory and Techniques*, Springer, 2009

Très bonne introduction aux réseaux à large multiplexage en longueur d'onde, avec des exemples de déploiement :

A. Gumaste, *DWDM Network Designs and Engineering Solutions*, Cisco Press, 2003

Une excellente introduction aux réseaux optiques. La technologie progressant tellement vite, les derniers développements en la matière ne sont évidemment pas pris en compte :

H. Hinton, *An Introduction to Photonic Switching Fabrics*, Plenum Publishing Corporation, 1993

Ce livre étudie les réseaux optiques utilisant de multiples longueurs d'ondes. Les techniques WDM sont maintenant fortement utilisées :

X. Jia, X.-D. Hu, D.-Z. Du, *Multiwavelength Optical Networks*, Springer, 2010

La technologie « burst switching » a connu un certain succès en ce qui concerne les études mais est encore relativement peu présente dans des produits. Ce livre en dresse un panorama complet :

J. Jue, V. Vokkarane, *Optical Burst Switched Networks*, Springer, 2010

Un livre qui introduit les technologies de pointe d'aujourd'hui, qui deviendront les grands standards de demain :

O. Krauss, *DWDM and Optical Networks: An Introduction to Terabit Technology*, Wiley, 2002

Un autre livre solide pour étudier en détail les réseaux optiques, en particulier les PON :

C. F. Lam, *Passive Optical Networks: Principles and Practice*, Academic Press, 2007

Un livre complet pour faire le tour des réseaux optiques et se rendre compte de l'importance de ces réseaux :

M. Maier, *Optical Switching Networks*, Cambridge University Press, 2008

Pour bien comprendre les bases des communications par les réseaux en fibre optique, le livre suivant est recommandé :

D. J. G. Mestdagh, *Fundamentals in Multiaccess Optical Fiber Networks*, Artech House, 1995

Les réseaux optiques vus au travers de la technique de multiplexage en longueur d'onde :

B. Mukherjee, *Optical WDM Networks (Optical Networks)*, Springer, 1re édition, 2006

Un livre intéressant, qui montre bien d'où l'on est parti et où l'on risque d'arriver dans quelques années dans le monde des réseaux optiques :

R. Ramaswami, K. Sivarajan, *Optical Networks: A Practical Perspective*, Morgan Kaufmann Publishers, 2001

Ce livre introduit les différents concepts permettant d'obtenir des réseaux à très haut débit. En particulier, les environnements optoélectroniques, SDH et ATM sont très bien décrits :

K. I. Sato, *Advances in Transport Network Technology: Photonic Networks, ATM, and SDH*, Artech House, 1997

Un livre technique sur la mise en place d'un réseau optique :

J. M. Simmons, *Optical Network Design and Planning*, Springer, 1re édition 2008

Un bon livre sur les réseaux optiques qui fait le point sur le multiplexage en longueur d'onde :

K. Sivalingam, S. Subramaniam, *Optical WDM Networks: Principles and Practice*, Springer, 2010

Un livre à retenir pour bien comprendre l'ensemble des techniques utilisées dans les réseaux optiques :

C. Siva Ram Murthy, M. Gurusamy, *WDM Optical Networks: Concepts, Design, and Algorithms*, Prentice Hall, 2001

Les réseaux en fibre optique ont un rôle important à jouer dans les réseaux cœur et les réseaux d'accès. Ce livre en fournit tous les détails :

A. Stavdas, *Core and Metro Networks*, Wiley, 2010

Un livre technique sur le multiplexage en longueur d'onde :

T. E. Stern, K. Bala, *Multiwavelength Optical Networks: A Layered Approach*, Prentice Hall, 1999

Un bon livre sur les commutateurs optiques :

C. Tocci, H. J. Caulfield, *Optical Interconnection, Foundations and Applications*, Artech House, 1994

Un excellent livre sur les réseaux métropolitains en fibre optique :

D. Warren, D. Hartmann, *Cisco Self-Study: Building Cisco Metro Optical Networks (METRO)*, Cisco Press, 1re édition, 2008

13. Les réseaux de niveau physique

Un livre très spécialisé sur la sécurité dans les réseaux de niveau physique :

S. Chowdhury, *Security in Fiber-Wireless (FiWi) Broadband Access Networks: Integrated EPON and Next-Generation LAN Networks*, VDM Verlag, 2010

Livre très complet permettant d'entrer dans le détail des environnements SONET et SDH :

W. J. Goralski, *SONET/SDH*, McGraw-Hill, 2002

La survie d'un réseau en cas de panne ou de rupture de composants est des plus importantes. Ce livre décrit ces problèmes et propose de nombreuses solutions dans le cadre des différentes technologies disponibles sur le marché :

W. D. Grover, *Mesh-based Survivable Transport Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking*, Prentice Hall, 2003

ATM utilise SONET/SDH comme technologie de base pour effectuer le transport des cellules. Tous les détails de cette solution se trouvent dans ce livre :

S. V. Kartalopoulos, *Understanding SONET/SDH and ATM: Communications Networks for the Next Millennium*, Wiley-IEEE Computer Society, 1999

L'intégration des données et de la parole téléphonique sur un même réseau est une des voies de l'avenir. Ce livre explique cette intégration dans le cadre des réseaux SONET/SDH :

S. V. Kartalopoulos, *Next Generation SONET/SDH: Voice and Data*, Wiley-IEEE Computer Society, 2004

Un autre livre solide pour étudier en détail les réseaux optiques, en particulier les PON :

C. F. Lam, *Passive Optical Networks: Principles and Practice*, Academic Press, 2007

Un livre sur les réseaux haut débit et large bande. Les différentes solutions du marché sont explicitées et en partie comparées :

B. G. Lee, W. Kim, W.-J. Kim, *Integrated Broadband Networks: TCP/IP, ATM, SDH/SONET, and WDM/Optics*, Artech House, 2002

Livre sur les réseaux métropolitains utilisant la technologie SONET. Cette solution est maintenant fortement concurrencée par les techniques Ethernet :

D. Minoli, P. Johnson, E. Minoli, *SONET-based Metro Area Networks*, McGraw-Hill, 2002

Cet article de la revue scientifique *Lightwave* décrit bien les techniques PON :

G. Pesavento, M. Kelsey, « PONs for the Broadband Local loop », *Lightwave*, vol. XVI, n° 10, septembre 1999, pp. 68-74

Ce livre présente les différents concepts permettant d'obtenir des réseaux à très haut débit. En particulier, l'environnement SDH est parfaitement décrit :

K.-I. Sato, *Advances in Transport Network Technology: Photonic Networks, ATM, and SDH*, Artech House, 1997

Excellent livre sur les architectures SONET et SDH pour ceux qui veulent aller loin dans ce domaine :

S. Shepard, *SONET/SDH Demystified*, McGraw-Hill, 2001

Ce livre présente de manière détaillée les couches basses de l'ATM et des réseaux large bande en général :

M. Sexton, A. Reid, *Broadband Networking: ATM, SDH, and SONET*, Artech House, 1997

Excellent livre sur les réseaux métropolitains et les technologies à mettre en œuvre pour les réaliser :

S. Shepard, *Metro Area Networking*, McGraw-Hill, 2002

Pour les hautes vitesses et les longues distances, il faut des réseaux synchrones. Ce livre étudie tous ces phénomènes en détail :

C. A. Siller, M. Shafi, *SONET/SDH: A Sourcebook of Synchronous Networking*, Wiley-IEEE Computer Society, 1996

Le premier livre sur MPLS-TP :

L. Surhone, M. Tennoe, S. henssonow, *MPLS-TP*, Betascrip Publishing, 2010

L'introduction de la fibre optique comme support de communication va permettre d'améliorer la qualité de service. Ce livre fournit un bon panorama de ces avantages :

T. H. Wu, *Fiber Network Service Survivability Architecture, Technologies and Design*, Artech House, 1992

14. Les réseaux Ethernet et ATM

Les techniques d'aloha sont à l'origine d'Ethernet. Elles peuvent encore être utiles dans certains cas particuliers. Le livre d'Abramson peut être considéré comme le premier ouvrage sur les réseaux locaux :

N. Abramson, F. F. Kuo (éd.), *The Aloha System: Computer Communication Networks*, Prentice Hall, 1973

Très bonne et très complète introduction aux réseaux ATM :

K. Asatani, *et al.*, *Introduction to ATM Networks and B-ISDN*, Wiley, 1997

Un bon livre pour comprendre la technologie du relais de trames :

R. J. Bates, *Frame Relay*, McGraw-Hill, 2002

Très bon livre sur le Gigabit Ethernet dans le cadre des réseaux métropolitains :

P. Bedell, *Gigabit Ethernet for Metro Area Networks*, McGraw-Hill, 2002

Un des premiers livres sur la technologie Ethernet Gigabit :

D. Cunningham, B. Lane, *Gigabit Ethernet Networking*, Que, 1999

Ethernet s'implante de plus en plus sur la boucle locale. Ce livre provenant de la normalisation de l'IEEE nous en donne tous les détails.

W. W. Diab, H. M. Frazier, *Ethernet in the First Mile: Access for Everyone*, IEEE Standards Information Network, 2006

Les grandes entreprises se sont dirigées vers la technologie ATM pour réaliser leur réseau cœur et interconnecter leurs réseaux d'accès. Ce livre montre bien cette démarche, même si aujourd'hui cette vision est en perte de vitesse :

D. Ginsburg, *ATM: Solutions for Enterprise Internetworking*, Addison Wesley, 1998

Le relais de trames a essayé de lutter contre la montée de l'ATM durant les années 1990. Ce livre relate les moyens d'aller vers le haut débit avec du relais de trames :

W. J. Goralski, *Frame Relay for High-Speed Networks*, Wiley, 1999

La survie d'un réseau en cas de panne ou de rupture de composants est des plus importantes. Ce livre décrit ces problèmes et propose de nombreuses solutions dans le cadre des différentes technologies disponibles sur le marché :

W. D. Grover, *Mesh-based Survivable Transport Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking*, Prentice Hall, 2003

Très bon livre d'introduction sur les réseaux métropolitains Ethernet, qui commencent à prendre une place importante sur le marché des équipements réseau :

S. Halabi, *Metro Ethernet*, Cisco Press, 2003

Un bon livre sur l'ATM, depuis les concepts de base jusqu'aux applications pour un environnement tout ATM d'entreprise :

R. Handel, *et al.*, *A Solution for Enterprise Internetworking. ATM Networks: Concepts, Protocols, Applications*, Addison Wesley, 1998

La signalisation des réseaux ATM est complexe ; ce livre en donne une bonne description :

C. Hapke, H. Brandt, *ATM Signaling: Protocols and Practice*, Wiley, 2001

Bon livre pour bien comprendre les mécanismes de base d'Ethernet :

J. Harrington, *Ethernet Networking Clearly Explained*, Morgan Kaufmann Publishers, 1999

Ethernet est partout dans les réseaux de domicile et dans les entreprises. Ce livre fournit tous les détails nécessaires à sa mise en œuvre :

J. L. Harrington, *Ethernet Networking for the Small Office and Professional Home Office*, Morgan Kaufmann, 2007

Les réseaux ATM sont de plus en plus amenés à transporter des paquets IP. Ce livre explique bien le passage d'une architecture à l'autre :

M. Hassan, M. Atiquzzaman, *Performance of TCP/IP over ATM Networks*, Artech House, 2000

Excellent livre pour bien comprendre l'enjeu de la technologie Ethernet et ses applications :

G. Held, *Ethernet Networks: Design, Implementation, Operation*, Wiley, 2002

Un petit livre introductif à l'Ethernet Carrier Grade, c'est-à-dire à l'Ethernet dévolu aux opérateurs :

G. Held, *Carrier Ethernet: Providing the Need for Speed*, Auerbach, 2008

Le relais de trames a la possibilité de transporter de la parole téléphonique IP avec ses synchronisations. Ce livre décrit cette intégration de la parole téléphonique avec les données :

O. C. Ibe, *Converged Network Architectures: Delivering Voice and Data over IP, ATM, and Frame Relay*, Wiley, 2001

L'IEEE a publié les différents standards de réseaux locaux acceptés par l'ISO. C'est dans ces documents que l'on trouvera le plus de détails sur ces normes :

IEEE Standard 802, « Local Network Standards », *IEEE Press*, 1989

Le nombre des réseaux Ethernet ne fait que s'accroître, et il est parfois difficile de savoir quand passer à la version supérieure. Ce livre répond à la question du passage vers le Gigabit Ethernet :

J. Kadambi, I. Crayford, M. Kalkunte, *Gigabit Ethernet: Migrating to High-Bandwidth LANs*, Prentice Hall, 1998

Certainement un des derniers livres à offrir un bilan complet de la technologie ATM :

S. Kasera, *ATM Networks*, McGraw-Hill Professional, 1re édition, 2006

Le livre suivant dresse un bilan assez complet du domaine de l'ATM, en particulier des interfaces de la couche physique :

O. Kyas, G. Crawford, *ATM Networks*, Prentice Hall, 2002

L'intégration voix et données est dans la logique du temps. Ce livre montre comment y arriver sous les différentes technologies qui se succèdent :

B. G. Lee, W. Kim, W.-J. Kim, *Integrated Broadband Networks: TCP/IP, ATM, SDH/SONET, and WDM/Optics*, Artech House, 2002

Bon livre complet sur les réseaux ATM :

D. E. McDysan, D. L. Spohn, *ATM: Theory and Application*, McGraw-Hill, 2000

Ce livre s'intéresse aux différentes technologies à mettre en œuvre pour transporter la parole téléphonique en paquets IP :

S. McQuerry, K. McGrew, *Cisco Voice Over Frame Relay, ATM and IP*, Pearson Higher Education, 2001

Un article fondamental sur Ethernet par deux de ses concepteurs :

R. M. METCALFE, D. R. BOGGS, « Ethernet-Distributed Packet Switching for Local Computer Networks », *Communications ACM*, vol. XIX, n° 7, juillet 1976, pp. 395-404

Un livre sur les réseaux métropolitains utilisant la technologie Ethernet :

D. MINOLI, P. JOHNSON, E. MINOLI, *Ethernet-based Metro Area Networks*, McGraw-Hill, 2002

Livre qui couvre bien tout l'environnement du Gigabit Ethernet :

M. NORRIS, *Gigabit Ethernet Technology and Applications*, Artech House, 2002

ATM est un point de passage pour aller vers les réseaux ATM ; ce livre explique en détail ce passage :

D. PAW, D. E. MCDYSAN, *ATM & MPLS Theory and Application: Foundations of Multi-Service Networking*, McGraw-Hill, 2002

Une excellente introduction au monde ATM :

H. G. PERROS, *An Introduction to ATM Networks*, Wiley, 2001

Les technologies de commutation Ethernet sont souvent mal expliquées. Ce livre donne les éléments nécessaires pour bien comprendre la poussée d'Ethernet vers la commutation et le haut débit :

S. RILEY, R. BREYER, *Switched, Fast, and Gigabit Ethernet*, Que, 1998

Un livre sur le Gigabit Ethernet :

S. SAUNDERS, *Gigabit Ethernet*, McGraw-Hill, 1998

Un livre entièrement consacré au Gigabit Ethernet, avec quelques compléments intéressants sur les réseaux locaux virtuels et les autres générations de réseaux Ethernet :

R. SEIFERT, *Gigabit Ethernet: Technology and Applications for High-Speed LAN*, Addison Wesley,1998

Livre pour entrer beaucoup plus en détail dans les couches basses de l'ATM et des réseaux large bande en général :

M. SEXTON, A. REID, *Broadband Networking: ATM, SDH, and SONET*, Artech House, 1998

Excellent livre sur les réseaux métropolitains et les technologies à mettre en œuvre pour les réaliser.

S. SHEPARD, *Metro Area Networking*, McGraw-Hill, 2002

Un très bon livre d'explication du monde des réseaux Ethernet :

C. E. SPURGEON, *Ethernet: The Definitive Guide*, O'Reilly, 2000

Ethernet est aussi un réseau qui s'installe avec force sur le marché un peu particulier des réseaux industriels, c'est-à-dire pour la gestion de processus temps réel. Ce livre en fournit les raisons :

D. J. STERLING, S. P. WISSLER, D. STERLING, *The Industrial Ethernet Networking Guide*, Delmar Publishers, 2002

Un livre à jour sur l'Ethernet Carrier Grade pour les réseaux d'opérateurs. Les éléments de la gestion Ethernet y sont bien exposés :

M. Toy, *Carrier Ethernet: Architecture, Services, OAM, Interworking*, Wiley, 2010

Très bon livre sur la place et l'avenir de l'ATM au début des années 2000 :

M. Wasniowski, *ATM Basics: High-Speed Packet Network Operation and Services*, Althos, 2004

15. MPLS et GMPLS

Ce livre de la collection Cisco Press donne des détails intéressants sur la mise en place de MPLS :

V. Alwayn, *Advanced MPLS Design and Implementation*, Cisco Press, 2001

Un article qui donne une bonne présentation de MPLS, avec ses avantages et ses inconvénients :

G. Armitage, « MPLS: The Magic Behind the Myths », *IEEE Communications Magazine*, janvier 2000

Autre article proposant une synthèse sur l'ingénierie du trafic dans MPLS :

D. O. Awduche, « MPLS and Traffic Engineering in IP Networks », *IEEE Communications Magazine*, décembre 1999

La technologie MPLS peut également être utilisée pour les réseaux métropolitains :

M. J. Bagajewicz, *MPLS for Metropolitan Area Networks*, Auerbach Publications, 2004

Excellent livre sur toutes les techniques modernes et notamment de commutation :

D. P. Black, *Building Switched Networks: Multilayer Switching, Qos, IP Multicast, Network Policy, and Service-Level Agreements*, Addison Wesley, 1999

Ce bon livre sur MPLS est un des très nombreux livres de U. Black :

U. Black, *MPLS and Label Switching Networks*, Prentice Hall, 2002

Le livre le plus orienté vers les techniques de commutation-routage de type Label-Switching et TCP/IP sur ATM :

B. Davie, P. Doolan, Y. Rekhter, *Switching in IP Networks*, Morgan Kaufmann Publishers, 1998

Livre complet sur MPLS :

B. S. Davie, Y. Rekhter, *MPLS: Technology and Applications*, Morgan Kaufmann Publishers, 2000

MPLS évolue pour garantir qualité de service, disponibilité, etc. Ce livre introduit les derniers développements de la standardisation de MPLS en la matière :

B. S. Davie, A. Farrel, *MPLS: Next Steps*, Morgan Kaufmann, 2008

Une excellente introduction à GMPLS :

A. Farrel, I. Bryskin, *GMPLS: Architecture and Applications*, Morgan Kaufmann, 2005

Excellent livre sur la qualité de service dans les différentes technologies (IP, ATM et Ethernet) :

P. Ferguson, G. Huston, *Quality of Service*, Wiley, 1998

Un très bon livre pour comprendre jusque dans les détails d'implémentation les points sensibles de la technologie MPLS :

R. Gallaher, *MPLS Training Guide: Building Multi-Protocol Label Switching Networks*, Syngress Publishing, 2003

Juniper et Cisco sont les deux grands équipementiers pour les routeurs et les LSR. Ce livre beaucoup plus large que MPLS introduit bien leurs deux visions, qui ne sont pas toujours compatibles :

W. J. Goralski, *Juniper and Cisco Routing: Policy and Protocols for Multivendor Networks*, Wiley, 2002

Les réseaux qui résistent aux pannes sont particulièrement importants pour les opérateurs de télécommunications. Le livre suivant introduit les différentes solutions, en particulier celle utilisant MPLS :

W. D. Grover, *Mesh-based Survivable Transport Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking*, Prentice Hall, 2003

Le livre suivant est fortement orienté VPN (Virtual Private Networks) :

J. Guichard, I. Pepelnjak, *MPLS and VPN Architectures: A Practical Guide to Understanding, Designing and Deploying MPLS and MPLS-Enabled VPNs*, Cisco Press, 2000

Excellent livre de départ sur MPLS :

S. Harbedy, *The MPLS Primer: An Introduction to Multi-Protocol Label Switching*, Prentice Hall, 2001

Très bon livre sur la place et l'avenir de l'ATM au début des années 2000 :

U. Lakshman, L. Lobo, *MPLS Configuration on Cisco IOS Software*, Cisco Press, 2010

Excellent livre de départ sur MPLS :

I. Minei, J. Lucek, *MPLS-Enabled Applications: Emerging Developments and New*, Wiley, 2e édition, 2008

Le livre suivant décrit en détail les différentes technologies de commutation et d'émulation :

D. Minoli, A. Alles, *LAN, ATM and LAN Emulation Technologies*, Artech House, 1997

Un livre orienté gestion de réseau et donc MPLS :

S. B. Morris, *Network Management, MIBs and MPLS: Principles, Design and Implementation*, Prentice Hall, 2003

Un excellent livre sur l'ingénierie du trafic dans les réseaux MPLS, qui est la raison d'être de ce type de réseau :

E. Osborne, A. Simha, *Traffic Engineering with MPLS*, Pearson Education, 2002

Un bon livre sur les technologies qui permettent de faire du multiservice. MPLS en fait partie :

D. Paw, *ATM & MPLS Theory & Application: of Multi-Service Networking*, McGraw-Hill, 2002

Les deux livres suivants donnent un panorama complet et d'excellente qualité des architectures MPLS et de leur application pour la réalisation de réseaux privés virtuels :

I. Pepelnjak, J. Guichard, *MPLS and VPN Architectures*, vol. I, Cisco Press, 2000

—, J. Apcar, *MPLS and VPN Architectures*, vol. II, Cisco Press, 2003

L'architecture du protocole MPLS provient de cette proposition de l'IETF :

E. Rosen, A. Viswanathan, R. Callon, « A Proposed Architecture for MPLS », *IETF Internet Draft*, juillet 1997

Livre proposant une bonne description de l'ATM et de ses possibilités en tant que technique de transfert supportant différents types de protocoles, en particulier IP :

G. C. Sackett, C. Y. Metz, *ATM and Multiprotocol Networking*, McGraw-Hill, 1997

Le NGN (Next Generation Network), qui représente les réseaux d'opérateurs pour les années 2010, est très bien introduit dans ce livre. Cette nouvelle génération est construite essentiellement sur la base de GMPLS :

P. Salina, *Next Generation Networks: Perspectives and Potentials*, Wiley, 2008

Toutes les bases à connaître pour aller vers la nouvelle génération NGN :

A. Sayeed, M. J. Morrow, *MPLS and Next Generation Networks: Foundations for NGN and Enterprise*, Cisco Press, 2006

Les protocoles de routage jouent un rôle important dans MPLS. Le livre suivant part de cette constatation pour introduire MPLS et les techniques IP sur ATM :

S. A. Thomas, *IP Switching and Routing Essentials: Understanding RIP, OSPF, BGP, MPLS, CR-LDP, and RSVP-TE*, Wiley, 2001

Parmi les architectures qui vont s'imposer, MPLS et sa généralisation GMPLS sont en première ligne :

T. Tronco, *New Network Architectures: The Path to the Future Internet*, Springer, 2010

16. Les réseaux IP : architecture

Les protocoles de routage du monde IP sont introduits dans ce livre par U. D. Black, un des auteurs ayant écrit le plus de livres sur le monde IP :

U. D. BLACK, *IP Routing Protocols: RIP, OSPF, BGP, PNNI and Cisco Routing Protocols*, Prentice Hall, 2000

Un livre simple pour démarrer avec les protocoles TCP/IP :

A. BLANK, *TCP/IP Jump Start: Internet Protocol Basics*, Sybex, 2002

Un petit guide bien fait sur l'architecture TCP/IP :

L. A. CHAPPELL, *Guide to TCP/IP*, Tittel, 2004

Le livre de D. E. Comer est complet et bien documenté sur l'environnement TCP/IP :

D. E. COMER, *Internetworking with TCP/IP. Vol. I: Principles, Protocols, and Architecture*, Prentice Hall, 4e édition, 2000 ; *TCP/IP : architecture, protocoles et applications*, Dunod, 2003

Une excellente comparaison des trois architectures de base du début des années 1990, à l'époque où TCP/IP n'avait pas encore conquis une bonne partie du marché des réseaux :

J. CYPSER, *Communication for Cooperating Systems: OSI, SNA, and TCP/IP*, Addison Wesley, 1991

Un livre très intéressant sur l'introduction de la qualité de service dans les réseaux IP et les applications possibles pour les réseaux commutés de type MPLS :

J.W. EVANS, C. FILS, *Deploying IP and MPLS QoS for Multiservice Networks: Theory & Practice*, Kaufmann, 1re édition, 2007

Très bon livre qui replace bien les différents protocoles les uns par rapport aux autres :

A. FARREL, *The Internet and Its Protocols: A Comparative Approach*, Morgan Kaufmann Publishers, 2004

Un autre livre sur l'ensemble des protocoles du monde IP :

B. A. FOROUZAN, T. G. HICKS, *TCP/IP Protocol Suite*, McGraw-Hill, 2003

Un livre dévolu à l'environnement IP mais orienté applications :

E. HALL, *Internet Application Protocols: The Definitive Guide*, O'Reilly, 2003

TCP/IP a été conçu pour des protocoles bas débit de l'ordre de quelques kilobits par seconde ; les hauts débits posent de nombreux problèmes qui sont bien étudiés dans ce livre :

M. HASSAN, R. JAIN, *High Performance TCP/IP Networking*, Prentice Hall, 2003

Excellent livre sur tous les protocoles de routage sur Internet :

C. HUITEMA, *Le Routage dans l'Internet*, Eyrolles, 1994

Christian Huitema a certainement écrit l'un des meilleurs livres sur l'environnement IPv6 :

C. HUITEMA, *IPv6 the New Internet Protocol*, Prentice Hall, 1998

L'environnement TCP/IP est considéré dans ce livre comme devant se trouver partout, à tout moment et pour tout faire. Les problèmes posés par cet Internet enfoui sont abordés en détail :

E. INSAM, *TCP/IP Embedded Internet Applications*, Newnes, 2003

Le monde Internet investit de plus en plus l'univers des mobiles et du sans-fil. De nombreux protocoles y sont dédiés. Ce livre en décrit la plupart :

K. MAKKI, N. PISSINOU, E. K. PARK, *Mobile and Wireless Internet: Protocols, Algorithms, and Systems*, Kluwer Academic Publishers, 2003

Bon livre sur les techniques de routage dans les réseaux IP :

R. MALHOTRA, *IP Routing*, O'Reilly, 2002

Les algorithmes de routage forment une part importante des réseaux TCP/IP. Ce livre en détaille presque tous les secrets :

D. MEDHI, K. RAMASAMY, *Network Routing: Algorithms, Protocols, and Architectures*, Morgan Kaufmann, 2007

En deux volumes et plus de mille pages, l'ensemble des protocoles du monde TCP/IP sont décrits et expliqués en détail :

P. MILLER, *TCP/IP, The Ultimate Protocol Guide*, Brown Walker Press, 2010

Un excellent livre sur l'architecture Internet :

D. MINOLI, *et al.*, *Internet Architectures*, Wiley, 1999

Très bonne description de l'un des protocoles de routage les plus importants d'Internet :

J. T. MOY, *OSPF: Anatomy of an Internet Routing Protocol*, Addison Wesley, 1998

La qualité de service (QoS) est très généralement gérée au niveau 3 de l'architecture des réseaux. Ce livre décrit les différentes solutions pour garantir cette qualité de service :

K. PARK, *QoS in Packet Networks*, Springer, 2010

Un livre nettement plus pratique que la plupart de ceux qui sont cités ici. Pour ceux qui veulent réaliser leur réseau d'entreprise, c'est un bon début :

D. REYNDERS, E. WRIGHT, *Practical TCP/IP and Ethernet Networking for Industry*, Newnes, 2003

Un livre récent focalisé sur la gestion des adresses, qui reste un problème majeur dans le monde Internet.

T. ROONEY, *Introduction to IP Adress Management*, Wiley-IEEE Press, 2010

Un livre électronique qui introduit bien l'environnement des protocoles de l'Internet :

T. SANCHEZ-CLARK, *TCP/IP*, édition Kindle, 2010

Internet avec une vision nouvelle et les derniers développements :

B. VAN SCHEWICK, *Internet Architecture and Innovation*, The MIT Press, 2010

La nouvelle génération de routage est présentée dans ce livre de J. Stewart. Très intéressant pour ceux qui veulent aller loin dans cette problématique :

J. W. Stewart, *BGP4: Inter-Domain Routing in the Internet*, Addison Wesley, 1998

L'environnement IP s'étend de plus en plus, et l'Internet des choses en fait partie. Le livre suivant se penche sur cette extension et plus particulièrement sur la connexion des objets intelligents :

J.-P. Vasseur, A. Dunkels, *Interconnecting Smart Objects with IP: the Next Internet*, Morgan Kaufman, 2010

Un excellent livre de moins de deux cents pages qui fait le point sur les réseaux de télécommunications :

J. Walrand, S. Parekh, *Communication Networks: A Concise Introduction*, Morgan and Claypool Publisher, 2010

Un livre intéressant sur les possibilités futures d'Internet :

J. Zittrain, *The Future of the Internet – And How to Stop It*, Yale University Press, 2008

17. Les réseaux IP : gestion et contrôle

Un livre intéressant sur l'ingénierie des réseaux IP :

P. T. Ammann, *Managing Dynamic IP Networks*, McGraw-Hill, 2000

Un excellent livre d'introduction aux techniques de qualité de service dans les réseaux IP :

G. Armitage, *Quality of Service in IP Networks*, Pearson Higher Education, 2000

Un livre complet sur les techniques permettant d'obtenir une qualité de service dans l'ensemble des réseaux pouvant transporter des paquets IP :

D. P. Black, *Building Switched Networks: Multilayer Switching, Qos, IP Multicast, Network Policy, and Service Level Agreements*, Addison Wesley, 1999

Un livre dédié aux protocoles de sécurité dans le monde IP :

U. D. Black, *Internet Security Protocols: Protecting IP Traffic*, Prentice Hall, 2000

La qualité de service est primordiale dans les réseaux à haut débit. Ce livre présente bien cette fonctionnalité dans un cadre général et la replace par rapport au monde IP :

H. J. Chao, X. Guo, *Quality of Service Control in High-Speed Networks*, Wiley, 2001

Un livre de base sur la gestion et l'administration des réseaux IP :

A. Clemm, *Network Management Fundamentals*, Cisco Press, 1re édition, 2006

Livre sur la qualité de service permettant de faire transiter des applications de type téléphonie sur un réseau IP :

D. Collins, *Carrier Grade Voice Over IP*, McGraw-Hill, 2000

Une excellente introduction à la téléphonie dans un environnement IP :

J. Davidson, L. Peters, B. Gracely, *Voice over IP Fundamentals*, Cisco Press, 2000

Un des nombreux livres sur la qualité de service. Celui-ci est intéressant par sa présentation pragmatique :

W. HARDY, *QoS: Measurement and Evaluation of Telecommunications Quality of Service*, Wiley, 2002

Un livre technique mais très intéressant sur les performances des environnements IP sur ATM :

M. HASSAN, M. ATIQUZZAMAN, *Performance of TCP/IP Over ATM Networks*, Artech House, 2000

Christian Huitema a certainement écrit l'un des meilleurs livres sur l'environnement IPv6 :

C. HUITEMA, *IPv6 the New Internet Protocol*, Prentice Hall, 1998

Livre qui s'intéresse plus particulièrement à la gestion des réseaux TCP/IP :

C. HUNT, *TCP/IP Network Administration*, O'Reilly, 2010

Le monde Internet est malheureusement peu disponible (seulement 99,9 % du temps en moyenne), et sa fiabilité est souvent mise en cause. Ce livre apporte des réponses à ces problèmes :

C. KALMANEK, S. MISRA, R. YANG, *Guide to Reliable Internet Services and Applications*, Springer, 2010

La mise en place d'un réseau IP pose de nombreuses questions, notamment sur le choix de l'architecture. Le livre suivant donne des réponses précises dans le domaine de l'ingénierie :

C. S. LONG, *IP Network Design*, McGraw-Hill, 2001

Livre qui aborde avec beaucoup de pédagogie la qualité de service dans les environnements IP et ATM ainsi que la gestion du trafic :

D. MCDYSAN, *QoS and Traffic Management in IP and ATM Networks*, McGraw-Hill, 1999

Un livre pointu sur les performances des réseaux IP en fonction de leurs algorithmes de contrôle de ressources :

J. MILBRANDT, *Moving on to Next Generation IP Networks, Performance Evaluation of Efficient Resource Management Concepts*, VDM Verlag, 2008

Un bon livre sur la qualité de service, en particulier dans le monde IP :

A. MISHRA, *Quality of Service in Communications Networks*, Wiley, 2002

Ce livre aborde les grandes orientations du monde des réseaux de télécommunications. On y retrouve en très bonne posture les réseaux IP, les services associés et les techniques de gestion :

T. PLEVYAK, V. SAHIN, *Next Generation Telecommunications Networks, Services, and Management*, Wiley, 2010

Un livre décrivant les évolutions du monde IP et en particulier la gestion et le contrôle :

G. PUJOLLE, *Management, Control, and Evolution of IP Networks*, ISTE Publishing Company, 2007

Un livre très intéressant sur les liaisons entre TCP/IP et UNIX :

R. SANTIFALLER, *TCP/IP and NFS, Internetworking in a UNIX Environment*, Addison Wesley, 1991

Excellent livre sur le protocole IP Mobile et l'Internet hertzien :

J. D. SOLOMON, *Mobile IP the Internet Unplugged*, Prentice Hall, 1998

Livre détaillé permettant d'entrer dans les détails des techniques de routage du monde IP ainsi que de leurs extensions pour MPLS :

S. A. THOMAS, *IP Switching and Routing Essentials: Understanding RIP, OSPF, BGP, MPLS, CR-LDP, and RSVP-TE*, Wiley, 2000

L'intégration du monde IP et des réseaux fibre optique est remarquablement introduite dans ce livre. À lire par ceux qui veulent y voir plus clair dans les futures architectures très haut débit du monde IP :

P. TOMSU, C. SCHMUTZER, *Next Generation Optical Networks: The Convergence of IP Intelligence and Optical Technologies*, Prentice Hall, 2001

Dans l'environnement TCP/IP, on intègre des applicatifs d'UNIX tels que NFS, qui gère les fichiers distribués :

J. R. TONG-TONG, *NFS : système de fichiers distribués sous Unix*, Eyrolles, 1993

Un très bon livre pour en savoir plus sur la qualité de service dans les environnements IP :

S. VEGESNA, *IP Quality of Service*, Cisco Press, 2001

Également un très bon livre qui introduit en détail tous les mécanismes pour la qualité de service dans le monde IP :

Z. WANG, *Internet QoS: Architectures and Mechanisms for Quality of Service*, Morgan Kaufmann Publishers, 2001

Un livre spécialisé sur l'approche multicast dans les réseaux IP :

B. WILLIAMSON, *Developing IP Multicast Networks: The Definitive Guide to Designing and Deploying CISCO IP Multi- cast*, Cisco Press, 2000

18. Les réseaux de mobiles 2G et 3G

Un livre technique et complet décrivant les processus de normalisation :

R. BEKKERS, *Mobile Telecommunications Standards: UMTS, GSM, TETRA*, Book News, 2001

Un livre très pédagogique sur l'ensemble des technologies de réseaux de mobiles et sans fil :

U. D. BLACK, *Second Generation Mobile and Wireless Networks*, Prentice Hall, 1998

Un livre au spectre assez large sur l'environnement UMTS :

C. Braithwaite, M. Scott, *UMTS Network Planning and Development: Design and Implementation of the 3G CDMA Infrastructure*, Newnes, 2004

Ce livre présente un panorama intéressant des réseaux sans fil pour les communications interpersonnelles :

I. Brodsky, *Wireless: The Revolution in Personal Telecommunications*, Artech House,1995

Les terminaux se connectent de partout, de telle sorte que l'on parle d'Internet ambiant :

J. Burkhart, *Pervasive Computing: Technology and Architecture of Mobile Internet Applications*, Addison Wesley, 2002

Un livre dédié à l'UMTS :

J. P. Castro, *The UMTS Network and Radio Access Technology*, Wiley, 2002

Un des deux standards de l'UMTS vu très en détail :

R. Esmailzadeh, M. Nakagawa, *TDD-CDMA for Wireless Communications*, Artech House, 2002

Un excellent livre sur la période intermédiaire qui mène de la deuxième à la troisième génération :

N. Faggion, *Le GPRS : du WAP à l'UMTS*, Dunod, 2001

Livre dédié à la 3G :

V. Garg, *IS-95 CDMA and cdma2000*, Prentice Hall, 1999

Un livre complet sur la technique CDMA dans les environnements sans fil :

V. K. Gar, K. Smolik, J. E. Wilkes, *Applications of CDMA in Wireless/Personal Communications*, Prentice Hall, 1997

Un des nombreux livres sur le GSM, très complet sur cette deuxième génération de mobiles :

G. Heine, *GSM Networks: Protocols, Terminology and Implementation*, Artech House, 1999

Un très bon livre, expliquant bien l'évolution des réseaux de mobiles :

T. Halonen, *GSM, GPRS and EDGE Performance-Evolution Towards 3G/UMTS*, Wiley, 2002

Un livre à lire pour ceux qui s'intéressent à l'interface radio :

L. Hanzo, C. H. Wong, M. S. Yee, *Adaptive Wireless Transceivers: Turbo-Coded, Turbo-Equalized and Space-Time Coded TDMA, CDMA, and OFDM Systems*, Wiley, 2002

Excellent livre technique sur l'UMTS et plus particulièrement la version W-CDMA :

H. Holma, A. Toskala, *UMTS : les réseaux mobiles de troisième génération*, Osman Eyrolles Multimédia, 2001

Un autre excellent livre sur le W-CDMA :

M. R. Karim, M. Sarraf, *W-CDMA and cdma2000 for 3G Mobile Networks*, McGraw-Hill, 2002

Un livre orienté vers la planification des réseaux téléphoniques, pour ceux qui s'intéressent à ce domaine connexe :

J. Laiho, *et al.*, *Radio Network Planning and Optimization for UMTS*, Wiley, 2001

Pour ceux qui veulent en savoir plus sur les développements poussés par l'Amérique du Nord :

S. Lee, *Spread Spectrum CDMA: IS-95 and IS-2000 for RF Communications*, McGraw-Hill, 2002

Un excellent livre, très complet, sur le mobile et le sans-fil :

Y. B. Lin, I. Chlamtac, *Wireless and Mobile Network Architectures*, Wiley, 2000

Un très bon livre, présentant les principes de base des réseaux cellulaires :

R. C. V. Macario, *Cellular Radio, Principles and Design*, Macmillan, 2e édition, 1997

Livre sur la transition vers la troisième génération et l'introduction des données à haut débit :

G. D. Mandyam, J. Lai, *Third Generation CDMA Systems for Enhanced Data Services*, Academic Press, 2002

Livre relativement technique sur l'introduction de services dans les réseaux de mobiles et sans fil :

M. Morisio, M. Torchiano, *Developing Services for the Wireless Internet*, Springer, 1re édition, 2006

Excellent livre, qui fait le point sur les réseaux sans fil pour le transport de données multimédias :

N. J. Muller, L. L. Tyke, *Wireless Data Networking*, Artech House, 1995

Un livre consacré à l'UMTS :

F. Muratore, *UMTS: Mobile Communications for the Future*, Wiley, 2000

Le W-CDMA est devenu le standard de l'interface air de la troisième génération pour l'UMTS. Il est présenté dans le livre suivant :

T. Ojanpera, R. Prasad, *Wideband CDMA for Third Generation Mobile Communications*, Artech House, 1998

Un livre complet sur les services de communication par réseau sans fil :

R. Prasad, *Universal Wireless Personal Communications*, Artech House, juillet 1998

L'interface radio est à la base des performances des réseaux de mobiles de troisième génération. Ce livre explique les raisons des choix techniques :

A. Rosenberg, S. Kemp, *CDMA Capacity and Quality Optimization*, McGraw-Hill, 2003

L'article de base précisant le débit d'une liaison en fonction de la bande passante du canal :

C. Shannon, « A Mathematical Theory of Communication », *Bell System Technical Journal*, vol. XXVII, 1948, pp. 379-423 et 623-656

Une bonne introduction aux réseaux de troisième génération :

C. Smith, *3G Wireless Networks*, McGraw-Hill Osborne Media, 2e édition, 2006

Ce livre de 2001 décrit bien les états transitoires entre les trois générations :

R. Steele, *GSM, cdmaOne and 3G Systems*, Wiley, 2001

Le passage des trois étapes, du GSM à l'UMTS, est très bien traité dans le livre suivant :

J. Tisal, *The GSM Network. The GPRS Evolution: One Step Towards UMTS*, Wiley, 2000

Une bonne introduction globale aux réseaux sans fil :

D. Tse, P. Viswanath, *Fundamentals of Wireless Communication*, Cambridge University Press, 2005

La version américaine de la 3G expliquée en détail :

V. Vanghi, A. Damnjanovic, B. Vojcic, *The cdma2000 System for Mobile Communications*, Prentice Hall, 2004

Viterbi est à l'origine de la technique d'accès CDMA. Il explique dans ce livre les principes du CDMA et les moyens de l'employer efficacement :

A. J. Viterbi, *CDMA Principles of Spread-Spectrum Communications*, Addison Wesley, 1995

19. Les réseaux de mobiles 3G+ et 4G

Un livre introductif sur la place des réseaux ad hoc dans le monde des réseaux mobiles et sans fil :

G. Aggelou, *Mobile Ad Hoc Networks: From Wireless LANs to 4G Networks*, McGraw-Hill Professional, 1re édition, 2004

Un livre au spectre assez large sur l'environnement UMTS :

C. Braithwaite, M. Scott, *UMTS Network Planning and Development: Design and Implementation of the 3G CDMA Infrastructure*, Newnes, 2004

Un livre dédié à l'UMTS :

J. P. Castro, *The UMTS Network and Radio Access Technology*, Wiley, 2002

Un livre à lire pour l'introduction du monde IP dans les réseaux de mobiles :

J. P. Castro, *All IP in 3G CDMA Networks: The UMTS Infrastructure and Service Platforms for Future Mobile Systems*, Wiley, 2004

Cet excellent livre introduit les éléments de la quatrième génération, qui permettra réellement au multimédia de s'installer sur les terminaux mobile :

L. M. Correia, *Mobile Broadband Multimedia Networks: Techniques, Models and Tools for 4G*, Academic Press, 1re édition, 2007

Ce livre complet s'intéresse aux techniques utilisées ainsi qu'aux outils nécessaires pour la mise en œuvre de la troisième génération :

E. Dalhman, S. Parkvall, J. Skold, P. Beming, *3G evolution: HSPA and LTE Mobile Broadband*, Academic Press, 2008

L'auteur s'intéresse dans ce livre aux phénomènes liés à la mobilité dans les nouvelles générations des réseaux de mobiles à haute vitesse :

M. Ergen, *Mobile Broadband, Including WiMAX and LTE*, Springer, 2009

Un des deux standards de l'UMTS vu très en détail :

R. Esmailzadeh, M. Nakagawa, *TDD-CDMA for Wireless Communications*, Artech House, 2009

Excellent livre technique sur le LTE et sur le démarrage du LTE-Advanced :

F. Khan, *LTE for 4G mobile broadband : Air Interface Technologies and Performance*, Cambridge University Press, 2009

Livre dédié à la 3G :

V. Garg, *IS-95 CDMA and cdma2000*, Prentice Hall, 1999

Un livre technique sur le LTE pour entrer dans les détails des techniques de transmission :

A. Ghosh, J. Zhang, J. Andrews, R. Muhamed, *Fundamentals of LTE*, Prentice Hall, 2010

Un livre à lire par ceux qui s'intéressent à l'interface radio :

L. Hanzo, C. H. Wong, M. S. Yee, *Adaptive Wireless Transceivers: Turbo-Coded, Turbo-Equalized and Space-Time Coded TDMA, CDMA, and OFDM Systems*, Wiley, 2002

Excellent livre technique sur l'UMTS et plus particulièrement la version W-CDMA :

H. Holma, A. Toskala, *UMTS : les réseaux mobiles de troisième génération*, Osman Eyrolles Multimédia, 2001

Par les mêmes auteurs, un livre sur le LTE :

H. Holma, A. Toskala, *LTE for UMTS, OFDMA and SC-FDMA based Radio Access*, Wiley, 2009

Le premier livre sur la sécurité dans la nouvelle génération du LTE :

G. Horn, D. Forsberg, W.-D. Moeller, V. Niemi, *LTE Security*, Wiley, 2010

Un autre excellent livre sur le W-CDMA :

M. R. Karim, M. Sarraf, *W-CDMA and cdma2000 for 3G Mobile Networks*, McGraw-Hill, 2002

Un livre consacré à la planification des réseaux téléphoniques :

J. Laiho, *et al.*, *Radio Network Planning and Optimization for UMTS*, Wiley, 2001

Livre sur la transition vers la troisième génération et l'introduction des données à haut débit :

G. D. Mandyam, J. Lai, *Third Generation CDMA Systems for Enhanced Data Services*, Academic Press, 2002

Livre relativement technique sur l'introduction de services dans les réseaux de mobiles et sans fil :

M. Morisio, M. Torchiano, *Developing Services for the Wireless Internet*, Springer, 1re édition, 2006

Un livre consacré à l'UMTS :

F. Muratore, *UMTS: Mobile Communications for the Future*, Wiley, 2000

L'interface radio est à la base des performances des réseaux de mobiles de troisième génération. Ce livre explique les raisons des choix techniques :

A. Rosenberg, S. Kemp, *CDMA Capacity and Quality Optimization*, McGraw-Hill, 2003

Un panorama très complet des solutions pour les réseaux de mobiles, incluant la 3G et la 4G ainsi que le WiMAX :

M. Sauter, *Beyong 3G*, Wiley, 2010

Un excellent livre dédié à l'introduction de la technique LTE :

S. Sesia, I. Toufik, M. Baker, *LTE, the UMTS Long Term Evolution: From Theory to Practice*, Wiley, 2009

Ce livre est une excellente introduction aux réseaux de capteurs et à leur intégration dans la vie de tous les jours. Le futur de cette technologie est également discuté en détail :

R. Shorey, A. Ananda, M. C. Chan, W. Tsang, *Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Directions*, Wiley-IEEE Press, 1re édition, 2006

Une bonne introduction aux réseaux de troisième génération :

C. Smith, *3G Wireless Networks*, McGraw-Hill Osborne Media, 2e édition, 2006

Ce livre introduit les éléments importants du déploiement des réseaux de mobiles à haute capacité et de son optimisation :

L. Song, J. Shen, *Evolved Cellular Network Planning and Optimization for UMTS and LTE*, CRC Press, 2010

Une bonne introduction globale aux réseaux sans fil :

D. Tse, P. Viswanath, *Fundamentals of Wireless Communication*, Cambridge University Press, 2005

La version américaine de la 3G expliquée en détail :

V. Vanghi, A. Damnjanovic, B. Vojcic, *The cdma2000 System for Mobile Communications*, Prentice Hall, 2004

20. Convergence fixe/mobile

En trois cents pages, ce livre présente bien l'IMS et la façon de le déployer dans un réseau d'opérateur :

K. Al-Begain, C. Balakrishna, L. Galindo, D. Fernandez, *IMS: A Development and Deployment Perspective*, Wiley, 2009

Un livre sur IPv6 et ses fonctionnalités pour réaliser la convergence fixe mobile :

M. Blanchet, *Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks*, Wiley, 1re édition, 2006

Livre sur l'IMS et la convergence IP. Bonne présentation de la convergence des réseaux fixes et mobiles :

G. Camarillo, M.-A. García-Martín, *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds*, Wiley, 2e édition, 2006

La convergence fixe/mobile dans les détails vue du côté de la normalisation :

C. Esteve Rothenberg, *Fixed-Mobile Convergence in TISPAN/3GPP IMS*, VDM Verlag, 2008

Présentation détaillée de la convergence fixe/mobile et de tous les attributs associés :

J. Ghetie, *Fixed-Mobile Wireless Networks Convergence: Technologies, Solutions, Services*, Cambridge University Press, 1re édition, 2008

L'IMS est l'élément principal de la convergence fixe/mobile. Ce livre le décrit en détail :

M. Poikselka, G. Mayer, *The IMS: IP Multimedia Concepts and Services*, Wiley, 2009

Un livre qui fournit tous les détails de l'IMS et de sa mise en œuvre :

T. Russell, *The IP Multimedia Subsystem (IMS): Session Control and Other Network Operations*, McGraw-Hill Osborne Media, 1re édition, 2007

Une vue totalement différente de la convergence fixe/mobile :

C. Saxtoft, *Convergence: User Expectations, Communications Enablers and Business Opportunities*, Wiley, 2008

Un livre dévolu à la convergence fixe/mobile :

A. Shneyderman, A. Casati, *Fixed Mobile Convergence*, McGraw-Hill Osborne Media, 1re édition, 2008

Un autre livre sur la convergence et les développements en cours et à venir :

R. Watson, *Fixed/Mobile Convergence and Beyond: Mobile Unified Communications*, Newnes, 2008

La conception d'une plate-forme IMS ainsi que son déploiement sont présentés en détail dans ce livre :

M. Wuthnow, J. Shih, M. Stafford, *IMS: A New Model for Blending Applications*, Auerbach Publications, 2009

21. Les réseaux personnels

Livre technique sur l'Ultra-Wideband :

B. Allen, M. Dohler, E. E. Okon, W. Q. Malik, A. K. Brown, D. J. Edwards, *Ultra-Wideband Antennas and Propagation for Communications, Radar and Imaging*, Wiley, 2006

Bon livre pour ceux qui veulent qui veulent aller plus loin dans les techniques UWB :

H. Arslan, Z. N. Chen, M.-G. Di Benedetto, *Ultra Wideband Wireless Communication*, Wiley, 2006

Excellent livre pour tout comprendre sur Bluetooth :

D. Bakker, D. McMichael Gilster, R. Gils, *Bluetooth End to End*, Wiley, 1re édition, 2002

Très bonne introduction à Bluetooth disponible en chargement sur Internet :

F. Banifatemi, *Basic Bluetooth Handbook*, édition Kindle, 2010

Livre assez complet sur l'environnement ZigBee :

S. Farahani, *ZigBee Wireless Networks and Transceivers*, Newnes, 2008

L'Ultra-Wideband est un environnement complexe. Ce livre en donne de façon précise les différents éléments :

M. Ghavami, L. Michael, R. Kohno, *Ultra Wideband Signals and Systems in Communication Engineering*, Wiley, 2e édition, 2007

Livre intéressant pour ceux qui veulent aller plus loin dans la mise en œuvre de réseaux Bluetooth :

A. S. Huang, L. Rudolp, *Bluetooth Essentials for Programmers*, Cambridge University Press, 1re édition, 2007

Un livre très pointu sur les passerelles avec les réseaux ZigBee dans le cadre des réseaux locaux industriels :

P. A. Kuban, *A Controller Area Network Gateway to ZigBee. A Proposition of an Architecture to Extend CAN*, VDM Verlag, 2007

Un livre complémentaire sur les capteurs à très faible consommation d'énergie :

M. Kuorilehto, M. Kohvakka, J. Suhonen, P. Hämäläinen, M. Hännikäinen, T. D. Hamalainen, *Ultra-Low Energy Wireless Sensor Networks in Practice: Theory, Realization and Deployment*, Wiley, 2008

Un livre intéressant sur les différents réseaux provenant de l'IEEE :

H. Labiod, H. Afifi, C. De Santis, *Wi-Fi, Bluetooth, Zigbee and WiMax*, Springer, 2010

Très bonne introduction aux réseaux UWB :

I. Oppermann, M. Hämäläinen, J. Iinatti, *UWB: Theory and Applications*, Wiley, 2004

Un livre technique sur l'Ultra-Wideband :

K. Siwiak, D. McKeown, *Ultra-Wideband Radio Technology*, Wiley, 2004

Une excellente première approche des réseaux Ultra-Wideband :

S. Wood, R. Aiello, *Essentials of UWB*, Cambridge University Press, 1re édition, 2008

Un livre qui introduit bien tous les aspects des réseaux ad hoc dans l'environnement des réseaux personnels :

S.-L. Wu, Y.-C. Tseng, *Wireless Ad Hoc Networking: Personal-Area, Local-Area, and the Sensory-Area Networks*, Auerbach, 1re édition, 2007

Un livre très complet qui déborde les PAN en présentant également les LAN et les MAN :

Y. Xiao, Y. Pan, *Emerging Wireless LANs, Wireless PANs, and Wireless MANs*, Wiley, 1re édition, 2009

22. Les réseaux Wi-Fi

Livre complet sur les réseaux de mobiles et les réseaux sans fil :

K. Al Agha, G. Pujolle, G. Vivier, *Réseaux de mobiles et réseaux sans fil*, 2e édition, Eyrolles, 2005

Un livre dévolu aux applications dans les réseaux sans fil :

H. P. Alesso, C. F. Smith, *The Intelligent Wireless Web*, Addison Wesley, 2001

Les réseaux de capteurs posent de nouveaux problèmes architecturaux et protocolaires. Le livre suivant en dresse l'inventaire :

E. H. Callaway, *Wireless Sensor Networks: Architectures and Protocols*, Auerbach Publications, 2003

Livre spécialisé sur la ToIP dans les réseaux Wi-Fi :

P. Chandra, D. Lide, *Wi-Fi Telephony: Challenges and Solutions for Voice over WLANs*, Newnes, 1re édition, 2006

La sécurité est le point faible des réseaux Wi-Fi avec la qualité de service. Ce livre fait le point sur ces questions dans l'environnement Windows :

J. Davies, *Deploying Secure 802.11 Wireless Networks with Microsoft Windows*, Microsoft Press, 2003

Livre intéressant par sa présentation très pédagogique du réseau Wi-Fi :

H. Davis, R. Mansfield, *The Wi-Fi Experience: Everyone's Guide to 802.11b Wireless Networking*, Que, 2001

Un excellent livre sur les applications que l'on peut mettre en place dans les réseaux sans fil :

A. Dorman, *The Essential Guide to Wireless Communications Applications*, Prentice Hall, 2002

Un livre qui se démarque par la façon de présenter les réseaux sans fil en examinant le problème de leur mise en place dans une communauté d'intérêt :

R. Flickenger, *Building Wireless Community Networks*, O'Reilly, 2001

Un livre très didactique sur les réseaux IEEE 802.11 :

M. S. Gast, *802.11 Wireless Networks: The Definitive Guide*, O'Reilly, 2e édition, 2005

Excellent livre sur l'installation de hotspots :

E. Geier, *Wi-Fi Hotspots: Setting Up Public Wireless Internet Access*, Cisco Press, 2006

Zigbee est un réseau qui a démarré doucement mais qui devient de plus en plus important dans le monde des réseaux personnel pour la signalisation. Ce livre en constitue une très bonne introduction :

D. Gislason, *Zigbee Wireless Networking*, Newnes, 2008

Livre technique sur les réseaux de mobiles et la problématique radio :

A. W. Graham, N. C. Kirkman, P. M. Paul, *Mobile Radio Network Design in the VHF and UHF Bands: A Practical Approach*, Wiley, 2007

Un excellent livre sur les réseaux de capteurs :

A. Hac, *Wireless Sensor Network Designs*, Wiley, 2003

Les réseaux sans fil forment une excellente solution pour l'accès à un modem ADSL ou un modem câble dans l'environnement domotique :

P. Heltzel, *Complete Wireless Home Networking*, Prentice Hall, 2003

Le livre suivant donne la plupart des outils qui peuvent être utilisés pour réaliser une étude de performance :

T. Janevski, *Traffic Analysis and Design of Wireless IP Networks*, Artech House, 2003

Un bon livre technique sur la sécurité dans les réseaux d'entreprise de type Wi-Fi :

J. Khan, A. Khwaja, *Building Secure Wireless Networks with 802.11*, Wiley, 2003

Excellente introduction aux réseaux Wi-Fi :

J. La Rocca, *802.11 Demystified: Wi-Fi Made Easy*, McGraw-Hill, 2002

L'histoire de Wi-Fi depuis son origine et sa normalisation :

W. LELMSTRA, V. HAYES, J. GROENEWEGEN, *The Innovation Journey of Wi-Fi: the Road to Global Success*, Cambridge University Press, 2010

Un livre détaillé sur les réseaux Wi-Fi et leur ingénierie :

D. MALES, G. PUJOLLE, *Wi-Fi par la pratique*, Eyrolles, 2e édition, 2004

L'ingénierie des réseaux Wi-Fi paraît simple. En réalité, selon la taille du réseau, la complexité augmente vite. Les règles élémentaires à mettre en œuvre sont très bien expliquées dans ce livre :

M. MALLICK, *Mobile and Wireless Design Essentials*, Wiley, 2003

La sécurité est un problème capital. Pour un lecteur intéressé plus spécifiquement par ce domaine dans les réseaux sans fil, ce livre devrait être utile :

M. MAXIM, D. POLLINO, *Wireless Security*, McGraw-Hill, 2002

Un livre complet sur les réseaux ad-hoc :

C. S. R. MURTHY, B. S. MANOJ, *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall, 2004

Un autre excellent livre sur la sécurité dans les réseaux sans fil :

R. K. NICHOLS, P. C. LEKKAS, *Wireless Security: Models, Threats, and Solutions*, McGraw-Hill, 2001

L'IEEE, qui gère les groupes de travail sur la normalisation du sans-fil, publie un bon livre technique sur le 802.11 :

B. O'HARA, A. PETRICK, *The IEEE 802.11 Handbook: A Designer's Companion*, IEEE Press, 1999

Un livre pour bien comprendre Wi-Fi et son installation dans l'entreprise :

F. OHRTMAN, K. ROEDER, *Wi-Fi Handbook: Building 802.11b Wireless Networks*, McGraw-Hill, 2003

Excellente approche, présentant les grands principes des technologies sans fil :

K. PAHLAVAN, P. KRISHNAMURTHY, *Principles of Wireless Networks: A Unified Approach*, Prentice Hall, 2001

Le livre de référence sur les réseaux ad-hoc :

C. PERKINS, *Ad-hoc Networking*, Addison Wesley, 2000

Un livre consacré aux communications personnelles dans un environnement sans fil :

R. PRASAD, *Universal Wireless Personal Communications*, Artech House, 1998

Très bon livre d'introduction aux réseaux sans fil :

T. S. RAPPAPORT, *Wireless Communications Principles and Practice*, Prentice Hall, 2001

Un livre orienté vers les solutions Wi-Fi Cisco :

P. ROSHAN, J. LEARY, *Wireless Local-Area Network Fundamentals*, Cisco Press, 2003

Un livre pour ceux qui veulent en savoir plus sur les réseaux sans fil :

C. W. Sayre, *Complete Wireless Design*, McGraw-Hill, 2001

Un des nombreux livres de Stallings, toujours très pédagogique et complet :

W. Stallings, *Wireless Communications & Networks*, Prentice Hall, 2001

Un livre pratique sur WiMax :

D. Sweeney, *WiMax Operator's Manual: Building 802.16 Wireless Networks*, Apress, 2004

Livre complet sur les réseaux ad-hoc. Pour tous ceux qui souhaitent entrer dans les détails des protocoles de routage :

C. K. Toh, *Ad-hoc Mobile Wireless Networks: Protocols and Systems*, Prentice Hall, 2001

Pour ceux qui veulent aller plus loin sur la couche physique des réseaux Wi-Fi :

X. Wang, H. V. Poor, *Wireless Communication Systems: Advanced Techniques for Signal Reception*, Prentice Hall, 2003

Excellent livre, qui introduit surtout les réseaux sans fil de la boucle locale :

W. Webb, *Introduction to Wireless Local Loop*, Artech House, 2000

Livre en complément pour les aspects de sécurité et de gestion des ressources :

Y. Zhang, H. Hu, M. Fujise, *Resource, Mobility, and Security Management in Wireless Networks and Mobile Communications*, Auerbach, 1re édition, 2006

Un très bon livre sur les réseaux de capteurs :

F. Zhao, L. Guibas, *Wireless Sensor Networks*, Morgan Kaufmann Publishers, 2004

23. Réseaux hertziens avec relais

Livre complet sur les réseaux de mobiles et les réseaux sans fil :

K. Al Agha, G. Pujolle, G. Vivier, *Réseaux de mobiles et réseaux sans fil*, 2e édition, Eyrolles, 2005

Un livre dévolu aux applications dans les réseaux sans fil :

H. P. Alesso, C. F. Smith, *The Intelligent Wireless Web*, Addison Wesley, 2001

Les réseaux de capteurs posent de nouveaux problèmes architecturaux et protocolaires. Le livre suivant en dresse l'inventaire :

E. H. Callaway, *Wireless Sensor Networks: Architectures and Protocols*, Auerbach Publications, 2003

Deux livres pour ceux qui veulent aller nettement plus loin sur les antennes :

Z. N. Chen, *Antennas for portable Devices*, Wiley, 2007

—, M. Y. W. Chia, *Broadband Planar Antennas: Design and Applications*, Wiley, 2006

La sécurité est le point faible des réseaux Wi-Fi avec la qualité de service. Ce livre fait le point sur ces questions dans l'environnement Windows :

J. Davies, *Deploying Secure 802.11 Wireless Networks with Microsoft Windows*, Microsoft Press, 2003

Livre intéressant par sa présentation très pédagogique des réseaux Wi-Fi :

H. Davis, R. Mansfield, *The Wi-Fi Experience: Everyone's Guide to 802.11b Wireless Networking*, Que, 2001

Un excellent livre sur les applications que l'on peut mettre en place dans les réseaux sans fil :

A. Dorman, *The Essential Guide to Wireless Communications Applications*, Prentice Hall, 2002

Un livre qui se démarque par la façon de présenter les réseaux sans fil en examinant le problème de leur mise en place dans une communauté d'intérêt :

R. Flickenger, *Building Wireless Community Networks*, O'Reilly, 2001

Un livre très didactique sur les réseaux 802.11 :

M. S. Gast, *802.11 Wireless Networks: The Definitive Guide*, O'Reilly, 2002

Un excellent livre sur les réseaux de capteurs :

A. Hac, *Wireless Sensor Network Designs*, Wiley, 2003

Les réseaux sans fil forment une excellente solution pour l'accès à un modem ADSL ou un modem câble dans l'environnement domotique :

P. Heltzel, *Complete Wireless Home Networking*, Prentice Hall, 2003

La radio cognitive consiste à émettre sur des fréquences laissées libres par leur utilisateur licencié. Cette technologie va être primordiale pour les futures générations de réseaux sans fil. Ce livre en donne une solide introduction :

E. Hossain, V. K. Bhargava, *Cognitive Wireless Communication Networks*, Springer; 1re édition, 2007

Livre complet sur les réseaux mesh dans lesquels les points d'accès servent de routeur :

E. Hossain, K. K. Leun, *Wireless Mesh Networks: Architectures and Protocols*, Springer, 2010

Un livre qui décrit l'ensemble des réseaux personnels, depuis leur standard jusqu'à leur implémentation :

N. Hunn, *Essentials of Short-Range Wireless*, Cambridge University Press, 2010

Le livre suivant donne la plupart des outils qui peuvent être utilisés pour réaliser une étude de performance :

T. Janevski, *Traffic Analysis and Design of Wireless IP Networks*, Artech House, 2003

Un bon livre technique sur la sécurité dans les réseaux d'entreprise de type Wi-Fi :

J. Khan, A. Khwaja, *Building Secure Wireless Networks with 802.11*, Wiley, 2003

Excellente introduction aux réseaux Wi-Fi :

J. La Rocca, *802.11 Demystified: Wi-Fi Made Easy*, McGraw-Hill, 2002

Un livre détaillé sur les réseaux Wi-Fi et leur ingénierie :

D. Males, G. Pujolle, *Wi-Fi par la pratique*, Eyrolles, 2e édition, 2004

L'ingénierie des réseaux Wi-Fi paraît simple. En réalité, selon la taille du réseau, la complexité augmente vite. Les règles élémentaires à mettre en œuvre sont très bien expliquées dans ce livre :

M. Mallick, *Mobile and Wireless Design Essentials*, Wiley, 2003

La sécurité est un problème capital. Pour un lecteur intéressé plus spécifiquement par ce domaine dans les réseaux sans fil, ce livre devrait être bien perçu :

M. Maxim, D. Pollino, *Wireless Security*, McGraw-Hill, 2002

Un livre complet sur les réseaux ad-hoc :

C. S. R. Murthy, B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall, 2004

Un autre excellent livre sur la sécurité dans les réseaux sans fil :

R. K. Nichols, P. C. Lekkas, *Wireless Security: Models, Threats, and Solutions*, McGraw-Hill, 2001

L'IEEE, qui gère les groupes de travail sur la normalisation du sans-fil, publie un bon livre technique sur le 802.11 :

B. O'Hara, A. Petrick, *The IEEE 802.11 Handbook: a Designer's Companion*, IEEE Press, 1999

Un livre pour bien comprendre Wi-Fi et son installation en entreprise :

F. Ohrtman, K. Roeder, *Wi-Fi Handbook: Building 802.11b Wireless Networks*, McGraw-Hill, 2003

Excellente approche, présentant les grands principes des technologies sans fil :

K. Pahlavan, P. Krishnamurthy, *Principles of Wireless Networks: A Unified Approach*, Prentice Hall, 2001

La sécurité dans les réseaux mesh/ad hoc est particulièrement complexe. Ce livre introduit bien les problèmes et propose des solutions :

A.-S. Pathan, *Security of Self-organizing Networks: MANET, WSN, WMN, VANET*, Springer, 2010

Le livre de référence sur les réseaux ad-hoc :

C. Perkins, *Ad-hoc Networking*, Addison Wesley, 2000

Un livre consacré aux communications personnelles dans un environnement sans fil :

R. Prasad, *Universal Wireless Personal Communications*, Artech House, 1998

Très bon livre d'introduction aux réseaux sans fil :

T. S. Rappaport, *Wireless Communications Principles and Practice*, Prentice Hall, 2001

Un livre orienté vers les solutions Wi-Fi Cisco :

P. Roshan, J. Leary, *Wireless Local-Area Network Fundamentals*, Cisco Press, 2003

Un livre d'introduction aux réseaux sans fil :

A. Santamaria, *et al.*, *Wireless LAN Systems*, Artech House, 1994

Une excellente introduction aux réseaux ad hoc :

S. K. Sarkar, T.G. Basavaraju, C. Puttamadappa, *Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications*, Auerbach, 2007

Un livre pour ceux qui veulent entrer dans les détails des réseaux sans fil :

C. W. Sayre, *Complete Wireless Design*, McGraw-Hill, 2001

Un livre très intéressant sur les performances des réseaux mesh :

N. Scalabrino, *Performance of Wireless Mesh Networks*, VDM Verlag, 2010

Livre technique spécialisé sur les antennes et la propagation dans un environnement personnel :

K. Siwiak, Y. Bahreini, *Radiowave Propagation and Antennas for Personal Communications*, Artech House, 3e édition, 2007.

Un des nombreux livres de Stallings, toujours très pédagogique et complet :

W. Stallings, *Wireless Communications & Networks*, Prentice Hall, 2001

Un livre pratique sur WiMAX :

D. Sweeney, *WiMAX Operator's Manual: Building 802.16 Wireless Networks*, Apress, 2004

Livre complet sur les réseaux ad-hoc. Pour tous ceux qui souhaitent entrer dans les détails des protocoles de routage :

C. K. Toh, *Ad-hoc Mobile Wireless Networks: Protocols and Systems*, Prentice Hall, 2001

Pour ceux qui veulent aller plus loin sur la couche physique des réseaux Wi-Fi :

X. Wang, H. V. Poor, *Wireless Communication Systems: Advanced Techniques for Signal Reception*, Prentice Hall, 2003

Excellent livre, qui introduit surtout les réseaux sans fil de la boucle locale :

W. Webb, *Introduction to Wireless Local Loop*, Artech House, 2000

Un bon livre sur les réseaux mesh, dans lesquels les points d'accès fixes jouent également le rôle de routeur :

Y. Zhang, J. Luo, H. Honglin, *Wireless Mesh Networking: Architectures, Protocols and Standards*, Auerbach, 2006

Un très bon livre sur les réseaux de capteurs :

F. Zhao, L. Guibas, *Wireless Sensor Networks*, Morgan Kaufmann Publishers, 2004

24. L'Internet des choses

Un livre de base pour aborder les réseaux de capteurs :

I. Akyildiz, M. Vuran, *Wireless Sensor Networks*, Wiley, 2010

Les réseaux de capteurs posent de nouveaux problèmes architecturaux et protocolaires. Le livre suivant en dresse l'inventaire :

E. H. Callaway, *Wireless Sensor Networks: Architectures and Protocols*, Auerbach Publications, 2003

Un excellent livre sur les réseaux de capteurs :

W. Dargie, C. Poellabauer, *Fundamentals of Wireless Sensor Networks: Theory and Practice*, Wiley, 2010

Un excellent livre sur les applications que l'on peut mettre en place dans les réseaux sans fil :

A. Dorman, *The Essential Guide to Wireless Communications Applications*, Prentice Hall, 2002

Un petit livre qui couvre bien les différents réseaux pour transporter les commandes :

R. Faludi, *Building Wireless Sensor Networks: With Zigbee, Xbee, Arduino, and Processing*, O'Reilly, 2010

Un excellent livre sur les réseaux de capteurs :

A. Hac, *Wireless Sensor Network Designs*, Wiley, 2003

Les réseaux sans fil forment une excellente solution pour l'accès à un modem ADSL ou un modem câble dans l'environnement domotique :

P. Heltzel, *Complete Wireless Home Networking*, Prentice Hall, 2003

Excellente approche, présentant les grands principes des technologies sans fil :

K. Pahlavan, P. Krishnamurthy, *Principles of Wireless Networks: A Unified Approach*, Prentice Hall, 2001

Un très bon livre sur les réseaux de capteurs :

F. Zhao, L. Guibas, *Wireless Sensor Networks*, Morgan Kaufmann Publishers, 2004

Un livre pour démarrer sur l'Internet des choses avec les RFID et les capteurs :

Y. Zhang, L. Yang, J. Chen, *RFID and Sensor Networks: Architecture, Protocols, Security, and Integrations*, CRC Press, 2009

25. VLAN et VPN

Un livre de base sur les réseaux privés virtuels, qui en donne une présentation générale de qualité :

P. C. Albrecht, *Virtual Private Network Handbook*, McGraw-Hill, 2000

Les VPN ont presque toujours un lien étroit avec la sécurité. Le livre suivant donne une synthèse complète de ce domaine :

N. Doraswamy, D. Harkins, *IPsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, Prentice Hall, 1999

Un livre très intéressant sur l'introduction des VPN dans les entreprises :

D. Fowler, *Virtual Private Networks: Making the Right Connection*, Morgan Kaufmann Publishers, 1999

Les VPN MPLS sont très bien traités dans le livre suivant :

J. Guichard, I. Pepelnjak, *MPLS and VPN Architectures: a Practical Guide to Understanding, Designing and Deploying MPLS and MPLS-Enabled VPNs*, Cisco Press, 2000

Le livre suivant se focalise sur les VPN bâtis autour de Linux :

O. Kolesnikov, B. Hatch, *Building Linux Virtual Private Networks*, New Riders Publishing, 2002

Un point important abordé dans ce livre concerne la gestion des VPN. Pour cette raison, ce livre reste intéressant, malgré sa date :

Dan. Kosiur, Dav. Kosiur, *Building & Managing Virtual Private Networks*, Wiley, 1998

Excellent livre sur les VPN et leur déploiement :

Y. Le Corvic, R. Corvalan, E. Corvalan, *Les Réseaux privés virtuels. Principes, conception et déploiement*, Dunod, 2003

Les VPN sont complexes à mettre en œuvre dans un grand réseau. La plupart des réponses aux difficultés de mise en œuvre se trouvent dans ce livre.

M. Lewis, *Troubleshooting Virtual Private Networks (VPN)*, Pearson Education, 2004

Un bon livre, faisant le tour des applications qui peuvent être mises en œuvre dans le cadre d'un VPN :

D. E. McDysan, *VPN Applications Guide: Real Solutions for Enterprise Networks*, Wiley, 2000

Un livre de base sur les VPN :

M. Murhammer, T. A. Bourne, T. Gaidosh, C. Kunzinger, *Guide to Virtual Private Networks*, Prentice Hall, 2000

Un excellent livre sur la sécurité des réseaux, dans lequel les VPN pour la sécurité sont très bien couverts :

S. Northcutt, S. Winters, L. Zeltser, *Inside Network Perimeter Security: the Definitive Guide to Firewalls, VPNs, Routers, and Network Intrusion Detection*, New Riders Publishing, 2002

Une présentation très orientée sécurité est apportée par le livre suivant :

B. Perlmutter, J. L. Zarkower, *Virtual Private Networking: a View from the Trenches*, Prentice Hall, 2000

La plupart des grands réseaux VPN des opérateurs utilisent une base de réseaux MPLS. Le livre suivant entre en détail dans cette catégorie de réseaux VPN :

I. Pepelnjak, J. Guichard, J. Apcar, *MPLS and VPN Architectures*, Pearson Education, 2003

Un livre orienté vers les réseaux privés virtuels d'entreprise de première génération :

C. Scott, P. Wolfe, M. Erwin, A. Oram, *Virtual Private Networks*, O'Reilly, 2e édition, 1998

Ce livre fait partie de la première génération de livres sur les VPN :

A. Shneyderman, A. Casati, *Mobile VPN: Delivering Advanced Services in Next Generation Wireless Systems*, Wiley, 2003

Check Point est l'industriel numéro un des pare-feu. Ce livre introduit son environnement de pare-feu et de VPN :

B. J. Stiefel, D. Maxwell, K. X. Hourihan, C. Amon, J. Noble, *Check Point NG VPN-1/Firewall-1: Advanced Configuration and Troubleshooting*, Syngress Publishing, 2003

Très bon livre pour aller dans les détails des VPN à base d'IPsec et MPLS :

N.-K. Tan, *Building VPNs with IPSec and MPLS*, McGraw-Hill, 2003

Un livre centré sur la sécurité *via* le protocole IPsec :

J. S. Tiller, Ji. S. Tiller, *A Technical Guide to IPSEC Virtual Private Networks*, Auerbach Publications, 2000

Le concept de réseau privé virtuel est assez simple. Son implémentation est en revanche beaucoup plus complexe. Le livre suivant permet de découvrir quelques problèmes intéressants d'implémentation :

C. Wilson, P. Doak, *Creating and Implementing Virtual Private Networks: the All-Encompassing Resource for Implementing VPNs*, The Coriolis Group, 2000

Un livre très complet sur les réseaux privés virtuels, présentant à la fois une vision technique détaillée et les raisons de réaliser de telles structures :

R. Yuan, W. T. Strayer, *Virtual Private Networks: Technologies and Solutions*, Addison Wesley, 2001

26. La gestion de réseau

Un excellent livre, réalisé par un ensemble de spécialistes de la gestion de réseau, qui fait le tour du problème :

S. Aidarous, *et al.*, *Managing IP Networks: Challenges and Opportunities*, Wiley-IEEE Press, 2003

Un livre général et complet sur la gestion de réseau :

R. J. Bates, *Network Management*, McGraw-Hill, 2002

Un des très nombreux livres de U. Black. Celui-ci porte sur les protocoles de gestion de réseau :

U. BLACK, *Network Management Standards: SNMP, CMIP, TMN, MIBs and Object Libraries*, McGraw-Hill, 1994

Un livre complet sur SNMPv3 :

U. BLUMENTHAL, N. HIEN, B. WIJNEN, *SNMPv3 Handbook*, Addison Wesley, 1999

Un excellent livre, à la fois conceptuel et pratique, sur la gestion de réseau :

J. R. BURKE, *Network Management: Concepts and Practice, A Hands-On Approach*, Prentice Hall, 2003

Les protocoles de gestion sont très bien décrits dans ce livre dévolu à l'ensemble des systèmes de communication :

P. BYRNES, *Protocol Management in Computer Networking*, Artech House, 2002

Ce livre plus orienté vers la gestion de l'ATM que du monde IP, comporte de nombreuses bonnes idées :

A. GILLESPIE, *Broadband Access Technology, Interfaces and Management*, Artech House, 2001

Livre complet sur le protocole SNMP :

S. J. HARNEDY, *Total SNMP: Exploring the Simple Network Management Protocol*, Prentice Hall, 1997

Livre complet sur tous les aspects de la gestion de réseau et de système :

H.-G. HEGERING, S. ABECK, *Integrated Network and System Management*, Addison Wesley, 1994

La gestion des réseaux passe de plus en plus par l'établissement de réseaux virtuels, qui doivent être correctement mis en place et gérés. Le livre suivant aborde ce problème de façon pragmatique :

G. HELD, *Virtual LANs: Construction, Implementation, and Management*, Wiley, 1997

Un autre livre de Gilbert Held très pédagogique et facile à lire :

G. HELD, *LAN Management with SNMP and RMON*, Wiley, 1996

Un des livres de base pour la gestion de l'environnement IP :

C. HUNT, *TCP/IP, administration de réseau*, O'Reilly, 1998

Une très bonne présentation de la problématique de gestion des réseaux IP :

F. JACQUENET, *Administration des réseaux*, CampusPress, 2002

Un livre pratique très complet :

T. L. LIMONCELLI, C. HIGAN, *The Practice of System and Network Administration*, Addison Wesley, 2001

Ce livre est beaucoup plus général que la seule gestion de réseau et s'intéresse à tout l'environnement réseau :

T. MANN-RUBINSON, K. TERPLAN, *Network Design: Management and Technical Perspectives*, CRC Press, 1998

Un livre pour ceux qui veulent se diriger vers la gestion de réseau :

J. P. MARTIN-FLATIN, *Web-based Management of IP Networks and Systems*, Wiley, 2002

Très bonne introduction à la gestion par le Web :

D. R. MAURO, K. J. SCHMIDT, *Essential SNMP*, O'Reilly, 2001

Un livre très complet sur la gestion des réseaux locaux, dans lequel de nombreux aspects, dont la sécurité, sont introduits.

A. MIKELSEN, P. BORGESEN, *Local Area Network Management, Design & Security*, Wiley, 2002

La généralisation de la gestion de réseaux prend le nom d'OSS (Operation Support System). Ce livre en propose une introduction.

K. MISRA, *OSS for Telecom Networks: An Introduction to Network Management*, Springer Verlag Telos, 2004

Un livre de gestion dévolu aux réseaux locaux de toute nature :

S. B. MORRIS, *Network Management, MIBs and MPLS: Principles, Design and Implementation*, Prentice Hall, 2003

Ce livre est dédié à la gestion de réseaux ATM effectuée par le protocole SNMP :

H. OAN, *SNMP-based ATM Network Management*, Artech House, 2002

La gestion de réseau ATM par un environnement SNMP est abordée avec beaucoup de précision dans ce livre :

H. PAN, *SNMP-based ATM Network Management*, Artech House, 1998

Les MIB sont particulièrement importantes dans le processus de normalisation du protocole SNMP. Ce livre en propose une analyse :

D. PERKINS, E. MCGINNIS, *Understanding SNMP MIBs*, Prentice Hall, 1996

Un livre consacré au protocole RMON :

D. T. PERKINS, *RMON: Remote Monitoring of SNMP-Managed*, Prentice Hall, 1998

Un excellent livre sur les techniques de gestion SNMP et RMON :

W. STALLINGS, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, Addison Wesley, 3e édition, 1990

Un excellent livre pour réaliser des MIB et s'occuper de la gestion SNMP :

L. A. STEINBERG, *Troubleshooting SNMP; Analyzing MIBs*, McGraw-Hill, 2000

Un des premiers livres sur la gestion de réseau, dont de nombreux développements sont toujours valables :

K. Terplan, *Communication Networks Management*, Prentice Hall, 1987

Un livre général très pédagogique de K. Terplan, un des meilleurs spécialistes en gestion de réseau :

K. Terplan, *OSS Essentials: Support System Solutions for Service Providers*, Wiley, 2001

Autre livre de Terplan, mais consacré à la gestion d'un réseau intranet :

K. Terplan, S. Zamir, *Intranet Performance Management*, CRC Press, 1999

Encore un livre de Terplan, cette fois consacré à la gestion par des techniques Web :

K. Terplan, S. Zamir, *Web-based Systems and Network Management*, CRC Press, 1999

Un livre dédié à un domaine spécifique de la gestion, la sécurité :

M. Webstom, *Managing Cisco Network Security*, Cisco Press, 2001

Livre très général sur la gestion de réseau :

S. Wisniewski, *Network Administration*, Prentice Hall, 2000

Livre entièrement consacré à SNMPv3, pour ceux qui souhaitent aller plus loin dans le domaine de la gestion :

D. Zeltserman, *Practical Guide to SNMPv3 and Network Management*, Prentice Hall, 1999

27. Le contrôle de réseau

Un excellent livre sur la qualité de service dans les réseaux IP :

G. Armitage, *Quality of Service in IP Networks*, Pearson Higher Education, 2000

Très bon livre sur le protocole CCITT n° 7 et ses extensions dans les réseaux de type circuit virtuel :

R. J. Bates, *Signaling System 7*, McGraw-Hill, 2002

Le livre suivant détaille les principales techniques de contrôle de flux que l'on peut trouver dans les réseaux optiques :

G. Bernstein, B. Rajagopalan, D. Saha, *Optical Network Control: Architecture, Protocols, and Standards*, Addison Wesley, 2003

Un très bon livre pour faire le tour des problèmes posés par la gestion de la qualité de service et le multipoint :

D. P. Black, *Building Switched Networks: Multilayer Switching, Qos, IP Multicast, Network Policy, and Service-Level Agreements,* Addison Wesley, 1999

Un excellent livre sur la signalisation classique du monde des télécommunications :

J. G. VAN BOSSE, *Signaling in Telecommunication Networks*, Wiley-Interscience, 1997

Un livre très intéressant pour tous ceux qui s'intéressent aux techniques mises en œuvre dans les réseaux à haut débit pour obtenir de la qualité de service :

H. J. CHAO, X. GUO, *Quality of Service Control in High-Speed Networks*, Wiley, 2001

Le livre le plus orienté vers les techniques de commutation-routage et qui introduit bien les contrôles de flux dans les réseaux TCP/IP sur ATM :

B. DAVIE, P. DOOLAN, Y. REKHTER, *Switching in IP Networks*, Morgan Kaufmann Publishers, 1998

Un livre très général mais très intéressant sur la définition et les principales techniques des contrôles de flux :

H. DE MEER, *The Genesis of Quality of Service*, Wiley, 2003

Un livre complet sur le CCITT n°7 :

L. DRYBURGH, J. HEWETT, *Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Applications*, Pearson Education, 2003

Cet excellent livre aborde les principaux protocoles de signalisation dans la téléphonie sur IP :

J. F. DURKIN, *Voice-Enabling the Data Network: H.323, MGCP, SIP, QoS, SLAs, and Security*, Pearson Education, 2002

Un excellent livre consacré à la qualité de service dans les différents types de réseaux :

P. FERGUSON, G. HUSTON, *Quality of Service*, Wiley, 1998

Proposer de la qualité de service est une chose. Être capable de démontrer par des mesures que la qualité de service a bien été offerte à l'utilisateur en est une autre. Ce livre introduit toutes ces notions :

W. HARDY, *QOS: Measurement and Evaluation of Telecommunications Quality of Service*, Wiley, 2002

Livre général sur l'ensemble des solutions de signalisation :

L. HARTE, *Introduction to SS7 and IP: Call Signaling using SIGTRAN, SCTP, MGCP, SIP, and H.323*, Althos, 2003

Un livre très complet sur le CCITT n°7 :

L. HARTE, R. DREHER, D. BOWLER, *Signaling System 7 (SS7) Basics*, Althos, 2003

Un livre beaucoup plus général que la seule signalisation consacré à l'ensemble des techniques de base dans les couches basses de l'architecture des réseaux :

L. HARTE, *Telecom Basics: Signal Processing, Signaling Control, and Call Processing*, Althos, 2003

Le protocole SIP est traité en détail dans ce livre ainsi que l'ensemble de la problématique de la téléphonie sur IP :

L. HARTE, D. BOWLER, *Introduction to SIP IP Telephony Systems: Technology Basics, Services, Economics, and Installation*, Althos, 2004

La signalisation est particulièrement importante dans les réseaux de mobiles comme le GSM, le GPRS ou l'UMTS. Ce livre est plus spécifiquement destiné au GPRS :

G. HEINE, *GPRS, Signaling and Protocol Analysis, Volume 2: The Core Network*, Artech House, 2003

Gilbert Held s'est intéressé dans ce livre très intéressant à la qualité de service dans les environnements Cisco :

G. HELD, *Quality of Service in a Cisco Networking Environment*, Wiley, 2002

Un livre très détaillé sur SIP, à lire pour aller plus loin dans ce domaine :

A. B. JOHNSTON, *SIP: Understanding the Session Initiation Protocol*, Artech House, 2e édition, 2004

Un livre à lire pour faire le tour des techniques de contrôle aussi bien pour les réseaux fixes que pour les réseaux de mobiles :

P. MASSAM, *Managing Service Level Quality: Across Wireless and Fixed Networks*, Wiley, 2003

Un excellent livre dédié aux techniques de qualité de service :

J.-L. MELIN, *Qualité de service sur IP, Ethernet, Frame Relay et ATM*, Eyrolles, 2001

Un très bon livre sur la qualité de service dans les différentes technologies réseau :

A. MISHRA, *Quality of Service in Communications Networks*, Wiley, 2002

Un livre assez général dans lequel le lecteur trouvera de nombreux exemples de techniques de contrôle :

V. RAISANEN, *Implementing Service Quality in IP Networks*, Wiley, 2003

Les techniques de base de la qualité de service dans les réseaux IP sont décrites dans ce volume, avec pour objectif de faire transiter des applications multimédias :

J. SHIN, D. C. LEE, J. KUO, *Quality of Service for Internet Multimedia*, Pearson Education, 2003

Le protocole SIP est à l'origine de nombreux livres, dont le suivant :

H. SINNREICH, A. B. JOHNSTON, *Internet Communications Using SIP*, Wiley, 2001

Un autre livre classique de William Stallings, toujours aussi complet et pédagogique :

W. STALLINGS, *High-Speed Networks and Internets: Performance and Quality of Service*, Prentice Hall, 2002

Un livre orienté vers la qualité de service dans le monde IP orienté Cisco :

S. VEGESNA, *IP Quality of Service*, Cisco Press, 2001

Excellent livre sur la qualité de service dans le monde IP :

Z. Wang, *Internet QoS: Architectures and Mechanisms for Quality of Service*, Morgan Kaufmann Publishers, 2001

Un livre qui permet d'entrer dans la technique des réseaux en ce qui concerne le contrôle de flux.

M. Welzl, *Scalable Performance Signaling and Congestion Avoidance*, Kluwer Academic Publishers, 2003

28. La sécurité et l'identité

Très bon livre sur les PKI pour ceux qui veulent aller plus loin dans cette direction :

C. Adams, S. Lloyd, S. Kent, *Understanding the Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*, New Riders Publishing, 1999

Un livre intéressant à consulter pour entrer facilement dans le domaine des PKI :

T. Austin, *PKI: A Wiley Tech Brief*, Wiley, 2000

Un livre à lire pour ceux qui souhaitent aller plus loin dans les PKI :

T. Autret, L. Bellefin, *Sécuriser ses échanges électroniques avec une PKI*, Eyrolles, 2002

Livre très complet sur toutes les questions de sécurité, même en dehors de l'aspect réseau :

S. Bosworth, M. E. Kabay, *Computer Security Handbook*, Wiley, 2002

Livre intéressant à consulter sur la problématique des signatures électroniques :

M. Cooper, S. Northcutt, M. Fearnow, K. Frederick, *Intrusion Signatures and Analysis*, New Riders Publishing, 2001

Très bon livre sur la sécurisation du Web et du commerce électronique :

S. Garfinkel, G. Spafford, D. Russell, *Web Security, Privacy and Commerce*, O'Reilly, 2002

Un livre dédié à Kerberos. À lire pour ceux qui souhaitent avoir des détails précis sur cette technique :

J. Garman, *Kerberos: The Definitive Guide*, O'Reilly, 2003

La sécurité dans le commerce électronique est une question clé. Ce livre en traite avec beaucoup de détails encore d'actualité :

A. K. Ghosh, *E-Commerce Security: Weak Links, Best Defenses*, Wiley, 1998

Un livre de bonne qualité sur les aspects pratiques de la sécurité dans les réseaux :

M. Hendry, *Practical Computer Network Security*, Artech House, 1999

Comment déployer un environnement PKI ? Le livre suivant donne toutes les réponses nécessaires pour se lancer :

R. Housley, T. Polk, *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*, Wiley, 2001

Bon livre sur les différents composants de la sécurité :

C. KAUFMAN, *et al.*, *Network Security: Private Communication in a Public World*, Prentice Hall, 2002

Un excellent livre sur les problèmes de sécurité dans les réseaux, qui en est à sa troisième édition :

S. MCCLURE, J. SCAMBRAY, G. KURTZ, *Hacking Exposed: Network Security Secrets & Solutions*, McGraw-Hill, 2001

Le livre suivant fait un tour d'horizon complet du domaine de la sécurité dans le monde des réseaux sans fil :

M. MAXIM, D. POLLINO, *Wireless Security*, McGraw-Hill, 2002

Un livre complet sur les performances des techniques de sécurité :

C. MCNAB, *Network Security Assessment*, O'Reilly, 2004

Un livre à lire pour ceux qui veulent aller plus loin sur la question du chiffrement :

H. X. MEL, D. M. BAKER, *Cryptography Decrypted*, Addison Wesley, 2000

Un livre de bonne tenue sur les PKI :

A. NASH, B. DUANE, D. BRINK, C. JOSEPH, *PKI: Implementing & Managing E-Security*, McGraw-Hill, 2001

Le domaine de la sécurité dans les réseaux sans fil sera très important dans les réseaux du futur :

R. K. NICHOLS, P. C. LEKKAS, *Wireless Security: Models, Threats, and Solutions*, McGraw-Hill, 2001

Livre qui sort un peu des sentiers battus en matière de sécurité dans les réseaux et dont l'approche tient compte d'une analyse des risques :

T. R. PELTIER, *Information Security Risk Analysis*, Auerbach Publications, 2001

La PKI est de plus en plus souvent utilisée dans les entreprises. Pour bien comprendre tous les détails d'une implémentation, le livre suivant est à recommander :

K. RAINA, *PKI Security Solutions for the Enterprise: Solving HIPAA, E-Paper Act, and Other Compliance Issues*, Wiley, 2003

Un livre général et facile à lire tout en étant complet :

M. Y. RHEE, *Internet Security: Cryptographic Principles, Algorithms and Protocols*, Wiley, 2003

L'article de base sur l'algorithme RSA :

R. L. RIVEST, A. SHAMIR, L. ADLEMAN, « A Method for Obtaining Digital Signatures and Public Key Cryptosystems », *C. ACM*, vol. XXI, n° 2, février 1978, pp. 120-126

Livre très complet sur le chiffrement et ses aspects plus pratiques :

D. STINSON, *Cryptography: Theory and Practice*, Chapman & Hall, 2002

Les virus et autres attaques à base de théorie des nombres sont décrits dans ce livre technique :

A. Young, M. Yung, *Malicious Cryptography: Exposing Cryptovirology*, Wiley, 2004

29. La sécurité dans l'environnement IP

Un excellent livre sur SSH :

D. J. Barrett, R. Silverman, *SSH*, *The Secure Shell*, O'Reilly, 2001

Un des très nombreux livres de U. Black, toujours fortement pédagogique :

U. D. Black, *Internet Security Protocols: Protecting IP Traffic*, Prentice Hall, 2000

Un bon livre pour apprendre à gérer la sécurité :

C. Brenton, *Mastering Network Security*, Sybex, 1999

Un livre assez facile à lire et concret avec un grand nombre d'exemples sur les pare-feu et plus généralement sur la sécurité dans les réseaux IP :

W. R. Cheswick, S. M. Bellovin, A. D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison Wesley, 2003

Un excellent livre sur les réseaux privés virtuels de type IPsec :

C. Davis, *IPsec: Securing VPNs*, McGraw-Hill, 2001

IPsec sous toutes ses coutures :

N. Doraswamy, D. Harkins, *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, Pearson Education, 2003

Petit livre facile à lire mais introduisant parfaitement les éléments à connaître sur la sécurité dans Internet :

B. Fabrot, *La Sécurité sur Internet*, Marabout, 2001

Très bon livre sur la problématique de la sécurité dans le commerce électronique :

W. Ford, M. S. Baum, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*, Prentice Hall, 2000

Très bonne introduction à IPsec et aux raisons de son succès :

S. Frankel, *Demystifying the IPsec Puzzle*, Artech House, 2001

Un excellent livre consacré à la sécurité sur Internet, qui aborde des aspects non classiques dans les stratégies à suivre pour sécuriser un réseau :

S. Ghernaouti-Hélie, *Sécurité Internet*, Dunod, 2000

Très bon livre pour entrer dans l'univers des virus :

D. Harlay, R. Slade, *Virus, définitions, mécanismes et antidotes*, Campus Press, 2002

Un livre très complet sur l'utilisation d'IPsec dans de nombreux contextes :

E. KAUFMAN, A. NEUMAN, *Implementing IPsec: Making Security Work on VPNs, Intranets, and Extranets*, Wiley, 1999

Un des nombreux livres de G. Held, qui porte sur la gestion des réseaux IP et plus particulièrement la sécurité :

G. HELD, *Managing TCP/IP Networks: Techniques, Tools and Security*, Wiley, 2000

Livre assez général qui aborde de nombreux éléments de la sécurité des réseaux IP :

O. KYAS, *Internet Security Risk Analysis, Strategies and Firewall*, Thomson Computer Press, 1997

Livre à lire par tous ceux qui s'intéressent à la sécurité sur Internet :

E. LARCHER, *L'Internet sécurisé*, Eyrolles, 2000

Un livre de base très complet, mais parfois technique, pour entrer dans la sécurité par IPsec :

P. LOSHIN, *Big Book of IPsec RFCs: Internet Security Architecture*, Morgan Kaufmann Publishers, 1999

Un excellent livre sur les techniques de détection d'intrusion dans les réseaux :

S. NURTHCUTT, *Network Intrusion Detection, an Analyst's Handbook*, New Riders Publishing, 1999

Un livre consacré aux protocoles SSL et TLS :

E. RESCORLA, *SSL and TLS: Designing and Building Secure Systems*, Addison Wesley, 2000

Le Web pose des problèmes spécifiques en matière de sécurité. Le livre suivant leur est consacré :

A. D. RUBIN, D. GEER, M. J. RANUM, *Web Security Sourcebook*, Wiley, 1997

Les réseaux privés virtuels de type IPsec sont très utilisés pour gérer la sécurité. Le livre suivant en donne un panorama :

Ja. M. TILLER, Ji. S. TILLER, *A Technical Guide to IPsec Virtual Private Networks*, Auerbach Publications, 2000

Un excellent livre, qui présente les algorithmes de chiffrement de façon pédagogique :

W. STALLINGS, *Cryptography and Networks Security*, Prentice Hall, 1998

Très bon livre sur les pare-feu et leur utilisation dans le contexte des entreprises :

E. D. ZWICKY, *et al.*, *Building Internet Firewalls*, O'Reilly, 2000

30. ToIP et IPTV

La téléphonie a beaucoup changé en quelques années. En particulier, les PABX se transforment en équipements de réseau IP. Le livre suivant décrit cette évolution.

J. R. ABRAHAMS, M. LOLLO, *CENTREX or PBX: The Impact of Internet Protocol*, Artech House, 2003

Un livre général sur la téléphonie sur IP. Pour ceux qui veulent commencer à entrer dans ce sujet :

U. Black, *Voice Over IP*, Prentice Hall, 2002

Un autre livre introductif à la téléphonie sur IP :

K. Camp, *IP Telephony Demystified*, McGraw-Hill, 2002

Un excellent livre sur les protocoles de signalisation utilisés dans la téléphonie, complété par la description des fonctions à mettre en œuvre, comme la qualité de service et la sécurité :

J. F. Durkin, *Voice-Enabling the Data Network: H.323, MGCP, SIP, QoS, SLAs, and Security*, Pearson Education, 2002

Un ouvrage très intéressant sur l'intégration informatique et les PABX :

S. Ghernaouti-Hélie, A. Dufour, *Ingénierie des réseaux locaux d'entreprise et des PABX*, Masson, 1995

La téléphonie sur les accès *x*DSL est devenue presque classique. Pour bien en comprendre les tenants et les aboutissants, il faut lire le livre suivant :

R. Grigonis, *Voice Over DSL*, CMP Books, 2002

Excellent livre technique pour comprendre et mettre œuvre de la téléphonie sur IP :

W. C. Hardy, *VoIP Service Quality: Measuring and Evaluating Packet-Switched Voice*, McGraw-Hill, 2003

Un petit livre très bien documenté sur la mise en place d'un environnement de téléphonie sur IP:

L. Harte, D. Bowler, *Introduction to SIP IP Telephony Systems: Technology Basics, Services, Economics, and Installation*, Althos, 2004

Le dimensionnement des organes du commutateur, en fonction des flux d'entrée, est un problème très complexe posé par les autocommutateurs. L'excellent livre suivant fait le point sur la question :

G. Hébuterne, *Écoulement du trafic dans les autocommutateurs*, Masson, 1985

Un livre dédié à SIP (Session Initiation Protocol) :

A. Johnston, *SIP: Understanding the Session Initiation Protocol*, Artech House, 2003

Pour comprendre le passage de la téléphonie classique à la téléphonie IP, il faut lire le livre suivant, qui en donne toutes les caractéristiques :

M. A. Miller, *Voice over IP Technologies: Building the Converged Network*, Wiley, 2002

La solution AVVID de Cisco est fortement orientée vers la pure téléphonie sur IP :

M. Nelson, A. Smith, D. Deel, *Developing Cisco IP Phone Services: A Cisco AVVID Solution*, Cisco Press, 2002

La téléphonie sur IEEE 802.11 commence à se développer. Ses problèmes spécifiques sont explicités dans ce livre :

F. OHRTMAN, *Voice over 802.11*, Artech House, 2004

Un excellent livre sur la téléphonie sur Internet :

J. PULVER, *The Internet Telephone Toolkit*, Wiley, 1996

Un des livres de base sur l'intégration téléphone-données, qui décrit en détail les possibilités de l'interface CTI :

W. ROB, *Computer Telephone Integration*, Artech House, 1993

Ce livre décrit l'introduction d'applications multimédias dans l'environnement CTI :

W. ROB, *Computer Mediated Communications: Multimedia Application*, Artech House, 1995

Un livre centré sur la signalisation et la commutation dans les réseaux pour y intégrer de la téléphonie :

M. STAFFORD, *Signaling and Switching For Packet Telephony*, Artech House, 2004

Un très bon livre explicatif sur le monde des PBX-IP :

A. SULKIN, *PBX Systems for IP Telephony*, McGraw-Hill, 2002

Livre très complet sur l'intégration informatique-téléphonie :

R. WALTERS, *Computer Telephony Integration*, Artech House, 1998

31. Les réseaux autonomiques

Un des livres les plus à jour sur les réseaux intelligents et les suites à en attendre :

R. S. J. BATES, *Advanced Intelligent Networks*, McGraw-Hill, 2002

Un excellent livre sur ODP et son utilisation pour les environnements multimédias :

G. BLAIR, J.-B. STEFANI, *Open Distributed Processing and Multimedia*, Addison Wesley, 1997

L'inévitable libre de U. Black sur les réseaux intelligents :

U. D. BLACK, *The Intelligent Network: Customizing Telecommunication Networks*, Prentice Hall, 1998

Pour les nuls, ou presque, car UML reste un sujet difficile, dont ce livre donne une très bonne introduction :

M. J. CHONOLES, J. A. SCHARDT, *UML 2 for Dummies*, For Dummies, 2003

Livre très intéressant sur la façon de gérer intelligemment un réseau sans fil :

G. CHRISTENSEN, R. DUNCAN, P. G. FLORACK, *Wireless Intelligent Networking*, Artech House, 2000

Un très bon livre pour ceux qui veulent aller plus loin dans le domaine de la standardisation des réseaux intelligents :

I. Faynberg, L. R. Gabuzda, M. P. Kaplan, *The Intelligent Network Standards: Their Application to Services*, McGraw-Hill, 1996

La référence en matière de systèmes multiagents :

J. Ferber, *Multi-Agent Systems: An Introduction to Distributed Artificial Intelligence*, Addison Wesley, 1999

Le premier livre en français à avoir introduit les principaux concepts de l'intelligence qui peuvent être utilisés en matière de réseau est le suivant :

D. Gaïti, G. Pujolle, *L'Intelligence dans les réseaux*, Eyrolles, 1992

Un des premiers articles sur l'introduction de l'intelligence dans les réseaux en vue d'une gestion des protocoles et des composants :

S. K. Goyal, R. W. Worrest, « Expert System Applications to Network Management », *in* J. Leibowitz, *Expert System Applications to Telecommunications*, Wiley-Interscience, 1988

Un livre qui donne de nombreuses informations sur les systèmes multiagents :

G. O'Hare, N. Jennings (*éd.*), *Foundations of Distributed Artificial Intelligence*, Wiley, 1996

Excellent livre sur l'utilisation des différentes technologies agent dans le domaine des communications :

A. L. Hayzelden, R. Bourne, *Agent Technology for Communication Infrastructures*, Wiley, 2001

Un livre très technique à lire pour aller dans les détails des systèmes multiagents et autonomes :

H. Hexmoor, C. Castelfranchi, R. Falcone, *Agent Autonomy*, Kluwer Academic Publishers, 2003

Livre très complet sur les systèmes à base d'agents pour ceux qui se destinent à l'introduction de l'intelligence dans les réseaux :

M. d'Inverno, M. Luck, *Understanding Agent Systems*, Springer Verlag, 2001

L'application des technologies multiagents au monde des systèmes distribués est très bien développée dans le livre suivant :

M. Knapik, J. B. Johnson, *Developing Intelligent Agents for Distributed Systems: Exploring Architectures, Techniques, and Applications*, McGraw-Hill, 1997

Le meilleur livre sur les réseaux intelligents :

T. Magedanz, R. Popescu-Zeletin, *Intelligent Networks*, International Thomson Publishing, 1996

Un livre très complet sur UML :

T. Pender, *UML Bible*, Wiley, 2003

Ce livre fournit un complément à ce chapitre en matière d'ingénierie des applications client-serveur dans un environnement ouvert :

W. Rauch, *Open Systems Engineering: How to Plan and Develop Client/Server Systems*, Wiley, 1996

Un bon livre sur les réseaux qui sont plus adaptables qu'intelligents :

I. Venieris, H. Hussmann, *Intelligent Broadband Networks*, Wiley, 2002

Excellent livre sur les technologies multiagents :

G. Weiss, *Multiagent Systems*, MIT Press, 1999

Introduction très pédagogique et excellente pour ceux qui veulent s'initier à la théorie des systèmes multiagents :

M. Woolridge, *Introduction to MultiAgent Systems*, Wiley, 2002

Ce livre explique bien la transition des réseaux intelligents vers les réseaux adaptatifs et autonomes :

J. Zuidweg, *Next Generation Intelligent Networks*, Artech House, 2002

32. Virtualisation, Post-IP et Cloud

Le livre suivant permet de bien comprendre l'arrivée en force de MPLS :

V. Alwayn, *Advanced MPLS Design and Implementation*, Cisco Press, 2001

Une vision du développement des mobiles dans les quelques années qui viennent :

J. P. Castro, *The UMTS Network and Radio Access Technology: Air Interface Techniques for Future Mobile Systems*, Wiley, 2001

Le livre suivant est dévolu à la technique du Gigabit Ethernet. Cette solution a un potentiel important pour s'implanter aussi bien dans l'entreprise que chez les opérateurs :

D. Cunningham, W. G. Lane, B. Lane, *Gigabit Ethernet Networking*, Pearson Higher Education, 1999

Un livre à lire pour comprendre les directions prises par les réseaux optiques :

S. Dixit, *IP over WDM: Building the Next Generation Optical Internet*, Wiley-Interscience, 2003

Excellente étude sur les prochaines générations du réseau Internet :

A. Farrel, *The Internet and Its Protocols: A Comparative Approach*, Morgan Kaufmann Publishers, 2004

Le futur est toujours difficile à prédire. Le livre suivant propose une vision autour de l'augmentation des débits des prochains réseaux étendus :

S. Feit, *Wide Area High Speed Networks*, Pearson Higher Education, 1999

Un excellent livre, qui prédisait bien ce qui est en train de se passer aujourd'hui :

A. Glowinski, *Télécommunications*, *Objectif 2000*, Dunod, 1980

Un livre sur l'environnement IP Mobile, qui semble devenir l'un des très grands standards de l'IETF :

A. S. MONDAL, *Mobile IP: Present State and Future*, Addison Wesley, 2002

Un excellent livre effectuant une synthèse des solutions bâties au-dessus d'un environnement ATM :

G. C. SACKETT, C. Y. METZ, *ATM and Multiprotocol Networking*, McGraw-Hill, 1997

Les réseaux de mobiles devraient devenir des réseaux IP natifs ; ce livre nous en montre les raisons :

A. SAKIB MONDAL, *Mobile IP: Present State and Future*, Plenum Publishing Corporation, 2003

Pour démarrer dans le Cloud Computing, ce livre est tout à fait bien fait :

D. SARNA, *Implementing and Developing Cloud Computing*, Auerbach, 2010

Livre simple mais indiquant bien les avantages et inconvénients d'Internet et les solutions pour le futur :

F. T. HOFSTETTER, *Internet Technologies at Work*, McGraw-Hill, 2004

Excellent livre sur les stratégies potentielles de développement des réseaux :

N. WILKINSON, *Next Generation Network Services: Technologies & Strategies*, Wiley, 2002

Index

Symboles

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Pujolle
Les RÉSEAUX
Édition 2011

***Guy Pujolle** est Professeur à l'Université Pierre et Marie Curie - Paris 6, membre de l'Institut Universitaire de France et responsable de nombreux grands projets de recherche français et européens. Auteur de plus de trois cent articles et de nombreux ouvrages en langues française et anglaise, il est également membre du conseil scientifique du groupe Orange/France Télécom. Il a été professeur invité à NCSU, Stanford, Rutgers et UQAM. Ses recherches portent actuellement sur la conception et le développement des réseaux post-IP. Il est cofondateur de la société QoSMOS, spécialisée dans la qualité de service, de la société Ucopia qui commercialise un logiciel de gestion du nomadisme, de Ginkgo-Networks, qui développe un système de pilotage de réseau, d'EtherTrust qui propose de la haute sécurité par carte à puce et de Green Communications qui divise au moins par deux mais souvent par dix la consommation électrique des réseaux d'accès sans fil.*

www.pujolle.com

La référence des professionnels en réseaux et télécoms

Avec près de 100 000 exemplaires vendus, « Les Réseaux » de Guy Pujolle s'est imposé comme la référence en langue française auprès des étudiants comme des professionnels en réseaux et télécoms.

À l'occasion de cette 7e édition, l'ouvrage a fait l'objet d'une refonte importante : réorganisation de la structure du livre, mise à jour des chapitres existants avec renvoi en annexes téléchargeables des technologies en perte de vitesse, ajout de nouveaux chapitres. Au total, plus de 40 % de contenu nouveau ou profondément remanié, et un ouvrage recentré sur les technologies réellement utilisées aujourd'hui.

Un ouvrage exhaustif, en prise sur l'évolution du marché et sur les avancées de la R&D

L'ouvrage témoigne ainsi des évolutions rapides des technologies et des usages, avec la domination plus forte que jamais d'IP et d'Ethernet, la course aux hauts débits dans les technologies mobiles (3G+ et 4G) comme dans les réseaux sans fil (Wi-Fi 802.11n/ac/af…), les solutions de convergence entre ces deux familles de réseaux hertziens, l'attention accrue portée à la sécurité, en particulier dans le monde IP et dans l'univers du sans fil, la maturité de la téléphonie sur IP, l'internet des choses (capteurs, RFID…), les perspectives offertes par la virtualisation et l'auto-configuration des réseaux (autonomic networks), etc.

Au sommaire

En complément sur www.editions-eyrolles.com

• Plus de 350 pages d'annexes : bases de traitement du signal, modèles théoriques, technologies en perte de vitesse (RNIS, X.25, relais de trame, IP sur ATM, réseaux de mobiles 1G et 2G, WiMAX, gestion par politiques…), compléments techniques (IEEE 802.11e, VPN IP, protocoles EAP…), bibliographie commentée.

www.editions-eyrolles.com
Groupe Eyrolles | Diffusion Geodif